¿NUEVOS PARADIGMAS DE VIGILANCIA?

Miradas desde América Latina

Memorias del IV Simposio Internacional

LAVITS
BUENOS AIRES

¿NUEVOS PARADIGMAS DE VIGILANCIA?

Miradas desde América Latina

¿NUEVOS PARADIGMAS DE LA VIGILANCIA?

Miradas desde América Latina.

Camilo Rios (Ed.)

Memorias del IV Simposio Internacional LAVITS, Buenos Aires.

Buenos Aires - 2017

Título:

¿Nuevos paradigmas de vigilancia? Miradas desde América Latina.
Memorias del IV Simposio Internacional Lavits, Buenos Aires.

Editor:

Camilo Rios.

Compiladores:

Camilo Rios, Andrés Pérez Esquivel, Laura Lacaze y Luciana Albuquerque.

Autores:

Maiana Abi, Luciana Santos Guilhon Albuquerque, Claudio Altenhain, Daniela Camila de Araújo, Nelson Arteaga Botello, Marcela de Moraes Batista, Elias Cunha Bitencourt, Fernanda Bruno, Janice Caiafa, Leda Maria Caira Gitahy, Mercedes Calzado, Sebastián Castelli, Enrique Chaparro, Gustavo Chirolla, Luiz Filipe da Silva Correia, Danilo Doneda, Brenda de Fraga Espindula, Eduardo Estévez, Paulo Faltay Filho, Eduardo Georjão Fernandes, Gustavo Fernandes, Rodrigo Firmino, Bruno Fonseca, Anna Carolina Franco Bentes, Martín Ariel Gendler, Juan Camilo Gómez Barrera, Yamila Gómez, Thiago Gonçalves Roberto, Leonardo Kazuhiko Kawazoe, Marcelo Toshiki Kozuma, Laura Lacaze, Manuel Ernesto Larrondo, Vanesa Lio, David Lyon, Paulo Eduardo Assis Maia, Lucas Melgaço, Valeria Milanes, Paravizo Mira, Camila Montagner, Thereza Nardelli, Thiago Nobayashi, María Alejandra Otamendi, Rosa María Leite Ribeiro Pedro, Paz Peña, Andrés Pérez Esquivel, Alcides Eduardo dos Reis Peron, Leonardo Piccioni de Almeida, Marta de Araújo Pinheiro, Julia Powles, Raquel Rennó, Márcio Moretto Ribeiro, Camilo Rios, Pablo Esteban Rodríguez, Fabián Ludueña Romandini, Irme Salete Bonamigo, Laura Siri, Jacqueline de Souza Abreu, Ricardo Urquizas Campello, Martín Javier Urtasún, Gabriela Fedrizzi Varela, Patricio Velasco Fuentes, Diego Vicentin, Maximiliano Vila Seoane, Gabriel Cunha Vituri, Juan Manuel Zaldúa y Joana Ziller.

Maquetación y Diseño:

Juan Pablo Suárez.

Agradecimientos Especiales:

LAVITS - Red Latinoamericana de Vigilancia, Tecnología y Sociedad / Fundación Vía Libre / Área 'Tecnología, Cultura y Política de la Carrera de Ciencias de la Comunicación de la Facultad de Ciencias Sociales de la Universidad de Buenos Aires.

Apoyos:

Ford Foundation / Labjor / Media Lab UFRJ / Programa de Posgrado en Comunicación y Cultura - UFRJ / Programa de Pós-Graduação em Gestão Urbana (PPGTU) - PUCPR / Programa de Pós-Graduação em Divulgação Cientifica e Cultural / Pimenta Lab / Sublínea de investigación "Estado, democracia y derechos humanos" - Proyecto “Vigilancia en Latinoamérica”, Facultad Latinoamericana de Ciencias Sociales - Flacso, México.

http://lavits.org http://lavits2016.vialibre.org.ar

Esta obra está licenciada bajo la Licencia Creative Commons Atribución-NoComercial-SinDerivadas 2.5 de Argentina. Para ver una copia de esta licencia, visite http://creativecommons.org/licenses/by-nc-nd/2.5/ar/ o envíe una carta a Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

© 2017, los autores de cada uno de los textos.
© 2017, de la edición Fundación Vía Libre.

¿Nuevos paradigmas de vigilancia? miradas desde América Latina : Memorias del IV Simposio Internacional Lavits, Buenos Aires, 2016 / compilado por Camilo Rios Rozo ... [et al.] ; editado por Camilo Rios Rozo. - 1a ed. - Córdoba : Fundación Vía Libre, 2017. Libro digital, PDF

Archivo Digital: descarga

ISBN 978-987-22486-8-0

1. Vigilancia. 2. Tecnología. 3. Actas de Congresos. I. Rios Rozo, Camilo, comp. II. Rios Rozo, Camilo, ed.

CDD 323.4482

ISBN 978-987-22486-8-0

TABLA DE CONTENIDOS

Presentación 11

Ponencias 23

Eje 1. Doctrina de seguridad y servicios de inteligencia

Vigilancia masiva de comunicaciones: Una (ciber)inquisición
Laura Lacaze 27

Peço perdão pelo vacilo: exercícios autoritários em vídeos amadores compartilhados no YouTube
Thereza Nardelli, Bruno Fonseca, Maiana Abi, Joana Ziller 45

O discurso de segurança e a privacidade no Marco Civil da Internet
Paulo Eduardo Assis Maia, Marta de Araújo Pinheiro, Gustavo Fernandes, Paravizo Mira 61

Vigilancia online y secreto periodístico. Reflexiones sobre la prrotección legal
Sebastián Castelli, Manuel Ernesto Larrondo 71

Eje 2. Vigilancia, espacio y territorio

Ciudades inteligentes en Latinoamérica, el ciudadano vigilado
Raquel Rennó, Valeria Milanes, Paz Peña, Patricio Velasco 91

Tropicalizing Surveillance: How big data policing "migrated" from New York to São Paulo
Claudio Altenhain, Alcides Eduardo dos Reis Peron 101

Automação e vigilância no metrô de São Paulo
Janice Caiafa 115

Objetos y nativos de la vigilancia. Reflexiones sobre la construcción de la videovigilancia como objeto etnográfico desde una investigación en curso
Martín Javier Urtasún 127

Más allá de lo «Smart»: implicancias sociales de las tecnologías de vigilancia en contextos urbanos
Patricio Velasco Fuentes 141

(In)segurança pública: cartografia de relações entre dispositivos de vigilância, políticas públicas e violências em espaços urbanos contemporâneos
Irme Salete Bonamigo, Rosa Pedro, Lucas Melgaço 153

A última porta do Estado. Aeroportos, vigilância e controle
Luiz Filipe da Silva Correia 163

Os olhares sobre a cidade: uma abordagem bibliométrica da vigilância nos estudos urbanos
Thiago Gonçalves Roberto, Marcela de Moraes Batista, Gabriela Fedrizzi Varela 171

«El reality de la inseguridad». Televisión, cámaras de vigilancia y nuevos modos de construcción de la noticia policial audiovisual
Mercedes Calzado, Yamila Gómez, Vanesa Lio 187

Escenas de la vida cotidiana. Actores, discursos y representaciones en torno a la videovigilancia pública en un municipio bonaerense
Vanesa Lio 197

Eje 3. Identificación y biometría

A ricos enriquecidos, pueblos vigilados: biometría, seguridad y evasión fiscal
Andrés Pérez Esquivel 213

Tecnologia e punição: o monitoramento eletrônico de presos no Brasil
Ricardo Urquizas Campello 229

Eje 4. La seducción del número: decisiones basadas en algoritmos y Big Data

Segurança preditiva? a incorporação de técnicas de mineração de dados e perfilização em conflitos internacionais com drones pelos eua e em práticas de vigilância pela policia militar do estado de São Paulo
Alcides Eduardo dos Reis Peron 241

Datos, Algoritmos, Neutralidad de la Red y Sociedades de Control
Martín Ariel Gendler 257

Eje 5. Nuevos desafíos en la protección de datos personales

Intelligence challenges in Latin America and prospects for reform: A comparative matrix on democratic governance
Alejandra Otamendi, Eduardo Estévez 277

Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais
Jacqueline de Souza Abreu 295

Uma Análise Sobre a Navegação no Modo Privativo do Google Chrome Mobile
Leonardo Kazuhiko Kawazoe, Marcelo Toshiki Kozuma, Thiago Nobayashi 307

Eje 6. Vigilancia corporativa

Wearable trackers e o risco oculto do conhecimento de si através do dado. Uma análise dos documentos endereçados a usuários e investidores da Fitbit
Elias Cunha Bitencourt 317

Empresas transnacionales de seguridad y vigilancia en la Argentina
Maximiliano Vila Seoane 329

Eje 7. Dimensiones culturales de la vigilancia

Guerra de imagens: a Polícia Militar de São Paulo sob vigilância
Gabriel Cunha Vituri 345

Una lectura en perspectiva de 'vigilancia' de La Hipótesis Cibernética de Tiqqun
Camilo Rios 357

Cuando algo «Me gusta» en Facebook: identificación y producción de perfiles a partir de sus preferencias
Juan Camilo Gómez Barrera 369

Reacciones públicas ante las revelaciones de Snowden: los memes de internet como indicio
Laura Siri 383

Eje 8. Resistencias y contravigilancia

Mulheres e a segurança da informação: a trajetória do primeiro hackerspace feminista no Brasil
Daniela Camila de Araújo, Leda Maria Caira Gitahy 409

Governança da Internet, infraestrutura e resistência
Diego Vicentin 419

Estratégias de contravigilância e resistência durante as manifestações de 2013 no Brasil
Rosa María Leite Ribeiro Pedro, Luciana Santos Guilhon Albuquerque 433

Defezap e NósPorNós: usos, operacionalizações e efeitos dos aplicativos de contravigilância
Brenda de Fraga Espindula, Eduardo Georjão Fernandes 443

Comparação de aplicativos móveis de comunicação segura
Leonardo Piccioni de Almeida, Márcio Moretto Ribeiro 455

O processo de implementação de salas de videomonitoramento no Brasil
Eduardo Georjão Fernandes 467

Eje 9. Arte, vigilancia y tecnología

ContraLab na nuvem: O laboratório tático antirrepressão como iniciativa de Resistência
Camila Montagner 481

Aportes para una estética del control
Juan Manuel Zaldúa 491

Como nos vê o que nos olha?
Anna Carolina Franco Bentes, Paulo Faltay Filho 503

Conferencias centrales 519

Visão mediada por algoritmo: cidade, controle, tempo
Fernanda Bruno 521

Lógica económica de la vigilancia como fenómeno indisociable del capitalismo posindustrial
Enrique Chaparro 521

Encountering and Engaging with Surveillance Culture
David Lyon 522

Closing the Circle?
Julia Powles 522

El poder escópico. Una mirada arqueológica de la vigilancia entre metafísica y Derecho
Fabián Ludueña Romandini 523

Genealogía de lo dividual. Una mirada arqueológica de la vigilancia entre metafísica y Derecho
Pablo Esteban Rodríguez & Fernanda Bruno 523

Pobreza, guerra civil mundial y sociedad de control
Gustavo Chirolla 523

Vigilancia y esfera civil en América Latina
Nelson Arteaga Botello 524

Algoritmo e vigilancia
Danilo Doneda 524

Securitização, vigilância e territorialização em espaços públicos na cidade Neoliberal
Rodrigo Firmino 524

INTRODUCCIÓN

Desde su fundación en el año 2009 la Red Latinoamericana de Estudios sobre Vigilancia, Tecnología y Sociedad (LAVITS) busca responder, por lo menos, a una inquietud y un deseo. La inquietud frente a la creciente presencia de prácticas y de tecnologías de vigilancia sobre nuestras vidas. El deseo de problematizar y debatir esa inquietud en un ámbito latinoamericano. Sabíamos que un debate como ese no solamente requeriría un buen número de compañeros, sino también una diversidad de perspectivas. Era necesario enfrentar la complejidad de las cuestiones colocadas por los entrecruzamientos cada vez más promiscuos entre tecnologías y prácticas de vigilancia y procesos sociales, afectivos, económicos, informacionales, gubernamentales, etc.

La Red LAVITS comienza, así, reuniendo un grupo interdisciplinar de investigadores y a lo largo de su trayectoria viene fortaleciendo no sólo a vinculación entre laboratorios y grupos de pesquisa latinoamericanos, sino también la colaboración con activistas, artistas y desarrolladoras. La apuesta por la diversidad de perspetivas y la heterogeneidad de sus integrantes y colaboradores fue decisva para esta red fuertemente marcada por la investigación académica. Combinar y confrontar no únicamente diversos puntos de vista, sino también diferentes velocidades, formas, énfasis y urgencias en el pensamiento y en las acciones ha resultado un aprendizaje constitutivo de LAVITS. Dentro del conjunto de proyectos desarrollados desde su creación (investigaciones, formación, publicaciones, etc) los Simposios Internacionales han sido una ocasión privilegiada de construcción de ese aprendizaje.

La realización del IV Simposio Internacional LAVITS en la Ciudad Autónoma de Buenos Aires, República Argentina, entre los días 21 y 23 de noviembre de 2016, no sólo dio continuidad a esa trayectoria, como consolidó en su propia organización la asociación entre una entidad de la sociedad civil – La Fundación Vía Libre – y la academia - el Área de investigación en Tecnología, Cultura y Política de la carrera de Ciencias de la Comunicación Social de la Facultad de Ciencias Sociales de la Universidad de Buenos Aires. La fundación Vía Libre es una organización sin fines de lucro de Argentina, dedicada a la defensa de los derechos civiles en entornos mediados por tecnologías. En su agenda de trabajo se encuentran temas de privacidad,

vigilancia, software libre, propiedad intelectual, libertad de expresión en Internet y voto electrónico. Por su parte, el Área de Tecnología, Cultura y Política fue creada en 2014 por un grupo de docentes, estudiantes e investigadores de la Carrera de Ciencias de la Comunicación de la Facultad de Ciencias Sociales, Universidad de Buenos Aires, para desarrollar y apoyar investigaciones, así como participar en debates, en los que se aborde el análisis de fenómenos comunicacionales, culturales, estéticos y políticos donde la dimensión tecnológica aparezca como constitutiva. Después de las ediciones realizadas en Brasil (2009 y 2015) y México (2011), el Simposio LAVITS se realizó por primera vez en Argentina y buscó debatir alrededor de la existencia de nuevos paradigmas de vigilancia favorecida por la tecnología, aportando una mirada propia desde América Latina.

Entonces, ¿por qué preguntarse sobre la existencia de nuevos paradigmas de vigilancia? El imaginario popular sobre la vigilancia incluye la existencia de espías y enormes redes de inteligencia dedicadas al seguimiento de ciudadanos "sospechosos". Sin embargo, mientras que este paradigma de vigilancia pudo haber tenido vigencia en otras décadas, lo cierto es que, con el advenimiento de las tecnologías digitales los costos de la vigilancia, tanto estatal como corporativa, han bajado dramáticamente. Esto permite que se acumulen datos sobre los ciudadanos de manera precautoria aun cuando no haya razones fundamentadas para la existencia de estas bases de datos.

El cambio en la narrativa de la seguridad a partir del atentado contra las Torres Gemelas permitió que se incorporara una nueva doctrina de vigilancia de "información total". Esta nueva doctrina es diametralmente opuesta a cualquier principio de Derechos Humanos, pero el secretismo en la gestión de la información y la aceitada cooperación entre el sector público y el privado en la recolección y procesamiento de datos convierten a este tipo de vigilancia en una práctica fuera del control público.

La incorporación de tecnología en numerosos ámbitos de la vida cotidiana –desde las calles con cámaras de vigilancia hasta los espacios más íntimos poblados con dispositivos inteligentes que informan datos sobre los usuarios a terceras partes– ha vuelto a la vigilancia más ubicua e invisible. Los marcos regulatorios que deberían proteger a los ciudadanos han quedado obsoletos frente a esta realidad, y la falta de rendición de cuentas en el sector público y privado complejiza el escenario a la hora de tomar acciones.

El desafío es, como nunca antes, global. Los datos que se producen sobre un usuario en América Latina se transfieren a un centro de procesamiento en Estados Unidos para que sea analizado en Europa. Las nuevas doctrinas de seguridad incluyen conceptos difusos como la "ciberguerra" para implementar mecanismos cada vez más complejos de recolección de datos digitales. Los ciudadanos se ven impotentes en su capacidad de reclamo, o directamente desconocen que están siendo observados.

El fenómeno no se da de manera homogénea e igual en todas partes; hay singularidades esenciales en el ámbito de América Latina que necesitan ser investigadas, resaltadas y puestas en

discusión. Este fue, precisamente, el propósito esencial del IV Simposio de LAVITS, para lo que se propusieron nueve ejes temáticos:

1. *Doctrina de seguridad y servicios de inteligencia.*
2. *Vigilancia, espacio y territorio.*
3. *Identificación y biometría.*
4. *La seducción del número: decisiones basadas en algoritmos y Big Data.*
5. *Nuevos desafíos en la protección de datos personales.*
6. *Vigilancia corporativa.*
7. *Dimensiones culturales de la vigilancia.*
8. *Resistencias y contravigilancia.*
9. *Arte, vigilancia y tecnología.*

Estos ejes convocaron y agruparon conferencias centrales, mesas de ponencias, mesas temáticas y workshops que desde miradas diversas nutrieron la discusión y el acercamiento a las problemáticas que el Simposio propuso.

Finalmente, es importante recordar que el Simposio fue absolutamente libre y gratuito tanto para expositores como para asistentes e interesados del público en general, lo que contribuyó a generar intercambios más nutridos, más plurales y de mayor pregnancia de estos temas que, normalmente, siempre se desarrollan a nuestras espaldas.

***

El Simposio hubiese sido imposible, y por tanto estas memorias, sin el apoyo de la *Ford Fundation*, del Centro Cultural San Martín, y de la Facultad de Ciencias Sociales de la Universidad de Buenos Aires, a quienes agradecemos especial y profundamente. Además, haciendo parte de un gran equipo de trabajo, es necesario mencionar al Programa de Posgrado en Comunicación y Cultura de la UFRJ, al MediaLab también de la UFRJ, al Laboratorio de Periodismo –Labjor– de la UNICAMP, al Programa de Posgrado en Divulgación Científica y Cultural también de la UNICAMP, al Programa de Posgrado en Sociología del Instituto de Filosofía y Ciencias Humanas también de la UNICAMP, al Programa de Posgrado en Gestión Urbana de la PUCPR, al Pimienta Lab, al Programa de Posgrado en Psicología de la UFRJ y a la Sublínea de Investigación "Estado, democracia y derechos humanos" de FLACSO México. Junto con ellos, todos nosotros fuimos en igual parte realizadores de este Simposio, por lo que el éxito es compartido. Sin embargo, todos los posibles errores de estas memorias son responsabilidad exclusiva de nosotros, los editores.

APRESENTAÇÃO

A Rede Latino-americana de Estudos sobre Vigilância, Tecnologia e Sociedade (LAVITS), desde a sua fundação em 2009, busca responder a, pelo menos, uma inquietação e um desejo. A inquietação frente à crescente presença de práticas e tecnologias de vigilância em nossas vidas. O desejo de problematizar e debater essa inquietação no âmbito da América Latina. Sabíamos que tal debate requeria não apenas um bom número de parceiros, mas também uma diversidade de perspectivas. Era necessário enfrentar a complexidade das questões colocadas pelos cruzamentos, cada vez mais promíscuos, das tecnologias e práticas de vigilância com os processos sociais, afetivos, econômicos, informacionais, governamentais etc.

A Rede LAVITS começa, assim, por reunir um grupo interdisciplinar de pesquisadores e, ao longo de sua trajetória, vem fortalecendo não apenas a interlocução entre laboratórios e grupos de pesquisa latino-americanos, como a colaboração com ativistas, artistas e desenvolvedores. A aposta na diversidade de perspectivas e na heterogeneidade dos seus integrantes e colaboradores tornou-se decisiva para essa rede, fortemente marcada pela pesquisa acadêmica. Combinar e confrontar não apenas pontos de vista, mas também velocidades, formas, ênfases e urgências distintas no pensamento e nas ações, vem sendo um aprendizado constituinte da LAVITS. Dentre os projetos desenvolvidos desde a sua criação (pesquisas, formação, publicações etc), os Simpósios Internacionais têm sido uma ocasião privilegiada de construção desse aprendizado.

A realização do IV Simpósio Internacional LAVITS na cidade de Buenos Aires, Argentina, entre 21 e 23 de novembro de 2016, não apenas dá continuidade a essa trajetória, como consolida, em sua própria organização, a parceria entre uma entidade da sociedade civil – A Fundação Vía Libre – e a Academia - a Área de pesquisa em Tecnologia, Cultura e Política do curso de Ciências da Comunicação Social da Faculdade de Ciências Sociais da Universidade de Buenos Aires (UBA). A Fundação Vía Libre é uma organização sem fins lucrativos da Argentina, dedicada à defesa dos direitos civis em ambientes mediados por tecnologias. Na sua agenda de trabalho se encontram temas como privacidade, vigilância, software livre, propriedade intelectual, liberdade de expressão na Internet e voto eletrônico. Por sua vez, a Área de pesquisa

em Tecnologia, Cultura e Política foi criada por um grupo de docentes, estudantes e pesquisadores do curso de Ciências da Comunicação Social da Faculdade de Ciências Sociais da UBA para desenvolver e apoiar pesquisas, assim como participar de debates que analisassem fenômenos comunicacionais, culturais, estéticos e políticos, nos quais a dimensão tecnológica aparecesse como constitutiva. Após as edições realizadas no Brasil (2009 y 2015) e no México (2011), o Simpósio LAVITS foi realizado, pela primeira vez, na Argentina e procurou debater a respeito da existência de novos paradigmas de vigilância pela tecnologia, contribuindo com um olhar próprio da América Latina.

Então, por que se perguntar a respeito da existência de novos paradigmas de vigilância?

O imaginário popular a respeito da vigilância inclui a existência de espiãos e enormes redes de inteligência dedicadas a monitorar cidadãos "suspeitos". No entanto, ainda que esse paradigma de vigilância tenha sido vigente em outras décadas, o fato é que, com o advento das tecnologias digitais, os custos da vigilância, tanto a estatal quanto a corporativa, tem diminuído drasticamente. Isto possibilitou que se acumulassem dados sobre os cidadãos de maneira cautelosa, ainda que não houvesse razões fundamentadas para a existência dessas bases de dados.

A mudança na narrativa em matéria de segurança, que seguiu ao atentado contra as Torres Gêmeas, possibilitou a incorporação de uma nova doutrina de vigilância de "informação total". Essa nova doutrina é diametralmente oposta a qualquer princípio de Direitos Humanos, mas o sigilo na gestão da informação e a cooperação cada vez mais consolidada entre o setor público e o setor privado na coleta e no processamento de dados têm transformado esse tipo de vigilância em uma prática fora do controle público.

A incorporação da tecnologia em numerosos âmbitos da vida cotidiana – desde as ruas com câmera de vigilância até os espaços mais íntimos povoados com dispositivos inteligentes que informam a respeito dos dados dos usuários a terceiros – tem tornado a vigilância mais ubíqua e invisível. Os marcos regulatórios, que deveriam proteger os cidadãos têm ficado obsoletos frente a essa realidade, e a falta de prestação de contas no setor público e no setor privado complexifica o cenário na hora de empreender ações.

O desafio é, como nunca antes, global. Os dados produzidos a respeito de um usuário na América Latina são transferidos a um centro de processamento nos Estados Unidos para serem analisados na Europa. As novas doutrinas de segurança incluem conceitos difusos como o da "ciberguerra" com o intuito de implementar mecanismos cada vez mais complexos de coleta de dados digitais. Os cidadãos se vêem impotentes na sua capacidade de reclamar ou, diretamente, desconhecem o fato de estarem sendo observados.

O fenômeno não se dá de forma homogênea e idêntica em todas as partes, há singularidades essenciais no âmbito da América Latina que precisam ser pesquisadas, salientadas e levadas à discussão. Este foi, precisamente, o objetivo central do IV Simpósio de LAVITS, para o qual fo-

ram propostos nove eixos temáticos:

1. *Doutrina de segurança e serviços de inteligência.*
2. *Vigilância, espaço e território.*
3. *Identificação e biometria.*
4. *A sedução do número: decisões baseadas em algoritmos e Big Data.*
5. *Novos desafios na proteção de dados pessoais.*
6. *Vigilância corporativa.*
7. *Dimensiões culturais da vigilância.*
8. *Resistências e contravigilância.*
9. *Arte, vigilância e tecnologia.*

Esses eixos convocaram e agruparam conferências centrais, mesas de trabalho, mesas temáticas e workshops, os quais, a partir de diversos olhares, nutriram o debate e a aproximação das problemáticas que o Simpósio propôs.

Finalmente, é importante lembrar que o Simpósio foi absolutamente livre e gratuito tanto para expositores quanto para ouvintes e interessados do público em geral, o que contribuiu para gerar intercâmbios mais proveitosos, mais plurais e de maior peso destes temas que, normalmente, sempre se desenvolvem nas nossas costas.

***

O Simpósio não teria sido possível, e por tanto também não essas memórias, sem o apoio da *Ford Fundation,* do Centro Cultural San Martín da Faculdade de Ciências Sociais da Universidade de Buenos Aires, a quem agradecemos especial e profundamente. Aliás, fazendo parte dessa grande equipe de trabalho, é preciso mencionar o Programa de Pós-Graduação em comunicação e Cultura da UFRJ, o MediaLab também da UFRJ, o Laboratório de Periodismo –Labjor– da UNICAMP, o Programa de Pós-Graduação em Divulgação Científica e Cultural também da UNICAMP, o Programa de Pós-Graduação em Sociologia do Filosofia e Ciências Humanas também da UNICAMP, o Programa de Pós-Graduação em Gestão Urbana da PUCPR, o Pimienta Lab, o Programa de Pós-Graduação em Psicologia da UFRJ e a Sublinha de Pesquisa "Estado, democracia e direitos humanos" da FLACSO México. Junto com eles, todos nós fomos, em igual medida, realizadores deste Simpósio, razão pela qual o êxito é compartilhado. Embora, todos os possíveis erros destas memórias são responsabilidade exclusiva de nós, os editores.

INTRODUCTION

Since its foundation, back in 2009, Latin American Network of Surveillance, Technology and Society (LAVITS) aims at answer, at least, an inquietude and a desire. The inquietude realted to the increasing presence of surveillance practices and technologies in our everyday lives. And the desire of problematazing and debating that inquietude at a latinamerican level. We knew that a debate as that one would need not only a great companion, but also a wide range of perspectives. It was necessary to face the complexity of the issues that emerged from the cross -links between technologies, surveillance practices and social, afective, economical, informational, governmental and other processes.

LAVITS Network starts like that, getting an interdisciplinary group of researchers. And along its way it has been reinforcing the links between investigation groups and laboratories, but also pomoting artirsts, developers and activists collaboration. The bet on perspective diversity and members heterogeneity has been decisive to this highly academicly marked network.

To combine and confront points of view, but also thought and action's velocities, modes, urgencies and emphasis has been a constitutive learning to LAVITS. Among the projects developed since its foundation (reseachs, formation, publishing, etc.) the International Symposiums have been a privilegiate opportunity to build knowledge.

IV LAVITS International Symposium was carried out in Buenos Aires, Argentina, from November the 21st to the 23rd, 2016, continued that line and experienced the association between a Civil Society Organization –Vía Libre Fundation– and the academy –Technology, Culture and Politics Division in Communication Sciences grade career of Social Sciences Faculty at buenos Aires University– organizing it.

Vía Libre is a non-profit organization from Argentina, dedicated to the defense of civil rights in technology-mediated environments. Within its field of study are issues related to privacy, surveillance, free software (libre software), intellectual property, freedom of speech on the Internet and electronic voting. On the other hand, The Technology, Culture and Politics Division was created in 2014 by a group of professors, students and researchers within the Communication

Sciences degree program of the Faculty of Social Sciences, at the Buenos Aires University. From the hypothesis of a mutual conditioning between technical and social phenomena, it proposes to develop and support research, as well as part-take in debates, that address the analysis of communicational, cultural, aesthetic and political phenomena were the technological dimension appears as constitutive.

After the Bazil (2009 and 2015) and Mexico (2011) editions, LAVITS Symposium was done for its first time in Argentina. Here, it aimed at discussing the existence of new surveillance paradigms, contributing its own views from Latin America.

Then, why to ask ourselves about the existence of new surveillance paradigms? The popular belief about surveillance includes the existence of spies and enormous intelligence networks devoted to following "suspected" citizens. While that surveillance paradigm may have been in effect in previous decades, the truth is that with the coming of digital technologies the costs of surveillance, both governmental and corporate, have dropped dramatically. This allows for the accumulation of data in a precautionary manner, even when there are no justified reasons for the existence of these databases.

After the World Trade Center attacks, the shift in the security narratives allowed for the inclusion of a new surveillance doctrine of "total information". This new doctrine is diametrically opposed to any human rights principle, but the secrecy of how the information is managed and the well -oiled cooperation between the public and private sectors for the collection and processing of data, make this type of surveillance a practice that escapes public control.

The introduction of technology in many aspects of everyday life, from surveillance cameras on streets to the vast number of smart devices in our most private environments reporting data to third parties, has made surveillance more ubiquitous and invisible. The normative framework that should protect citizens in this respect, has become obsolete and the lack of accountability in the public and private sectors complicate the situation when it comes to taking action.

The challenge, as never before, is global. The data collected about a user in Latin America are transferred to a processing center in the United States to be analyzed in Europe. The new security doctrines include vague concepts, as "cyberwar", to implement increasingly complex mechanisms for collecting digital data. Citizens are helpless regarding their ability to claim, or they are absolutely unaware of the fact that they´re being watched.

The phenomenon doesn´t occur in a uniform or equal manner everywhere, there are fundamental singularities in the context of Latin America that need to be investigated, highlighted and discussed. This is, in essence, the purpose of the Fourth LAVITS Symposium. In order to achieve it, there were proposed the following nine key topics:

1. *Security doctrine and intelligence services.*

2. Surveillance, space and territory.

1. Identification and biometrics.

4. The seduction of numbers: decisions based on algorithms and Big Data.

5. New challenges in the protection of personal data.

6. Corporate surveillance.

7. Cultural dimensions of surveillance.

8. Resistance and counter surveillance.

9. Art, surveillance and technology.

These main topics called and grouped central conferences, papers presentations, thematic tables and workshops that developed the dialogue as well as the approach to the central questions proposed by the Symposium itself from different perspectives.

Finally, it's important to recall the Symposium was completely free for listeners, exponents and general public. That contributed to more nourished and more plural exchanges and, as a consequence, more pregnancy of the topics involved, some of which are developed mostly behind us.

***

The Symposium would have been impossible, and therefore this book, without the support of the *Ford Fundation,* the San Martín Cultural Center and the Social Sciences Faculty of the Buenos Aires University. We are deeply grateful with all of them.

Also, as part of the team, we want to mention specially the Culture and Communication postgraduate program of UFRJ; the MediaLab, also of UFRJ; the Journalism Laboratory –Labjor– of UNICAMP; the Cientific and Cultural Divulgation postgraduate program of UNICAMP; the Sociology postgraduate programa of the Philosophy and Human Sciences of UNICAMP; the Urban Gestion postgraduate program of PUCPR; the Pimienta Lab; the Psycology postgraduate program of UFRJ; and the Sub-line of investigation "State, Democracy and Human Rights" of FLACSO, Mexico. All of them, with us, were part of the organization of this Symposium. That's why any success is shared. However, all mistakes in this book are exlusive responsability of us, the editors.

PONENCIAS

EJE 1

DOCTRINA DE SEGURIDAD Y SERVICIOS DE INTELIGENCIA

VIGILANCIA MASIVA DE COMUNICACIONES: UNA (CIBER)INQUISICIÓN

Resumen: Vivimos bajo un régimen de vigilancia masiva y global de comunicaciones. Este se sustenta tecnológica y económicamente en las capacidades creadas en torno a una industria digital surgida de las entrañas del aparato militar estadounidense y se legitima a partir del discurso articulado en torno a la Guerra Global al Terror.

El argumento central del presente artículo es que dicha narrativa no constituye una novedad argumentativa propia de la naturaleza de los conflictos del Siglo XXI sino, por el contrario, una reversión discursiva a los tiempos de la Inquisición.

En este sentido el trabajo fue organizado en tres secciones. En la primera, siguiendo a Zaffaroni, se detallan las características centrales del discurso inquisitorial en su versión demonológica. Con esto se pretende exponer la lógica central del discurso punitivo y mostrar que, pese a las diferentes modalidades en que se presenta en la Edad Media y en la actualidad, mantiene su lógica estructural, consistente en que, bajo la enunciación de un peligro inminente, se avanza sobre el control de la población. En este caso en un cibercontrol centrado en el fichaje de individuos a una escala sin precedentes.

En la segunda, se analizan los discursos sobre la vigilancia masiva de comunicaciones, tal como enunciados por los principales representantes del sistema político estadounidense y de las corporaciones líderes de la economía digital. De esta manera, se intenta mostrar la coherencia que, en relación con la matriz argumentativa, ostentan ambas narrativas. Finalmente, se hace una breve referencia a la resistencia. Se argumenta que, tal como aconteció cuatro siglos atrás, el avance del punitivismo global encuentra también en la actualidad sus focos de oposición. Salvando las particularidades propias de cada época lo cierto es que, entonces como ahora, quienes encarnan la resistencia arriesgan sus propias vidas al intentar contrarrestar o deslegitimar el accionar del poder punitivo exponiendo sus excesos y su irracionalidad selectiva.

Palabras clave: Vigilancia masiva de comunicaciones, Guerra Global al Terror, Cibercontrol.

LAURA MABEL LACAZE*

Vigilância massiva de comunicações: uma (ciber) inquisição

Resumo: Vivemos sob um regime de vigilância massiva y global de comunicações. Este sustenta-se tecnológica e economicamente nas capacidades criadas por parte de uma indústria digital surgida do coração do aparelho militar estadunidense e que se legitima através de um discurso articulado em torno a la Guerra Global ao Terror.

O argumento central do presente artículo é que dita narrativa no constitui uma novidade argumentativa própria da natureza dos conflitos do século XXI, mas pelo contrário, uma reversão discursiva aos tempos da inquisição.

O trabalho foi organizado em três seções. Na primeira, seguindo a Zaffaroni, detalham-se as características centrais do discurso inquisidor na sua versão demonológica. Com isto pretende-se expor a lógica central desse discurso punitivo e mostrar que, embora as diferentes modalidades nas quais se apresenta na Idade Média e na atualidade, este conserva sua lógica estrutural, consistente em que, sob a enunciação de um perigo iminente, avança-se sob o controle da população. Neste caso, em um cibercontrole centrado no fichamento indivíduo em uma escala sem precedentes.

Na segunda, analisam-se os discursos ligados a vigilância massiva e global comunicações, tal como enunciados pelos representantes principais do sistema político estadunidense e das corporações líderes de chamada economia digital. Desta maneira, tenta-se mostrar a coerência que, em relação com a matriz argumentativa, possuem ambas narrativas. Finalmente, faz-se uma breve referência à resistência. Argumenta-se que, tal como aconteceu quatro séculos atrás, o avanço do punitivismo global encontra também na atualidade focos de oposição. Embora as particularidades de cada época o fato é que, então como agora, aqueles que encarnam a resistência arriscam suas próprias vidas ao tentar contrarrestar ou delegitimar a ação do poder punitivo expondo seus excessos e sua irracionalidade seletiva.

Palavras chave: Vigilância massiva de comunicações, Guerra Global ao Terror, cibercontrol.

Mass surveillance of communications: A (cyber) inquisition

Abstract: We live under a regime of mass communications and global monitoring. This regime is based on technological and economic capacities which were built around the digital industry and it legitimizes the speech articulated around the global war on terror.

The central argument of this article is that this narrative is not an argumentative novelty inherent to the nature of the conflicts of the XXI century but, on the contrary, a discursive reversal to the times of the Inquisition.

In this regard we organize this article into three sections. In the first, according to what was argued by Zafaroni, we´ll develop the main features of inquisitorial discourse. With this we intend to expose the logic of punitive discourse and it shows that, despite the different modalities presented in the Middle Ages and Nowadays, it maintains the structural logic, which is, under the enunciation of an imminent danger, it progress on population control. In this case in a Cyber-Control focused on the signing of individuals to an unprecedented scale.

In the second, we´ll analyze the discourses on mass surveillance of communications, such as statements by leading representatives of the American political system and the leaders of the digital economy corporations with the intention of exposing the consistency in terms of argumentative matrix, which is presented in both narratives. Finally we´ll briefly refer to the resistance. We´ll argue as it happened four centuries ago, the overall progress punitive damages is also currently the focus of opposition. Saving the particularities of each time it is certain that, then as now, who embody the resistance take the risk their own lives to try to counter or delegitimize the actions of the punitive power of exposing their excesses and their selective irrationality.

Key-words: Mass surveillance of communications, Global war on terror, Cyber-Control.

INTRODUCCIÓN

> No quiero vivir en un mundo donde todo lo que digo, todo lo que hago, todos aquellos con los que hablo, toda expresión de creatividad y amor o amistad es grabada (Snowden, 2013 apud Poitras, 2014).

La publicación de un conjunto de documentos secretos por parte del ex agente de inteligencia estadounidense Edward Snowden en 2013 posibilitó que autoridades políticas y la comunidad internacional pudieran conocer de manera detallada las características del sistema de vigilancia de las comunicaciones digitales llevado adelante, principalmente, por los Estados Unidos de América. Su importancia radica en que sirvieron como instancia de información sobre las

características de los mecanismos de recolección, de análisis y de almacenamiento de datos así como de los arreglos institucionales bajo los cuales opera el sistema.

Tal como conocido a partir de los documentos[1], el sistema de vigilancia masiva de comunicaciones es el resultado de la progresiva construcción de una estructura transnacional de monitoreo encabezada por la Agencia Nacional de Seguridad estadounidense (NSA, por su sigla en inglés) en coordinación con otros organismos de ese país como el Buró Federal de Inteligencia (FBI, por su sigla en inglés) y con sus agencias pares de países colaboradores. Esta red es responsable por la ejecución de manera rutinaria de un conjunto de programas que contribuyen a la colecta, el análisis y el almacenamiento de un datos personales e institucionales (Greenwald, 2014) que circulan en las redes de computadores de forma masiva y a escala planetaria.

Tanto la recolección cuanto el análisis de la misma se orienta siguiendo la lógica de la masividad. Entre muchos otros, registros de conexiones, metadatos de comunicaciones, nombres y fechas de nacimiento y datos de tarjetas de crédito de un conjunto significativo de la población mundial son interceptados por las agencias de seguridad o accedidos directamente desde los centros de almacenamiento de los operadores privados configurando un esquema de fichaje orientado por la pretensión de abarcarlo todo. Esto último ha sido elocuentemente ilustrado en una de la presentaciones internas de la NSA (2011) al resumir que la orientación de las actividades de la agencia sigue los principios de "recolectar todo, analizar todo y husmear todo".

La vigilancia masiva, como aspecto saliente de las tecnologías digitales, se distingue por la inexistencia de una sospecha previa. Aún más las *sospechas,* los *indicadores de peligrosidad,* constituyen un resultado de la vigilancia. Como explica Bruno (2012: 349), la *nueva* vigilancia se caracteriza porque el "individuo emerge como un objetivo *a posteriori* , como un resultado del proceso de vigilancia en lugar de estar presente desde el comienzo". Esta característica impide que exista un examen independiente de la información y una evaluación acerca de la proporcionalidad de las medidas adoptadas razón por la cual, entre otras, fue considerada por Emmerson (2014), Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo de las Naciones Unidas, como violadora del Pacto Internacional de los Derechos Civiles y Políticos.

Aunque este tipo de práctica no necesariamente constituya una pretensión novedosa se da en la actualidad en un contexto que la vuelve técnicamente posible y económicamente viable. Esto porque la convergencia al uso de tecnologías digitales en espectros cada vez más amplios de actividades tiene como contrapartida la centralización de un conjunto progresivamente variado de informaciones en un único vehículo. Adicionalmente, la continua caída de los costos de transmisión, de procesamiento y de almacenamiento posibilitaron prácticas que antiguamente eran inviables (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2013: 41–53). En paralelo la valorización de la información emerge como núcleo fundamental de negocios de las empresas ligadas a la actividad de Internet. Estas firmas como argumentan Fuchs y Trottier (2015), entre otros, presentan modelos de acumulación basados en estrategias de compilación y venta de datos producidos por los usuarios en su interacción con las plataformas.

En este punto lo que rápidamente se concluye a partir del estudio de los documentos Snowden es que en términos materiales (esto es, económicos e institucionales) dicho sistema se sustenta sobre el predominio estadounidense sobre la infraestructura de comunicaciones y sobre los principales operadores de Internet. Ambos factores posibilitan a las agencias de seguridad de ese país el acceso tanto a los flujos de datos digitales en circulación como a los volúmenes de información que se encuentran almacenados en los servidores de los proveedores de servicios de Internet. En otras palabras, lo que puede afirmarse es que la vigilancia sobre las comunicaciones digitales constituye un fenómeno complejo que involucra actores estatales y no estatales, así como también intereses guiados por una lógica vinculadas a la acumulación de capital y otros de naturaleza eminentemente política.

Dentro de esta complejidad la Ley Patriota[2] (EUA, 2001) marcó un punto de inflexión. Sancionada por el Congreso de los Estados Unidos en el año 2001, apenas seis semanas después de los atentados del 11 de septiembre, esta norma amplió significativamente las potestades de investigación de los diversos órganos de inteligencia, al tiempo que incrementó exponencialmente los recursos públicos destinados al área de la seguridad y la defensa. Por sus previsiones, se constituyó en un elemento fundacional del sistema de vigilancia al ofrecer un marco legal, dentro del ordenamiento jurídico estadounidense, para su desarrollo posterior (Finley & Esposito, 2014; Lefébure, 2014).

El argumento central de la Ley Patriota consiste en que la vigilancia de comunicaciones constituye una herramienta esencial en la prevención de nuevos actos de terrorismo a nivel internacional y en el castigo a quienes incurren en estos actos. Con diversos matices, que no alteran lo central de la estructura argumentativa, esta narrativa fue repetida por diversos actores políticos y de la industria de las telecomunicaciones estadounidense a lo largo de los años posteriores inclusive en momentos de reforma de dichas normativas declaradamente orientadas a reducir los *excesos* generados a partir de la aplicación de estas.

El idea central en torno a la cual se organiza el presente artículo es que estas nociones, lejos de resultar una novedad argumentativa emergente de las particularidades de los conflictos en el Siglo XXI, conforman un discurso orientado por una lógica presente de forma regular en la historia de la humanidad desde, por lo menos, la Edad Media. En este sentido, el objetivo perseguido es el de mostrar la correspondencia entre los pronunciamientos actuales que encuadran la vigilancia masiva y global de comunicaciones como una herramienta indispensable en la lucha contra el terrorismo y aquellos que hace cinco siglos propugnaban la necesidad de quemar brujas para garantizar la salvación de las almas.

La intención de trazar este paralelismo, cabe señalar, no obedece al deseo de registrar un hecho simplemente curioso o llamativo. Lo que se pretende, por el contrario, es explicitar que estas estrategias del presente observan las mismas características que aquellas del pasado y de las que se siguen las mismas consecuencias en términos de poder: esto es la verticalización social o centralización de las instancias de toma de decisiones que abarcan, ahora, el territorio planetario.

La vigilancia y el discurso del poder punitivo

> ¿Dónde está, pues, la importancia política del poder punitivo? La clave la dio hace años Michel Foucault: el poder punitivo no se ejerce sobre los que están presos, sino sobre los que estamos sueltos pues es poder de vigilancia (Zaffaroni, 2011a: 506).

La noción de que un determinado peligro puede ser eliminado o contenido a partir de una acción punitiva (esto es, de castigo) no constituye una retórica propia de los discursos sobre seguridad doméstica e internacional de comienzos del Siglo XXI. Siguiendo a Zaffaroni, esta debe ser entendida como núcleo central del discurso del poder punitivo el cual tiene su primera formulación condensada conocida en el *Malleus Maleficarum* o *El martillo de las brujas* publicado en el año 1846.[3] Lo central en este punto es que, pese a que el contenido haya cambiado en los últimos cinco siglos y no se hable hoy ya de brujas y encantamientos, la estructura del discurso permanece vigente. La lógica que orienta la intervención es la misma, llevando a la utilización de las mismas prácticas y con iguales consecuencias en términos de poder.

A continuación se desarrollan, de forma abreviada, las principales características de este discurso para lo cual se sigue a Zaffaroni (2011a, 2013). El autor enumera los elementos salientes del discurso contenido en el Malleus los cuales expresan, tal el argumento, las regularidades propias del discurso del poder punitivo. Con la pretensión de simplificar la exposición se ha realizado una adaptación de la lista original presentada por el autor compuesta por 27 ítems (Zaffaroni, 2013: 30–36). Intentando hacer énfasis en el sentido que se imprime al argumento se ha reagrupado estos elementos a partir a las cinco funciones en torno a las cuales se organiza una narrativa, a saber: qué, quién, cuándo, por qué y cómo.

Cabe destacar que estos elementos, o regularidades, identificados a continuación se vinculan a partir de una lógica unificadora orientada a la producción de un sentido específico. Es por esto que la subdivisión presentada a continuación debe entenderse como fruto de una elección que, si bien obedece a ciertos criterios analíticos, no deja de ser de carácter arbitrario.

1. **¿Qué?** – En primera instancia, de lo que se habla en el discurso del poder punitivo es de acciones preventivas de carácter punitivo (esto es, vinculadas al castigo).
   La relevancia política de un discurso, su importancia como mecanismo de condicionamiento de las conductas humanas, reside en que este se remite a prácticas concretas. Como argumenta Foucault (2005: 30) al momento de proponer su *crítica política del saber,* aquello que posibilita en un momento del tiempo afirmar un idea determinada como verdadera es justamente su vinculación a una serie de prácticas específicas. No se trata, entonces, de contraponer práctica y discurso, acciones y narrativas, sino de estudiar la articulación entre una serie de prácticas y un tipo específico de discurso. La importancia política del discurso, *el alcance de las palabras* según Gómez (2016), está en el hecho de que a partir de él se construye un entendimiento específico sobre un conjunto de prácticas que tienen consecuencias concretas en términos de poder.
   Los dispositivos a los cuales remite el discurso del poder punitivo son, como su nombre lo indica, vinculados al castigo. Esto se observa claramente en el Malleus el cual, como se afirma

en la Carta Oficial a partir de la cual el texto es aprobado por la Universidad de Colonia, incluye "variadas y ponderadas orientaciones para el exterminio de brujas" de cuya acción se deseaba prevenir y salvaguardar a todos los hombres buenos (Kramer & Sprenger, 2002: 520).

2. **¿Quién?** - La característica central del discurso punitivo es la afirmación de una autoridad central como sujeto legítimo de la toma de decisiones. En este sentido, en el Malleus se hace una cuidadosa narrativa vinculada a la determinación de la autoridad de intervención y de los alcances de la misma.

   a) La afirmación de la autoridad y la confiscación del conflicto. Las narrativas del poder punitivo se basan en lo que Zaffaroni (2006: 22, 2013: 19) llama la *confiscación del conflicto* o *la confiscación de la víctima*. Esto es, el proceso por medio del cual una autoridad (política, religiosa, etc) se identifica como damnificado por el fenómeno en cuestión y se arroga la legitimidad para actuar en respuesta. El Malleus en este punto es muy preciso y establece que, siendo parcialmente un crimen contra la fe, la herejía constituía un crimen contra Dios en cuya representación debía intervenir la autoridad eclesiástica (Kramer & Sprenger, 2002: 377-395).

   b) Las aseveración de las capacidades superlativas de la autoridad para encarar la intervención: Constituye también una regularidad discursiva del discurso del poder punitivo el afirmar que la autoridad central y sus agencias poseen capacidades superlativas para encarar la intervención. Lógicamente vinculado a la racionalidad preventiva, en donde el objetivo declarado es el de actuar antes de que los acontecimientos se produzcan, la legitimidad de las agencias se refuerza al afirmar que estas poseen ciertos atributos de detección anticipada. En el Malleus se afirma que los Inquisidores poseen una *percepción privilegiada* , aunque no participen de los rituales de brujería Obispos, Inquisidores y otros teóricos argumentaban tener un conocimiento detallado sobre los procedimientos y actividades generales de brujas y demonios. Conocimiento que, además, sólo era posible gracias a que los administradores de justicia eran inmunes a los encantamientos y otras formas de engañar los sentidos (Kramer & Sprenger, 2002: 197-198).

3. **¿Por qué?** - La intervención es presentada como una respuesta derivada de la necesidad de neutralizar un peligro inminente.
   Un conjunto aleatorio de enunciados no conforman un discurso coherente y, así, no resulta capaz de producir sentido, de ofrecer una lectura acabada sobre la realidad. Por el contrario, siguiendo a Foucault (2008), lo que caracteriza a un discurso es que los enunciados siguen una ordenación lógica la cual se vincula a un principio de racionalización específico que posibilita interpretar acciones concretas. En otras palabras, lo característico de un discurso es la lógica a partir de la cual se ordena para ofrecer una interpretación coherente de la realidad.
   En este punto, lo que es propio del discurso del poder punitivo es identificar que un conjunto de prácticas de castigo se orientan, o es deseable que se orienten, a prevenir que una serie de fenómenos se produzcan. En otras palabras, el articularse en torno a la idea de que existe una peligrosidad y de que esta puede ser eliminada o contenida a partir de encarar un conjunto

de acciones punitivas.
En este sentido, constituyen regularidades de este discurso:

a) La aseveración de que la amenaza es máxima: Constituye una regularidad de este discurso el emplear una narrativa en la cual se argumenta la necesidad de enfrentar un fenómeno que por sus características reviste un peligro de gravedad máxima, superior a cualquier otro y, en general, por sobre cualquier otra experiencia histórica. Siguiendo la retórica propia del discurso religioso a partir del cual se organiza el Malleus la brujería, esto es el blanco principal de la inquisición medieval, es identificada como un fenómeno de gravedad mayúscula. De hecho, en el libro se la presenta como la "más maligna y la peor de todas" entre las diversas formas de herejía. Como explica Zaffaroni, la exaltación de esta dimensión resulta esencial, porque es de ella que se deriva la percepción construida en relación a la peligrosidad del momento en cuestión y, con esto, de la magnitud del poder que será conferido al represor para neutralizarla.

b) La amenaza es concebida como un mal potencial. El fenómeno en cuestión es caracterizado como un riesgo para algo que se identifica como arquetipo de lo bueno en una narrativa que se articula en torno a la contraposición del bien y el mal. En el Malleus, la brujería es caracterizada como un fenómeno que supone un riesgo para nada menos que la salvación eterna no ya de aquellos que la practican sino todos los miembros de la comunidad cristiana. El discurso del poder punitivo se caracteriza por atribuir al otro la intencionalidad explícita de hacer daño.

c) El contenido específico de lo peligroso se vincula a los prejuicios de la época. Una conclusión bastante obvia de la lectura del Malleus es que los argumentos en torno a la caracterización de la brujería y, más específicamente, de la importancia de las mujeres en esta práctica se consolidaron como discurso dominante a partir de estar basados en alguna medida en los prejuicios vigentes en la época.
En este sentido, cuando Kramer y Sprenger (2002: 115-116) abordan la cuestión de por qué eran las mujeres las principales exponentes de la brujería algunos de los argumentos presentados fueron: que las mujeres "hablan mucho y comparten con otras mujeres", "porque son más débiles en mente y cuerpo", "porque en lo que se refiere a la comprensión de las cosas parecen de una naturaleza diferente a la del hombre y, en definitiva, porque siendo formadas de una "costilla curva del hombre" presenta ya en su naturaleza una dirección contraria de este.
La identificación de aquellos catalogados como *indeseables,* esto es del foco de la acción punitiva, generalmente se sostiene sobre la base de un conjunto de creencias previamente difundidas en la sociedad (que, por su parte, sirve para reforzar). En particular se vincula con aquellos grupos sociales que no se adaptan a aquello que es considerado como aceptable en cada momento histórico.

d) Invertir la valoración de los hechos: Si hay algo que resulta expresivo en la lectura del Malleus es que la lógica argumentativa se articula para pautar la interpretación de los hechos

propuesta independientemente de cuáles sean sus manifestaciones observadas. De hecho, una misma acción debía ser interpretada por los inquisidores en función de quien la realizara. Por ejemplo, en el Malleus se argumenta que la *observación del tiempo y las estaciones* debía ser considerada un ejercicio vano y ocioso u orientado a la adquisición de conocimientos que lleven a una mejora en su cuerpo cuando era realizada por un hombre. Por el contrario, si dicha acción era observada en una mujer debía ser entendida como una adivinación y, así, un acto de brujería (Kramer & Sprenger, 2002: 27).

e) Se intenta neutralizar cualquier fuente de autoridad que establezca una interpretación contraria de los hechos. Las primeras secciones del Malleus están destinadas a rebatir las posiciones de aquellos que aseguraban o bien que las brujas no tenían una existencia real, o bien que sus acciones no tenían efectos reales y permanentes. Kramer y Sprenger (2002: 59-63) argumentan, en definitiva, que aquellos que desafiaran la narrativa oficial sobre la cuestión debían ser considerados como "sospechosos de sostener opiniones heréticas".

4. **¿Cuándo?** – Otra regularidad propia del discurso del poder punitivo consiste en argumentar que la intervención reviste un carácter urgente dado que el fenómeno en cuestión presenta una frecuencia alarmante. En tanto la acción sigue el principio lógico de la prevención la intervención debe ser de carácter inmediato. Como argumentó Foucault (2004: 73) el ejercicio del poder punitivo obedece a una lógica esencialmente disciplinaria que recae sobre la virtualidad del comportamiento, esto es, "antes inclusive de que el gesto sea una realidad". Así:

a) Se afirma que la intervención debe ser efectuada con urgencia. En el Malleus se argumenta que la acción de las brujas se había multiplicado en los años recientes, que su práctica había aumentado notablemente y que la cantidad de brujas había aumentado como consecuencia de la rivalidad entre personas casadas y solteras (2002: 77-102). Como afirma Zaffaroni, es característico del discurso punitivo el argumento consistente en que la coyuntura vigente se define por la presencia de un fenómeno cuya elevada frecuencia constituye un riesgo inminente y que, por tanto, configura una situación emergencial. Es por esto que el miedo aparece como fundamento último de la acción.

5. **¿Cómo?** – En tanto discurso orientado al castigo preventivo, de forma regular se argumenta la necesidad de emprender acciones de tipo extraordinario. Fundada sobre una serie de caracterizaciones sobre la naturaleza del conflicto y del enemigo, el argumento central se orienta a sostener que sólo una intervención que articule medios extraordinarios tiene la oportunidad de ser exitosa. Para esto se invoca frecuentemente la imagen de una guerra que configura un estado de excepción contra un enemigo cuya imagen se desvalorizada el que presenta una organización de características difusas, pero al mismo tiempo de acción coordinada.

a) Se emplea una retórica belicista. Tal como destacado por Zaffaroni, una de las características del Malleus es el apelo constante a un lenguaje de tipo bélico. En este sentido, citando a Santo Tomás, Kramer y Sprenger (2002: 363) aseveran que "existe una guerra declarada entre hombres y demonios". Siendo que ese conflicto es retratado en función de la caracterización que se hace de la persona del enemigo y de su estrategia.

b) Se caracteriza al enemigo como de presencia difusa, pero de acción coordinada. En el caso del Malleus este argumento se ilustra en la afirmación de que los demonios se presentaban en forma humana a partir de encantamientos, al tiempo que resultaba una *verdad católica* el hecho de que en lo que hace a la generación de daño, "las brujas y el demonio trabajan juntos". Esto porque "como se encuentran en guerra con la raza humana la combaten de manera ordenada; juzgan así perjudicar más a los hombres y, efectivamente, lo consiguen" (Kramer & Sprenger, 2002: 92)
En otras palabras lo que es colocado es que las supuestas múltiples manifestaciones del fenómeno (su frecuencia elevada) se corresponden con la acción de grupos que siguen una lógica única y que, por tanto, deben ser combatidos con una acción también única y total.

c) Se desvaloriza la imagen del enemigo y se diferencia su trato. La narrativa se orienta a la desvalorización de la imagen del enemigo (lo que, como referido, se sustenta sobre los prejuicios de cada época) y a argumentar que, dadas sus características (difusa y coordinada) y la lógica que orienta su accionar (hacer daño) su neutralización sólo puede ser alcanzada mediante acciones de tipo extraordinario, esto es diferentes de las formas de intervención entendidas como regulares. Como destaca Zaffaroni (2006: 11), al enemigo se le niega su condición de persona y solamente es considerado como un ente peligroso o dañino eximiendo de toda ética a aquellos que encaran las acciones represivas.

d) Presentación de la estrategia del enemigo como orientada a explotar vulnerabilidades. Este constituye un elemento central en la justificación de las tareas de vigilancia y disciplinamiento de la comunidad, estas últimas orientadas a evitar que dichas vulnerabilidades emerjan.
Como expresado por Zaffaroni del Malleus se desprende claramente la idea de que el *vicio genera vulnerabilidad* . En el discurso se encuentran claramente presentes elementos normatizantes en el sentido de que se afirma la necesidad de *vivir ordenadamente* , de obedecer las normas sociales para evitar ser víctima del enemigo. Así, los autores expresaban que la vulnerabilidad se vinculaba al *libertinaje de la carne* : "tres vicios generales parecen tener un dominio especial sobre los males de las mujeres: la infidelidad, la ambición y la lujuria" (Kramer & Sprenger, 2002: 121). Esto, lógicamente, resulta en un discurso moralizante que condena todas aquellas expresiones que la autoridad en cuestión considere como anormales.
Las mujeres en el Malleus son pensadas como un grupo vulnerable ya que su mente es más débil. Según la narrativa, las mujeres constituían el colectivo que más pactaba con Satán porque eran más supersticiosas y más crédulas como resultado de una mente más débil por lo que resultaba más fácil menoscabar su fé (Kramer & Sprenger, 2002: 119-120).

En definitiva, las regularidades agrupadas en este punto 5 apuntan, precisamente, al tipo de prácticas que se corresponden lógicamente con el principio de racionalización del discurso punitivo. Se trata así del ejercicio de una vigilancia continua, sustentado sobre un registro permanente, constante y centralizado. Del imperativo de actuar de forma preventiva, contra la acción potencial de un enemigo difuso cuya acción es coordinada y orientada a explotar las vulnerabilidades de diversos miembros de la comunidad emerge el mecanismo de monitoreo como respuesta lógica.

La vigilancia no constituye una práctica novedosa sino más bien una técnica de control que, al decir de Foucault, tiene sus orígenes en el medioevo pero se tornó relativamente generalizada en el final del siglo XVIII. En este sentido, cuando dicho autor analiza el dispositivo panóptico en *Vigilar y castigar* (1983: 238) argumenta que su relevancia conceptual no radica en ser un modelo de diseño de edificaciones de tipo penitenciario, sino que debía de ser pensado como una tecnología política cuya comprensión requería el desvincularla de todo uso específico. Así, para Foucault el *panoptismo* constituye un modelo de vigilancia cuya generalización se ilustra en el hecho de que el autor emplea esa clave analítica como marco interpretativo de fenómenos que intuitivamente se presentan tan diversos como los reglamentos de organización urbana o los esquemas sanitarios del siglo XVIII. En otras palabras, para el autor en ese momento histórico el dispositivo de vigilancia se tornó una forma de gobernar generalizada, esto es una manera de "guiar a los hombres, de dirigir su conducta, de forzar sus acciones y reacciones" (Foucault, 2008: 4).

El listado anterior resume los principales elementos que componen la estructura lógica del discurso del poder punitivo. Estos son empleados en la sección siguiente como categorías de interpretación de una serie de pronunciamientos que encuadran la práctica de la vigilancia de comunicaciones como una herramienta esencial en la garantía de la seguridad doméstica e internacional. La intención es la de mostrar que, aunque temporalmente distantes, estos repiten el mismo eje argumental. En otras palabras lo que se afirma es que pese a la contemporaneidad del fenómeno aquí estudiado y del carácter eminentemente actual de las tecnologías empleadas, se siguen mecanismos de racionalización idénticos a los que cinco siglos atrás justificaban la quema de brujas y otros criminales de la época.

La (ciber)inquisición

> Estamos ingresando en la edad de oro de la HLT [Tecnología del lenguaje humano, sigla en inglés]. Computadoras poderosas y de bajo costo, redes de alta velocidad y algoritmos avanzados están siendo combinados para revolucionar la estación de trabajo del analista (NSA, 2006).

> El gobierno trató de justificar el programa secreto de la NSA evocando exactamente el tipo de teoría extremista del poder ejecutivo que me había motivado a empezar a escribir: la idea de que la amenaza del terrorismo internacional daba al presidente la autoridad prácticamente ilimitada para hacer cualquier cosa de modo de garantizar la seguridad de la nación (Greenwald, 2014: 11).

A lo largo de la historia en el lugar de amenaza máxima fueron encuadrados diversos grupos como ser las brujas en el Malleus, y más cercano en el tiempo, los comunistas, los subversivos y los narcotraficantes, entre otros. Es en este sentido que el poder punitivo es estructuralmente selectivo, porque siempre se funda en la capacidad de escoger de forma arbitraria a su enemigo. La elevación de este último a la categoría de amenaza máxima hace que, más allá de que se reconozca la existencia de otros conflictos, se presente un escenario en el cual "todos los males provienen del enemigo fuente de la emergencia", de esta manera se justifica cualquier tipo de medidas orientadas a su represión (Zaffaroni, 2012: 46).

De ahí la relevancia de los acontecimientos del 11 de septiembre de 2001 en los Estados Unidos para comprender la actual estructura del sistema de vigilancia masiva de comunicaciones. Visto en retrospectiva, la centralidad de ese evento radica en que configuró un factor de posibilidad para expansión del aparato punitivo estadounidense sobre, prácticamente, la totalidad del planeta. A partir de ese día el terrorismo como fenómeno y el terrorista como sujeto, con algunos derivados como el del ciberterrrorista, pasaron a encarnar el lugar de amenaza máxima preconfigurado en el discurso del poder punitivo. Como argumenta Zaffaroni (2011b: 2): "La lucha contra el terrorismo se ha convertido en la nueva doctrina planetaria de la seguridad nacional, que pretende legitimar procedimientos extraordinarios internacionales".

Entre otras cuestiones, a partir de la Ley Patriota se sustituyó el principio de causa probable por el de relevancia como fundamento para la legitima violación de la privacidad (Greenwald, 2014: 37) y se reforzó la diferenciación existente en materia de garantías para nacionales y extranjeros habilitando la práctica de la vigilancia masiva y global dentro del ordenamiento jurídico estadounidense.

Tal como se la presenta en la propia Ley Patriota, así como en los más variados pronunciamientos de actores del sistema político estadounidense y de la industria de las telecomunicaciones, esta medida se justifica en tanto configura una herramienta central en la neutralización de las amenazas que en la actualidad enfrenta ese país y, en términos más generales, el mundo.

Como expresado por el subsecretario de prensa de los Estados Unidos, Josh Earnest, en defensa de los mecanismos de recolección de datos previstos en el Ley Patriota luego de la filtración de los documentos Snowden, la colecta de metadatos:

> ha sido una herramienta crítica en la protección de la nación frente a las amenazas terroristas al posibilitar que los funcionarios de contraterrorismo descubran si terroristas conocidos o sospechados han mantenido contacto con otras personas que podrían estar involucradas en actividades terroristas, particularmente personas localizadas dentro de los Estados Unidos (Earnest & Duncan, 2013: 30).

En igual sentido se manifestó el entonces Director de la NSA, el General Keith Alexander, quien cuando cuestionado sobre los programas de vigilancia precisó acerca de la necesidad de conseguir que los Estados Unidos "comprenda por qué necesitamos estas herramientas". Destacó, además, la supuesta relevancia que habría tenido el monitoreo de comunicaciones como insumo para los organismos de inteligencia en su tarea de evitar nuevos ataques terroristas concluyendo que: "[e]llos no pueden hacerlo sin estas herramientas. Entonces, nosotros vamos a tener un debate en este país: vamos a abandonar estas herramientas? Estoy preocupado con que adoptemos la decisión incorrecta" (Romm, 2013: 2–5).

Del análisis de los discursos y de los textos legislativos surge un relato coherente y definido en el cual los Estados Unidos se identifica como un actor estatal que reclama su derecho a intervenir para proteger a su población y al mundo entero al tiempo que sostiene que se encuentra en una posición privilegiada para hacerlo. La retórica empleada es abiertamente

bélica con conceptos que van desde la conocida Guerra Global al Terror hasta sus aplicaciones más vinculadas a las tecnologías de información y comunicaciones como los de: ciberguerra, ciberarmas, ciberataque, ciberdefensa, ciberdisuación y ciberespacio como dominio operacional de las Fuerzas Armadas.

También aquí se sostiene la necesidad de intervenir con urgencia ante un fenómeno en franco crecimiento. Las brujas de ayer son los terroristas de hoy, acompañados por sus pares específicos de la era digital, ciberterroristas, cibercriminales, etc. Sobre estos, tal como en el pasado, se afirma que orientan su accionar a hacer el mal (generar terror en este caso) lo que consiguen fundamentalmente a partir de explotar vulnerabilidades. Como identifican Hansen y Nissembaum (2009) la analogía con los conceptos de la epidemiología, tales como el de virus y computadoras infectadas, terminó configurando un discurso en el cual la imagen predominante es la de que la situación de inseguridad se deriva del comportamiento irresponsable de individuos que comprometen la salud del conjunto.

En sentido similar se sostiene que una de las dimensiones de la amenaza actual es que los jóvenes son permeables a las ideas de los *grupos extremistas.* Con una formulación idéntica a la que hace cinco siglos posibilitaba afirmar que las mujeres eran débiles mentalmente y que esto tornaba fácil el menoscabar su fe, en el presente se argumenta que los jóvenes son vulnerables, referenciándolos como en el caso de los ejecutivos de Google como una *juventud alienada* (Schmidt & Cohen, 2013: 187-188), y que "los radicales tienen influencia radicalizante" al difundir su mensaje "al conjunto de personas susceptibles" (NSA, 2012).

Con el objetivo de mostrar de una manera más exhaustiva la correspondencia en términos argumentativos entre el discurso legitimante de la vigilancia masiva y global de comunicaciones y el discurso demonológico presentado en el sección precedente se seleccionaron dos pronunciamientos correspondientes a dos presidentes de los Estados Unidos enunciados en dos contextos diferentes. El primero de ellos, corresponde al discurso del ex presidente Bush (2005) en el año 2001 en el momento de la promulgación de la Ley Patriota. El segundo es un discurso del presidente Obama (2014) en el año 2014 en ocasión del anuncio de la revisión de las disposiciones sobre vigilancia de comunicaciones. Así, mientras que el primero se da en un escenario de fervor marcado por los acontecimientos del 11 de septiembre, el segundo se da con posterioridad a la publicación de los documentos Snowden y en un contexto de fuertes críticas nacionales e internacionales al programa de vigilancia de comunicaciones. El punto central del argumento en este sentido es que si bien ambos guardan matices que los diferencian siguen idéntica estructura ya que se ordenan siguiendo la lógica del poder punitivo.

Para la presentación de los resultados se eligió el formato de tabla el cual, si bien exige incurrir en ciertas simplificaciones, posibilita al mismo tiempo, claridad expositiva.

TABLA 1

Estructura argumentativa del Malleus Maleficarum del año 1486 y de discursos sobre vigilancia masiva y global de comunicaciones de Bush del año 2001 y de Obama (2014)

Regularidades discursivas	Malleus (1486)	Bush (2001)	Obama (2014)
¿Qué? - Caracterización del conjunto de prácticas a las cuales el discurso se refiere.			
Enunciación de intervenciones de neutralización, de acciones preventivas de carácter punitivo.	Nosotros, en cumplimiento de nuestras obligaciones, nos mostramos absolutamente deseosos [...] de aplicar remedios potentes para prevenir la enfermedad de la herejía y de otras torpezas que difunden su veneno causando la destrucción de muchas almas inocentes (p.2)	"Ley Patriota. Para impedir y castigar actos terroristas" "Auxiliará a las agencias de aplicación de la ley a identificar, a desmantelar, a impedir y a castigar terroristas antes de que ellos ataquen"	"Entonces nosotros demandamos que nuestra comunidad de inteligencia aumente sus capacidades y que las agencias policiales cambien sus prácticas para enfocarse más en prevenir ataques antes de que ocurran que en perseguir a los terroristas después de que hayan atacado"
¿Quién / dónde? - Afirmación de una autoridad central como sujeto legítimo de toma de decisiones			
La afirmación de la autoridad y la confiscación del conflicto	La brujería es entendida como un crimen contra Dios en cuya representación intervenía la autoridad eclesiástica, para ello Kramer y Sprenger "fueron nombrados por medio de las Cartas Apostólicas Inquisidores de estas depravaciones heréticas, y lo son desde ya. El primero actuando en las mencionadas regiones de Alemania septentrional [...] y el segundo en ciertos territorios que se extienden a lo largo de las márgenes del Rin" (p.2)	"esta ley le otorgará a los agentes de inteligencia y de aplicación de la ley las nuevas herramientas que precisan para combatir este peligro actual" "Una ley para detener y castigar actos terroristas em los Estados Unidos y alrededor del mundo" (p.1306)	"la tecnología ha borrado las fronteras" (p.2) "América [Estados Unidos] tiene responsabilidades especiales derivadas del hecho de constituir la única superpotencia mundial" (p.9)
Las capacidades superlativas de la autoridad para encarar la intervención	Tal como se afirma en el Malleus los encargados de la administración de justicia contra las brujas eran inmunes a sus encantamientos (p. 82).		"Como he señalado, los Estados Unidos tienen responsabilidades únicas cuando nos referimos a la recolección de información de inteligencia. Nuestras capacidades ayudan no sólo a proteger a nuestra nación, así como también a nuestros amigos y aliados" (p.15)
¿Por qué? - Se racionalizan las prácticas en tanto orientadas a la prevención. La intervención es presentada como una respuesta derivada de la necesidad de neutralizar un peligro inminente.			
Aseveración de que la amenaza es máxima	"Los males perpetrados por las brujas modernas exceden todos los pecados ya permitidos por Dios" (p.164) "de todos los criminales del mundo, son las brujas las que merecen el castigo más severo" (p.174)	"una amenaza como ninguna otra nación ha enfrentado jamás"	"las amenazas emergentes de los grupos terroristas y la proliferación de armas de destrucción masiva constituyeron demandas nuevas, y en algún sentido, más complicadas" (p.2) "los desafíos derivados de amenazas como el terrorismo y la proliferación y los ciberataques no irán a desaparecer a la brevedad. Continuarán siendo un problema mayúsculo (p.7)
La amenaza constituye un mal potencial. Narrativa moralizante que enfrenta el bien y el mal	"la brujería se diferencia de todas las demás artes perniciosas y misteriosas por el hecho de que, de todas las supersticiones, es la más vil y más maligna, la más hedionda – su nombre latino *maleficarum* significa exactamente practicar el mal y blasfemar contra la Fé verdadera" (p.77)	La conceptualización del terrorismo: acciones orientadas a generar pánico. Esta legislación es esencial, no sólo para perseguir y castigar a los terroristas, sino también para prevenir más atrocidades de parte de los malvados [evil ones]" (p.1307)	La conceptualización del terrorismo: acciones orientadas a generar pánico. "La globalización y la Internet han transformado a las amenazas en más agudas, dado que la tecnología ha eliminado las fronteras y ha empoderado a los individuos posibilitándoles proyectar tanto una gran violencia como un gran bien" (p.2)
El contenido específico de lo peligroso se vincula a los prejuicios de la época	Idea de mujer como ser inferior, susceptible de supersticiones. Foco en las mujeres que ocupaban ciertos papeles destacados como las parteras.	Utilización reiterada de la imagen del 11/09 "ya hemos visto los horrores que los terroristas pueden causar" (p.1307). "Estamos luchando contra personas que odian nuestros valores (p.1308)"	Utilización reiterada de la imagen del 11/09. "[y] respecto de la colección en masa de señales de inteligencia, las agencias estadounidense utilizarán esos datos únicamente para alcanzar objetivos de seguridad específicos: contrainteligencia, contraterrorismo, contraproliferación, ciberseguridad, protección de nuestras tropas y nuestros aliados e combatir el crimen transnacional, incluyendo la evasión de sanciones" (p.16)

TABLA 1 (CONTINUACIÓN)

Estructura argumentativa del Malleus Maleficarum del año 1486 y de discursos sobre vigilancia masiva y global de comunicaciones de Bush del año 2001 y de Obama (2014)

Regularidades discursivas	Malleus (1486)	Bush (2001)	Obama (2014)
¿Cuándo? Establecimiento de un plazo perentorio para la acción.			
Afirmación del carácter emergencial vinculado a la elevada frecuencia del fenómeno	"Pasemos ahora a analizar el origen de las brujas y el modo en el que en los últimos años sus actos comenzaron a multiplicarse entre nosotros" "Infelizmente, el juzgamiento de la Fé Apostólica, única soberana y mentora de toda verdad, expresada en la Bula de nuestro Santo Padre, nos asegura y nos concientiza sobre el florecimiento entre nosotros de tales crímenes y maleficios y no habremos de nos abstener de proseguir con la inquisición para no poner en riesgo nuestra propia salvación" (p.77)	"El gobierno apoyará esta ley con toda la urgencia de una nación en guerra" (p.1306)	"Los americanos reconocieron que tuvimos que adaptarnos a un mundo en el cual una bomba puede ser construida en un sótano y nuestras redes eléctricas pueden ser desconectadas por operadores a un océano de distancia (p.3)
¿Cómo? - Racionalización de las características de la intervención. Afirmación de la necesidad de emplear medios extraordinarios en la neutralización de la amenaza			
Empleo de una retórica belicista	"existe una guerra declarada entre hombres y demonios" (p.155)	"El gobierno apoyará esta ley con toda la urgencia de una nación en guerra" (p.1306)	"Una variedad de factores han permanentemente dificultado los esfuerzos americanos de, simultáneamente, defender nuestra nación y mantener nuestras libertades civiles"(4)
Afirmación de la necesidad de encarar la intervención haciendo uso de medios extraordinarios, se amplía el poder de las agencias.	"Mostrándonos absolutamente deseosos de remover todos los obstáculos que dificultan la obra de los Inquisidores [declaramos que su poder se] extiende a todas las mencionadas provincias, diócesis, aldeas..." (p. 3)	Las investigaciones son lentificadas, frecuentemente, por las limitaciones em el alcance de las órdenes federales de búsqueda [...] bajo esta nueva legislación, las órdenes son válidas em todos los distritos a lo largo de todos los estados (p.1306).	"No podemos prevenir ataques terroristas o ciber amenazas sin algún grado de capacidad para penetrar las comunicaciones digitales. Y, como un Presidente que analiza [los informes de] inteligencia cada mañana, no puedo sino recordar permanentemente de que America necesita permanecer vigilante respecto de estas amenazas" (p.10) "interceptar las comunicaciones de objetivos extranjeros en el exterior que poseen información vital para nuestra seguridad nacional" (p.11)
Desvalorización del enemigo y diferenciación del trato que merece	"[c]astigar a las brujas de esta manera no parece ser suficiente [...] por su propia abnegación incluso homenajean a los demonios ofreciéndoles sus cuerpos y sus almas" (p.165)	"No reconocen parámetros morales. No tienen conciencia. No se puede razonar con los terroristas" (p.1306)	Utilización reiterada de fórmulas que refieren a la maldad como, por ejemplo, "actores maliciosos".
El enemigo es difuso, pero su acción coordinada	Los demonios se presentan en forma humana a partir de encantamientos, al tiempo que "le]s católico afirmar que existe cierto orden de acciones interiores y exteriores y un grado de preferencia entre los demonios [...] porque siendo que están en guerra con la raza humana, combaten de forma ordenada, porque de este modo pueden hacer un daño mayor a los hombres" (p.38)	"Estamos lidiando con terroristas que operan empleando métodos y tecnologías altamente sofisticados" (p.1306)	"esta es una era de amenazas difusas y revolución tecnológica. ¿Por qué esto es necesario? El programa [de vigilancia] emerge del deseo de cubrir una brecha identificada luego del 11/9 [...]. El programa de metadatos telefónicos comprendido en la sección 215 fue diseñado para mapear las comunicaciones de los terroristas para posibilitarnos ver con quién están haciendo contacto lo más rápido posible. [...] y considero que es importante que esta capacidad que el programa está diseñado para proveer sea preservada (p. 12- 13)
Presentación de la estrategia del enemigo como orientada a explotar vulnerabilidades	Las conductas "desordenadas" facilitan la acción de brujas y demonios "tres vicios generales parecen tener un dominio especial sobre los males de las mujeres: la infidelidad, la ambición y la lujuria". Las debilidad de las mujeres las convertía en vulnerables porque era fácil menoscabar su fe.	La vigilancia de comunicaciones constituye otra herramienta esencial para perseguir terroristas [...] esta nueva ley habilita la vigilancia de todas las comunicaciones empleadas por terroristas, incluyendo los correos electrónicos, la Internet y los teléfonos celulares. De esta manera, estaremos en mejores condiciones para enfrentar los desafíos tecnológicos causados por la proliferación de tecnologías de comunicaciones (p.1306)	

Fuente: Elaboración propia.

CONSIDERACIONES FINALES

Idéntico principio de racionalización, iguales argumentos, prácticas similares y, consecuentemente, mismas consecuencias en términos de poder. En la actualidad, al igual que durante los últimos cinco siglos, el discurso del poder punitivo se mantiene vigente. Se argumentan las mimas ideas, se ejecutan las mismas prácticas. En ese punto radica la importancia de estudiar, también, esta dimensión del sistema de vigilancia.

Es por eso que el presente artículo tuvo el objetivo de estudiar los discursos sobre vigilancia masiva de comunicaciones. Ese análisis, inspirado en la obra de Zaffaroni, intenta mostrar que la misma estructura argumental que hoy posibilita a algunos afirmar que la vigilancia de comunicaciones es herramienta indispensable para la garantía de la seguridad es la que cuatro siglos atrás permitía afirmar, a algunos otros, que aquellos que resultaba necesario era quemar mujeres. En otras palabras lo que se afirma es que pese a la contemporaneidad del fenómeno aquí estudiado y del carácter eminentemente actual de las tecnologías empleadas, se siguen los mismos mecanismos de racionalización sobre los cuales se estructuró la práctica inquisitorial.

Ayer como hoy, el poder punitivo revela su verdadero poder. Lejos de restringirse a su objetivo declarado de *perseguir a los malos* estructura un sistema de vigilancia que avanza sobre la población mundial. Si se considera como un número indicativo el hecho de que en la actualidad Internet posee aproximadamente 3000 millones de usuarios, entonces casi la mitad de la población está sujeta a este sistema de fichaje digital.

También hoy como ayer se expresa la resistencia. Con diversos grados de organicidad grupos e individuos emprendieron, desde los orígenes de la red, acciones orientadas a proteger la su propia privacidad y la de de los usuarios en general. Este tipo de prácticas, entendidas por el poder como formas de resistencia a la autoridad, pasaron entonces a ser etiquetadas como sospechosas tal como en los tiempos de la inquisición las denuncias sobre la estructura del sistema eran consideradas herejía y prueba de que quien las enunciaba era un hereje. Hoy el uso de sistemas de protección de datos por parte de la población en general, como por ejemplo el uso de criptografía para proteger el contenido de las conversaciones, es señalado como indicio de culpabilidad. Esta idea de que la privacidad es una preocupación exclusiva de aquellos que tienen *algo para esconder,* o para gente *indecente,* fue expresada con singular claridad por Eric Schmidt, CEO de Google, en 2009 al afirmar en una entrevista con la cadena CNBC (2009) "si tienes algo que no quieres que nadie sepa, tal vez no deberías estar haciéndolo en primer lugar".

Otros, a lo largo de la historia, han argumentado directamente contra la estructura sobre la cual se ejercen controles punitivos sobre la sociedad, denunciando su selectividad y su irracionalidad. Zaffaroni (2013: 39-40) destaca el caso de Spee quien, en el siglo XVII, siguió el camino que pocos antes habían transitado para articular la voz de aquellos que entienden en el poder punitivo una estructura de permanente legitimación de masacres. Mostró la disparidad existente entre los objetivos declarados y las funciones específicas reales que el poder punitivo encarnaba en su época,

la arbitrariedad de las agencias y la necesidad de encarar el debate (y la acción) sobre el principio de la cautela. Esa cautela que nos muestra que lo único que de manera eficaz podemos prevenir, son las acciones encaradas de forma colectiva por la sociedad.

En la actualidad otros han entrado en la historia por denunciar las mismas irracionalidades, legitimadas a partir del mismo discurso pero contra otros grupos objetivos. Conocidos los casos de Julian Assange, de Jacob Appelbaum y de Aaron Schwartz como cara visible de otros que con su práctica cotidiana se contrapusieron al avance de la vigilancia sobre la actividad de las personas y que con su trabajo posibilitaron crear herramientas y alternativas que sirvan de protección efectiva y reflexión colectiva. En una provocadora expresión, Assange destaca que el escenario actual se caracteriza por ser un Estado de excepción en el cual la recolección de datos personales es habilitada por vía administrativa. En este sentido afirma: "todos vivimos bajo Ley Marcial en lo que a nuestras comunicaciones respecta" (Assange, Appelbaum, Müller-Maguhn, & Zimmerman, 2013: 39)

Desde el corazón mismo del sistema, la filtración de documentos secretos por parte de Manning y Snowden expusieron de forma cabal y concreta la irracionalidad del punitivismo en su máxima expresión. En particular, este último permitió conocer las alternativas de la vigilancia a gran escala ofreciendo pruebas acabadas de que se trata de un esquema que alcanza a la población total sin mecanismos de selectividad al tiempo que presenta una escasa efectividad en términos de sus objetivos declarados.

La mayoría de los que constituyen hoy la cara visible de estas fuerzas de contraposición sufren, al igual que cinco siglos atrás, el ataque de aquellos que los perciben como efectivos focos de resistencia a la autoridad. Hoy como ayer el miedo constituye un motor fundamental del avance del sistema punitivo la alternativa, como la señala Zaffaroni, es la cautela.

NOTAS

* Licenciada en Economía por la Universidad de Buenos Aires (UBA). Alumna del curso de Pos graduación en Relaciones Internacionales por de la Universidad de Santa Catarina (PPGRI-UFSC). lauralacaze@riseup.net

1. La consulta de los documentos puede realizarse a partir del sitio: `https://edwardsnowden.com` accedido el 26/09/2016.

2. En el marco del presente artículo se utilizará el término Ley Patriota en referencia a la USA PATRIOT ACT: ''Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001' (EUA, 2001)'.

3. La relevancia del Malleus Maleficarum radica, siguiendo a Zaffaroni, en que constituye el primer tratado que integró de forma sistemática el saber existente hasta el momento sobre el origen del mal (saber criminológico), sobre las manifestaciones del mal (saber penal) y sobre las prácticas para su correcta identificación (saber criminalístico) (Zaffaroni, 2011a: 29).

REFERENCIAS

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2013). *Criptopunks: la libertad y el futuro de internet*. (N. Lerner, Trad.). Buenos Aires: Marea Editorial.

Bruno, F. (2012). Surveillance and participation on Web 2.0. En D. Lyon, K. D. Haggerty, & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 343–351). Abingdon, Oxon; New York: Routledge.

Bush, J. W. (2005). Remarks on Signing the USA PATRIOT ACT of 2001 (26/10/2001). En Estados Unidos da América (EUA) (Ed.), *George W. Bush (book II — july 1 to december 31, 2001)* (pp. 1036-1037). Washington D. C.: United States Government Printing Office. Recuperado a partir de https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf

CNBC. (2009, noviembre 30). Inside the Mind of Google. New Jersey: CNBC. Recuperado a partir de: http://www.cnbc.com/inside-the-mind-of-google/?__source=vty|insidegoogle|&par=vty

Earnest, J., & Duncan, A. (2013). Barack Obama: Press Gaggle by Deputy Principal Press Secretary Josh Earnest and Secretary of Education Arne Duncan [The American Presidency Project]. Recuperado a partir de: http://www.presidency.ucsb.edu/ws/?pid=103689

Emmerson, B. (2014). *Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo* (Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo No. A/69/397). New York: Nações Unidas.

Estados Unidos da América (EUA). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 115 STAT. 272 132 (2001). Recuperado a partir de: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

Finley, L., & Esposito, L. (2014). "Digital Blackwater": The National Security Administration, Telecommunications Companies and State-Corporate Crime. *State Crime Journal* , *3* (2), 182–199.

Foucault, M. (1983). *Vigilar y castigar: nacimiento de la prisión* (1a Reimp.). Buenos Aires: Siglo Veintiuno Editores S.A.

Foucault, M. (1987). *A arqueologia do saber* . (L. F. B. Neves, Trad.) (3ª). Rio de Janeiro: Forense Universitária.

Foucault, M. (2004). A evolução da noção de "indivíduo perigoso" na psiquiatria legal do século XIX. *Ditos e escritos*, *5*, 1–25.

Foucault, M. (2005). *El poder psiquiátrico: curso en el Collège de France (1973-1974)*. Buenos Aires: Fondo de Cultura Económica.

Foucault, M. (2008). *Nascimento da Biopolítica: curso dado no Collège de France (1977-1978)*. (M. Senellart, Ed., E. Brandão & C. Berliner, Trads.) (1ª). São Paulo: Martins Fontes.

Fuchs, C., & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications*, *40* (1).

Gómez, S. M. (2016). *El alcance de las palabras*. Recuperado a partir de: http://observatorio-riqueza.org/wp-content/uploads/sites/15/2016/09/Ensayo_-El-alcance-de-las-palabras-Observatorio.pdf

Greenwald, G. (2014). *Sem Lugar Para Se Esconder - Edward Snowden, A Nsa e A Espionagem do Governo Americano*. (F. Abreu, Trad.). Rio de Janeiro: Sextante.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53* (4), 1155–1175.

Kramer, H., & Sprenger, J. (2002). *O Martelo das feiticeiras: malleus maleficarum*. (P. Fróes, Trad.). Rio de Janeiro: Rosa dos Tempos.

Lefébure, A. (2014). *El caso Snowden: así espía Estados Unidos al mundo* (1a ed.). Buenos Aires: Capital Intelectual.

National Security Agency (NSA). (2006, enero 8). For Media Mining, the future is now! Recuperado a partir de: https://assets.documentcloud.org/documents/2072019/sidtoday-future-is-now-final.pdf

National Security Agency (NSA). (2011). *New Collection Posture*. Recuperado a partir de: https://edwardsnowden.com/2014/05/13/new-collection-posture/

National Security Agency (NSA). (2012, marzo). *Global Radicalizers Vulnerable in Terms of Authority*. Recuperado a partir de: https://edwardsnowden.com/2013/11/27/global-radicalizers-vulnerable-in-terms-of-authority/

Obama, B. (2014, ene). *Remarks by the President on Review of Signals Intelligence*. Declaração do Presidente presentado en Department of Justice, Washington D. C. Recuperado a partir de: https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

Poitras, L. (2014). *Citizenfour*. Recuperado a partir de: https://citizenfourfilm.com/

Romm, T. (2013, septiembre 25). NSA chief Gen. Keith Alexander slams "sensationalized" reporting. *Politico*. Recuperado a partir de: http://www.politico.com/story/2013/09/nsa-chief-slams-sensationalized-reporting-97337.html

Schmidt, E., & Cohen, J. (2013). *A nova era digital*. (A. B. Rodrigues & R. Durst, Trads.) (1.ª ed.). Rio de Janeiro: Intrínseca.

Zaffaroni, E. R. (2006). *El Enemigo en el Derecho Penal*. Buenos Aires: Ediar.

Zaffaroni, E. R. (2011a). *La palabra de los muertos: conferencias de criminología cautelar* (1. reimpr). Buenos Aires: Ediar.

Zaffaroni, E. R. (2011b, mayo 8). "Fue una ejecución sin proceso" [Página/12]. Recuperado a partir de: http://www.pagina12.com.ar/diario/elpais/1-167766-2011-05-08.html

Zaffaroni, E. R. (2012). *Crímenes de masa* (2a ed.). Buenos Aires: Ediciones Madres de Plaza de Mayo.

Zaffaroni, E. R. (2013). *La cuestión criminal* (5. ed). Buenos Aires: Planeta.

PEÇO PERDÃO PELO VACILO: EXERCÍCIOS AUTORITÁRIOS EM VÍDEOS AMADORES COMPARTILHADOS NO YOUTUBE

Resumo: Neste artigo, nos voltamos para o canal brasileiro de YouTube "Apoio Policial Oficial", que possui mais de 107 mil inscritos e de 44 milhões de visualizações. Nele, são veiculados vídeos amadores, em sua maioria editados a partir de imagens de camêras de segurança ou filmados por aparelhos celulares. Dentre esses conteúdos, um modelo específico chama a atenção: vídeos que exibem pessoas que cometeram algum delito ou insultaram a Polícia, se arrependendo perante as câmeras, muitas vezes explicitamente sob coerção dos policiais. Analisamos o conteúdo e a narratividade audiovisual desse conjunto, assim como suas particularidades midiáticas (HEPP, 2014; HJARVARD, 2012).

A produção e compartilhamento de vídeos de humilhação por parte dos policiais militares e apoiadores parece corroborar mas, também, tensionar o que Michel Foucault escreveu sobre a disciplinarização da sociedade (FOUCAULT, 1970, 1979, 1988, 2000). Por um lado, essa prática parece reforçar o papel disciplinador da PM, exercido através de um intrincado feixe de microrealizações de poder (FOUCAULT, 1979). Por outro lado, a humilhação do cidadão em praça pública (neste caso, na "praça" digital das redes sociais), parece se aproximar de práticas prédisciplinares, os flagelos públicos, operando em lógicas prédisciplinares e antidemocráticas.

Especialmente em um país como Brasil, no qual as forças policiais cometem uma série de violações aos direitos humanos (MESQUITA NETO, 1999), torna-se pertinente a investigação de redes de apoio a condutas repressivas, que respaldam essas ações. Nossa avaliação é que a produção e compartilhamento desses vídeos podem ser vistos como práticas em uma rede de vigilância que não estão amparadas oficialmente pelo aparato estatal legal, tampouco estão ancoradas em coletas ostensivas autorizadas de *b*ig data.* Antes, ultrapassam as instituições, e se dão a partir de um uso pessoal das redes que, compartilhadas e comentadas publicamente, expressam uma complexa imbricação de ações legais e ilegais, individuais e coletivas.

Palavras-chave: Vigilância, Polícia militar, YouTube, Disciplina; Violência policial.

THEREZA NARDELLI*
MAIANA ABI**
BRUNO FONSECA***
JOANA ZILLER****

Pido perdón por la "vacilación": ejercicios autoritarios en videos caseros compartidos en YouTube

Resumen: En este artículo, investigamos el canal brasileño de YouTube "Apoio Policial Oficial" (Apoyo Policial Oficial), que suma 107 mil suscriptores y 44 millones de visualizaciones. En el canal, se transmiten videos amadores, en su gran parte creados desde imágenes de cámaras de seguridad o desde smartphones. Dentre los contenidos presentados, hay un tipo que despierta interés: videos de delincuentes o de personas que ofendieron oficiales de policía arrepintiéndose para la cámara, muchas veces bajo la coacción de la policía.

Nosotros analizamos el contenido y la narración audiovisual del conjunto de videos, así como sus particularidades mediáticas(HEPP, 2014; HJARVARD, 2012). La creación y el compartir de videos de humillación por parte de los oficiales de la Policía Militar y de sus apoyadores parece dar mayor forza - pero también ponerse frente - al argumento de Michel Foucault en orden a la disciplina de la sociedad (FOUCAULT, 1970, 1979, 1988, 2000).

Esa práctica suena una confirmación del rol disciplinar de la policía, hecho a través de un nudoso conjunto de micro realizaciones del poder (FOUCAULT, 1979). Por otro lado, la humillación del ciudadano en plaza pública (en esta situación, la "plaza digital" de las redes sociales), parece comportarse como las prácticas pre disciplinares, los azotes públicos, operando por lógicas antidemocráticas. En particular en la realidad brasileña, en la cual las fuerzas policiales cometen varias violaciones de los Derechos Humanos (MESQUITA NETO, 1999), es pertinente investigar las redes de apoyo a prácticas represivas, que soportan a esas prácticas.

Nuestra evaluación es que la producción y el compartir de eses videos pueden ser entendidos como prácticas de vigilancia que no están apoyadas de modo oficial por el Estado, ni en recolecciones aparentes de Big Data. Antes de todo, exceden a las instituciones y se realizan a partir de la práctica personal en las redes que, compartidas en el público, expresan una compleja red de acciones legales e ilegales, individuales y colectivas.

Palabras clave: Vigilancia, Policía militar, YouTube, Disciplina, Brutalidad policial.

I beg you forgiveness for my fault: exercises of authority in amateur videos shared on YouTube

Abstract: In this paper, we look at the Brazilian YouTube channel "Apoio Policial Oficial" ("Oficial Police Support"), which has more than 107,000 subscribers and over 44 million views. In it, it's aired several amateur videos, mostly edited from images of security cameras or filmed by mobile devices. Among these contents, a specific model is prominently outlined: videos showing people, who have supposedly committed a crime or insulted the police, repenting before the cameras, often explicitly under duress from police. Here, we offer an analysis from the content and audiovisual narrative of this set, as well as their mediatic particularities (HEPP, 2014; HJARVARD, 2012).

The production and sharing of humiliation videos by the Brazilian Military Police and their supporters seem to both relate and put in perspective what Michel Foucault wrote about the disciplinary society (Foucault, 1970, 1979, 1988, 2000). On one hand, this practices seem to reinforce the disciplining role of the military police, exercised through an intricate bundle of power micro-realizations (Foucault, 1979). On the other hand, the humiliation of the citizen at the public square (in this case, the digital "square" of social networks), seems to approach pre-disciplinary practices, the public scourges, operating in a pre-disciplinary and anti-democratic logic.

Especially in a country like Brazil, where the police commits a number of human rights violations (MOSQUE NETO, 1999), it becomes relevant to research the networks of support to repressive conducts, that endorse these actions. Our evaluation is that the production and sharing of these videos can be understood as surveillance practices that are neither officially supported by State's legal apparatus, nor based upon ostensible authorized gathering of big data. Rather, it seems to surpass these institutions, as it takes place from personal usage of social networks which, shared and commented publicly, express a complex intertwining of legal and illegal, individual and collective actions.

Keywords: Surveillance, Military police, YouTube, Discipline, Police violence.

INTRODUÇÃO

Neste artigo, nos voltamos para o canal brasileiro de YouTube "Apoio Policial Oficial", que possui mais de 107[1] mil inscritos e de 44 milhões de visualizações. Nele, são veiculados vídeos amadores, em sua maioria editados a partir de imagens de camêras de segurança ou filmados

por aparelhos celulares. Dentre esses conteúdos, um modelo específico chama a atenção: vídeos que exibem pessoas que cometeram algum delito ou ofenderam a Polícia Militar (PM) de alguma forma se arrependendo perante as câmeras, muitas vezes explicitamente sob coerção dos policiais. Para fins deste artigo, optamos por um recorte de análise que considerou a *playlist*[2] intitulada "Perdão pelo vacilo",[3] por ser uma espécie de coletânea do tipo de vídeo que descrevemos acima.

Analisamos a estrutura narrativa e as especificidades midiáticas (Hepp, 2014; Hjarvard, 2012) dos vídeos dessa playlist, traçando categorias de análise e quantificando a ocorrência dessas categorias no objeto analisado. Também relacionamos os conteúdos da playlist a práticas de vigilância (Bruno, 2013), por exemplo, a partir de vídeos que trazem postagens de pessoas em redes sociais e que são "capturadas" pelos policiais, para em seguida serem apresentadas como os delitos aos quais se deve pedir perdão.

Por fim, refletimos sobre como a midiatização dos pedidos de perdão, em certa medida, distancia-se das práticas de julgamento estabelecidas pelos Estados Modernos, a partir do que Foucault descreveu em relação aos processos disciplinares. Como uma espécie de vestígio de práticas anteriores aos processos disciplinares de condenação, os conteúdos da playlist analisada parecem ser, antes, uma forma de reforço e manutenção das relações de poder das autoridades policiais a partir da midiatização de um arco narrativo da transgressão e do flagelo do transgressor. Entendemos aqui a importância de um olhar sobre a midiatização a partir do que indica Hepp (2014) quanto ao potencial crítico do conceito para analisar as mudanças tanto da mídia e de seus recursos técnicos quanto de hábitos culturais e sociais, avaliando as particularidades dessas imbricações. Acreditamos que tais práticas policiais são reflexo de um contexto social mais amplo no Brasil (Mesquita Neto, 1999), no qual as forças policiais cometem uma série de violações aos direitos humanos, como as levantadas pelo 10º Anuário Brasileiro de Segurança - nove pessoas foram mortas por policiais por dia no Brasil em 2015, número 6,3% maior do que o registrado em 2014.

Pretendemos, portanto, entender melhor, ainda que de forma preliminar, através da análise de seu conteúdo, o que são esses vídeos e o que eles querem dizer, com um olhar interessado em práticas midiáticas contemporâneas e exercícios de poder.

A MIDIATIZAÇÃO DA AÇÃO POLICIAL NOS VÍDEOS DE "PEÇO PERDÃO PELO VACILO"

O canal Apoio Policial Oficial existe na plataforma Youtube desde maio de 2014 e conta com 113.042 inscritos e mais de 47 milhões de visualizações ao todo em seus vídeos.[4] Assim como o Apoio Policial Oficial, existem muitos outros canais que se posicionam como espaços de suporte à atuação da polícia, como Go Tropa, Patrulha Policial, Admiradores Rota Oficial, Força Tática TV, TV Polícia. Na descrição do canal, é ressaltada a intenção de divulgar "a realidade que a mídia omite" (Apoio Policial Oficial, 2016), e os vídeos publicados são em grande parte advindos de câmeras de segurança e gravados com celulares.

A imagem de perfil usada pelo canal é composta pela ilustração em estilo amigável e infantil de um policial homem e uma mulher, com uniformes azuis e em postura de continência. Abaixo dos dois mascotes, lê-se "apoio policial fanpage" ao lado do desenho de algemas. O texto na imagem e a descrição do canal indicam que há uma conexão entre plataformas de mídias digitais, existindo uma página (*fanpage*) no Facebook, onde se desenrolam interações entre os participantes e divulgação dos vídeos postados no canal de YouTube e de outros conteúdos.

O canal Apoio Policial Oficial possui *playlists* , em que são criadas algumas categorias e agrupamento temáticos dentro do universo de vídeos disponibilizados. Uma dessas *playlists* do canal, que coincide com a estrutura de vídeos de retratação já observada circulando pelas redes, é a escolhida para o recorte da análise apresentada nesse artigo. A lista "Perdão pelo vacilo" possui 36 itens e agrupa montagens de vídeos que, em geral, são finalizados com declarações de reconhecimento de erro e pedidos de desculpas direcionados à polícia. Não é possível ver a data de criação da playlist, porém nela estão adicionados vídeos desde março de 2014 e a última atualização foi feita em junho de 2016. A *playlist* aqui analisada é a quarta maior em número de vídeos adicionados, de um total de dez listas. As outras três com maior número de itens são chamadas "Bandidos que se deram mal" (57 vídeos), "Curiosidades do cotidiano policial" (45 vídeos) e "Olho vivo e pé ligeiro" (42 vídeos).[5]

Convém retomar que a playlist "Perdão pelo vacilo" não surge de uma proposta isolada do canal, e se insere no contexto de um meme de internet (Shifman, 2014), identificável também pela expressão "peço perdão pelo vacilo" e que circula por blogs de humor e em outras plataformas digitais (nas quais é possível, por exemplo, localizar postagens marcadas com a hashtag #perdaopelovacilo e variações). Esse meme de internet compreende imagens de pessoas segurando cartazes com pedidos de desculpa direcionados à polícia. Muitas vezes é composto por uma sequência de duas imagens: a primeira mostrando afronta simbólica à polícia (como fotos de pessoas pisando em viaturas policiais ou capturas de telas que mostram postagens desafiadoras ou ofensivas contra policiais em redes sociais) e a segunda imagem apresentada como consequência e punição pela primeira, onde a mesma pessoa aparece retraída e portando cartaz com pedidos de desculpas redigidos. Não é possível precisar quando e onde esse tipo de conteúdo começa a circular e se replicar pelas redes, adquirindo status de meme de internet, mas é possível achar exemplos nesse formato divulgados já no ano de 2008, como na FIG.1 abaixo.

FIGURA 1

Manifestação do meme de internet Peço perdão pelo vacilo, em circulação em blogs de humor. Disponível em:http://tec-life.blogspot.com.br/2008/09/peo-perdo-polcia-civil-pelo-vacilo.html. Consulta em 25 de outubro de 2016.

As manifestações desse meme em formato de vídeo trazem algumas interferências a mais (como letreiros de comentário, música, remix com outros vídeos), mas operam reiterando a proposta das manifestações do meme como imagem estática, onde o interesse e efeito de humor se dão pela humilhação pública e explicitação da força policial subjugando aqueles que a ameaçaram ou desrespeitaram.

NOTAS METODOLÓGICAS

Para a análise, buscamos formar operadores analíticos que possibilitassem visualizar a proposta narrativa dos vídeos, buscando entender a lógica das histórias que são contadas ali, para que pudéssemos mapear características de seu repertório narrativo. Como bem lembra Bruno Leal, ao retomar Paul Ricoeur, Marc Lits, e outros, que

> toda narrativa nasce da realidade social, que lhe fornece o 'substrato' ético-social e histórico, a partir do qual cada história é contada. Ao ser posta em linguagem, ao ser composta, essa história se torna outra coisa, se afasta desse mundo anterior, pois seleciona, ordena e dispõe os elementos dele extraídos em uma configuração nova, única, peculiar. Surge então o mundo do texto (...) (Leal, 2014: 9).

Nesse sentido, tentamos observar elementos tais como temporalidade, espacialidade, personagens e narração, para buscar a narratividade desses vídeos e, através do texto audiovisual que apresentam. Aliada a essa observação, distinguimos alguns marcos de conteúdo que consideramos relevantes para a proposta do artigo, que podem ser melhor visualizados na tabela 1, que contém os critérios de análise sistematizados.

TABELA 1

Categorias de análise e percentuais encontrados. Fonte: elaborada pelos autores.

Categorias de análise	variáveis e resultados
Gerais	
Há "Momento 1" e "Momento 2"	sim (72,2%); não (5,6%); apenas 1 (8,3%); apenas 2 (13,9%)
Narração	1ª pessoa (13,9%); 3ª pessoa (66,7%); não tem (19,4%); NSA (0%)
Há remix com outros vídeos ou músicas?	sim (61,1%); não (38,9%); NSA (0%)
Há a "risada maléfica"?	sim (27,8%); não (72,2%); NSA (0%)
Momento 1	
Formato	câmera de celular (38,9%); câmera de tv (0%); câmera de segurança (2,8%); print de redes sociais (25%); fotografia (5,6%); câmera digital não especificada (8,3%); NSA (19,4%)
Quem filma	policial (2,8%); pessoa comum (5,6%); o próprio sujeito (27,8%); profissionais (0%); incerto (13,9%); NSA (50%)
Local	ambiente fechado não especificado (8,3%); ambiente externo isolado (5,6%); ambiente externo público (22,2%); delegacia (5,6%); viatura (2,8%); casa ou estabelecimento (11,1%); NSA (44,4%)
Mote principal	ameaça de morte direta a policial (8,3%); ameaça de morte indireta (33,3%); ofensa à polícia (33,3%); suposto crime (5,6%); flagra de crime (2,8%); NSA (16,7%)
Momento 2	
Formato	câmera de celular (72,2%); câmera de tv (5,6%); câmera de segurança (0%); print de redes sociais (0%); fotografia (0%); câmera digital não especificada (8,3%); NSA (13,9%)
Quem filma	policial (25%); pessoa comum (2,8%); o próprio sujeito (5,6%); profissionais (5,6%); incerto (47,2%); NSA (13,9%)
Local	ambiente fechado não especificado (44,4%); ambiente externo isolado (11,1%); ambiente externo público (8,3%); delegacia (2,8%); viatura (11,1%); casa ou estabelecimento (8,3%); NSA (13,9%)
Há indícios de coerção?	sim (47,2%); não (30,6%); incerto (8,3%); NSA (13,9%).
Há identificação pessoal de policiais ou da delegacia específica?	sim (19,4%); não (41,7%); NSA (38,9%).
Há pedido de desculpas?	sim (77,1%); não (8,6%); NSA (14,3%).
Se houve detenção, é explicitado o motivo?	sim (16,7%); não (62,1%); NSA (22,2%).

Em um primeiro contato com a playlist, realizamos uma análise livre, de cunho qualitativo. Nessa primeira etapa, buscamos já identificar os principais motivos dos pedidos de desculpas, a história que é contada, alguns elementos formais (como a presença de legendas e remixes) e o formato dos vídeos apresentados nas colagens audiovisuais. Simultaneamente, coletamos falas

que consideramos relevantes, e sistematizamos observações gerais. A partir desta primeira aproximação analítica, elaboramos a Tabela 1 e revimos o material com base em critérios mais sistematizados. As categorias propostas acima foram úteis para dar suporte e ajudar na verificação de percepções antes observadas. Dessa forma, a análise que realizamos aqui é, notavelmente, de cunho qualitativo. A seguir, esperamos esclarecer um pouco mais sobre as categorias propostas a partir da apresentação dos pontos que consideramos mais relevantes para o estudo de caso inaugural desse objeto.

UM ARCO NARRATIVO COM DOIS MOMENTOS

Dentre os principais achados deste estudo, está a identificação de dois elementos narrativos de temporalidade bem demarcada na edição dos vídeos. Percebemos que eles apresentam uma formação que se divide prioritariamente em dois momentos, que denominamos de "Momento 1" e "Momento 2". Apesar de não se apresentarem necessariamente em ordem cronológica linear, essa denominação pretende demarcar duas fases distintas da narrativa que promovem um encadeamento lógico-sequencial dos acontecimentos ali apresentados. É este encadeamento que chamamos de "arco narrativo", pois trata-se de uma sequência que se abre com a apresentação do que o canal entende por delito, e se fecha com a punição e/ou pedido de perdão pelo delito cometido. Esse arco é realizado através de recursos narrativos de edição, como letreiros que explicitam o que ocorreu antes e depois, ou pela própria montagem, que divide o que são esses dois momentos.

O Momento 1 compreende a demonstração de uma ação considerada uma infração legal ou ofensa em relação à polícia, por vezes atreladas a uma manifestação de orgulho com relação à disposição de afrontar a autoridade policial. Essa ação, que define o motivo do pedido de desculpas conseguinte, pode se dar a ver em distintos formatos: em sua maioria, são textos, fotografias, ou vídeos produzidos pelos próprios acusados de transgressão, postadas em redes sociais ou não, aos quais os policiais tiveram acesso. Há ainda vídeos que são produzidos pelos próprios policiais.

Já o Momento 2 se refere à demonstração de arrependimento e pedido de desculpas por parte do sujeito, pela ação apresentada no Momento 1, que pode incluir a exibição de punição (seja em forma de humilhação ou até de constrangimento físico visível) e elogios ao corpo policial. Os vídeos que apresentam ambos os momentos de forma bem demarcada são 72% da nossa amostra (26 em 36 vídeos analisados). Outros 5,6% (2/36) mostram apenas algo mais próximo do Momento 1, ou seja, uma demonstração de um possível ato considerado ofensivo à polícia ou criminoso. É esse o caso do vídeo 26 da playlist no qual é exibido o vídeo de dois jovens ao volante, com uma arma e um cigarro (que o letreiro insinua ser de maconha) nas mãos, no qual não se efetiva um pedido de desculpas, e há um letreiro chamando o espectador para a procura e reconhecimento dos rapazes com a frase: "Compartilhe. Vamos ajudar a localizar esses vagabundos". Podemos perceber que, apesar de não haver um pedido de perdão, existe o desejo explicitado de que eles sejam encontrados para que ele se efetive. Nesse vídeo, particularmente,

é possível entrever uma relação imbricada entre aspectos da vigilância e do flagelo em praça pública: é preciso rastrear esses sujeitos para, então, expor sua miséria em um momento de punição público.

Alguns vídeos (14%, 5 em 36) apresentam apenas o que poderia se caracterizar como Momento 2: o vídeo 2, por exemplo, exibe uma cena, filmada com celular, de um corpo boiando em um rio urbano e, logo em seguida é inserido um outro vídeo no qual um sujeito (que quer-se dar a entender ser o mesmo do momento anterior o que, porém, é possível averiguar) aparentemente hospitalizado e com dor, com um colar cervical, diz que tentou fugir e emite palavras de apoio à polícia.[6]

É importante ressaltar que, em diversos vídeos, o Momento 2 parece ocorrer dentro de uma delegacia policial. Por exemplo, no vídeo 9, no qual o sujeito é filmado contra uma parede com o emblema da Polícia Militar do Alagoas, ou no 27, uma compilação de outros oito vídeos provenientes de emissoras diversas que mostram entrevistas com pessoas detidas, em diversos estados de vulnerabilidade, sendo expostas às câmeras. Há ainda quatro vídeos nos quais o Momento 2 ocorre dentro de viaturas. Esses exemplos ressaltam um caráter de ilegalidade[7] não apenas dos produtores dessas imagens, sejam eles repórteres, policiais ou amadores, como também do próprio canal Apoio Policial como um todo, por exibir conteúdo sem autorização expressa das pessoas retratadas.

Momento 1, o delito

O material midiático apropriado como fonte para a composição do Momento 1 na edição dos vídeos tem origem em dois formatos principais: em torno de 40% (14/36) deles são vídeos filmados com câmeras de celulares e em torno de 25% (10/36) são prints provenientes de redes sociais (notoriamente, do Facebook). Ainda, encontramos fotografias (2/36), câmeras digitais que não conseguimos especificar (3/36) e uma ocorrência de imagens de câmera de segurança (1/26).

Na categoria “mote principal”, buscamos identificar o motivo central para a represália sofrida pelo sujeito em vídeo. Os mais recorrentes foram ameaça de morte indireta (33%) e ofensa direcionada à polícia (33%). No primeiro caso, foram considerados os vídeos em que havia afirmação de que "a polícia", de modo amplo, deveria morrer ou iria sucumbir em confronto. No segundo caso, contabilizaram-se os materiais midiáticos que não mencionavam morte mas traziam xingamentos, gestos considerados ofensivos direcionados a policiais, viaturas ou delegacias, e atos de vandalismo contra propriedade policial. É interessante notar ainda que apenas em 8% dos casos (3 vídeos) o momento 1 é conformado por ameaça objetiva de morte direcionada a policiais individualmente. E em apenas um vídeo há flagrante de infração.

Momento 2, a punição e o arrependimento

Dos 36 vídeos analisados, em 27, o Momento 2 é filmado a partir de celular. Há ainda três vídeos

filmados por câmeras digitais e dois vídeos que trazem trechos de programas de televisão, notadamente, de programas que acompanham a ação policial de emissoras como SBT, Record e Band.

A grande maioria, 27 dos 36 vídeos, traz um pedido de desculpas explícito no Momento 2. Há também um vídeo no qual não há pedido, mas os sujeitos aparecem em situação de humilhação. Além disso, em 16 vídeos o Momento 2 ocorre em um ambiente fechado, que pode ser uma delegacia policial, como no vídeo 9, já mencionado. Há ainda quatro vídeos nos quais o Momento 2 ocorre dentro de viaturas. Em 17 vídeos, o acusado da transgressão é explicitamente coagido a pedir perdão no Momento 2. No vídeo 6, por exemplo, um jovem é obrigado a ler um rap escrito em uma folha de papel, pelos policiais, no qual pede perdão pelos seus atos - o ato que havia levado à ação policial foi justamente um vídeo do jovem cantando um rap crítico à polícia, com ameaças que matariam policiais caso entrassem na favela. É curioso como, contraditoriamente, esse tipo de situação exibe um arrependimento que ocorre mediante a coerção policial, o que poderia inclusive relativizar a veracidade desses depoimentos.

Em quase metade dos vídeos do Momento 2 não é possível afirmar quem filma (17 dos 36). Há nove vídeos explicitamente filmados por policiais e dois nos quais são os próprios sujeitos acusados da transgressão que filmam. Há sete vídeos nos quais o policial que participa do Momento 2 ou a delegacia no qual o vídeo é gravado são identificados explicitamente. Não é possível afirmar se isso ocorre por desinteresse dos policiais em aparecerem, por uma questão de segurança pessoal ou mesmo para evitarem serem acusados de abuso policial.

Narração

Buscamos estudar, com essa categoria, como se dá a voz narrativa nesse vídeo. Para tal, utilizamos a noção oferecida por Uri Margolin, segundo a qual "um narrador é uma função, lugar ou categoria linguisticamente indicada, textualmente projetada e construída pelo leitor, na qual o ocupante não precisa ser pensado em termos além do papel comunicativo"[8] (Margolin, 2009: 351). Observamos que a função do narrador está principalmente associada aos letreiros, com a adição de textos escritos sobre o conteúdo audiovisual apresentado,[9] que se encarregam de definir direcionamentos factuais ou de falar ao espectador.

Encontramos que dois terços (24/36) dos vídeos apresentam narração na 3ª pessoa do discurso que, em português, designa o narrador impessoal, observador. Outros 5 vídeos o posicionam 1ª pessoa, o “eu” narrador. A narração está presente em torno de 80% dos vídeos. Essa maioria representa, ao nosso ver, uma forte interferência de função interpretativa das imagens que são mostradas, na sequência em que são mostradas, de tom assertivo e com o uso informal da linguagem.[10] Além disso, acreditamos que o uso da terceira pessoa, que se mostra onisciente nos vídeos (demonstra conhecimento dos desfechos e repercussões dos fatos narrados) é um recurso linguístico que reforça o papel de autoridade em relação aos registros editados. Essa autoridade, por sua vez, apoia e valida a ação policial a partir de trechos como “Respeite a dor alheia. Respeite os policiais. E saiba que policiais tbm tem amigos”,[11] e “Depois que morre uma praga

dessa, aparece um monte de 'defensores', viram trabalhadores e pai de família".[12] Há ainda exceções nas quais a terceira pessoa cede espaço para um narrador em primeira pessoa que se apresenta como parte da Polícia, como nos vídeos 23 e 28 nos quais podemos ver as frases "Não me pergunte se sou capaz, apenas me dê a missão"[13] e "Beleza. Já que ele é o terror, vamos trocar uma ideia 'bigode a bigode'",[14] respectivamente.

Edição: práticas de remix

A maior parte dos vídeos da playlist é composta pela montagem e justaposição de materiais midiáticos diversos. A estrutura mais recorrente na playlist – que apresenta a vinheta de abertura do canal Apoio Policial Oficial, o momento 1 e o momento 2 – já é por si só uma colagem, e o sentido é dado pela concatenação desses recortes midiáticos em sucessão narrativa. Ressaltamos a particularidade de produção ligada à circulação digital como aspecto fundante da playlist "Perdão pelo vacilo" - caracterizando todo seu conteúdo, invariavelmente, como original e ressaltando o caráter narrativo de suas produções.

Na categoria específica de observação de remix, registramos se havia mais elementos inseridos na estrutura, a dizer, vídeos, imagens, músicas e efeitos sonoros (externos aos enquadrados em Momentos 1 ou 2), tendo em vista o entendimento de remixes como operações de montagem, cópia, recorte e colagem viabilizadas pelas tecnologias digitais (Lemos, 2004; Navas, 2010). Dos 36 vídeos da playlist, 14 (39%) se enquadraram nessa categoria.

Punição e divertimento

Um elemento de remix, particularmente, nos chamou atenção. A categoria relativa à presença do que chamamos de "risada maléfica" surge da observação da repetição desse elemento adicionado na edição. Trata-se do som de uma risada masculina em tom bastante grave, lenta e caricata – típica de personagens ficcionais associados com o mal, como vilões e monstros – que é adicionado em 28% dos vídeos. A observação desse recurso se mostrou interessante pois, juntamente com outros elementos de edição (como remix com vídeos, sons de choro infantil, músicas e letreiros com termos jocosos), parece apontar para uma dimensão humorística que perpassa o conjunto dos vídeos de "perdão pelo vacilo". O som da risada é adicionado normalmente ao final dos vídeos, compondo uma espécie de conclusão que demonstra divertimento com a subjugação praticada pelo poder policial.

Um exemplo que demarca bem o uso do som de risada pode ser visto no vídeo 16, "Um recado para os 'parças'". Neste vídeo, são apresentados maços de dinheiro e armas em uma mesa, enquanto uma voz masculina, com sotaques e gírias comumente associados à periferia da cidade de São Paulo, enaltece as posses ali apresentadas e diz que indicará a receita para chegar ao sucesso. Nesse momento, a câmera passa por algemas que não tinham sido mostradas antes, a voz muda de sotaque, assumindo um tom padrão, e diz que a receita é trabalhar o mês inteiro para

ter seu próprio dinheiro. Assim, o vídeo se revela como uma "brincadeira", indo da simulação de ostentação do crime à cena de uma apreensão policial. No momento em que essa transição acontece, é inserida na edição do vídeo o som de risada maligna. Apesar deste ser um vídeo anômalo na lista, por não mostrar tão marcadamente os momentos 1 e 2, o som da risada é conjugado ao momento em que a mensagem é de derrota do crime, reiterando que há apreciação pela mudança de discurso e indicando a dimensão humorística da peça audiovisual.

Além do vínculo da playlist com o meme de internet "peço perdão pelo vacilo", conforme indicado anteriormente, há outros recursos utilizados que reforçam o possível entendimento de humor nos vídeos. No vídeo "Zuou no banco da frente e parou no corró na parte de trás", por exemplo, a transição entre o momento 1 e o momento 2 é feita com a inserção de uma cena do clássico seriado de comédia Chaves, em que o personagem recita uma fala sobre arrependimento.

Outro exemplo pode ser visto no vídeo 32, "Plantou ameaça contra a PM e colheu coisa pior",[15] onde um jovem é filmado pintando uma parede por cima de uma pixação que incita a morte de policiais. Como é possível ver na FIG. 2, o vídeo é editado com a inserção de um emoji e letreiro, ambos de cunho descontraído e contrastantes com a ocasião de punição, explicitando que a piada é justamente a exibição da redenção coagida do jovem que presumidamente ameaçou a polícia. Vale notar que a inserção do emoji cobrindo o rosto da pessoa na imagem não cumpre função de anonimização do indivíduo, uma vez que suas feições são mostradas abertamente em momento anterior no vídeo: trata-se mesmo de recurso gráfico para produção de humor.

FIGURA 2

Captura de tela mostrando a edição feita no vídeo 32, com adição de letreiro e*emoji.* Fonte: Disponível em: `https://www.youtube.com/user/ApoioPolicialOficial`. Consulta em 25 de outubro de 2016.

VIGILÂNCIAS E PRAÇAS PÚBLICAS DIGITAIS

Em primeiro lugar, percebemos que parte dos vídeos produzidos - os que potencialmente são realizados a partir das autoridades policiais "capturando" conteúdos expostos nas redes para a consequente gravação do momento de humilhação - são possíveis graças a um ambiente de vigilância distribuída no ambiente digital. Explicamos: para Fernanda Bruno, ao utilizarmos redes sociais, produzimos rastros digitais, "pegadas que deixamos nas redes de comunicação distribuída, especialmente na internet, onde toda ação deixa um rastro potencialmente recuperável, constituindo um vasto, dinâmico e polifônico arquivo de nossas ações, escolhas, interesses, hábitos, opiniões, etc. (Bruno, 2013: 684). A vigilância distribuída, segundo Bruno, é o "monitoramento de ações e comunicações no ciberespaço", que é convertido em "informações que irão compor bancos de dados e perfis computacionais que buscam antecipar preferências, tendências, escolhas, traços psíquicos ou comportamentais de indivíduos ou grupos." (Bruno, 2006: 153).

É importante ressaltar que, embora se trate de práticas que são realizadas em um ambiente de *big data* , a vigilância realizada nos vídeos de "Peço perdão pelo vacilo" não são apresentadas como fruto de análises de grandes bancos de dados ou resultados de perfis computacionalmente traçados. Antes, o contrário: a ação parece ser bastante manual, pessoal e localizada, com as autoridades policiais ou apoiadores "capturando" conteúdos expostos nas redes. Aparentemente, o que é realizado na playlist se aproxima de uma "versão rudimentar" do que formulou Fernanda Bruno sobre a vigilância distribuída no ambiente digital, mas que só é possível graças à rastreabilidade que esse ambiente propicia.

Em segundo lugar, acreditamos que a midiatização do perdão a partir de uma coerção explícita da ação policial (ou de apoiadores dessa ação) que constatamos na playlist "Perdão pelo vacilo", em certa medida, distancia-se das práticas de julgamento estabelecidas pelos Estados Modernos. Em outras palavras, quando policiais - ou apoiadores da polícia - atuam à revelia das atribuições da corporação, inclusive de forma ilegal, e se dedicam a filmar e dar publicidade a um arrependimento que foge ao processo de condenação (nem ao menos é peça formal para o inquérito), eles se distanciam dos métodos burocratizados pelos quais o Estado Moderno estabeleceu seus processos de penalização: a detenção, o inquérito, a acusação, o julgamento, a condenação e a prisão. O arrependimento dos que "pedem perdão pelo vacilo" não é um julgamento efetivo perante a legislação, mas um julgamento perante a opinião pública, mais especificamente, de uma "praça pública digital", dos usuários de redes sociais que acessem e compartilhem esses conteúdos.

Nesse sentido, percebemos que esse flagelo midiatizado do "peço perdão pelo vacilo" se aproxima, ainda que com ressalvas, das práticas que Foucault descreve no período anterior aos Estados Modernos, isto é, da aplicação de penas em praça pública com o objetivo de comover a sociedade e, a partir dessa comoção, reforçar relações de poder do Estado perante a ordem pública. Não por acaso, selecionamos o trecho de Vigiar e Punir (1999) no qual Damiens, francês

condenado à morte em 1757, precisa pedir perdão pelo crime ainda que sua sentença já esteja dada - o esquartejamento. Aos confessores, presentes durante todo o ritual de execução, Damiens pede "Perdão, meu Deus! Perdão, Senhor" (Foucault, 1999: 3).

É importante ressaltar que, obviamente, não estamos afirmando que a "peço perdão pelo vacilo" é equivalente às brutais penas anteriores ao estabelecimento do Estado Moderno. Até o ponto que os vídeos podem comprovar, apesar de alguns indícios, não há agressão física explícita aos transgressores que são representados na playlist, o que é regra nas condenações em praças públicas medievais. Além disso, há um elemento metafísico no pedido de perdão medieval que não percebemos nos vídeos de humilhação policial atuais, que é a súplica não apenas aos executores, mas também a Deus, ou em última instância, à possibilidade de expiação no inferno.

Contudo, em ambas as situações, há uma necessidade de publicização do perdão, ainda que isso não tenha impacto algum na condenação do transgressor. Em ambas as praças públicas, na medieval e na digital, existe um esforço de que o pedido de arrependimento do fora-da-lei se torne público, e alcance e comova uma audiência que vai além dos executores da pena: é preciso que a sociedade veja que o criminoso se arrepende de seus atos e que reforce a autoridade de quem o condena, que ele sirva de exemplo. E mais, em ambas as situações, as "autoridades" cuidam para que o arco narrativo se encerre com o transgressor subjugado, desprovido de poder, preferencialmente imobilizado.

Essas práticas parecem não se encaixar no que Foucault descreve como o processo disciplinar dos Estados Modernos, que são marcados pela transformação da pena em "um setor autônomo, em que um mecanismo administrativo desonera a justiça", mecanismo esse exercido por "um exército inteiro de técnicos" que "substitui o carrasco, anatomista imediato do sofrimento" (Fouccault, 1999: 15-16). Os vídeos de "peço perdão pelo vacilo" são antes o contrário: não são técnicos, mas pessoais, por vezes sarcásticos; não possuem um mecanismo administrativo que desonera a justiça, antes o contrário, pouco contribuem com os inquéritos ou a execução das penas judiciais, mas servem a outros propósitos; e, talvez o mais relevante: todo o produto é uma autonomia imediata do sofrimento.

Dessa forma, propomos a reflexão que os vídeos "peço perdão pelo vacilo" tensionam o que Foucault descreveu em relação aos processos disciplinares. O que a polícia (ou seus apoiadores) fazem é um processo de coerção distinto, que se aproveita das possibilidades de uma sociedade midiatizada para empregar ações personalistas de vigilância em rede e que culminam em um flagelo público, no mínimo, distinto do que é previsto para a corporação. Como uma espécie de vestígio de práticas anteriores aos processos disciplinares de condenação, os conteúdos de "peço perdão pelo vacilo" parecem ser uma forma de reforço e manutenção das relações de poder das autoridades policiais a partir da publicização do arco narrativo da transgressão e do flagelo.

NOTAS

* Programa de Pós-Graduação em Comunicação Social da Universidade Federal de Minas Gerais, mestranda, therezanardelli@gmail.com

** Programa de Pós-Graduação em Comunicação Social da Universidade Federal de Minas Gerais, mestranda, maiana.assc@gmail.com

*** Programa de Pós-Graduação em Comunicação Social da Universidade Federal de Minas Gerais, mestrando, obruno10@gmail.com

**** Programa de Pós-Graduação em Comunicação Social da Universidade Federal de Minas Gerais, Professora Doutora, joana.ziller@gmail.com

1. Até a data da publicação deste artigo, o canal já contava com mais de 113 mil inscritos.

2. Uma playlist é uma série de vídeos ordenados que se reproduzem sucessiva e automaticamente para o usuário do YouTube. No caso da playlist selecionada, ela foi criada pelos administradores do perfil "Apoio Policial Oficial". Há playlists que são geradas automaticamente pelo YouTube.

3. A playlist se encontra disponível através do link https://www.youtube.com/playlist ?list=PLSgOG2170fo1b2mAPN0Fj7nuPtaVqAR8B. Consultado em 4 de novembro de 2016.

4. Disponível em: https://www.youtube.com/user/ApoioPolicialOficial/about. Consulta em 25 de outubro de 2016.

5. Disponível em: https://www.youtube.com/user/ApoioPolicialOficial/playlists. Consulta em 25 de outubro de 2016.

6. Mais especificamente à ROCAM (Ronda Ostensiva com Apoio de Motocicletas), subdivisão da Polícia Militar. O jovem diz: "tentei dar o pinote na ROCAM, parece que não, mas a ROCAM é foda". Disponível em: https://www.youtube.com/watch?v=o9dl-TEHjnQ&index=2& list=PLSgOG2170fo1b2mAP-N0Fj7nuPtaVqAR8B. Consulta em 04/10/2016.

7. Segundo o Artigo 20, Capítulo 2 do Código Civil Brasileiro, garante o direito de imagem. (Código Civil Brasileiro, 2008).

8. Tradução livre para: "A narrator is a linguistically indicated, textually projected and readerly constructed function, slot or category whose occupant need not be thought of in any terms but those of a communicative role"

9. Aqui, analisamos apenas os textos inseridos no qual localizamos uma função narrativa, e ignoramos um texto frequente que é o de "Visite nossa Página no Facebook FANPAGE APOIO POLICIAL" (*sic*), por não o considerarmos relevante nesse sentido.

10. Exemplo em terceira pessoa: "No *face* todo mundo é valente" (grifo nosso). Vídeo 29, disponível em: https://www.youtube.com/watch?v=Y-cFCW-KR8k&list=PLSgOG2170fo1b2mAPN0Fj7nuP-taVqAR8B&index=29. Consulta em 04 nov. 2016. Exemplo em terceira pessoa: "Missão cumprida? *Opa!!!* Não...*Espera um pouquinho* ...Não me pergunte se sou capaz, apenas me dê a missão (*sic*; grifo no-

sso). Vídeo 23, disponível em: https://www.youtube.com/watch?v=i808Zns3fEo&index=23&list=PLSg0G2170fo162mAPN0Fj7nuPtaVqAR8B. Consulta em 04 nov. 2016.

11. Vídeo 35 da playlist: "Zombou a morte do PM e a casa caiu - Apoio Policial". Disponível em: https://www.youtube.com/watch?v=ZS0gd73IQGs&list=PLSg0G2170fo162mAPN0Fj7nuPtaVqAR8B&index=35. Consulta em: 04 nov. 2016.

12. Vídeo 21 da playlist: "Meliantes armados fazem ameaças". Disponível em: https://www.youtube.com/watch?v=JXsbJP7VaFM&list=PLSg0G2170fo162mAPN0Fj7nuPtaVqAR8B&index=21. Consulta em: 04 nov. 2016.

13. Vídeo 23 da playlist: "Jogaram bomba na base da PM e... ". Disponível em: https://www.youtube.com/watch?v=i808Zns3fEo&index=23&list=PLSg0G2170fo162mAPN0Fj7nuPtaVqAR8B. Consulta em: 04 nov. 2016.

14. Vídeo 28 da playlist: "Quando o crime vira o creme". Disponível em: https://www.youtube.com/watch?v=GbutY9cz7z4&list=PLSg0G2170fo162mAPN0Fj7nuPtaVqAR8B&index=28. Consulta em: 04 nov. 2016.

15. Vídeo disponível em: https://www.youtube.com/watch?v=172geTRTmyU&index=32&list=PLSg0G2170fo162mAPN0Fj7nuPtaVqAR8B. Consulta em 04 nov. 2016.

REFERÊNCIAS

Brasil. Código Civil (2008). *Código civil brasileiro e legislação correlata*. – 2. ed. – Brasília: Senado Federal, Subsecretaria de Edições Técnicas.

Bruno, F. (2006). Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. *Fronteiras -estudos midiáticos*, *8* (2), 152-159.

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina.

Foucault, M. (1996). *Ordem do discurso (A)* (Vol. 1). Edições Loyola.

Foucault, M. (1988). *História da sexualidade I: a vontade de saber*; tradução de Maria Thereza da Costa Albuquerque e JA Guilhon Albuquerque. Rio de Janeiro: Edições Graal.

Foucault, M. (1979). *Microfísica do poder*; organização e tradução de Roberto Machado. Rio de Janeiro: Edições Graal, 4.

Foucault, M. (2000). *Vigiar e Punir: nascimento da prisão*; tradução de Raquel Ramalhete. 22º ed. Petrópolis: Ed. *Vozes*.

Hepp, A. (2014). As configurações comunicativas de mundos midiatizados: pesquisa da midiatização na era da "mediação de tudo". *MATRIZes*, *8* (1), 45-64.

Margolin, U. (2009). Narrator. In Hühn, Peter et al.(eds.): Handbook of narratology. Berlin, New York: Walter de Gruyter

Neto, P. M. (1999). Violência policial no Brasil: abordagens teóricas e práticas de controle. In Carvalho, J. M. et.

al. *Cidadania, justiça e violência.* Rio de Janeiro: Fundação Getulio Vargas, 129-148.

Leal, B. S. (2014). Quando uma notícia é parte da história: as mídias informativas e a identidade narrativa. *Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação*, 17(3).

Lemos, A. (2004). *Cibercultura: Tecnologia e Vida Social na Cultura Contemporânea*. Porto Alegre: Sulina.

Navas, E. (2010). Regressive and reflexive mashups in sampling culture. In Sonvilla-Weiss, S. *Mashup cultures*. New York: Springer.

Shifman, L. (2014). *Memes in digital culture*. Mit Press

O DISCURSO DE SEGURANÇA E A PRIVACIDADE NO MARCO CIVIL DA INTERNET

Resumo: A discussão sobre segurança, no âmbito do combate aos cibercrimes, foi um dos pontos de conflito ao longo da elaboração do Marco Civil da Internet. A proposta deste artigo foi desenvolver uma análise das notas da Câmara dos Deputados brasileira a fim de entender como se travaram os embates no âmbito da segurança, do cibercrime e da vigilância. Com o intuito de se preservar a garantia pela guarda de dados de conexão e aplicação no projeto de lei, deputados da frente parlamentar contra crimes cibernéticos fizeram forte apelo pelo estabelecimento de um prazo de 12 meses para guarda de registros de conexão e aplicação, favorecendo o trabalho de investigação criminal. No entanto, a guarda de dados por um longo tempo era vista como uma ameaça à privacidade. Neste trabalho, será possível refletir sobre os embates e enfrentamentos em torno do discurso de segurança, pensando nos impactos que ele oferece à privacidade dos usuários da Internet.

Palavras-chave: Privacidade, Vigilância, Internet, Segurança.

El discurso de la seguridad y la privacidad en el Marco Civil da Internet

Resumen: La discusión sur la seguridad en la lucha contra el delito cibernético fue uno de los puntos de conflicto en relación a la elaboración del Marco Civil de Internet en Brasil. El propósito del trabajo es la análisis de las notas del Congreso Nacional con la finalidad de comprender cómo los conflictos ocurren en el campo de la seguridad, de la delincuencia informática y la vigilancia. Con el fin de preservar la garantía de mantener los datos de conexión y aplicación en el proyecto de ley, los diputados de la Frente Parlamentario contra el delito cibernético hicieron fuerte presión para el establecimiento de un período de 12 meses para asegurar la guarda de los registros de conexión y de aplicación, favoreciendo los procedimientos de investigación criminal. Sin embargo, la guardia de datos durante mucho tiempo fuera vista como una amenaza a la privacidad. En este trabajo reflexionamos respecto de los conflictos y enfrentamientos en todo el discurso de la seguridad, pensando en el impacto que la cuestión ofrece a la privacidad de los usuarios de Internet.

Palabras clave: Privacidad, Vigilancia, Internet, Seguridad.

The security speech and privacy on the Marco Civil da Internet

Abstract: The discussion of security in context of the fight against cybercrime was one of the points of conflict over the drafting of the Marco Civil da Internet on Brazil. The purpose of this paper is develop an analysis of the Chamber of Brazilian Deputies' notes in order to understand how conflicts were waged in the field of security, cybercrime and surveillance. In order to preserve the guarantee of keeping connection data and application in the bill, members of parliamentary group against cybercrime made strong appeal to establish a period of 12 months to guard connection and application records, favoring criminal investigations by police. However, the data guard for a long time was seen as a threat to privacy. In this work, we reflect on the conflicts and confrontations around the security discourse, thinking of the impact that it offers to the privacy of internet users.

Keywords: Privacy, Surveillance, Internet, Security.

PAULO EDUARDO ASSIS MAIA
MARTA DE ARAÚJO PINHEIRO
GUSTAVO FERNANDES PARAVIZO MIRA

Um dos grandes pontos de conflito que se estabeleceu durante a tramitação do Marco Civil da Internet, lei brasileira que estabelece diretrizes para o uso e a operacionalização da rede, se refere à questão da segurança. O embate entre forças policiais, representadas por órgãos de segurança pública como a Polícia Federal e a associação dos peritos e forças políticas, como os deputados, o Governo e os movimentos sociais, se consolidou na Câmara dos Deputados quando a matéria foi apreciada pelos parlamentares, alguns deles reforçando a caracterização de usuários da rede como suspeitos, e defendendo a criação de ferramentas de punição.

A princípio, o texto do projeto de lei determinava aos provedores de conexão (teles, operadoras e empresas que comercializam o acesso à internet) a guarda de registros de acesso e facultava aos provedores de aplicação (Google, Facebook, navegadores, desenvolvedores de aplicativos) este armazenamento. O ponto gerou divergências entre os atores em questão, uma vez que a preocupação pela guarda de dados por empresas como o Facebook, Google, Microsoft poderia se configurar, na visão de alguns, a violação da privacidade. No entanto, deputados que representavam órgãos policiais, bem como entidades representativas desse segmento, defendiam a obrigatoriedade de guarda de logs por um período pré-estabelecido, de maneira a contribuir com o exercício da investigação de cibercrimes ou mesmo a chegar até hackers que tivessem colocado em xeque a própria segurança de autoridades, violando suas privacidades.

Este artigo propõe uma análise das disputas que se estabeleceram no âmbito da discussão sobre a guarda de dados, enfocando a preocupação com a segurança e os confrontos gerados por posicionamentos divergentes entre órgãos policiais e movimentos sociais. Para isso, buscou-se pensar nas seguintes questões: de que forma o discurso que classifica o usuário da rede como um suspeito se estabeleceu no processo de elaboração do Marco Civil e como as soluções de combate ao cibercrime implicam em um prejuízo à privacidade dos usuários, a partir de um modelo de vigilância que passa a ser institucionalizada? Inicialmente, será feita uma contextualização do caso, apresentando os principais atores em debate. Em um segundo momento, uma revisão teórica sobre a vigilância na sociedade de controle, os efeitos do monitoramento dos indivíduos pelo Estado e a questão da segurança a partir do risco. Na terceira parte deste artigo, serão apresentados os conflitos ocorridos no debate sobre o Marco Civil.

A pesquisa desenvolvida levou em conta um escopo de 89 discursos registrados pelo Departamento de Taquigrafia e Revisão da Câmara dos Deputados ao longo das sessões de discussão do Marco Civil da Internet, enfocando a questão privacidade como um dos tópicos da elaboração do texto. As falas foram proferidas por 27 oradores, sendo eles deputados, representantes de entidades de classe, acadêmicos, lideranças de movimentos sociais e membros do Governo federal. Tendo em vista o grande embate gerado em relação à obrigatoriedade da guarda de dados por provedores de aplicação, inicialmente sendo facultativa, observa-se que 63% dos oradores abordaram o tema da guarda de dados em uma de suas falas, seja empunhando-o como uma bandeira a ser defendida na discussão do Marco Civil, cuja preocupação com a segurança se sobressaía, seja simplesmente a título de menção como tópico importante que o projeto abrangia. Os posicionamentos mais incisivos, considerando o termo, vieram da frente parlamentar contra

crimes cibernéticos, que se predispôs a defender um período maior para a guarda de registros tanto para provedores de conexão quanto para provedores de aplicação.

GARANTIA DA AÇÃO POLICIAL E O COMBATE À PEDOFILIA E À PORNOGRAFIA

Atuando de forma incisiva nas discussões do projeto, a frente parlamentar era composta por alguns deputados como Fernando Francischini (SDD) e Sandro Alex (PPS), os quais defendiam que o prazo para a guarda de dados dos usuários por provedores de aplicação fosse aumentado, a fim de garantir a ação policial. Esse processo passou a ser visto por movimentos sociais e acadêmicos como uma institucionalização da vigilância, sendo duramente criticado. A argumentação dos parlamentares insistiu muito no combate a pedofilia e a pornografia na internet. Tal posicionamento não está restrito ao quadro nacional, pois, segundo Jacob Appelbaum (apud Assange, 2012), os órgãos de inteligência, em geral, elaboram um discurso com os "Quatro Cavaleiros do Infoapocalipse: pornografia infantil, terrorismo, lavagem de dinheiro e a guerra contra certas drogas", a fim de convencer às pessoas sobre a necessidade de se empregar medidas restritivas na Internet.

Na tentativa de emplacar a obrigatoriedade da guarda desses dados, esses deputados e representantes de entidades ligadas à investigação diziam que o projeto poderia tornar o país um paraíso para pedófilos e para a pornografia infantil, uma vez que, por preocupação com os custos de provedores, as investigações ficariam mais difíceis. Eles também questionavam o prazo estabelecido, tendo em vista que muitas vítimas tomam conhecimento do ilícito somente tempos depois de que ele tenha sido praticado, sendo 12 meses já insuficientes para a ação policial. O discurso usado pelos parlamentares remete à iniciativa tradicional de atrelar aguarda de informações como forma de garantir a segurança, assemelhando-se ao discurso sustentado por órgãos de inteligência estatal como a própria NSA, nos Estados Unidos, ou o Serpro, no Brasil, que avaliavam serem essas medidas necessárias para sustentar medidas de segurança, tornando-se uma justificativa aceitável para que a população consinta com a guarda de suas informações pessoais.

Outro ponto importante da discussão sobre a guarda de dados, segundo Silveira (2014), é que, ao buscarem facilitar o seu trabalho, policiais batalharam pela obrigatoriedade da guarda de registros de conexão de todas as pessoas, inocentes ou suspeitas, uma vez que a maioria das pessoas não usa IPs fixos. O autor lembra que neste embate político travado pela guarda de dados, o resultado foi positivo, mas as forças vigilantistas conseguiram aprovar alguns pontos "extremamente nefastos ao espírito original da lei" (Silveira, 2014). Com o prazo de seis meses para que os provedores de aplicação fizessem a guarda dos dados, estabelecidos no artigo 15, tal ponto é considerado uma violação à privacidade, por expandir o armazenamento de nossas informações. A abordagem se dá principalmente pelos termos técnicos empregados na lei, que classificam as aplicações de internet como "conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet". Assim, qualquer empresa de conteúdo, como

Facebook, Twitter e Google, poderá armazenar esses dados para processá-los, analisá-los, agrupá-los com a finalidade de entender o comportamento de seus usuários (Silveira, 2014).

Promovendo um discurso que estimula uma adesão envolta pelo temor da insegurança e do medo, como será demonstrado abaixo, as forças policiais inseriram na lei um dispositivo que permitirá que as informações de usuários estejam vulneráveis ao acesso dos governos e das grandes corporações, reforçando aspectos de controle.

VIGILÂNCIA E A SOCIEDADE DE CONTROLE

O monitoramento de informações em bancos de dados está atrelado à compreensão sobre a nossa sociedade atual que, para muitos analistas e teóricos, se caracteriza como a "sociedade de controle". As denúncias de Edward Snowden, em 2013, trazem à tona uma discussão sobre a forma pela qual a vigilância se estabelece nas interações entre os indivíduos. Quando se propõe a analisar a vigilância no cenário posterior a estas revelações, Lyon (2015) entende que essa não pode ser definida apenas como uma sistemática atenção de rotina às informações pessoais para uma finalidade definida. Segundo ele, a intenção prática da vigilância pode ser tanto proteção, inteligência, cuidado, segurança, direito de posse, gerenciamento ou influência individual ou grupal. O autor analisa a prática de monitoramento exercida pelo Estado, que existe há muito tempo, ressaltando o Big Brother, de George Orwell, para descrever a compreensão sobre o tema durante o século XX. No entanto, observa que, com os atentados ao World Trade Center, em 11 de setembro de 2001, houve uma intensificação da cultura da vigilância com o aumento da coleta de informações pessoais. Tal ação era justificada por um discurso que reforçava a segurança contra ataques terroristas, já que esses poderiam se utilizar de ferramentas tecnológicas.

Com as revelações de Snowden, aumenta o monitoramento estatal de informações pessoais contida nos posts no Facebook, feeds do Twitter, *cloudservices* como o Google Docs, além de dados de GPS instalados em smartphones. Esses dispositivos digitais se transformaram em "sensores em nossos bolsos, que nos rastreiam a qualquer lugar que formos" (Lyon, 2015). Dessa forma, participamos "como nunca" da cultura da vigilância.

A identificação de endereços de IP, identidade de contato, a localização de chamadas ou mensagens e a duração do contato são chamados de "metadados". Segundo Lyon, talvez essa tenha sido a palavra mais recorrente durante o caso Snowden. Quando se trata dos tipos de atividades da NSA, trata-se de monitoramento de conteúdo de telefonemas e mensagens de texto, bem como o armazenamento em grande escala e análise dos metadados, os quais tiveram sua importância minimizada pelo governo norte-americano posteriormente.

O aspecto crucial dessa realidade é o leque de alvos desse sistema de monitoramento por ele alcançado, entre eles, jornalistas, ativistas e ambientalistas. O primeiro objetivo explícito são terroristas, no entanto, é cada vez mais claro aos pesquisadores do tema que ativistas ou pessoas que discordem da política governamental são também alvos potenciais.

De forma não menos importante, a atividade de monitoramento de redes sociais também propicia a criação do "estado de vigilância", em que indivíduos são monitorados de maneira frequente, e aparatos de vigilância são cada vez mais vultosos, tanto para sustentar este modelo de controle quanto para prover o armazenamento de dados (Lyon, 2014: 6).

A análise da vigilância contemporânea é compreendida por Bruno (2003) para além dos modelos historicamente conhecidos, pensando em processos que estão distribuídos entre múltiplos agentes, técnicas, funções, propósitos, etc. A pesquisadora afirma que a vigilância comporta três circuitos capazes de gerar uma significação subjetiva e plural, reunindo aspectos de segurança, cuidado, temor, suspeição, prazer, entretenimento, entre outros. São eles: os circuitos de segurança e controle; os circuitos de visibilidade midiática; os circuitos de eficácia informacional, que dão um caráter multifacetado à vigilância, com registros de legitimação superpostos (Bruno, 2003: 21).

Trata-se do dispositivo de vigilância distribuída, vigente na contemporaneidade, que abrange jogos de poder e formações específicas de saber que vêm se constituindo a partir do monitoramento de dados pessoais, principalmente no ciberespaço. Essa ação se difere, em parte, da vigilância no âmbito da modernidade, centrada especificamente na ação disciplinar dos indivíduos monitorados. Num passado recente, as práticas de vigilância envolviam grupo específicos, enquanto no mundo contemporâneo se torna uma vigilância para todos.

A SEGURANÇA E O RISCO

Ao se pensar a questão da segurança, entende-se que os aspectos de temor e risco emergem como um forte argumento a fim de estimular a aceitação de mecanismos de vigilância. É necessário pensar, portanto, como a gestão do risco se torna um instrumento defendido para combater, principalmente, os ataques terroristas, abrindo brechas para o monitoramento de indivíduos. Bennet e outros autores (2014) abordam a perspectiva dos riscos analisando a expansão da vigilância no Canadá e seus resultados com base na gestão de risco e de segurança. A preocupação com a segurança se expande para além da questão dos atentados de 11 de setembro e do discurso antiterrorismo, sendo identificadas antes desses acontecimentos. Tal discussão aborda uma vigilância nova e mais intensa, a qual cria riscos para a privacidade, a justiça e a liberdade. Ela surge a partir dos anos 1980 com a gestão de riscos, a qual está relacionada com previsões sobre o comportamento humano.

Com o aumento desta vigilância gerada por uma fome de dados para cálculos de riscos, há um enfraquecimento das normas de privacidade, uma vez que, em muitos casos, não se pede permissão antes de se coletar informações pessoais sobre usuários da internet, por exemplo. Um segundo ponto se refere à vigilância usada para monitorar pessoas uma vez que os riscos sejam identificados, garantindo que estas pessoas não se comportem de uma maneira arriscada, além de gerir as consequências quando cometem algum ato.

De modo irônico, o grande foco na segurança pode gerar ainda mais insegurança, uma vez que

a própria discussão do tema e os esforços para controlar os riscos levam a sociedade a um clima de dúvida e medo. Cria-se um ciclo vicioso que passa a reforçar a justificativa da vigilância como necessária para a busca da segurança. A maior consciência sobre o risco, embora estejamos mais seguros do que antes, tende a gerar um gasto de energia maior para deter aqueles riscos que ainda permanecem. Contribuem para este cenário as rápidas mudanças que implicam na quebra de certezas e instituições tradicionais, como a família. "A vida é vivida como mais individualizada; há uma sensação de que os indivíduos estão sozinhos para se defenderem sozinhos em um mundo arriscado" (Bennet, 2014: 43).

Neste sistema da gestão de riscos, o molde que ela estabelece em torno dos medos favorece cada vez mais o emprego de mecanismos de vigilância. As pessoas tendem a se concentrar em certos riscos devido à sua "natureza terrível", mesmo que eles sejam improváveis. Os riscos são apontados por especialistas mais na sua natureza dramática do que realmente em sua probabilidade, de forma que algo que possa ocorrer, ainda que improvável, não possa ser descartado. Essa estratégia, por outro lado, é muito mais eficaz, uma vez que as pessoas assimilam mais as impressões e sentimentos em relação a um risco que lhes é colocado, do que por probabilidades numéricas. A mídia exerce um papel fundamental neste caso, especialmente por abordar de forma mais aterrorizante tais riscos, ampliando seus efeitos.

> A vigilância torna-se uma resposta adequada a um sentimento generalizado de insegurança. Tendências psicológicas, a mídia e os políticos contribuem para um ambiente em que as medidas de vigilância são muitas vezes introduzidas com base em um incidente dramático e terrível, mas estatisticamente improvável que recebe uma grande quantidade de meios de comunicação social, política e atenção do público (Bennet, 2014: 45).

Esta intolerância crescente ao risco torna-se mais importante do que a verdadeira natureza e o nível dos riscos. Um exemplo disso é a introdução de medidas de lei e ordem radicais e dispendiosas pelo governo do Canadá em 2012, considerando a violência da criminalidade, agiu na contramão dos dados estatísticos, os quais apontavam uma baixa na criminalidade em quarenta anos. O risco de que algo ruim poderia acontecer introduzia a justificativa de mais medidas de segurança.

Por outro lado, Bennet (2014) argumenta que a evolução das mudanças tecnológicas também gerou a produção de novos riscos, de consequências inesperadas. Ao mesmo tempo em que a gestão da informação facilitou a ação de governos e negócios, também levanta questões acerca da vigilância e da privacidade, especialmente pelo avanço em áreas como câmeras de vigilância, biometria, localização e rastreamento de sistemas, sistemas de telecomunicações. Tais artifícios têm facilitado a coleta e o processamento de informações, fazendo com que a regulamentação esteja muito aquém da implantação dessas novas tecnologias. O número de dados gerados pelos dispositivos tem se transformado em um grandioso aparato que coloca em xeque a segurança de tais informações.

O CASO BRASILEIRO

Diante dos conceitos de vigilância e controle e da questão dos riscos, busca-se agora analisar a

forma como esses pontos permearam o debate do Marco Civil. O tema da segurança contra o cibercrime pode ser verificado na questão da responsabilização dos provedores pelo armazenamento de dados, a fim de se identificar usuários e de se contribuir com investigações criminais. Como já ressaltado neste artigo, a discussão sobre segurança entre agentes da Polícia Federal, peritos, delegados e advogados ligados ao Direito digital era sobre a possibilidade de detectarem dificuldades nas suas atividades de investigação, como o chamado "apagão da perícia", ou seja, dos rastros deixados pelos usuários em seus logins nos aplicativos móveis e de navegação. Eles chegaram a usar inúmeros exemplos para convencer parlamentares acerca da importância desses dados no caminho das investigações e confiaram na pessoa do relator Alessandro Molon a mudança da redação do artigo de modo a atendê-los.

A visão desses representantes se assemelhava às propostas que já haviam sido apresentadas por deputados federais em anos anteriores, que traziam instrumentos capazes de futuramente criminalizar usuários de forma errônea ou mesmo cercear a liberdade no uso da rede. Uma delas foi o famoso projeto de lei 84/1999, apresentado pelo deputado Eduardo Azeredo (PSDB), denominado AI-5 Digital, que visava criminalizar o usuário, permitindo o acesso a dados pessoais pela polícia e o Ministério Público sem o aval judicial.

No âmbito do Marco Civil, o maior ponto de conflito estava na possibilidade de facultar aos provedores de aplicação, ou seja, às empresas que fornecem o aplicativo como Skype, Facebook, Twitter, Microsoft, Apple, a guarda dos dados. Essas corporações passariam a não ter que armazenar os logs de acesso dos usuários em suas aplicações: o usuário quando entra em sua conta no Facebook, digita ali o seu e-mail e sua senha. Nesse momento, o próprio sistema registra o horário que foi feito o login, de qual IP foi realizado o login, sua localização e possivelmente as páginas acessadas ou curtidas, os contatos feitos, a duração da conversa. Ainda que a empresa garanta que este tipo de informação não significa a guarda de conteúdo das mensagens ali trocadas, mas sim dos chamados logs, ela não seria obrigada a armazená-los.

Em resposta às reivindicações, o relator da matéria explicou que impor a retenção desse material a pequenos provedores de aplicação poderia incidir em custos enormes para o pequeno empresário, citando, por exemplo, sites que teriam de registrar quaisquer tipos de informação em uma simples pesquisa realizada por seu cliente. Seguindo essa informação, defensores da garantia da privacidade se manifestaram a fim de proibir ao provedor de aplicações essa guarda, uma vez que isso poderia implicar no armazenamento, sem consentimento, de informações sigilosas dos usuários. Também alertavam sobre a possível vulnerabilidade à qual se submeteria o grande volume desses dados, uma vez que uma ação hacker poderia inclusive acessá-los, filtrá-los, distribuí-los, criar perfis de consumo e vendê-los. Tal ação poderia gerar consequências graves para o usuário, tendo em vista que informações pessoais estariam ali armazenadas, consentidas ou não, sendo elas fruto do mecanismo de rastreamento de sistemas que possibilitaria o seu armazenamento.

Diante desse cenário, acadêmicos chegaram a sugerir que se fizesse a guarda dessas informações "no menor tempo possível", a fim de evitar a retenção exagerada dessas informações por bancos

de dados "amplos e desregulados demais". Um dos criadores do texto base do Marco Civil da Internet, o professor da Fundação Getúlio Vargas, Luiz Fernando Marrey Moncau, já havia defendido a Internet Livre em comissão de discussão da matéria, sem a intervenção do estado ou empresas. Ele considerou que o texto do projeto de lei, que ainda estava em tramitação, seria uma importante ferramenta para assegurar a privacidade, incluindo a vedação à prática de empresas que "bisbilhotam" as comunicações entre os usuários.

Os deputados ligados à bancada da segurança, como Sandro Alex (PPS-PR) e Fernando Francischini (SDD-PR), que chegaram a apresentar emendas parlamentares para guarda de dados de aplicação pelo prazo de 12 meses, citavam como exemplo o caso de investigações em que a Polícia Federal necessitou do uso dessas informações para chegar até o autor do ato ilícito. Eles criticavam o estabelecimento de 12 meses apenas para a guarda de registro de conexão por provedores de conexão, ou seja, do horário, localização e IP em que o usuário teve acesso à internet, mas sem o mesmo prazo para a guarda de informações pelos aplicativos que o usuário teria acessado. Na argumentação, afirmavam sobre o risco de que a investigação criminal pudesse ser interrompida, uma vez que tais provedores poderiam apenas alegar que não teriam armazenado os dados, já que a lei não os obriga, o que possivelmente geraria um vácuo para o investigador. Na tentativa de coibir a facultação dessa guarda, o deputado Mendonça Filho (DEM) também chegou a apresentar uma emenda para inserir a obrigatoriedade desse armazenamento.

O deputado Alessandro Molon, relator da matéria, chegou a mencionar a necessidade de um "equilíbrio fino" em relação aos dados e à segurança. Informou que a nova lei garante a presunção de inocência na internet, respeitando preceitos constitucionais. Os posicionamentos do Ministério da Justiça e do Instituto Brasileiro de Defesa do Consumidor (IDEC) também levantaram uma importante questão acerca da garantia da presunção da inocência, mas alimentavam uma pergunta: até que ponto vale colocar em xeque a inocência do usuário, quebrando sua privacidade, para se consolidar a ação de mecanismos de segurança? Assumindo um caráter de estabelecer princípios, como defendeu o relator da matéria, e deixando para lei específica as situações envolvendo crimes na rede, como reforçou o presidente da comissão, João Arruda, o Marco Civil pensaria mais em termos de disciplina e garantia de direitos aos usuários e menos em criminalização, ponto esse que foi um dos de maior conflito.

Buscando estabelecer o consenso entre as partes e garantir uma redação ao texto de forma que atendesse as partes em disputa, e sem risco de prejuízo ao projeto de lei por causa desse embate, o relator Alessandro Molon (PT) inseriu no texto a obrigatoriedade por um período menor, de seis meses para a guarda de aplicações, delimitando que os dados fossem armazenados em local seguro. Outra ponderação foi a de que os provedores de conexão (como teles, operadoras, empresas que fornecem internet) não tivessem acesso a estes dados de aplicação, uma vez que eles têm consigo dados cadastrais de usuários da internet, como RG e CPF, informados no ato da contratação, o que poderia ocasionar uma compreensão global acerca de gostos e preferências de indivíduos, prejudicando sua privacidade.

Molon afirmou que a proibição de guardar dados ao provedor de conexão seria uma importante forma de vedar o monitoramento ou a análise do conteúdo postado pelos usuários na rede. Em seu relatório, destacou os princípios de liberdade e controle como pilares da internet, inclusive mencionando os protocolos que sustentam a comunicação interativa. O deputado citou os rastros digitais deixados pelos usuários, explicando que é muito mais fácil monitorar as pessoas na internet do que na vida real. E, dessa forma, o monitoramento é realizado de forma indevida, e deve ser coibido para que a liberdade de expressão e a privacidade não sejam tolhidas. Destaca ainda que foram feitas alterações no texto do projeto para garantir maior proteção à privacidade dos internautas, sem que isso prejudique a inovação ou os modelos de negócio.

O respeito à legislação brasileira na coleta de dados também foi um dos pontos inserido pelo relator no texto, considerado como um instrumento "para proteger ainda mais a privacidade e o sigilo dos dados pessoais, das comunicações privadas e dos registros". A medida abrange qualquer empresa sediada no exterior, desde que pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil, "de modo que a simples localização de dados em bancos de dados no exterior não exclua a aplicabilidade da legislação brasileira, quando pelo menos uma empresa integrante do mesmo grupo econômico tiver estabelecimento no Brasil", aponta o relator.

CONSIDERAÇÕES FINAIS

A forma como se revela o anseio pela segurança em um debate acerca da regulamentação da Internet torna-se um fator preocupante diante do cenário de controle e ampliação do investimento em ferramentas de monitoramento e prospecção de informações. Criando um modelo de institucionalização da vigilância, provocado por amparo legal que autoriza o armazenamento de informações, percebe-se que o discurso do medo e da insegurança se tornam argumentos para favorecer os trabalhos de investigação e ação de órgãos vigilantistas. Pode-se constatar, portanto, que aspectos de natureza conservadora tomam o debate sobre a regulamentação da rede, principalmente pelos deputados e órgãos que representam o segmento policial. São discursos que buscam ampliar a sensação de insegurança, irrompendo os princípios da presunção da inocência e classificando os usuários da internet como suspeitos. A privacidade entra como o fator chave justamente pelas ações de monitoramento e comercialização de dados que poderiam se estabelecer com a guarda de dados de aplicações por muito tempo. O equilíbrio buscado pelo relator Alessandro Molon acabou se consolidando com a estipulação de um prazo menor do que os registros de conexão, sendo esse de apenas seis meses.

Um aspecto que se pode observar é o lugar em que o Governo brasileiro se posiciona em toda a discussão sobre o armazenamento de dados. Diferentemente do discurso norte-americano, de se fortalecer as ações de combate ao terrorismo monitorando indivíduos, o governo, pelo menos na esfera do Marco Civil, atua inicialmente de modo a facultar aos provedores de aplicação a guarda desses registros. Cabe aos deputados de oposição ao Governo Dilma a fala mais veemente

para estabelecer a obrigatoriedade, inclusive ameaçando derrubar o projeto de lei no caso de não se garantir o período de guarda.

Outro ponto que permite maior discussão é a questão da jurisdição, a qual, embora pertença a uma questão específica do Direito digital, merece aqui um destaque especialmente pela preocupação mundial em torno da efetividade das políticas que possam ser desenvolvidas, tendo em vista o advento da comunicação em rede. O respeito à legislação brasileira na coleta de dados foi um aspecto inserido pelo relator no texto, considerando-o um instrumento "para proteger ainda mais a privacidade e o sigilo dos dados pessoais, das comunicações privadas e dos registros", nas palavras do relator. A medida abrange qualquer empresa sediada no exterior, desde que pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. Na tentativa de se preservar mecanismos jurídicos que remetam ao território, ou seja, que responsabilize empresas por atos cometidos em âmbito nacional, o crime cometido em um ambiente que não se estabelece sobre o "território", mas em cabos ópticos, a quem cabe julgar o ilícito? A questão demonstra como a organização transfronteiras do mundo em rede provocou uma mudança em todo o sistema, permitindo refletir não somente sobre as ações dos indivíduos neste cenário, mas as possíveis implicações que essas ações possam gerar, sem que haja respostas imediatamente claras.

REFERÊNCIAS

Assange, J. (2013).*Cypherpunks: liberdade e o futuro da internet* . São Paulo: Boitempo.

Bennett, C. (2014). Transparent Lives Surveillance in Canada (pp.39-51). Edmonton: AU Press, Athabasca University.

Bruno, F. (2004). Máquinas de ver, modos de ser: visibilidade e subjetividade nas novas tecnologias de informação e de comunicação. *Revista Famecos* , 24, 110-124.

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade* . Porto Alegre: Sulina.

Lei 12.965, de 23 de abril de 2014. Dispõe sobre o Marco Civil da Internet. Recuperado em 10 fevereiro, 2016, de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Lyon, D. (2015). *Surveillance After Snowden* . Cambridge, UK: Polity Press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Revista Big Data &Society. Recuperado em 29 março, 2016, de http://bds.sagepub.com/content/1/2/2053951714541861.

Silveira, S. A. (2012). Poder tecnológico como poder político. In: Cultura, política e ativismo nas redes sociais (pp. 15-29). São Paulo: Fundação Perseu Abramo.

Silveira, S. A. (2014). Regulamentação e liberdade na rede: o Marco Civil da Internet. In: Lima, V. A., Guimarães, J., Amorim, A. P. Em defesa de uma opinião pública democrática: conceitos, entraves e desafios (1ª Ed. Cap.8, pp.239-255). São Paulo: Paulus.

VIGILANCIA ON LINE Y SECRETO PERIODÍSTICO: ANÁLISIS Y REFLEXIONES SOBRE SU NECESARIA PROTECCIÓN LEGAL

TALLER: VIGILANCIA ON LINE Y SECRETO PERIODISTICO.

Descripción del taller: Desde mediados del S. XX a la fecha en diferentes partes del mundo han tenido lugar diversos conflictos jurídicos a raíz de pedidos judiciales tendientes a que se revele la identidad de la fuente de una información periodística invocándose, como justificación, de ello su vital importancia para la resolución de un caso en particular.

Ante esta situación, con justa razón los periodistas han invocado como impedimento de tal pedido su derecho profesional a preservar el anonimato de su fuente. En Argentina, tal derecho se encuentra garantizado en el último párrafo del art. 43 de la Constitución Nacional donde expresamente reza que "No podrá afectarse el secreto de las fuentes de información periodística". Ahora bien, a partir de las revelaciones de Chelsea Manning y Edward Snowden, se ha tomado conocimiento de cómo las Agencias de inteligencia y Empresas privadas monitorean y vigilan toda clase de actividad on line de cualquier persona, entre quienes se encuentran por supuesto los periodistas. ¿La reserva de la identidad de las fuentes periodísticas merece una protección absoluta o, por el contrario, debe ceder frente a una situación particular en la cual, por ej., se encuentre en juego la seguridad nacional? ¿Debe permitirse a las Agencias de inteligencia que puedan interferir o acceder a cualquier clase de comunicación de los periodistas sin intervención de una autoridad judicial con basamento en la potencial inseguridad? ¿Quién controla a las agencias? ¿Cómo? ¿Sería viable ese control?

El objetivo del taller consistirá en exponer el marco jurídico que brinda protección al periodista para preservar el anonimato de la fuente. Acto seguido analizar diversos casos que han tenido lugar en diversos países de Latinoamérica y del resto del mundo donde se ha vulnerado el derecho del profesional a mantener el secreto de su fuente de información, fundado en que se corría un riesgo contra la seguridad nacional (posibles actos de terrorismo por ej) para finalmente realizar ejercicios prácticos de reflexión y razonamiento grupales con los asistentes.

Público al que va dirigido: licenciados en comunicación social, periodistas, docentes universitarios, abogados, público en general.

Requerimientos especiales del taller: PC, Proyector, micrófono.

Palabras clave: Vigilancia, Secreto periodístico, Intimidad, Comunicación, Expresión.

SEBASTIÁN CASTELLI*
MANUEL ERNESTO LARRONDO**

Online surveillance and journalistic secret. Reflections on the legal protection.

WORKSHOP: ON LINE SURVEILLANCE AND JOURNALISTIC SECRET

Abstract: Since the mid-twentieth century to date, in different parts of the world many legal disputes have occurred as a result of tending court orders that the identity of the source of journalistic information invoked as a justification, it is revealed its vital importance for the resolution of a particular case.

In this situation, journalists rightly had invoked as an impediment in such order his professional right to preserve the anonymity of its source. In Argentina, this right is guaranteed in the last paragraph of art. 43 of the Constitution which expressly states that "it will not affect the secrecy of journalistic information sources." Now, from the revelations of Chelsea Manning and Edward Snowden, it has taken note of how the intelligence agencies and private companies monitor all kinds of online activity of any person, including those who are, of course, journalists. Does the reservation of the identity of journalistic sources deserve absolute protection or, on the contrary, must yield to a particular situation in which, eg., Is in the national security game? You should be allowed to intelligence agencies that may interfere or access any kind of communication of journalists without intervention of a judicial authority with basement in the potential insecurity? Who controls the agencies? How? Would it be feasible that control?

The aim of the workshop will expose the legal framework that protects the journalist to preserve the anonymity of the source. Then analyze various cases that have taken place in several countries in Latin America and around the world where it has infringed the right of professional secrecy of their source of information, based on a risk that ran against national security (eg acts of terrorism) to finally practical exercises and group reflection reasoning with attendees.

Audience it is addressed: graduates in social communication, journalists, university professors, lawyers, public in general.

Keywords: Surveillance, Journalistic secret, Intimacy, Communication, Expression.

Monitoramento on-line e secreto jornalística. Reflexões sobre a protecção jurídica.

WORKSHOP: VIGILÂNCIA ON LINE E SECRETO PERIODISTICO

Resumo: Desde meados do século XX até hoje em diferentes partes do mundo, muitas disputas legais ocorreram como resultado da tendência ordens judiciais que a identidade da fonte da informação jornalística invocada como justificação, é revelado sua importância vital para a resolução de um caso particular.

Nesta situação, os jornalistas, com razão, sido invocadas como um impedimento de tal modo o seu direito profissional para preservar o anonimato de sua fonte. Na Argentina, esse direito é garantido no último parágrafo do art. 43 da Constituição, que expressamente afirma que "não vai afetar o sigilo das fontes de informação jornalísticas." Agora, Monitoramento on-line e secreto jornalística. Reflexões sobre a protecção jurídicaa partir das revelações de Chelsea Manning e Edward Snowden, ele tomou conhecimento de como as agências de inteligência e empresas privadas monitorar e controlar todos os tipos de atividade on-line de qualquer pessoa, incluindo aqueles que são de jornalistas do curso. Será que a reserva da identidade das fontes jornalísticas merecem proteção absoluta ou, pelo contrário, deve ceder a uma situação particular em que, por exemplo, é no jogo a segurança nacional? Você deve ter permissão para agências de inteligência que podem interferir ou acesso a qualquer tipo de comunicação de jornalistas sem a intervenção de uma autoridade judiciária com cave na insegurança potencial? Quem controla as agências? Como? Seria possível que o controle?

O objetivo do workshop irá expor o quadro jurídico que protege o jornalista para preservar o anonimato da fonte. Em seguida, analisar vários casos que ocorreram em vários países da América Latina e em todo o mundo onde ele violou o direito de sigilo profissional de sua fonte de informação, com base em um risco ele correu contra a segurança nacional (possível por exemplo, atos de terrorismo) para, finalmente, exercícios práticos e grupo de reflexão de raciocínio com os participantes.

Audiência é dirigida: graduados em Comunicação Social, jornalistas, professores universitários, advogados, público

Palavras-chave: Vigilância, Segredo jornalístico, Intimidade, Comunicação, Expressão.

INTRODUCCIÓN

Desde la reforma constitucional de 1994, en Argentina se ha debatido y escrito en demasía en torno a los conflictos jurídicos que han tenido lugar frente a pedidos de informes a periodistas y/o empresas de medios de comunicación por parte de la Justicia a fin de que se suministre la identidad de una fuente periodística invocándose como justificación de ello, su vital importancia para la resolución de un caso en particular.

Ante esta situación con justa razón los periodistas han invocado como impedimento de tal pedido la protección constitucional prevista en el último párrafo del Art. 43 de la Norma Fundamental cuando, luego de referirse al Habeas Data, expresamente reza que **"No podrá afectarse el secreto de las fuentes de información periodística"**.

La reserva de la identidad de las fuentes periodísticas es y será el eje central en la eterna discusión jurídica respecto a si merece una protección absoluta o si, por el contrario, debe ceder frente a una situación particular en la cual, por ej., esté en juego la vida de un inocente. Los partidarios de la primera postura sostienen que dejar abierta la posibilidad de que un periodista deba identificar su fuente pone en serio riesgo el derecho humano de recibir, investigar y difundir información de toda índole a la opinión pública (Art. 13 de la Convención Americana de Derechos Humanos).

Sin ir más lejos, debe tenerse en cuenta que los profesionales de la prensa arriesgan su vida con el único objetivo de dar a conocer información a la opinión pública. Un ejemplo de ello es el caso de la periodista rusa Anna Politkovskaia cuando a fines de 2006 fue asesinada mientras investigaba el conflicto entre Rusia y Chechenia (ex república soviética). Otro caso es el de Judith Miller, del diario The New York Times, quien estuvo detenida por negarse a testificar sobre sus conversaciones confidenciales con fuentes gubernamentales, en un caso que buscaba determinar quién -del Gobierno de EEUU- filtró la identidad de la agente secreta Valerie Plame, esposa de un ex diplomático ("La SIP pide la puesta en libertad de la periodista Judith Miller", 19 de agosto de 2005).[1]

En nuestro país sobran los ejemplos en los cuales la Justicia ha requerido en innumerables ocasiones que los periodistas revelaren sus fuentes ya que así se contribuiría a la resolución de un caso de trascendencia pública. Por ejemplo, el del periodista Thomas Catan del diario Financial Times de Londres que explicaremos en detalle más adelante; o bien el del bodeguero de la Pcia de San Juan que fue entrevistado en 1993 por periodistas mientras se encontraba prófugo por ser sospechoso de haber comercializado vino en damajuana en mal estado, ocasionando la muerte de varias personas por su ingesta. Al leer la crónica, el Fiscal de la causa solicitó que los periodistas revelaren donde estaba el imputado bajo apercibimiento de considerarlos cómplices. El Juez no hizo lugar al pedido justamente sosteniendo que, de acceder, se afectaría el derecho colectivo de la sociedad a ser informada ya que los periodistas perderían todas sus fuentes.

En los casos brevemente reseñados advertimos que ha intervenido formalmente la Justicia analizando la pertinencia o no del pedido de revelación de la fuente periodística en miras a solucionar un caso concreto.

Ahora bien, a partir de las revelaciones realizadas por Chelsea Manning y Edward Snowden se ha tomado conocimiento público, entre otros asuntos, de cómo las Agencias estatales de inteligencia e incluso Empresas privadas monitorean y vigilan toda clase de actividad on line o vía telefonía móvil de cualquier persona, entre quienes se encuentran, por supuesto, los periodistas. Al mismo tiempo, la situación personal tanto de Manning (condenada a 35 años de cárcel en EEUU) como de Snowden (asilado en Rusia, ya que si regresa a EEUU se expone a igual condena que Manning) demuestran el peligro al que se encuentran expuestas aquellas personas que actúen como fuentes periodísticas revelando información vinculada con la vigilancia social estatal o privada.

Por otra parte, debe tenerse en cuenta que, en el ejercicio profesional, el periodista enfrenta en principio muchas situaciones distintas a los de cualquier ciudadano común. Sin embargo, como su trabajo y su vida personal se encuentran en cierta forma subsumidas en el necesario empleo de la tecnología y redes sociales, es claro que ello implica dejar en el camino una enorme y variada cantidad de registros electrónicos y metadatos como por ejemplo: destinos y recepción de llamadas telefónicas, mensajes de texto, conexiones temporales a determinadas antenas de telefonía celular, uso de GPS, intercambio de correos electrónicos y mensajes a través de las plataformas web, entre otros. El uso de todas estas plataformas sin dudas conlleva dejar cientos de registros que, bajo vigilancia masiva estatal o privada, podrían ser usados en perjuicio de sus fuentes de información. De allí que, dependiendo del caso sobre el que el periodista se encuentre trabajando, se infiere que bien podrían o deberían emplear tecnologías de encriptación en sus comunicaciones a fin de evitar, justamente, que tenga lugar la recolección on line de sus datos de contactos o interacción en la web.

Sin dudas el caso de Edward Snowden es sumamente revelador. Luego de haber realizado un análisis de los documentos revelados por el ex dependiente de una Empresa contratista de la Agencia Nacional de Seguridad de EEUU, el diario británico "The Guardian" informó el 19 de Enero de 2015 que en Noviembre de 2009, la British Global Communications Headquarters (GCHQ, la Agencia de Seguridad Británica) interceptó alrededor de 70.000 correos electrónicos incluidos algunas direcciones de empresas periodísticas como la BBC, Reuters, los diarios The Guardian, The New York Times, Le Monde, The Sun, NBC y The Washington Post.[2]

Se informó que la Agencia Británica interceptó los correos electrónicos a través de un uso de la fibra óptica como parte de un entrenamiento. Luego compartieron esos correos electrónicos interceptados en su propia Intranet. El informe periodístico del diario inglés reveló además que el GCHQ entiende que la información sobre la que trabajan los periodistas de investigación es comparable a la actividad que realizan los "terroristas" y "hackers." Concluye el reporte que los documentos de dicha Agencia de Inteligencia sostienen que los *"periodistas y reporteros representan*

una potencial amenaza a la seguridad. " La idea que se desprende de este reporte es que sería "potencialmente riesgoso" ejercer el derecho humano a recibir, investigar y difundir información. Inaudito.

La vigilancia masiva de la actividad de los periodistas implica, tal como referimos, poder acceder a los metadatos de las comunicaciones. A través de ellos, informa la ONG "Necessary & Proportionate" que se puede crear un perfil de la vida de un individuo, incluyendo condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones. A pesar del gran potencial para la intromisión en vida del individuo y el efecto negativo sobre las asociaciones políticas y otras, las leyes, normas, poderes o autoridades a menudo ofrecen a los metadatos de las comunicaciones un menor nivel de protección y no ponen restricciones suficientes sobre cómo pueden ser posteriormente utilizado por los Estados.[3]

Juan Diego Castañeda (2016) apunta que *"los datos que se recogen son, por ejemplo, el número que recibe una llamada, el tiempo de la llamada, la ubicación geográfica del dispositivo o sus identificadores únicos (IMEI e IMSI) en telefonía móvil o fija, y las direcciones IP en internet. Esto es, en un nivel simple, diferente de la recolección de las comunicaciones en sí mismas y, por tanto, han sido llamados "metadatos", es decir, datos acerca de los datos de comunicación. Esta clasificación puede llevar a concluir erróneamente que los metadatos o los datos de identificación del suscriptor merecen una protección menor a la que está establecida para las comunicaciones en sí mismas. La agregación de datos, en realidad, es más reveladora que el contenido de las comunicaciones. Por esta razón, se ha establecido que la retención de datos es una medida que restringe y afecta los derechos a la intimidad y a la libertad de expresión."*

Ante esta alarmante situación, surgen algunos interrogantes que planteamos como disparadores de este trabajo: ¿La reserva de la identidad de las fuentes periodísticas merece una protección absoluta o, por el contrario, debe ceder frente a una situación particular en la cual, por ej., se encuentre en juego la seguridad nacional? ¿Debe permitirse a las Agencias de inteligencia que puedan interferir o acceder a cualquier clase de dato derivado de una comunicación telefónica o electrónica que realice un periodista sin intervención de una autoridad judicial? ¿Es justificable el fundamento de la vigilancia masiva en miras a proteger la "seguridad nacional"?

El objetivo de este trabajo consistirá en exponer el marco jurídico argentino e internacional que brinda protección al periodista para preservar el anonimato de la fuente. Acto seguido analizaremos diversos casos que han tenido lugar en diversos países de Latinoamérica y del resto del mundo en los que se intentado avasallar el derecho del periodista a mantener el secreto de su fuente de información de parte de Organos estatales, fundando tal proceder en que habría un peligro inminente o bien se corría un riesgo contra la seguridad nacional (posibles actos de terrorismo por ej).

SECRETO DE LA FUENTE PERIODISTICA. NATURALEZA JURIDICA. TITULARIDAD. PRINCIPIOS REGULATORIOS DE VIGILANCIA EN LAS COMUNICACIONES

Empezaremos el análisis de este punto formulándonos un nuevo interrogante: ¿Quién es el titular del derecho a mantener en reserva la identidad de la fuente? ¿Será la Empresa de medios de comunicación o el periodista?

Titularidad del derecho.

Por empezar, siguiendo a Badeni (2002) "**el secreto profesional es un derecho subjetivo de naturaleza pública que integra la libertad institucional de prensa**. Ese secreto coadyuva a obtener y difundir la información que interesa a la sociedad, ya que tanto en el ámbito privado como público se generan datos y noticias que son revelados bajo la condición expresa de preservarse la reserva de la fuente del informante".

En nuestra opinión, este derecho pertenece con exclusividad a los periodistas y también a quienes ocasionalmente publiquen información en cualquier medio de comunicación (Portal de Internet, redes sociales, por ej.). En concordancia con lo expuesto, afirma Silvana Catucci (1997) que "el titular de esta garantía es el periodista" y Javier De Lucca (1999) expresa por su parte que "no parecen existir razones constitucionales por las cuales el privilegio del secreto, si así quiere llamárselo, no pueda extenderse a toda persona que realiza una actividad periodística en sentido material, aún cuando no lo haga habitualmente o no sea un profesional".

Por el contrario, esta prerrogativa no se extendería **a las empresas propietarias de los "medios" o "multimedios**" en tanto, justamente, no son ellos los titulares de ese derecho público subjetivo.

Es decir, los protegidos por esta garantía son los periodistas comprendidos en el art. 2° del Estatuto del Periodista Profesional (Ley 12908 "Estatuto del Periodista Profesional", Boletín Oficial de la República Argentina Nº15813, Buenos Aires, Argentina, 11 de Julio de 1947) y **toda persona** que publique noticias, opiniones, escritos por medios gráficos, por radio, televisión, Internet u otro mecanismo de divulgación conforme a lo previsto por el art. 14 de la Constitución Nacional y el art. 13 del Pacto de San José de Costa Rica (con jerarquía constitucional en Argentina conforme se desprende del art. 75 inc. 22 de la C.N.).

Sobre este punto, vale la pena traer a colación un fallo judicial de fecha 26/5/06 dictado por la Corte de Apelaciones de California, EEUU, en los autos JASON O'GRADY et al., Petitioners, v. THE SUPERIOR COURT OF SANTA CLARA COUNTY, Respondent; APPLE COMPUTER, INC., Real Party in Interest. H028579.[4]

En este caso, la Corte de apelaciones de California decidió que los 'bloggers' –personas que son titulares de un portal en Internet y que en él publican cualquier tipo de información–, al igual que los periodistas tradicionales, tienen derecho a mantener la confidencialidad de

sus fuentes.

Los hechos consistieron en que un grupo de 'bloggers' acudió a los tribunales después de que *Apple* – Empresa Americana que desarrolla tecnología en computación hardware – tratara de forzarles a revelar la identidad de la persona -probablemente un empleado de la compañía- que les facilitó los detalles de un proyecto de la empresa denominado 'Asteroid'. Los datos del producto fueron difundidos en varios sitios de Internet.

La sentencia, en síntesis, estableció que los 'bloggers' **no tienen obligación de revelar sus fuentes** y pueden acogerse a las leyes que protegen a los periodistas tradicionales, la **Primera Enmienda** de la Constitución Americana y la **California's Shield Law.**

Este fallo de la justicia norteamericana confirma entonces nuestra postura por cuanto la Constitución Nacional y los Tratados Internacionales de Derechos Humanos que poseen jerarquía constitucional deben ser interpretados en forma amplia y flexible en clara protección a la libertad de expresión del ser humano indistintamente si la acción de recibir, investigar y difundir se realice en forma profesional o amateur.

Ahora bien, en concordancia con la constitucionalista María Angélica Gelli (2005) *"la preservación de las fuentes de información periodística – como la integridad de los derechos que constituyen la libertad expresiva – tienen como finalidad el descubrimiento de la verdad a través de la libre circulación de las noticias obtenidas, éstas muchas veces bajo reserva y que, de otro modo, no se conocerían. El descubrimiento de la verdad de los hechos tiene particular importancia en la investigación de los delitos y en el control del gobierno y de las eventuales ilegalidades que afectan directamente al proceso democrático. En este sentido* ***el privilegio de los periodistas no es un fuero personal****, sino que opera en resguardo de aquellos objetivos y para favorecerlos"*.

Es acertada esta posición por cuanto no podría invocarse la protección de esta garantía constitucional como si fuera un fuero personal asimilable a quien desempeña una función pública (Juez, legislador, etc.). Por el contrario, debe remarcarse que se trata de una garantía constitucional de todo ser humano que ejerce profesional u ocasionalmente la tarea de informar por cualquier medio de comunicación, en tanto la acción de recibir, investigar y difundir información es un derecho humano conforme lo prevé el art. 13 del Pacto de San José de Costa Rica. Ello ha sido reafirmado por la Corte Interamericana de Derechos Humanos en la Opinión Consultiva Nº 5 del 13/11/1985 rechazando la Colegiación Obligatoria de Periodistas **(Arts. 13 y 29 de la Convención Americana sobre Derechos Humanos)**.[5]

En síntesis, como primera conclusión de este estudio podemos afirmar entonces que la reserva de identidad de la fuente periodística pertenece al ser humano como tal y no a la Empresa periodística que eventualmente lo emplee.

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones fueron desarrollados a partir de las conceptualizaciones que se han realizado en torno al derecho internacional de los derechos humanos en el entorno digital en un proceso que distintas organizaciones de la sociedad civil lideraron y que contó con la participación de representantes de la industria y expertos en la materia.

De acuerdo a lo que se informa en el sitio web de Necessary & Proportionate *"el proceso de elaboración de estos Principios se inició en octubre de 2012 en una reunión de más de 40 expertos de seguridad y privacidad en Bruselas. Después de una amplia consulta inicial, que incluyó una segunda reunión en Río de Janeiro en Diciembre de 2012, Access, EFF y Privacy International condujeron un proceso de redacción colaborativa inspirada en la pericia sobre derechos humanos y derechos digitales de expertos de todo el mundo. La primera versión de los Principios se finalizó el 10 de julio de 2013, y fue lanzada oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en Septiembre de 2013"*[6].

En ese sentido, los principios que deben regir la aplicación de medidas de vigilancia de las comunicaciones son: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autorización judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y los sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo, y derecho a un recurso efectivo.

Siguiendo estos principios, el Relator para libertad de expresión de la OEA, a propósito de las revelaciones sobre el uso de productos y servicios de la empresa italiana Hacking Team por parte de gobiernos alrededor del mundo, expresó que, de acuerdo con los estándares internacionales, el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación.[7]

Veamos entonces brevemente que sostiene cada uno de los Principios reseñados

Principio 1: Legalidad

Cualquier limitación a los derechos humanos debe ser prescrita por ley, cumplir con un estándar de claridad y precisión suficiente para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Asimismo exige que esa misma ley sea objeto de revisión periódica.

Principio 2: Objetivo Legítimo

Esa misma ley solo debería permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico

preponderante e importante y que sea necesario en una sociedad democrática. Por supuesto su aplicación no debería implicar discriminación alguna por cualquier razón o circunstancia.

Principio 3: Necesidad

La ley debe limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo y la justificación de ello debe recaer en el Estado.

Principio 4: Idoneidad

Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.

Principio 5: Proporcionalidad

La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Por eso este Principio requiere que el Estado, como mínimo, demuestre que:

1) Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo, y;

2) Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la la Información Protegida, y;

3) Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica. Y;

4) La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza especifica al fin legitimo alegado; y

5) Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud; y

6) La información será accesada solo por la autoridad especifica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y

7) Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

Principio 6: Autoridad Judicial Competente

Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe:

1) Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones.

2) Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y

3) Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

Principio 7: Debido Proceso

El debido proceso exige que, entre otras garantías, toda persona tenga derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley,salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.

En nuestra opinión, la última situación prevista en este Principio debería ser la que mayor reglamentación y previsión legal debiera tener ya que podría prestarse a que se cometan abusos que en consecuencia afecten garantías constitucionales.

Principio 8: Notificación del Usuario

Este principio prevé que aquellas personas cuyas comunicaciones están siendo vigiladas deben ser notificados por el Estado de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:

1) La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y

2) La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y

3) El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.

Principio 9: Transparencia

Se exige que los Estados sean transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, debiendo publicar como mínimo informes globales de esta temática.

Principio 10: Supervisión Pública

Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones.

Principio 11: Integridad de las Comunicaciones y Sistemas

Los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado. El fin es garantizar a las personas su derecho a expresarse anónimamente.

Principio 12: Garantías para la Cooperación Internacional

Los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la estandar disponible con el mayor nivel de protección para las personas.

Principio 13: Garantías Contra el Acceso Ilegítimo y Derecho a Recurso Efectivo

Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados así como también proteger a los "whistle blowers" (soplones) y medios de reparación a las personas afectadas. Asimismo, deben prever que el material obtenido a través de la Vigilancia de las Comunicaciones ya utilizado debe ser destruido o devuelto a los afectados.

Secreto de la fuente periodística: ¿protección absoluta o relativa?

De igual forma, la doctrina y jurisprudencia han dado sus puntos de vista tanto a favor como en contra de la protección de la reserva de la fuente así como también hay posiciones eclécticas que ameritan que a continuación los tratemos a fin de dilucidar la respuesta a este interrogante.

Doctrina.

PIERINI, LORENCES y TORNABENE (1998) sostienen que "el derecho a no revelar las fuentes es absoluto e incondicional" y agregan que **la reserva de la fuente no debe ceder ante autoridad o reclamo alguno por tener una garantía constitucional absoluta. Los autores mencionados sólo aceptan la excepcionalidad en caso de un delito no ejecutado o que está siendo consumado**, en estos términos: "Aquél que posea una información no deberá, por decisión de autoridad alguna, aportar datos sobre sus fuentes, pero estará obligado, si se refiere a un delito no cometido aún, a realizar todas las denuncias para evitarlo; o sabiendo de la existencia de un delito que está siendo consumado a realizar la denuncia para evitar la prosecución y reiteración de hechos disvaliosos".

Una opinión distinta es sostenida por otra corriente doctrinaria representada por COLAUTTI (1996) para quien **la veda constitucional no es absoluta pues encuentra su restricción en la facultad de los jueces para ordenar requisas en empresas periodísticas cuando sea imprescindible para encontrar pruebas en un caso criminal**.

EKMEKDJIÁN (1997) agrega que "el secreto a las fuentes de información sólo cede cuando encontrándose el periodista ante la comisión inmediata del delito, éste pudiera lesionar un derecho de jerarquía superior al de la prensa (vgr. la dignidad, la vida, etc.)".

VANOSSI (1988) coincide también con el carácter absoluto del secreto de las fuentes pero cuando se trata de opiniones y datos no relacionados con causas penales. En cambio, cuando sí existe causa penal, distingue entre delitos ya juzgados y eventualmente condenados, y delitos que estén en curso de ejecución. En el primer caso predomina la reserva, en el segundo no, del mismo modo cuando la falta de dato puede llevar a la condena a un inocente.

Por su parte, GOZAÍNI (2001) sostiene que es necesario ponderar el caso en concreto: "En los hechos, nos parece más razonable adoptar un criterio propio y adecuado a las circunstancias y contextos en los que cada información se origina. De este modo, la reserva y confidencialidad de las fuentes es una garantía impermeable, como lo es la libertad de prensa y el derecho a la información. Pero, al mismo tiempo, proporciona un deber inexcusable a los medios de comunicación para que desde una perspectiva ética y moral no difundan aquella información que, siendo disponible, pueda afectar la sensibilidad de las personas. La diferencia entre el *poder* de contar una gran cantidad de información sobre cada individuo y el *deber* de no difundirla sería más que nunca fundamental en este terreno".

Sin embargo, las nuevas tecnologías implementadas por Empresas privadas y por los Gobiernos en ciertas ocasiones implica que las Agencias de inteligencia, Policía o cualquier otra autoridad estatal considere necesario contar con una orden judicial para obtener datos o vigilancia de ciertas comunicaciones.

Así lo explica Martin Shelton (2015) en relación a EEUU, en tanto sostiene que "los registros electrónicos (por ejemplo, los metadatos relacionados a llamadas telefónicas) proporcionan suficiente evidencia para vincular a un periodista con una fuente. Las agencias de Estados Unidos en general, tienen la autoridad para obligar a las personas jurídicas (por ejemplo, compañías de teléfono) para dar a los registros electrónicos del gobierno, incluyendo información sobre las comunicaciones electrónicas en virtud de múltiples autoridades. El gobierno no tiene que pedir a un periodista a revelar información sobre fuentes confidenciales si el gobierno puede en lugar de obtener una orden judicial para obtener los registros, y entregar la citación a la empresa que gestiona los registros pertinentes. En otros casos, el gobierno recoge la información de inteligencia con potencial."

Agrega Shelton (2015, pág. 44) que en 1967 tuvo lugar el caso del Tribunal Supremo EE.UU., Katz v. Estados Unidos (EE.UU. 389 347), en el cual se examinó la definición legal de una "búsqueda" de la información. El tribunal estableció que la "expectativa razonable de privacidad" prueba para determinar si ciertos tipos de información deben ser protegidos bajo la Cuarta Enmienda. Sin embargo, en el caso criminal Smith v. Maryland (EE.UU. 442 735, 1979), el Tribunal Supremo reafirmó que la policía podría interceptar los registros de llamadas sin una orden judicial, **porque**

la persona que llama renuncia a cualquier expectativa razonable de privacidad, proporcionando registros de las comunicaciones a un tercero- la compañía telefónica. El principio de que las personas no tienen ninguna expectativa razonable de privacidad cuando la información de ruta a través de una parte exterior es ahora conocida como la "doctrina de terceros", es un concepto que se ha convertido en la piedra angular para la interpretación moderna de las protecciones de la Cuarta Enmienda de datos de los consumidores en los tribunales (por ejemplo, Kerr, 2012; Newell, 2013; Newell & Tennis, 2013).”

Esta doctrina americana que data de unos casi 40 años estaría vulnerando claramente los principios regulatorios de vigilancia en las comunicaciones referidos anteriormente, tales como el de notificación al usuario, debido proceso, autoridad judicial competente, entre otros.

Jurisprudencia Argentina.

Entre las causas judiciales argentina de mayor relevancia donde se ha producido un conflicto de derechos se destaca aquella que tuvo de protagonista al fallecido ex miembro del ERP (Ejército Revolucionario del Pueblo) "**Gorriarán Merlo**" en la cual **se admitió la posibilidad de que este secreto ceda "cuando razones de orden público de relevante jerarquía así lo aconsejen y cuando ello no vulnere el derecho a no autoincriminarse ni afecte los límites previstos en el art. 28 C.N. (...) Otorgándole un alcance absoluto terminaría afectando intereses del propio estado de derecho que motivara el reconocimiento y necesidad de una prensa libre..."**[8].

Particular atención merece prestarse al caso “Thomas Catán” al que hicimos mención al comienzo. El Juez instructor, Dr. Claudio Bonadío, ordenó confeccionar un listado con la totalidad de las llamadas entrantes y salientes registradas entre los días 15 y 29 de agosto de 2002 de la línea telefónica celular del periodista inglés Thomas Catan del diario Financial Times de Londres quien, en un primer momento, fue citado como testigo en esta causa habiéndose negado a revelar la identidad de su fuente ante el pedido del Juez. Recordemos que el periodista fue autor de dos notas en las que reveló la posible existencia del presunto delito de cohecho en el Senado de la Nación a legisladores que dieron su voto para reformar la ley laboral y que el aludido magistrado investigaba[9].

Frente a la orden judicial, el periodista planteó la nulidad y apeló la medida con fundamento en que ella afectaba el secreto a las fuentes de información periodística protegido en el artículo 43 de la Constitución Nacional.

La sentencia de Cámara resolvió desestimar la orden del Juez de instrucción en tanto entendió que **no había necesidad de que ella sea adoptada teniendo en cuenta que se podía avanzar en la pesquisa mediante otros cursos de investigación que resulten igual de útiles y eficaces sin que el secreto a las fuentes de información periodística resulte afectado**. De hecho, se tuvo en cuenta que, contemporánea e indepedientemente, habían sido dispuestas

otras vías que se dirigían a determinar la verdad de la hipótesis delictiva investigada.

Adviértase que la sentencia deja la "puerta abierta" para entender que, dependiendo del caso y del momento, podría eventualmente recurrirse a esa medida, es decir, a requerir el listado de llamadas salientes y entrantes del teléfono del periodista si no hubiera otros caminos de investigación para averiguar la verdad del caso. Esto significa que la mentada inviolabilidad del secreto de la identidad de la fuente periodística, según surge de este fallo, podría ceder dependiendo del caso judicial y del estado en que éste se encuentre.

Así todo, se visualiza que en tal situación se impone que sea un magistrado quien ordene tal proceder y, en ese caso, el periodista debería evaluar si corresponde impugnarla por las vías judiciales pertinentes.

Jurisprudencia de Paraguay

Jorge Rolón Luna, Maricarmen Sequera Buzarquis con las contribuciones de Katitza Rodríguez y David Bogado (2016) refieren un caso judicial que llegó hasta la Corte Suprema de Justicia de Paraguay en el que se validó la intervención de comunicaciones sin contar con una orden de un Juez obteniendo así un conjunto de metadatos. Es importante destacar que si bien en el caso no surge que se vieran involucrados periodistas, la doctrina que emerge del fallo amerita a reflexionar acerca de que –eventualmente- el día de mañana podría validarse la vigilancia de comunicaciones de un comunicador con su fuente.

En concreto, la resolución judicial fue dictada en la causa que investigó el secuestro y asesinato de Cecilia Cubas, la hija del ex Presidente de la República Raúl Cubas Grau (agosto 1998 – marzo 1999). Cecilia Cubas fue raptada el 21 de septiembre de 2004, cuando un grupo de criminales rodeó su vehículo, a metros de su domicilio en las afueras de la capital Asunción. Cubas fue brutalmente asesinada y posteriormente, hallada muerta el 16 de febrero de 2005.

Los acusados de su secuestro y asesinato de la Sra Cubas habían interpuesto recurso extraordinario de casación, el cual fue rechazado por el Máximo Tribunal. Para tal fin, la Corte Suprema sostuvo que la Fiscalía cumplió todas las garantías procesales y que no hubo violación de las comunicaciones al **solicitar —y obtener— sin orden judicial**, los metadatos de las llamadas telefónicas producidas por los sospechosos autores del secuestro y asesinato. Para fundar tal postura, entendió que el derecho a la inviolabilidad del patrimonio documental y la comunicación privada, protege la comunicación en sí, no así los datos relativos de estas comunicaciones (con quién, cuándo, frecuencia, horarios, entre otros).

La crítica concreta a la conclusión a la que arriba la sentencia es que, al no estar regulado por ley, el Tribunal ha validado un accionar estatal ilegítimo de una autoridad estatal (Fiscal) que vulneró el derecho a la intimidad de las comunicaciones en miras de obtener metadatos.

Concluyen Rolón y Sequera Buzarquis (2016) que tampoco se tomó en cuenta la decisión de la Corte Interamericana de Derechos Humanos sobre el caso contencioso en el que se condenó al Brasil por el uso ilegal de escuchas telefónicas en un proceso penal: la misma Corte señaló que el derecho a la privacidad protege tanto al contenido de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación como los metadatos o datos de tráfico, entendidos éstos como "el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar contenido de la llamada mediante la grabación de las conversaciones"[10].

CONCLUSIONES FINALES

Hemos analizado a lo largo de este trabajo el marco jurídico nacional e internacional así como también las diversas opiniones doctrinarias y algunos antecedentes jurisprudenciales vinculados con la pertinencia o no de que la protección al secreto periodístico deba o pueda ceder cuando los hechos se relacionan con una investigación penal o bien por razones de "seguridad nacional".

A ésta de por sí conflictiva situación sumamos la problemática referida a la vigilancia en las comunicaciones que realizan ciertos Estados sin contar con una orden judicial expresa, lo cual suelen justificar en base al mentado deber de brindar "seguridad" a la ciudadanía en detrimento del derecho humano a la privacidad en las comunicaciones.

Para concluir, debemos hacer una breve referencia a la investigación desarrollada por John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri y Marion Marschalek (2015) del "Citizen Lab" –de la Universidad de Toronto- titulada "Packrat: Siete Años de un Actor de Amenaza en América del Sur". Se trata de un informe de investigación que describe un uso intensivo de malware, phishing y una campaña activa de desinformación en varios países latinoamericanos, incluyendo Ecuador, Argentina, Paraguay, Venezuela, y Brasil. Entre otros casos, se menciona que algunos países han hecho uso del sistema FinFisher que posee una funcionalidad similar al de la empresa italiana Hacking Team, la cual provee un sistema que permite interceptar computadores, videollamadas, correos electrónicos, mensajes instantáneos y contraseñas.

El software empleado por este tipo de sistemas puede eludir el cifrado de los programas informáticos, por lo que es capaz de revisar la comunicación y el registro de llamadas, ver el historial de navegación web, archivos y fotos eliminadas de un dispositivo. Además, puede utilizarse para tomar control del micrófono y de las cámaras integradas del teléfono móvil y usarlos para espiar.

En ese sentido, Shelton (2015) ilustra muy claramente el peligro en el que se encuentran subsumidos los periodistas al ejercer su profesión. Así comenta que entre una de las principales

causas de espionaje en 2006, el periodista del diario The New York Times, James Risen publicó su libro Estado de guerra donde detalla las actividades encubiertas del gobierno de EEUU en guerras en el extranjero.

En un capítulo del libro, Risen reveló que en la era de Clinton la Agencia Central de Inteligencia tenía un plan para sabotear el programa de desarrollo nuclear de Irán de modo que cuente con los modelos defectuosos. Sin embargo, su plan fracasó. En 2008 y 2010, al salir el libro, Risen fue citado ante los Tribunales para declarar sobre el caso a fin de quee revelare sus fuentes, a lo cual se negó a través de una larga serie de apelaciones en la Corte. Sin embargo, el Tribunal Supremo rechazó su apelación en junio de 2014, dejando abierta la posibilidad de que Risen pasara un tiempo en la cárcel por negarse a revelar sus fuentes.

A principios de 2015, la batalla legal de Risen llegó a su fin cuando el Departamento de Justicia decidió que no era más necesario contar con su testimonio. En efecto, el Gobierno había podido identificar que su fuente era un ex agente de la CIA llamado Jeffrey Sterling ¿Que había ocurrido? El Gobierno de EEUU había interceptado correos electrónicos entre Risen y Sterling, quien más tarde fue acusado y condenado en virtud de la Ley de Espionaje, la misma ley que fue aplicada a Chelsea Manning y por los mismos cargos que le son imputados a Edward Snowden.

Como periodista, Risen había tenido una considerable protección legal, pero su supuesta fuente no. Mientras que su sentencia fue significativamente más corta que la pena de prisión de 19 a 24 años que los fiscales del gobierno previeron inicialmente, Jeffrey Sterling todavía deberá pasar tres años y medio en una prisión federal.

Sin dudas esta situación latente de vulnerabilidad a la que en particular se encuentran expuestos las fuentes periodísticas en distintos países del mundo genera un peligro cierto de daño irreparable al derecho humano de recibir, investigar y difundir información de conformidad a la protección que brinda el art. 13 del PSJCR y en particular nuestro art. 43 de la CN al proteger expresamente la preservación de la identidad de la fuente periodística.

En coincidencia con la postura adoptada por el Relator para la Libertad de Expresión ante la OEA, sin duda algunael uso de programas o sistemas de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en una ley, ser verdaderamente excepcional y selectivo, y estar limitado en función a lo estrictamente necesario para el cumplimiento de fines imperativos como la investigación de delitos graves definidos en la legislación. Para tal fin, es vital que las legislaciones del mundo incorporen y apliquen los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

NOTAS

* castelli.sebastian@gmail.com

** Facultad de Periodismo y Comunicación Social UNLP. larrondomanuel@gmail.com.

1. El Mundo. Recuperado de: http://www.elmundo.es/elmundo/2005/08/18/comunicacion/1124361853.html.
2. Ball J. (19 de Enero de 2015). "GCHQ captured emails of journalists from top international media." The Guardian. Recuperado de: https://www.theguardian.com/uk-news/2015/-jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post
3. *Necessary and Proportionate Coalition, Necesarios y Proporcionados (Mayo 2014)* https://necessaryandproportionate.org/es/necesarios-proporcionados.
4. Santa Clara County Super. Ct. No. CV032178 Recuperado de: http://www.internetlibrary.com/pdf/OGrady-Apple-Cal-Crt-App.pdf
5. Corte Interamericana de Derechos Humanos (13 de Noviembre de 1985). Opinión Consultiva Nº5. Recuperado de: http://www.corteidh.or.cr/docs/opiniones/-seriea_05_esp.pdf
6. *Necessary and Proportionate Coalition, Necesarios y Proporcionados (Mayo 2014)* https://necessaryandproportionate.org/es/necesarios-proporcionados
7. Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA (2015, 21 de julio). Comunicado de prensa sobre la adquisición e implementación de programas de vigilancia por parte de Estados del hemisferio Recuperado de: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2
8. Cámara Federal de Apelaciones de San Martín, Sala I, Buenos Aires, Argentina (2 de Mayo de 1996) Revista Jurídica "La Ley" Tomo 1996 C, pág 637
9. Cámara Federal de Apelaciones en lo Criminal y Correccional, Sala II, Buenos Aires, Argentina (28 de Octubre de 2002) Causa n° 19.480 caratulada "Incidente de Thomas Catan en autos n° 14.829/2002" Juzg. Federal n° 11 - Secretaría n° 22 Registro nº 20.377, Publicado en Revista Jurídica "LaLey", 1º/11/02
10. Corte Interamericana de Derechos Humanos (6 de Julio de 2009) (Cecilia Medina Quiroga, Presidenta). Recuperado de: https://web.archive.org/web/20140527113509/http:/www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

REFERENCIAS

Juan Diego Castañeda https://karisma.org.co/es-legitima-la-retencion-de-datos-en-colombia/ pág 10

BADENI, Gregorio. Tratado de Libertad de Prensa, pág. 344, Ed. Lexis Nexis, 2002

CATUCCI, G., Silvana, "Libertad de Prensa. Calumnias e Injurias", p. 99, Ediar, Buenos Aires, 1997

DE LUCCA, Javier Augusto, "El secreto de las fuentes periodísticas en el proceso penal", Ad Hoc, Buenos Aires, 1999

GELLI Maria Angélica, El resaltado nos pertenece; Constitución de la Nación Argentina comentada y anotada, 3º Ed. La Ley, 2005, pág. 515

PIERINI, Alicia, LORENCES, Valentín, TORNABENE, María I., “Hábeas Data. Derecho a la intimidad”, Universidad, Bs. As., 1998, pág. 202

COLAUTTI, Carlos E., “Reflexiones preliminares sobre el “Hábeas Data”, en L.L. 1996-C-917

De Lucca, Javier Augusto, "El secreto de las fuentes periodísticas en el proceso penal", Ad Hoc, Buenos Aires, 1999

EKMEKDJIÁN, Miguel A., “El derecho al secreto de las fuentes de información”, en L.L. 1997-C-666

VANOSSI, Jorge Reinaldo, Disertación pronunciada en el Primer seminario Profesional sobre "Aspectos Jurídicos de la empresa periodística", Buenos Aires, 28 y 29 de junio de 1988 según cita de CATUCCI, Silvana, op. cit.

GOZAÍNI, Osvaldo A. “Hábeas Data. Protección de datos personales”. Rubinzal-Culzoni Editores. Buenos Aires, 2001. Pág. 380

SHELTON MARTIN, “The Role of Corporate and Government Surveillance in Shifting Journalistic Information Security Practices. DISSERTATION. Submitted in partial satisfaction of the requirements for the degree of DOCTOR OF PHILOSOPHY in Information and Computer Science https://mshelt.onl/p/shelton_2015.pdf (pág. 43)

Jorge Rolón Luna, Maricarmen Sequera Buzarquis con las contribuciones de Katitza Rodríguez y David Bogado Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay - TEDIC y Electronic Frontier Foundation está disponible bajo Licencia Creative Commons Reconocimiento 4.0 Licencia Internaciona, Marzo 2016 https://www.eff.org/es/country-reports/Paraguay-ES-final pág 23/26

Scott-Railton John, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek, “Packrat: Seven Years of a South American Threat Actor”, Citizen Lab, Diciembre, 2015, https://citizenlab.org/2015/12/packrat-report/#.Vm81JgRqlvQ.twitter

EJE 2

VIGILANCIA, ESPACIO Y TERRITORIO

CIUDADES INTELIGENTES EN LATINOAMÉRICA, EL CIUDADANO VIGILADO

Resumen: El estudio tiene como tema el análisis comparativo entre soluciones y herramientas *de las llamadas smart cities* en las siguientes ciudades de Latinoamérica: Buenos Aires, Santiago y Río de Janeiro. El trabajo combina distintos estudios de caso buscando analizar las particularidades de cada propuesta en distintos mecanismos (tarjeta *smart* y tarjeta multifunción, cámaras de videovigilancia y sistemas de gestión de transporte público) y cómo opera esta red tecnológica al nivel de vigilancia en las calles y los riesgos para la manutención del anonimato de los ciudadanos. Los ejemplos evidencian cómo los procesos de exclusión y control tradicionalmente presentes en ciudades de Latinoamérica adquieren un nuevo significado y anuncian impactos significativos a partir del concepto de gestión de la ciudad comprendida como máquina y llevan la figura del ciudadano a la de productor de datos que alimentan el propio sistema, con consecuencias directas en cuestiones de privacidad y libertad de expresión en el espacio público.

Palabras clave: Ciudades inteligentes, Privacidad, Vigilancia, Espacio público, Transporte inteligente.

Cidades inteligentes em latinoamerica, o cidadão vigiado

Resumo: O estudo tem como tema a análise comparativa de soluções e ferramentas das chamadas *smart cities* nas seguintes cidades da América Latina: Buenos Aires, Santiago e Rio de Janeiro. O trabalho combina diferentes estudos de caso que procuram analisar as particularidades de cada proposta sobre diferentes mecanismos (cartão inteligente e cartão multifuncional, câmeras de vigilância e sistemas de gestão de transportes públicos) e operação dessa rede tecnológica em termos de de vigilância das ruas e seus riscos para a manutenção do anonimato dos cidadãos. Os exemplos estudados mostram como os processos de exclusão e controle tradicionalmente presentes em cidades da América Latina adquirem um novo significado e anunciam impactos significativos a partir do conceito de gestão da cidade entendida como máquina ao transportar a figura do cidadão à de produtor de dados que alimentam o próprio sistema, com consequências diretas sobre questões de privacidade e liberdade de expressão no espaço público.

Palavras-Chave: Cidades inteligentes, Privacidade, Segurança, Espaço público, Transporte inteligente.

Smart cities in Latin America, the surveilled citizen

Abstract: The study aims to compare solutions and tools of the so called smart cities in the following cities in Latin America: Buenos Aires, Santiago and Rio de Janeiro. The paper combines different case studies seeking to analyze the particularities of each proposal on different mechanisms (smart card and multifunction card, surveillance cameras and systems management of public transport) and how this technology network operates regarding the surveillance in the streets and possible risks for the maintenance of the anonymity of citizens. The examples show how the processes of exclusion and control traditionally present in cities in Latin America take on new meaning and announce significant impacts from the concept of city management understood as a machine and carry the figure of the citizen to the producer of data that feed the system itself, with direct consequences on privacy issues and freedom of expression in the public space.

Keywords: Smart cities, Privacy, Surveillance, Public space, Smart transportation.

RAQUEL RENNÓ*
VALERIA MILANES**
PAZ PEÑA***
PATRICIO VELASCO****

En los países emergentes, el discurso de la insuficiencia de las ciudades toma fuerza; estamos frente a una gran masa informe que debe ser controlada para garantizar la seguridad y el buen funcionamiento de los flujos. Sin embargo, algunos ejemplos dejan claro cómo las propuestas de *smartización* de la ciudad pueden contribuir directamente a expandir y no resolver las ya profundas diferencias económicas y sociales entre estos contextos. Sai Balakrishnan, en el artículo *How smart cities will force the poor out* realizada por Devika Kohli (2015), afirma que "si el gobierno llega a construir 100 ciudades inteligentes prometidas en India, pero no hacen nada para aliviar la pobreza y la precariedad de los servicios en estas áreas puede incluso generar una situación volátil. Las formas visibles de desequilibrio espacial generan desconfianza social e incluso la violencia".

De cámaras de reconocimiento facial hasta postes que detectan la presencia de personas en la acera, los dispositivos de control automático de las funciones de los servicios urbanos se están convirtiendo en parte del paisaje urbano, lo que nos lleva a cuestionar si estas nuevas tecnologías sirven como una alternativa a las tensiones y los conflictos en la ciudad o simplemente refuerzan los ya presentes sistemas de exclusión. Por lo tanto, es necesario cuestionar las suposiciones implícitas sobre las tecnologías además de la seguridad, la comodidad y la facilidad que parecen ofrecer.

Las empresas, incluso las de tecnología continúan trabajando en un proceso que involucra producción y consumo de arriba hacia abajo. Como consumidores, los ciudadanos son informados de las soluciones sólo después de que se adoptan y se ven limitados a elegir entre las opciones predeterminadas en un menú. La invisibilidad de los procesos y su complejidad alejan a los ciudadanos de los procesos que generan el espacio público, en el que sólo son "invitados" a colaborar mediante el envío de más datos al sistema previamente impuesto.

¿Qué significa esto en un momento en que la economía de los datos es la base de funcionamiento de las soluciones de tecnología? En el caso del poder privado, los intereses de lucro no se limitan simplemente a proporcionar soluciones de ciudades inteligentes. La adquisición de estos productos no sella el final de una transacción comercial, sino el comienzo de una larga colaboración con el gobierno en el que el individuo ya no es sólo un usuario sino que también toma la figura de generador de datos (e ingresos) para las empresas. Si el sistema tiene como objetivo la tecnología y no la demanda y propone soluciones generalizantes, puede generar riesgos en el éxito del proyecto como un todo (Nemet, 2009 y McDonalds, 2000). Es importante contar con un modelo que dé a los ciudadanos una voz activa sobre su movilidad en lugar de ponerlos en la posición de testeadores de un sistema tecnológico.

TARJETA MULTIFUNCIÓN EN BUENOS AIRES, UN PASO MÁS HACIA LA CIUDAD INTELIGENTE

El marco de una convocatoria global denominada Quantified Society: Examining the Consequences of Algorithmic Decision Making for Open Societies[1], ADC llevó adelante una investigación que nos permitió incursionar en la investigación de técnicas de Big Data, uso algorítmico para la toma de decisiones, minería de datos. Esta investigación fue publicada en Octubre de 2015.

El caso de estudio fue la tarjeta VOS[2], que es una iniciativa del Gobierno de la Ciudad Autónoma de Buenos Aires, capital de Argentina, que además de permitirnos explorar las diversas técnicas de big data, sus implicancias y repercusión en derechos como el de la privacidad, nos puso también frente a la figura de la ciudad inteligente.

La tarjeta VOS es multifunción y permite a los habitantes, visitantes regulares e incluso a los turistas realizar diferentes tipos de tareas vinculadas a la gestión administrativa del gobierno de la ciudad, como el sistema de bicicleta urbano, cobertura local de salud, prestaciones sociales, y tiene previsto incluir el acceso al subte el almacenamiento de la historia clínica de los pacientes de los centros de salud dependientes del gobierno local. Pero también permite acceder a descuentos en la compra de productos y/o servicios en diferentes negocios de la ciudad, que nada tienen que ver con la gestión estatal. Desde el lanzamiento de la tarjeta en noviembre de 2013 hasta el mes de agosto de 2015 se entregaron 314.008 tarjetas.

La tarjeta VOS es uno de los tantos proyectos encarados por la Subsecretaría de Ciudad Inteligente, dependiente del Ministerio de Modernización de la Ciudad, facultado para diseñar e implementar políticas de incorporación y mejoramiento de los procesos, tecnologías, infraestructura informática, y sistemas y tecnologías de gestión del Gobierno de la Ciudad. En ese marco, la tarjeta VOS resultó ser el vehículo idóneo para producir un flujo de información segmentada para la disposición inteligente de los beneficios, promociones, descuentos y servicios que se le proveerán a los futuros usuarios del Programa, permitiendo a los mismos utilizar servicios y disfrutar de beneficios de una manera fácil, ágil y segura, sean éstos provistos por el Estado o por privados.

Para solicitar la tarjeta VOS, el interesado debe suministrar online una serie de datos, algunos de carácter obligatorio (tipo de documento, número, nombre, apellido, fecha de nacimiento, género, ocupación, nacionalidad, provincia, localidad, correo electrónico, sede de retiro de la tarjeta) y otros no obligatorios (estado civil, clave de identificación tributaria o laboral, calle, altura, código postal, teléfono fijo, teléfono móvil).

Como en la mayoría de las suscripciones efectuadas online, los Términos y Condiciones suelen ser el único "contrato" entre las partes, en este caso, entre el usuario de la tarjeta y el Gobierno de la Ciudad. Sin embargo, en el curso de nuestra investigación detectamos una serie de aspectos que llamaron nuestra atención, en algunos casos por su inconsistencia y en otros casos por parecernos muy débiles los recaudos adoptados respecto de una adecuada protección de datos personales. Por ejemplo:

- Se refiere que la base de datos que contenga los datos del suscriptor y la información relativa a las transacciones realizadas con la tarjeta estará registrada en la Dirección Nacional de Protección de Datos Personales, cuando por una cuestión de jurisdicción y tipo de base (base pública), corresponde que la misma esté registrada en el Centro de Protección de Datos Personales dependiente del gobierno local, no nacional.

- la tarjeta **VOS** está apoyada en una dinámica de explotación de información, creación de perfiles de usuario y sistemas de recomendación.

- la tarjeta **VOS** trata o puede transferir la información contenida en su base de datos, a sus agentes y/o a los Establecimientos Adheridos con fines publicitarios, promocionales y comerciales y conocer los intereses y/o afinidades del suscriptor

- el Gobierno local está recolectando una significativa cantidad de información a través de las relaciones que el uso de la tarjeta genera entre Gobierno/usuario, usuario/prestador, Gobierno/ prestador.

- La tarjeta contiene tecnología RFDI, que permite leer o grabar información que corresponde a la actividad específica de lo que se está trabajando sobre ellas; aunque no contiene tecnología de geolocalización. La tarjeta almacena información tanto en la estructura RFID como en la banda magnética, sin contar con mayores recaudos de seguridad.

La situación descrita nos permitió establecer algunos retos y desafíos para nuestras ciudades, tales como la ausencia de expertos especializados atento la novedad del tema, la falta de presupuesto para el desarrollo de tecnologías de big data y tecnologías derivadas.

También pudimos detectar como obstáculo la adecuada integración de estas tecnologías con los procesos de gestión por parte del estado, ya que para una apropiada inclusión de big data deben cuidarse al menos cuatro dimensiones: volumen, variedad, velocidad y valor. A este modelo de las cuatro V, agregamos la dimensión conocida como Veracidad, relativa a la calidad de los datos.

En nuestro caso de estudio, hemos advertido dos problemas más: la falta de regulación legal sobre el tema y, asimismo, la cuestión de la privacidad y protección de datos personales.

En este sentido, la privacidad de la información se ve vulnerada por el fenómeno big data si no se toman los recaudos de seguridad suficientes y si no se anonimiza y encripta la misma. Y esto podría dar lugar, según surge de la investigación que efectuamos, a una nueva dimensión a tenerse en cuenta, a una nueva V: la de Vulnerabilidad de derechos.

RIO DE JANEIRO: HOUSTON, WE HAVE A PROBLEM

Mientras varios proyectos de smart cities e Internet de las Cosas anuncian su apuesta a la ubiquidad, el ejemplo más conocido de proyecto de smart city en Brasil se estructura en la sala de control, conocida desde los años 20 como una estructura de monitoreo de industrias. Mattern (2013) va más allá y relata que Uffizi, construida en el siglo 16, ya sería un gran edificio para centralización y procesamiento de datos sobre la ciudad. El Centro de Operaciones (COR) inaugurado en la ciudad de Río de Janeiro en ocasión de la Copa Mundial de Fútbol de 2014 celebra el aumento de las 93 cámaras instaladas cuando inició sus operaciones a las 530 actuales. Imágenes de la sala de control aparecen con frecuencia en los medios de comunicación como símbolo de una propuesta eficiente de gestión moderna de la ciudad, no por casualidad recordando lo que se ve en películas de aventuras espaciales.

Las funcionalidades se desarrollaron a partir del API de Google Earth y la empresa desarrolladora IPNET Soluções recibió el sello de socia premier de Google (Google's Enterprise Maps for Business Premier Partner). Concesionarios, organismos públicos y la misma población (por medio de la

aplicación Olhos da Cidade -Ojos de la Ciudad, desarrollada específicamente para la alcaldía de Río) colaboran enviando al COR datos sobre tráfico, incendios, lluvias, manifestaciones, etc., a pesar de que los usuarios solo pueden acceder a boletines y análisis que el COR pone a disposición. Otros productos de Google, como Waze y Hangout, también forman parte del paquete de la alianza de la alcaldía como apoyo a los usuarios. Allí tenemos problemas de acceso unidireccional a los datos, ya que mientras la central tiene acceso a todo, el usuario depende de las alternativas que el COR decide publicar. También debemos considerar la limitación de las interfaces de estas aplicaciones -solo se pueden seguir los caminos ofrecidos por el servicio, es decir, el usuario se adapta al formato previamente diseñado- y del mapa de Google, ya cuestionado por muchos por sus contratos de uso restringido, la poca transparencia en cuanto al acceso y administración de los datos y cuyas alternativas abiertas, como OpenStreetMaps, han demostrado ser bastante más eficientes para compartir y utilizar datos de manera horizontal en la relación entre el poder público y la sociedad civil.

Otro proyecto aclamado por los medios de comunicación debido a que atrae grandes inversiones a la ciudad y revitaliza el área portuaria es el Porto Maravilha (Puerto Maravilla). Uno de los mayores proyectos en ejecución en la ciudad, y parte del proyecto Ciudad Olímpica, el Porto Maravilha además de los principales equipamientos culturales del área, como el Museo de Arte de Río (MAR) y el Museo del Mañana, son objeto de grandes polémicas. Las acusaciones varían desde la privatización del espacio público a la elitización de lo que se concibe como cultura en el área (asumiendo de forma equivocada que allí nunca hubo un tejido cultural antes de la construcción de los museos), además de erradicaciones violentas que los habitantes pobres de la zona vienen sufriendo desde los preparativos para la Copa.

Grandes empresas multinacionales y los principales canales de comunicación masiva vienen apoyando la opción de Río por las soluciones smart cities, lo que muestra visiones bastante divergentes sobre lo que se debe priorizar en la ciudad. La ciudad más conectada del país es, por ejemplo la que altera el trayecto de autobuses para evitar que haya una conexión directa entre los suburbios y las playas de la zona sur, la área más rica de la ciudad. Las soluciones smart no se limitan a macroproyectos de impacto simbólico como los antes expuestos. El gobernador del Estado, por ejemplo, ya anunció un proyecto de ley que obliga a la identificación de los usuarios del Bilhete Único (Boleto Único, una tarjeta que permite que el usuario realice hasta 4 viajes de autobús durante 3 horas seguidas pagando solamente un pasaje) a través de biometría con el objetivo de reducir los fraudes en el uso del beneficio.

SANTIAGO Y LA DEFENSA POR UNA CIUDAD ESTÚPIDA

Santiago, con poco más de seis millones de habitantes y siendo una de las ciudades más desiguales del continente (Martínez Villareal, 2010), tiene tareas aún no resueltas respecto a urbanismo, infraestructura, vivienda, transporte, entre tantas otras. Para eso, nos dicen, es necesario emigrar hacia el modelo de Smart City, donde las tecnologías digitales emergen como facilitadoras de una ciudad más eficiente, que sería capaz de integrar los intereses de la ciudadanía en general,

el sector privado y la academia, y donde el Estado -como desde la dictadura cívico-militar de Pinochet en Chile- tendrá un rol subsidiario.

Las políticas digitales en Chile son parte de una tradición neoliberal, donde el Estado toma el rol subsidiario, es decir, no asume acción donde supone que los privados tendrán iniciativa e incentivos unilaterales para desplegar su presencia. Así, desde el primer documento sobre estrategia digital con el gobierno de Eduardo Frei Ruiz-Tagle hasta el día de hoy, ha sido el mercado -con una lógica puramente economicista- el que ha liderado problemas de política pública digital, como la infraestructura en tecnología, el acceso a internet y, últimamente, el uso más sofisticado de las tecnologías y las nuevas industrias de servicios tecnológicas.

Los planes de ciudades inteligentes parecen seguir esa tradición. Así se observa, por ejemplo, en la "Estrategia de Ciudad Inteligente para el Transporte. Chile 2020", realizada por la Subsecretaría de Transportes y presentada en agosto del 2014. En ella, se adelanta la importancia de la participación no solo del gobierno en la construcción de una ciudad inteligente, sino también de la academia, los ciudadanos y el sector privado, como si estos -concebidos en un laboratorio o, como parece que se prefiere decir en jerga de start-up, "lab"- tuvieran el mismo poder. En este contexto, las controversias propias de un organismo complejo como la ciudad surgen desafectadas de su historia, sus intereses, pasiones y resistencias: tan neutras y universalistas como el discurso de "los tecnócratas" que busca maximizar la eficiencia y que, con ello, muchas veces no hacen sino reproducir su propia ideología:

> "Dicho cambio, se sustenta a partir de un reconocimiento: el que, a pesar de todos los esfuerzos que se han hecho y se harán bajo la lógica sectorial, el Estado no podrá resolver la complejidad de los problemas que surgen en las ciudades. Esta "ceguera cognitiva" nos ha llevado a perder de vista nuestro foco en las personas y el territorio y sobre todo a entender que se requiere, como condición de éxito, la colaboración activa de los diversos actores".(Subsecretaria de Transportes, 2014, p.16).

Cuando en la construcción de las ciudades se niega el conflicto -o más bien el conflicto se reduce al estorbo del Estado y la mera falta de coordinación entre actores-, las soluciones a los problemas pueden ser perfectamente diseñadas a la distancia de un clic. Pareciera ser, de este modo, que la emergencia de las ciudades inteligentes supone, paradójicamente, diagnósticos algo estúpidos.

LA CIUDAD PARTICIPATIVA VS. LA CIUDAD VIGILADA

La complejidad de la ciudad debe ser entendida más allá de un sistema generado por las empresas de tecnología, controlado por los intereses del gobierno. Esto no es rechazar las tecnologías en su relación con la ciudad. La presencia digital en la cultura ya muestra que el espacio urbano está impregnado por ella. La cuestión que se plantea es qué tipo de tecnología queremos, teniendo en cuenta que no existe un concepto general y único de tecnología, y esto está directamente relacionado con la cuestión de qué ciudad queremos. Si las ciudades inteligentes son simplemente el uso de productos de las principales compañías de tecnología que asignan una nueva capa de control de los ciudadanos y una mayor privatización del espacio público, entonces el resultado

será la ciudad al servicio de la tecnología con la reducción continua de la libertad individual. Ellos serían traducidos a la operación de los problemas de ciudades inteligentes ya vistos en las compañías propietarias de TI: poca o ninguna transparencia en la gestión, el acceso y el intercambio de datos, contratos restringidos y presentación al ciclo de obsolescencia impuesta por la industria.

Las preguntas básicas que estos sistemas de datos que se generan en el nombre de la eficiencia y la seguridad suscitan deben ser discutidos ampliamente por la sociedad civil. ¿Esos datos se pueden recoger en la ciudad y sus ciudadanos? Esto es técnicamente posible, pero además deben considerarse sus implicaciones políticas, éticas y legales. ¿Cómo deben ser procesados, almacenados, cuál es el nivel y el alcance y el acceso a estas posibilidades de datos? ¿Qué leyes o necesitan ser pensado para regular estas máquinas de generación de datos sobre la ciudad y la población? Hasta ahora, estas discusiones no se han llevado a cabo con la amplitud y la profundidad requerida, ya que muchos ciudadanos desconocen por completo los proyectos de ciudades inteligentes que se han implementado en sus propias ciudades. Con las ciudades inteligentes se convierte en imprescindible que la población, ahora parte de la producción masiva de datos de una estructura vertical, participe de la discusión que se refiere a la tecnología que queremos con la ciudad que queremos.

NOTAS

* Coding Rights y profesora doctora adjunta UFRB, Brasil. Contacto: raquelrenno@codingrights.org

** Asociación por los Derechos Civiles, ADC, Argentina. Contacto: vmilanes@adc.org.ar

*** Consultora independiente, Chile. Contacto: paz@pazpena.com

**** Derechos Digitales, Chile. Contacto: patricio@derechosdigitales.org

1. Para más información ingresar em línea a: http://mediademocracyfund.org/quantified-society-grants-announced/
2. Análisis completo del caso de estudio (en inglés): https://adcdigital.org.ar/wp-content/uploads/2016/02/Research-Report.pdf

REFERENCIAS

Ackerman, S.; Thielman, S. (9 de febrero de 2016) US intelligence chief: we might use the internet of things to spy on you. *The Guardian*. Recuperado de: https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

Astudillo, D. (27 de enero de 2016) Control de identidad: aprueban que policía pueda retener por una hora a menores. *La Tercera*. Recuperado de: http://www.latercera.com/noticia/control-de-identidad-aprueban-que-policia-pueda-retener-por-una-hora-a-menores/

Campusano, R. (11 de marzo de 2015) Protección de datos personales: ¿compromiso real del Gobierno?. *Derechos Digitales*. Recuperado de: https://www.derechosdigitales.org/8453/proteccion-de-datos-personales-en-chile-buena-iniciativa-del-congreso-nacional-compromiso-real-del-gobierno/

Dempsey, P. (2008) Privacy issues with the use of smart cards. *Legal Research Digest, 25*. Transit Cooperative Research Program.

EFE. (21 de novembro de 2013). Rio vence premiação de cidade mais inteligente do mundo. *Revista Exame*. Recuperado de: http://exame.abril.com.br/brasil/noticias/rio-vence-premiacao-de-cidade-mais-inteligente-do-mundo

Endesa. (11 de julio de 2011) Endesa proyecta la primera "ciudad inteligente" de Iberoamérica. Electricidad, *La revista Energética de Chile*. Recuperado de: http://www.revistaei.cl/2011/07/11/endesa-proyecta-la-primera-ciudad-inteligente-de-iberoamerica/

G1 (10 de dezembro de 2015) Lei da biometria para usuários do Bilhete Único é sancionada no RJ. *Jornal O Globo*. Recuperado de: http://g1.globo.com/rio-de-janeiro/noticia/2015/12/lei-da-biometria-para-usuarios-do-bilhete-unico-e-sancionada-no-rj.html

Gorelik, A. (1998) *La grilla y el parque: espacio público y cultura urbana en Buenos Aires, 1887-1936*. Buenos Aires: Universidad Nacional de Quilmes.

Huber, J. (23 de octubre de 2013) La visión de telefónica de una ciudad inteligente. *IoT Telefónica*. Recuperado de: https://iot.telefonica.com/blog/la-vision-de-telefonica-de-una-ciudad-inteligente

Innovación CL. Cisco se suma a proyecto "Santiago Ciudad Inteligente". *Innovación CL*. Recuperado de: http://www.innovacion.cl/2014/11/cisco-se-suma-a-proyecto-santiago-ciudad-inteligente/

Jaramillo, P. (12 de septiembre de 2016) Registro público de evasores del Transantiago: más problemas que soluciones Santiago. *Derechos Digitales*. Recuperado de: https://www.derechosdigitales.org/10486/registro-publico-de-evasores-del-transantiago-solucion-o-problema/

Kohli, Devika. (06 de julio de 2015) How Smart Cities Will Force The Poor Out. *YKA*. Recuperado de: http://www.youthkiawaaz.com/2015/07/smart-cities-keep-the-poor-out

Laranja, Cristina. (2011) A arte de provocar ruínas: especulações na Zona Portuária. *Revista Nômade Brasil Global*, Universidade Nômade. Recuperado de: http://www.revistaglobalbrasil.com.br/?p=697

McDonough, Meghan (28 de julio de 2013). Google map maker vs. Openstreetmap: which mapping service rules them all? Digital Trends. *Technology News and Products Reviews.* Recuperado de: http://www.digitaltrends.com/computing/google-map-maker-vs-openstreetmap-id-editor/

Mattern, S. (Noviembre de 2013) Methodolatry and the Art of Measure, the new wave of urban data science. *Places Journal*. Recuperado de: https://placesjournal.org/article/methodolatry-and-the-art-of-measure/

Martínez Villareal, J. (19 de noviembre de 2010) Las ciudades mas desiguales de latinoamerica. *Plataforma Urbana*. Recuperado de: http://www.plataformaurbana.cl/archive/2010/11/19/las-ciudades-mas-desiguales-de-latinoamerica/

Mcdonald N. (2000) *Multipurpose smart cards in transportation: benefits and barriers to use*. University of California Transportation Research Center 630, p. 27

Nemet, G.F., (2009) Demand-pull, technology-push, and government-led incentives for nonincremental technical change. *Research Policy*, 38(5), pp.700–709.

Payão, Felipe. (3 de agosto de 2015) Smart Cities: Rio de Janeiro é a cidade mais conectada do Brasil. *Revista Tec Mundo*. Recuperado de: http://www.tecmundo.com.br/internet/84148-smart-cities-rio-janeiro-cidade-conectada-brasil.htm

Peña, P.; Velasco, P. (3 de março de 2016) En defensa de las ciudades estúpidas. Boletín Antivigilancia 13 Ciudades Inteligentes y la vigilancia. *Coding Rights*. Recuperado de: https://antivigilancia.org/es/2016/03/santiago-smart-city-en-defensa-de-las-ciudades-estupidas/

Poole, S. (17 de diciembre de 2014) The truth about smart cities: 'In the end, they will destroy democracy'. *The Guardian*. Recuperado de: https://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase

Rama, A. (1984) La ciudad letrada. Mexico: Ediciones del Norte.
Rolnik, Raquel. (20 de abril de 2012) Copa e Olimpíadas: dossiê lançado ontem no Rio denuncia violações de direitos humanos. *Blog da Raquel Rolnik*. Recuperado de: https://raquelrolnik.wordpress.com/tag/remocoes-forcadas/

Ruiz, C. (17 de agosto de 2015) Las Condes y Lo Barnechea niegan el derecho a la privacidad de sus vecinos. *Derechos Digitales*. Recuperado de: https://www.derechosdigitales.org/9256/las-condes-y-lo-barnechea-niegan-el-derecho-a-la-privacidad-de-sus-vecinos/

Subsecretaría de transporte (2014) *Estrategia de Ciudad Inteligente para el transporte, Chile 2020*. Recuperado de: http://www.ciudadesinteligentes.cl/wp-content/uploads/2015/09/estrategia_uci.pdf

Takahashi, H. (14 de agosto de 2014) ¿Cuál es la ruta para una ciudad inteligente? *Forbes Mexico*. Recuperado de: http://www.forbes.com.mx/cual-es-la-ruta-para-una-ciudad-inteligente/

Uchoas, Leandro. (22 de julho de 2011) Porto é maravilha, mas para poucos. *Brasil de Fato*. Recuperado de: https://www.brasildefato.com.br/node/6908/

Veerman, Olaf. (15 de abril de 2015) An OpenStreetMap for the government. *Development Seed*. Recuperado de: https://developmentseed.org/blog/2015/04/15/openstreetmap-for-government/

TROPICALIZING SURVEILLANCE: HOW BIG DATA POLICING "MIGRATED" FROM NEW YORK TO SÃO PAULO

Abstract: The present article is about a new "intelligent" policing scheme which was developed in New York and is now being implemented in São Paulo. Originally designed to prevent terrorist attacks, the system will predominantly be used to combat theft and violent street crime in São Paulo. Based upon extensive databanks and specialized algorithms, the program promises a more effective, more efficient, and potentially predictive form of policing. The present piece of work analyzes first how the system emerged in New York, as the result of an "anti-terrorist" public-private partnership. In a second step, the aim is to come up with a critical evaluation of the algorithmic mode of governmentality which is at the core of such programs, and which defines new, preemptive approaches to public security. Finally, the article will develop some preliminary ideas concerning the system's "tropicalization", that is: its socio-technical adaptation to the Brazilian context – with a particular emphasis upon the emergent and non-linear dynamics which unfold in such kinds of "translations".

Key words: Big data policing, Algorithmic governmentality, Postcolonial science, technology studies.

Tropicalizando a vigilância: Como o policiamento big data "migrou" de Nova York para São Paulo

Resumo: O presente artigo trata dum novo sistema de policiamento "inteligente" que foi desenvolvido em Nova York e que agora está sendo implementado em São Paulo. Originalmente um programa para previr ataques terroristas, em São Paulo o sistema será utilizado para combater roubos e crime violento no espaço público. Baseando-se em bancos de dados abrangentes e algoritmos especializados, o programa promete um policiamento mais efetivo, mais eficiente, e potencialmente preditivo. O presente trabalho analisa primeiro como o sistema surgiu em Nova York, como resultado dum parceiro público-privado "antiterrorista". Num segundo passo, se propõe uma avaliação crítica da governamentalidade algorítmica que age detrás esse tipo de programas, e que vem a definir novas abordagens preemptivas à segurança pública. Finalmente, desenvolve-se algumas ideias preliminares respeito à "tropicalização" do programa, ou seja: à adequação sócio-técnica ao contexto brasileiro. Nesse sentido, coloca-se uma ênfase particular nas dinâmicas emergentes e não lineares que se manifestam nessas "traduções".

Palavras chave: Policiamento big data, Governamentalidade algorítmica, Estudos de ciência e tecnologia pos-coloniais.

Tropicalizando la vigilancia: Como el policiamiento big data "migró" de Nueva York a San Pablo

Resumen: El presente artículo trata de un nuevo sistema de policiamiento "inteligente" que fue desarrollado en Nueva York y que ahora está siendo implementado en San Pablo. Originalmente un programa para prevenir ataques terroristas, en San Pablo el sistema será utilizado para combatir robos y delincuencia violenta en el espacio público. Basándose en bancos de dados extensos y algoritmos especializados, el programa promete un policiamiento más efectivo, más eficiente y potencialmente predictivo. El presente trabajo analiza primero como el sistema surgió en Nueva York, como resultado de una alianza público privada "antiterrorista". En un segundo paso, se propone una evaluación crítica de la gubernamentalidad algorítmica detrás de tal sistema, y que viene a definir nuevos abordajes preemptivos hacia la seguridad pública. Finalmente, se desenvuelve algunas ideas preliminares acerca de la "tropicalización" del programa, o sea: de la adaptación socio-técnica al contexto brasileño. En ese sentido, se mira particularmente por las dinámicas emergentes y non-lineares que se desdoblan en tal "traducciones".

Palabras Clave: Policiamento big data, Gubernamentalidad algorítmica, Estudios de ciencia y tecnología pos-coloniales.

CLAUDIO ALTENHAIN*

TOTAL DOMAIN AWARENESS: NEW YORK CITY "LEADS THE PACK"

Two years ago Geraldo Alckmin, governor of São Paulo, announced a bold anti-crime measure: his administration had acquired the license of the *Domain Awareness System* (DAS), the state-of-the-art big data policing scheme operated by the New York Police Department. Amongst the features highlighted in the advertisements – the acquisition formed an integral part of Alckmin's re-election campaign – was an automatized recognition of "suspicious" situations, such as people walking between cars in a traffic jam or somebody trying to enter private property while wearing a motorcycle helmet. The tool was thus introduced as a revamped, automatized embodiment of actuarial justice and preemptive efficiency (Harcourt, 2007). Ironically enough, in São Paulo the DAS goes by the name of *Detecta,* even though the promises it was sold with have very little in common with the clue-based, reconstructive style of investigation which is at the core of a detective's work (Boltanski, 2014; Ginzburg & Davin, 1980): given its future-oriented as well as risk-based approach to crime, *Preventa* or *Predicta* would most certainly have been more adequate monikers for the "smart" policing scheme which is currently being implemented in Brazil's major city.

For a globally oriented criminological research agenda, DAS/*Detecta* is a stimulating case – crucially so because, as mentioned above, the system "migrated" from one policing context into another. Inaugurated in 2012 by Michael Bloomberg, then Mayor of New York City, the scheme was announced as "the most sophisticated camera system that you will see around the world". [1] Its promises were compelling – or, as others would sustain, disturbing: a tightly knit network of digital CCTV and radiation scanners would cover the better part of Lower and Midtown Manhattan and keep it under permanent surveillance; geospatial, criminal justice, and emergency services' data banks would be merged and analyzed by means of customized algorithms; and the information would appear in real time on an intuitive user's interface which could be accessed in the command center as well as by police officers on the beat (New York City, 2012).

The DAS emerged out of a public-private partnership between the New York Police Department and Microsoft in which the latter "handled the coding and system architecture, and the NYPD set out the system requirements" (ibid.): software developers would gather with police officers in order to find out how best to "translate" their everyday working routines into a tailor-made ICT application. In fact, this approach dovetails with the company's rhetoric of "empowering" governmental agencies to better address their respective "challenges" and to "achieve more"[2] – without specifying, nota bene, what this "more" might actually consist in. From such a perspective, it is the client who defines the respective institutional objectives, and Microsoft who provides the algorithmic infrastructure necessary to attain them more efficiently. Code is presented as neutral: aggregate institutional knowledge, "smart" insofar as it facilitates the correlation of data and enables accelerated modes of access, but not endowed with any kind of agency of its own. Consequently, the company abstains from sensationalist rhetoric and leaves the bragging to governmental agencies: Bloomberg, standing in for the whole NYPD, boasted

that "we're not your mom and pop's police department any more. We are in the next century; we are leading the pack."[3]

Significantly, the city government left little doubt concerning the DAS's raison d'être: Even though it was introduced as a tool which would support the NYPD in fighting crime, the risk of further terrorist attacks (and the system's capacity to prevent them) was perpetually evoked. Consequently, the program was first presented to a larger audience in the public-private Lower Manhattan Security Command Center, "our city's state-of-the-art anti-terrorism, counter-terrorism coordination center", as Bloomberg did not fail to point out on the very same occasion .[4] Likewise, the DAS's "Public Security Privacy Guidelines" state that "[g]iven the ongoing threat of terrorist attack, the Domain Awareness System is an important part of the NYPD's integrated approach to providing protection for those who work in, live in, and visit New York City" (New York Police Department, n.d.).

Semantically and functionally resembling the controversial (and now officially defunct) "Total Information Awareness" doctrine adopted by the US government in 2003, the DAS provides a viable example of David Lyon's (2004: 307) affirmation concerning post-9/11 surveillance measures – namely that "they extend, enhance, or place in an unfamiliar context technologies whose promise has been advertised for some time or whose use has been proven in some other context": databases, surveillance cameras, and algorithms were around long before the terrorist attacks; however, the unique assemblage they formed in New York City was enabled by a particular event and the specific governmental rationalities it was met with. In addition to this, the DAS might also be described as a spin-off emerging from the US Armed Forces' "Revolution in Military Affairs" (RMA) including its pivot to urban warfare and the concomitant prominence of "real-time situational awareness" (Graham, 2006: 253) – a strategic readjustment which, while chronologically preceding the United States' "War on Terror", gained a lot of momentum during the military interventions in Afghanistan and, especially, Iraq (ibid.: 251; Graham, 2011).

While efficacy concerning their stated aim is hard to determine – mostly due to the scarce occurrence of terrorist attacks in Western metropoles –, it is amply known that the consequences of urban "counter-terrorism" measures typically affect those groups and individuals unwilling or unable to fit within the increasingly streamlined, cleaned-up, and depoliticized version of public space which has become characteristic of contemporary "global cities" as well as of those municipalities aspiring a similar status. Again, while these developments are certainly not new – consider Davis' (1990) polemic treatise on "Fortress LA" –, there is clear evidence that the accelerated securitization[5] of major urban centers since 9/11 coincides with the corporate interest of the financial as well as the real estate industry and, consequently, has further reinforced processes of socio-economic segregation and the "citadelization" of urban space (Marcuse, 2004: 264). In New York City, this configuration became notorious when FBI documents revealed a veritable "joint venture" between public law enforcement and intelligence agencies, private security forces, and even various investment banks when it came to violently cracking down

upon Occupy Wall Street – all under the banner of preventing potential terrorist activities (Wolf, 2012). Significantly, there were even reports according to which the abovementioned Lower Manhattan Security Command Center – originally established with a $ 10 million grant from the Department of Homeland Security (New York City, 2007) – was permanently staffed with employees of Goldman Sachs, JP Morgan, and other private banks (Martens, 2012). This dubious heritage of public-private "security partnerships" in New York City must not be ignored when further analyzing the DAS and, subsequently, the implementation of *Detecta*.

BIG DATA AND PUBLIC ORDER: SOME REMARKS ON ALGORITHMIC GOVERNMENTALITY

If we are to believe its advocates, the DAS's main novelty consists in the fact that it is a "smart" solution promising, most crucially, *integration* (of a broad range of different databases, cameras, and electronic sensors) as well as *automation* (of certain routines which, hitherto, had to be performed manually) and, therefore, to turn policing into a much more efficient endeavor. There is, however, a tendency to underplay that the kind of "intelligence" which is at stake here differs substantially from the retrospective mode of reasoning which is commonly associated with police investigations – although, to be fair, this (mis)representation of contemporary policing has been debunked way before the advent of sophisticated predictive software tools (Ericson & Haggerty, 1997). Nonetheless, big data policing is novel insofar as it is based upon the algorithmic parsing of vast amounts of data which could impossibly be sifted through by officers made of flesh and blood; the software is therefore able to establish "non-obvious relationship[s]" (Perry et al. 2013: 2) among the information it deals with and, beyond that, to extrapolate likely futures to act upon. Big data policing thus shares in the performative logic of pre-emption; its "algorithmic architectures" entail "not only epistemological resources but also ontological sources" (Clough and others, 2015: 146).

Far from being a mere representational tool enabling law enforcement agencies to fulfil their tasks in a more efficient and, therefore, "smarter" way, DAS/*Detecta* might thus be described in terms of the famous analysis provided by Scott (2008): making reality legible for governmental reasons is not necessarily limited to streamlining the categories by and along which it is conceived; more often than not, it actually entails a "normalizing" intervention upon the object of government itself. Meanwhile, the main difference between the disciplinal logic of Scott's "authoritarian high modernism" (Scott, 2008: 87) and contemporary "advanced liberal" governmentality (Rose, 1999), especially after its "datalogical turn" (Clough and others, 2015), is that the latter abstains from making its substrate "fit into" a set of idealized, often binary categories; instead, its yardstick emerges as "an interplay of differential normalities" (Foucault, 2009: 91) from the factual knowledge it holds about its subjects. And while Foucault's concept of a liberal biopolitics was, not least, inspired by the early-modern proliferation of scientific knowledge and its impact upon the art of government, it may be stated that the automated, permanent, and "distributed" (Bruno, 2013: 17) production of data to be witnessed since the past decade represents nothing less than

a quantum leap towards an even more thoroughly "empirical" – and, therefore, startlingly post -ideological – kind of governmentality.

Government would, in this sense, have lost its interest in simplification; meanwhile, the kind of information which used to be discarded as "noise" would have gained center stage as the locus of reality-in-becoming (Clough and others, 2015: 153), corresponding to a shift of governmental focus from the actual towards the potential and towards the pre-emptive temporality of the future perfect: "it will (not) have been". It is not least for this reason that algorithmic governmentality can afford to be lenient with "the irregularities, contradictions, and incoherences" of its subjects (Rouvroy & Berns, 2010: 94); strictly speaking, it does not even care about them as it "prehends" (Clough and others, 2015: 153) social reality on a level which is simultaneously supra- and infra-individual. What this kind of governmentality enacts or performs is, then, a pre-emptive domestication of potential actualities in all domains where it is deployed – a mechanism which can be theorized, but not apprehended insofar as it literally attempts to govern the present from the future. It is in this sense that Microsoft's rhetoric is misleading: far from being a simple means to achieve an end more efficiently, big data does have an eminent – and that is: qualitative – impact upon the way power is exercised in contemporary societies.

However, it has to be conceded that, in practice, the algorithmic governmentality outlined above always overlaps and interferes with other forms of exercising power – especially so when the phenomenon at stake is policing. While, as a contemporary "imperial project" (Graham, 2006: 263), algorithmic governmentality deserves all our critical attention, it is thus indispensable to analyze how and where it relates to sovereign and/or disciplinary forms of government, especially considering the increasing indistinguishability of (il)liberal governmental practices in *dispositifs* of securitization (Opitz, 2011). This is all the more valid in postcolonial contexts where (il)liberal modes of "private indirect government" (Mbembe, 2001) have been a salient feature since their conquest by the European empires (Hansen & Stepputat, 2006; Hönke & Müller, 2012). From such a vantage point, the technocratic narrative of the system's straightforward "adaptation" to the Brazilian context, sustained by both Microsoft and the government of São Paulo, is incomplete insofar as it omits how it materializes differently in different diagrams of power (Deleuze, 2006: 23-44) – subject to dynamics or, rather, "translations" which cannot be grasped if one conceives of the "technical" and the "social" as two spheres which are neatly separated from each other: "machines are social before being technical" (Deleuze, 2006: 39).

Meanwhile, a critical evaluation must neither limit itself to opposing an ideal type of big data policing to the "messy reality" which would constantly belie those pipe dreams of an algorithmically enacted, clinical social order – as pointed out succinctly by Foucault (1991: 81), such an approach would entail "a very impoverished notion of the real". In other words, the challenge will consist in conceiving of DAS/*Detecta* and its implementation in São Paulo in terms which do not measure its degree of reality – or, in another register, its potential – according to rigid criteria of failure and success. It thus entails cracking open the scheme's glossy surface and depicting its malfunctions

and incoherences, but also analyzing the work it performs "on the ground" and the knowledges, practices, and controversies it engenders along the way – that is, to trace its productivity even where it might not be immediately apparent.

TROPICALIZING SURVEILLANCE: DETOURS AND DEVIATIONS OF BIG DATA POLICING

Heuristically, I would like to address these dynamics as the system's "tropicalization", a term I was first confronted with while interviewing a member of the São Paulo police forces working on *Detecta's* implementation. The dictionary definition holds that "to tropicalize" designates the adaptation of electronic devices so as to make them fit for hot and damp climate, mostly by means of minor technical modifications (Oxford English Dictionary 2014); in Brazil, I found that the term also may denote an adaptation to national industry standards, road conditions, business practices and -laws, aesthetic preferences, or safety requirements. In and by itself, the notion thus encompasses a broad – and, consequently, rather generic – range of adjustments necessitated by the specificity of national or regional sales markets; notably, it does *not* categorically discriminate between "technical" factors on the one hand and "cultural" or "social" aspects on the other, an indeterminacy which might actually turn out helpful for describing the phenomenon at stake.

Besides, it is noteworthy that the term is opposed to the literally u-topian notion of "globalization" insofar as it indicates a phenomenon which is explicitly located (albeit not necessarily localized) within the circuits of the (post)colonial international order and its enduring juxtaposition of "central" and "peripheral" settings: akin to the prominent case of the Orient (Said 1978), the tropes turned into an echo chamber for Western fears and desires soon after their "discovery" by tradesmen and scientists – an imaginary space within and against which Europe could articulate its own fragile modernity (Arnold, 2000). Hence, the term "tropicalization" inevitably relegates to politically fraught conceptual pairs such as original/derivative, civilized/savage or modern/archaic and reverberates with some of the major faultlines of Brazilian national identity up until the present day (Nava & Lauerhass, Jr., 2006).

Against this backdrop, the concept shall serve as a critique of orthodox, "diffusionist" models of innovation which tend to presuppose a smooth, orderly, and one-directional "transfer" of new technologies from one setting into another – frequently couched in terms of enabling an economic "catch up" in "developing countries" (Radosevic, 1999; Saggi, 2004). Against these teleological narratives of technologically induced modernization, "tropicalization" might be likened to the concept of "translation" as derived from actor-network theory and certain strands of science and technology studies. From such a perspective, "there is no such thing as technology transfer" insofar as "*traduction* is also *trahison* " (Law, 1999: n.p.): even the most faithful translation is a form of betrayal, in semiotics as well as in the realm of science and technology. Therefore, what can be observed resembles much more a series of negotiations among a multiplicity of actors, human as

well as non-human, who have to agree upon a common denominator – an "obligatory passage point" (Callon, 1986) – before their respective trajectories become commensurable. Technology, then, never migrates *en bloc* but is "de-scripted" (Akrich, 1992) as it travels: the gap "between the designer's projected user and the real user, between *the world inscribed in the object* and *the world described by its displacement*" (Akrich, 1992: 209) stirs controversies and thus impedes or, at least, delays its effective "blackboxing".[6] This occurs most prominently – albeit certainly not exclusively – as technologies are "translated" from the former imperial center to its peripheries, a fact which has triggered the timely appeal to go "beyond imported magic" (Medina and others, 2014) when studying science and technology in the "Global South" – namely, by re-focusing attention upon "processes of reinvention, adaptation, and use" (Medina and others, 2014: 2), not least in the realm of ICT (Ames, 2014; Marques, 2005; Nhampossa, 2005).

In a similar vein, a final remark might be made concerning the global meanders of policing, understood as a technology of government:[7] as famously pointed out by Foucault (2003: 103) when talking about the "boomerang effect" of colonial rule, namely that "[a] whole series of colonial models was brought back to the West, and the result was that the West could practice something resembling colonization, or an internal colonialism, on itself". A vivid example for such a (post)colonial entanglement can be found in McCoy (2009; 2016) who shows how the inventions behind "America's first information revolution" of the 1870s (the telegraph and the telephone on the one hand; the typewriter and new large-scale data storage schemes on the other) were crucial for the "capillary" policing of the Philippines after their colonization in 1898 – so much so that the author draws a historical parallel to the NSA's global cyber-espionage activities of the present (McCoy, 2016: 25ff.). Importantly, McCoy highlights how those novel intelligence devices and technologies "travelled" from the Philippines to Europe, where they would be deployed on the battlegrounds of World War I, and then "back home" to the US, where they were put to use to suppress the socialist workers' movement (McCoy, 2016: 24).

In the given context, what is insightful about the example – apart from the fact that it underlines the importance of non-human agency for colonial rule[8] – is that it shows how technologies of government "migrate" bi- or even polydirectionally across national borders, along as well as against the supposed main vectors of the imperial age: Foucault's boomerang keeps hovering, even in a world order seemingly out of joint with several major categories of 20th century IR scholarship. In accordance with the increasing fragmentation, multiplication, and overlapping of sovereignties which could be witnessed in the past few decades, it might have become difficult to spot the kind of quasi-symmetrical backlash described by McCoy; however, directing attention towards the "global making of policing" (Hönke & Müller, 2016) will most likely unearth far-reaching circuits and ramifications which refute orthodox accounts of policing as a predominantly national endeavor when, in fact, it has turned into "an essentially transnational and transcultural process" (Hönke & Müller, 2016: 6).

It is with these considerations in mind that one might start to think about the "tropicalization"

of DAS/*Detecta* – especially in terms of the techno-social translations to which it is subject and which it brings about in turn. A possible starting point for such an endeavor might consist in the kind of threat the system is supposed to fend off and the fears it plugs into: in New York, the DAS was presented and legitimized as a measure of counter-terrorism, designed to catch the "lone wolf" or to identify the "suspicious bag" before the situation gets out of control (New York Police Department, n.d.) whereas, in São Paulo, *Detecta* was introduced as a silver bullet against street crime such as robberies and car theft. Importantly, these different threat scenarios mobilize quite distinct typologies of suspicion and the corresponding epistemological promises: terrorists, for one, are threatening because there are hardly any "markers" by which they can be recognized beforehand – as in the case of Dzhokhar Tsarnaev, one of the "Boston bombers", who was described as "one of us" by his fellow students (Williams & Elder, 2013). In this sense, the promise of big data policing is to apprehend those crucial, yet minuscule clues which would otherwise escape the investigators – counter-terrorism's "unknown unknowns", as Donald Rumsfeld once put it (in)famously.

Something quite different applies in São Paulo, where the perceived threat is anything but anonymous and, instead, carries the face of the *marginal,* the young, poor, and mostly dark-skinned "other" of the *pessoa do bem,* the hard-working and law-abiding citizen (Caldeira, 2001). A substantial part of the city's inhabitants is thus earmarked as potentially dangerous – and as can be witnessed by its staggering death toll among the very same group (Caldeira, 2002), in Brazil "the enforcement of the class order and the enforcement of public order are merged" (Wacquant, 2003: 199). Under such circumstances, *Detecta's* utilization as a tool for the control and containment of undesirable populations seems an educated guess – however, just like the streamlined governmental discourse ought to be distrusted, it is advisable not to rush into a hermetic counter-narrative leaving little space for variations and contingencies. As pointed out by Barry (2006: 241), the "construction of technological zones generates active and passive forms of resistance" which, in the given context, could be confirmed by São Paulo's board of audit: in a recently published report on *Detecta's* implementation, it listed a whole catalogue of shortcomings running the gamut from incompatible operating systems and a deficient infrastructure to an insufficiently trained police staff unwilling to adapt its working routines to the new program. The auditors conclude that, as yet, *Detecta* "does not present effective results for public security" (Tribunal de Contas do Estado, 2016: 75).

Acknowledging the system's many imperfections thus helps to stay clear of overly teleological depictions; meanwhile, it should neither encourage a "technoskeptic" account which fundamentally disputes the governmental significance and/or novelty of algorithmic policing. The (otherwise perfectly legitimate) question to which extent it actually "works" does not quite grasp what is at stake insofar as it already buys into a certain economy of means and purposes which might obscure more than it reveals. Put more polemically, maybe "predictive crime software has nothing to do with preventing crime" (Scannell, n.d.) – and it might have nothing to do with any straightforward notion of class oppression either, one could add. Instead, *Detecta* might function

already even where, measured by the promises it was sold with publicly, it does not actually "work" – for instance, as a huge data mining *dispositif* feeding back into the perfection of Microsoft's algorithms. In fact, as I was told by an insider, various IT routines and protocols which were developed in São Paulo did already "travel back" to New York. In this sense, any kind of "local" difference (which, at the outset, may well manifest itself as a fault, a bug, a maladjustment) would make the system more versatile and, therefore, more desirable on the booming market for predictive policing "solutions". The question who is served by whom (and with what) thus attains a whole new dimension, the implications and consequences of which are yet to be fathomed by scholars and activists alike.

NOTES

* PhD candidate: Doctorate in Cultural and Global Criminology, University of Hamburg (Germany) and ELTE Budapest (Hungary). Email: ca359@kent.ac.uk.

1. This affirmation was made by Jessica Tisch, the NYPD's Deputy Commissioner for Information Technology. Cf. "New York City - Domain Awareness", https://www.youtube.com/watch?v=ozUH0HAAhzg. Last access on 05/18/2016.

2. Cf. https://www.microsoft.com/en-us/government/EmpoweringUS/default.aspx. Last access on 05/18/2016.

3. Cf. "Total Surveillance: NYPD launches new 'all-seeing' Domain Awareness System (Aug 12, 2012)", https://www.youtube.com/watch?v=GcGpgvTh2W4. Last access on 05/21/2016.

4. Cf. „Mayor Bloomberg Unveils New State-of-the-Art Law Enforcement Technology", https://www.youtube.com/watch?v=TxMz0Yoa2-Y. Last access on 06/08/2016.

5. In accordance with the "Copenhagen School" of international relations, I would like to apply the concept to those performative speech acts which effectively "securitize" particular policy fields and, thereby, partly or wholly withdraw them from processes of public deliberation (Buzan et al. 1998); meanwhile, I would also like to extend the notion so that it can effectively be applied to non-discursive phenomena as well (Schuilenburg 2015). The act of successfully defining a public park as a "security-sensitive" area, the institutional decision to police it more thoroughly, and the street lights set up along its paths so as to dissuade criminals would, then, all qualify as events, processes and/or materializations of securitization.

6. Following Latour (1999: 304), blackboxing "refers to the way scientific and technical work is made invisible by its own success. When a machine runs efficiently, when a matter of fact is settled, one need focus only on its inputs and outputs and not on its internal complexity. Thus, paradoxically, the more science and technology succeed, the more opaque and obscure they become."

7. When talking about technologies of government, the present paper adheres to the definition brought up by Rose (1999: 52), namely that they have to be understood as "an assemblage of forms of practical knowledge, with modes of perception, practices of calculation, vocabularies, types of authority, forms of judgement, architectural forms, human capacities, non-human objects and devices, inscription techniques and so forth, traversed and transected by aspirations to achieve certain outcomes in terms of the conduct

of the governed [...].” While thus sharing the decentering as well as destabilizing gesture of actor-network -theoretical approaches, Rose’s definition explicitly makes reference to “the shaping of [human] conduct” insofar as “within these assemblages, it is human capacities that are to be understood and acted upon by technical means” (ibid.).

8. For a seminal account of this topic, cf. Law (1986).

REFERENCES

Akrich, M. (1992). The De-Scription of Technical Objects. In W. E. Bijker & J. Law (Eds.), *Shaping Technology/ Building Society: Studies in Sociotechnical Change* (pp. 205–224). Cambridge: MIT Press.

Ames, M. G. (2014). Translating Magic: The Charisma of One Laptop per Child’s XO Laptop in Paraguay. In E. Medina, I. da C. Marques, & C. Holmes (Eds.), *Beyond Imported Magic: Essays on Science, Technology, and Society in Latin America* (pp. 207–224). London, Cambridge: MIT Press.

Arnold, D. (2000). “Illusory Riches”: Representations of the Tropical World, 1840–1950. *Singapore Journal of Tropical Geography*, *21* (1), 6–18.

Barry, A. (2006). Technological Zones. *European Journal of Social Theory*, *9* (2), 239–253.

Boltanski, L. (2014). *Mysteries and Conspiracies: Detective Stories, Spy Novels and the Making of Modern Societies*. Cambridge: Polity Press.

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Editora Sulina.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder, London: Lynne Rienner.

Caldeira, T. (2001). *City of Walls: Crime, Segregation, and Citizenship in São Paulo*. Berkeley: University of California Press.

Caldeira, T. (2002). The Paradox of Police Violence in Democratic Brazil. *Ethnography*, *3* (3), 235–263.

Callon, M. (1986). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of Saint Brieuc Bay. In J. Law (Ed.), *Power, Action and Belief: A New Sociology of Knowledge?* (pp. 196–223). London: Routledge.

Clough, P. T., Gregory, K., Haber, B., & Scannell, R. J. (2015). The Datalogical Turn. In P. Vannini (Ed.), *Non-Representational Methodologies: Re-Envisioning Research* (pp. 146–164). New York, London: Routledge.

Davis, M. (1990). *City of Quartz: Excavating the Future in Los Angeles*. London, New York: Verso.

Deleuze, G. (2006). *Foucault*. Minneapolis, London: University of Minnesota Press.

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the Risk Society*. Toronto, Buffalo: University of Toronto Press.

Foucault, M. (1991). Questions of Method. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault Effect: Studies in Governmentality* (pp. 73–86). Chicago: University of Chicago Press.

Foucault, M. (2003). *Society Must be Defended: Lectures at the Collège de France, 1975-76*. New York: Picador.

Foucault, M. (2009). *Security, Territory, Population: Lectures at the Collège de France, 1977-1978*. New York: Picador.

Ginzburg, C., & Davin, A. (1980). Morelli, Freud and Sherlock Holmes: Clues and Scientific Method. *History Workshop*, *9* , 5–36.

Graham, S. (2006). Surveillance, urbanization and the US "Revolution in Military Affairs." In D. Lyon (Ed.), *Theorizing Surveillance: The panopticon and beyond* (pp. 247–269). Cullompton, Portland: Willan.

Graham, S. (2011). *Cities Under Siege: The New Military Urbanism*. London, New York: Verso.

Hansen, T. B., & Stepputat, F. (2006). Sovereignty Revisited. *Annual Review of Anthropology*, *35* (1), 295–315.

Harcourt, B. E. (2007). *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. Chicago: University of Chicago Press.

Hönke, J., & Müller, M.-M. (2012). Governing (in)security in a postcolonial world: Transnational entanglements and the worldliness of "local" practice. *Security Dialogue*, *43* (5), 383–401.

Hönke, J., & Müller, M.-M. (2016). The global making of policing. In J. Hönke & M.-M. Müller (Eds.), *The Global Making of Policing: Postcolonial perspectives* (pp. 1–19). London, New York: Routledge.

Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, London: Harvard University Press.

Law, J. (1986). On the Methods of Long Distance Control: Vessels, Navigation, and the Portuguese Route to India. In J. Law (Ed.), *Power, Action and Belief: A New Sociology of Knowledge?* (pp. 234–263). London: Routledge.

Law, J. (1999). Traduction/Trahison: Notes on ANT. Centre for Science Studies, Lancaster University. Retrieved fromhttp://www.lancaster.ac.uk/fass/resources/sociology-online-papers/papers/law-traduction-trahison.pdf

Lyon, D. (2004). Technology vs. "'Terrorism'": Circuits of City Surveillance Since September 11, 2001. In S. Graham (Ed.), *Cities, War, and Terrorism: Towards an Urban Geopolitics* (pp. 297–311). Malden: Blackwell.

Marcuse, P. (2004). The "War on Terrorism" and Life in Cities after September 11, 2001. In S. Graham (Ed.), *Cities, War, and Terrorism: Towards an Urban Geopolitics* (pp. 263–275). Malden, Oxford, Carlton: Blackwell.

Marques, I. da C. (2005). Cloning computers: From rights of possession to rights of creation. *Science as Culture*, *14* (2), 139–160.

Martens, P. (2012, February 6). Wall Street's Secret Spy Center, Run for the 1% by NYPD. *Counterpunch*. Retrieved from http://www.counterpunch.org/2012/02/06/wall-streets-secret-spy-center-run-for-the-1-by-nypd/

Mbembe, A. (2001). *On the Postcolony*. Berkeley, Los Angeles, London: University of California Press.

McCoy, A. W. (2009). *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State*. Madison: University of Wisconsin Press.

McCoy, A. W. (2016). Capillaries of empire: Colonial pacification and the origins of US global surveillance. In J. Hönke & M.-M. Müller (Eds.), *The Global Making of Policing: Postcolonial perspectives* (pp. 20–39). London, New York: Routledge.

Medina, E., Marques, I. da C., & Holmes, C. (2014). Introduction: Beyond Imported Magic. In E. Medina, I. da C. Marques, & C. Holmes (Eds.), *Beyond Imported Magic: Essays on Science, Technology, and Society in Latin America* (pp. 1–23). London, Cambridge: MIT Press.

Nava, C., & Lauerhass, Jr., L. (Eds.). (2006). *Brazil in the Making: Facets of National Identity*. Lanham et al.: Rowman & Littlefield.

New York City. (2007). Mayor Bloomberg Presents $ 57.1 Billion FY 2008 Preliminary Budget. Retrieved October 18, 2016, from: http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2007a%2Fpr025-07.html&cc=unused1978&rc=1194&ndi=1

New York City. (2012). Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-of-the-Art Law Enforcement Technology That Aggregates and Analyzes Existing Public Safety Data in Real Time to Provide a Comprehensive View of Potential Threats and Criminal Activity. Retrieved December 26, 2015, from http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http%3A%2F%2Fwww.nyc.gov%2Fhtml%2Fom%2Fhtml%2F2012b%2Fpr291-12.html&cc=unused1978&rc=1194&ndi=1

New York Police Department. (n.d.). Public Security Privacy Guidelines. Retrieved from: http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

Nhampossa, J. L. (2005). *Re-Thinking Technology Transfer as Technology Translation: A Case Study of Health Information Systems in Mozambique* (Doctoral Thesis). University of Oslo.

Opitz, S. (2011). Government Unlimited: The Security Dispositif of Illiberal Governmentality. In U. Bröckling, S. Krasmann, & T. Lemke (Eds.), *Governmentality: Current Issues and Future Challenges* (pp. 93–114). New York, London: Routledge.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica: RAND Corporation.

Radosevic, S. (1999). *International Technology Transfer and "Catch Up" in Economic Development*. Cheltenham: Edward Elgar.

Rose, N. (1999). *Powers of Freedom: Reframing Political Thought*. Cambridge, New York: Cambridge University Press.

Rouvroy, A., & Berns, T. (2010). Le nouveau pouvoir statistique, Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps «numériques»... *Multitudes*, (40), 88–103.

Saggi, K. (2004). *International Technology Transfer to Developing Countries*. London: Commowealth Secretariat.

Said, E. W. (1978). *Orientalism*. New York: Vintage Books.

Scannell, R. J. (n.d.). What Can an Algorithm Do? *Dis Magazine*. Retrieved from: http://dismagazine.com

/discussion/72975/josh-scannell-what-can-an-algorithm-do/

Schuilenburg, M. (2015). *The Securitization of Society: Crime, Risk, and Social Order*. New York: NYU Press.

Scott, J. C. (2008). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

Tribunal de Contas do Estado. (2016). *Relatório de Fiscalização de Natureza Operacional: Solução de Consciência Situacional - DAS Detecta*. São Paulo.

tropicalize, v. (2014). In *Oxford English Dictionary*. Retrieved from http://www.oed.com.chain.kent.ac.uk/view/Entry/206705?redirectedFrom=tropicalize&

Wacquant, L. (2003). Toward a Dictatorship Over the Poor? Notes on the Penalization of Poverty in Brazil. *Punishment & Society*, *5* (2), 197–205.

Williams, M., & Elder, M. (2013, April 19). Dzhokhar Tsarnaev: Boston bombing suspect was "a lovely, lovely kid." *The Guardian*. Retrieved from: https://www.theguardian.com/world/2013/apr/19/boston-suspect-dzhokhar-tsarnaev-school

Wolf, N. (2012, December 29). Revealed: how the FBI coordinated the crackdown on Occupy. *The Guardian*. Retrieved from: https://www.theguardian.com/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy

AUTOMAÇÃO E VIGILÂNCIA NO METRÔ DE SÃO PAULO

Resumo: Este trabalho foi produzido no âmbito de uma pesquisa sobre a Linha 4-Amarela do metrô de São Paulo, inaugurada em 2010, em que a condução dos trens é integralmente automática (sem piloto humano). Os trens são conduzidos pelo equipamento embarcado sob supervisão de um posto de comando central. Mostro, no texto, como o ambiente sócio-técnico da linha, e o restante da rede, são afetados por essa inovação e exploro uma de suas consequências mais notáveis: o investimento na *vigilância* . Através de trabalho etnográfico — envolvendo a observação-participação no espaço do metrô e entrevistas com usuários, agentes e membros dos quadros diretores da Companhia do Metropolitano de São Paulo e da concessionária ViaQuatro — e do apoio em literatura sobre vigilância, inovação tecnológica, transportes, comunicação e experiência urbana, examino as mutações importantes que surgem no trabalho do metroviário e na relação dos usuários com os agentes e com o espaço construído, que também se reconfigura.

Sobretudo a partir do advento das tecnologias digitais, os ambientes dos metrôs do mundo se veem povoados cada vez mais por automatismos, sendo a automação integral da condução o experimento mais audacioso. O edifício do metrô é denominado "inteligente", assim como a cidade em que a gestão de equipamentos e serviços tende a ser feita através de tecnologias de informação e comunicação. Tanto no caso da cidade tecnológica ou inteligente quanto no dos metrôs e, especificamente, na experiência da Linha 4-Amarela, observamos a ênfase no*monitoramento* e a construção de uma *pilotagem a distância* com repercussões na produção da vida social nesses ambientes.

Palavras chave: Metrô, São Paulo, Vigilância, Tecnologias digitais.

JANICE CAIAFA*

Automatización y vigilancia en el metro de São Paulo

Resumen: Este texto fue elaborado como parte de una investigación sobre la Línea 4 del Metro de São Paulo, inaugurada en 2010, en la cual la conducción del tren es totalmente automática (sin piloto humano). Los trenes son conducidos por los equipos a bordo bajo la supervisión de un puesto de control central. Mostro como el ambiente socio -técnico de la línea, y el resto de la red, se ven afectados por esta innovación y exploro una de sus consecuencias más notables: el énfasis en la *vigilancia* . A través de trabajo etnográfico — que incluye observación participante en el espacio del metro y entrevistas con pasajeros, agentes y directores de la Companhia do Metropolitano de São Paulo y de la concesionaria ViaQuatro — y el apoyo en la literatura sobre vigilancia, innovación tecnológica, transporte, comunicación y experiencia urbana, examino los principales cambios en la rutina de los trabajadores del metro y en la relación entre los pasajeros y los agentes y con el espacio construido, que también es afectado.

Con la llegada de las tecnologías digitales, el ambiente del metro se encuentra cada vez más poblado por mecanismos automáticos. La conducción totalmente automatizada de los trenes es, en este contexto, el experimento más audaz. El edificio de metro es llamado "inteligente", así como la ciudad donde la gestión de equipos y servicios tienden a realizarse a través de tecnologías de la información y la comunicación. Tanto en la ciudad tecnológica o inteligente como en el metro — y específicamente en la experiencia de la Línea 4 – se observa el énfasis en los*dispositivos de monitoreo* y en el *pilotaje a distancia* , con repercusiones en la producción de la vida social en estos ambientes.

Palabras clave: Metro, São Paulo, Vigilancia, Tecnologías digitales.

Automation and Surveillance in the São Paulo Subway

Abstract: This paper presents a few results of a research on the fully automated line of the São Paulo subway, Line 4, open to commercial operation in 2010. The trains are operated by the onboard equipment and under the supervision of a central control room. I show how this innovation affects the sociotechnical environment of Line 4, as well as the rest of the network, and explore one of its most noticeable consequences: the investment on *surveillance* . Relying on ethnographic work — that includes participant observation in the subway facilities and interviews with riders, subway employees, and members of the directorial board of Companhia do Metropolitano de São Paulo and ViaQuatro, the private operator of Line 4— and resorting to the literature on surveillance, technological innovation, transportation, communication, and urban experience, I examine the changes in the routine of transport workers and in the relations between riders, subway employees, and the subway built space, which also undergoes a process of reconfiguration.

With the emergence of digital technologies, the subway environment tends to work increasingly through automatic mechanisms, the fully automation of conduction representing its most ambitious experiment. The subway building is named “smart”, just like the city where urban services and assets tend to be managed through information and communication technologies. Both in technological or smart cities and in subways — and, specifically, in the case of Line 4 — we observe the emphasis on*monitoringprocedures* and *remote piloting* , with consequences for the production of social life in these environments.

Keywords: Subway, São Paulo, Surveillance, Digital technologies.

O METRÔ DE SÃO PAULO, A CIDADE E LINHA 4-AMARELA

O metrô desempenhou um papel importante desde os seus inícios na ordenação do crescimento de São Paulo, uma das cidades mais populosas do mundo, com mais de 11 milhões de habitantes[1]. Nessa grande metrópole brasileira, a mobilidade se apresenta particularmente problemática. A construção de grandes avenidas voltadas para o escoamento do tráfego de veículos, caracterizando a opção rodoviária, contribuiu para gerar um dos problemas centrais da cidade: a presença maciça do automóvel particular. Outras características do processo de urbanização, como a violenta segregação dos pobres, fizeram da orientação para o carro um fator particularmente virulento de desorganização e agravamento dos problemas urbanos. Nesse contexto, o metrô veio criar acesso, como costuma fazer um metrô, percorrendo vastas distâncias com rapidez e economia,

ora em vias subterrâneas ou elevando-se acima das vias congestionadas. Funcionou como uma espécie de "eixo mestre" para os deslocamentos de destino ao Centro (Peter Alouche, 1987) e introduziu o conceito de integração dos diferentes modais.

A Companhia do Metropolitano de São Paulo foi constituída em 1968, vinculada à Secretaria de Estado dos Transportes Metropolitanos e, logo em seguida, a Linha 1-Azul, servindo o eixo Norte -Sul, começou a ser construída. Em 1974 foi iniciada a operação comercial do primeiro trecho, Jabaquara-Vila Mariana.[2] Atualmente, o metrô de São Paulo possui 5 linhas em operação: Linha 1-Azul, Linha 2-Verde, Linha 3-Vermelha, Linha 4-Amarela e Linha 5-Lilás, totalizando 61 estações. Em 2014 transportou 1,4 bilhões de passageiros (São Paulo não para de crescer, s/d).

A Linha 4-Amarela, de implementação bem mais recente, inaugurou o primeiro trecho — Faria Lima-Paulista — em maio de 2010. Mais 5 estações foram construídas e o trecho hoje em operação compreende Butantã, Pinheiros, Faria Lima, Fradique Coutinho, Paulista, República e Luz. A segunda fase de implementação da linha, que não se concluiu no prazo previsto, acrescentará as estações Higienópolis-Mackenzie, Oscar Freire, São Paulo-Morumbi e Vila Sônia. Em maio de 2014, a linha transportou 785 mil passageiros por dia (Paula, 2015: 24).

Além do seu papel particularmente integrador, conectando as outras linhas e reduzindo o tempo de viagem dos usuários, a Linha 4-Amarela introduziu várias novidades no contexto da rede paulista. A inovação tecnológica mais expressiva consiste na adoção da modalidade de condução dos trens denominada UTO (*Unattended Train Operation*), sem condutor humano. Trata-se da primeira linha metroviária totalmente automatizada da América Latina. Uma outra novidade aportada consiste em que a Linha 4 é a primeira linha do metrô paulista concedida ao setor privado para operação no âmbito do primeiro contrato de Parceria Público Privada do país.[3]

Como costuma ocorrer nos processos de automação, a inovação tecnológica carreou um novo modelo de gestão humana norteado pelos imperativos de otimização e produtividade. No contexto desse modelo, o trabalho do metroviário se tornou, em alguma medida, polivalente, com a convergência das funções de operação, segurança e manutenção. A tecnologia se apresenta frequentemente como um pretexto para que essas intervenções se realizem (Villoutreix, 1990). A experiência de automatização integral da condução fez-se igualmente acompanhar da implementação de outros automatismos no edifício do metrô. Nesses processos costuma ocorrer uma redistribuição dos agentes nas estações e nas salas técnicas e novas interfaces maquínicas e humanas se estabelecem — e não foi diferente na Linha 4 e nem tampouco na automatização da condução no metrô de Paris, que inspirou a experiência brasileira (David, 1995; Caiafa, 2014, 2015b). Os usuários ingressam nesses circuitos, aprendendo a abordar ou a conviver com as novas máquinas e construindo relações entre si e com os agentes que, nesse ambiente marcadamente tecnológico, podem ser mediadas por elas (Caiafa, 2015, 2016).

O ambiente complexo povoado por tais interfaces passa a demandar muito mais *vigilância* — de máquinas e de humanos. Um sistema integrado de automatismos, envolvendo tecnologia de

ponta, está sujeito a um novo tipo de pane e requer, assim, uma grande reatividade dos operadores humanos. Ao mesmo tempo, ao suprimir o agente humano em alguns contextos, se expõe mais à ação dos usuários, que podem degradá-lo, seja intencionalmente ou não. A operação se torna mais refinada e mais vigilante, como testemunha, por exemplo, a multiplicação de câmeras e de sofisticados *dispositivos de observação e intervenção*.

Neste texto abordo, a partir de pesquisa etnográfica, alguns aspectos do sobre-investimento na vigilância no contexto dessa *reconfiguraçãodo ambiente metroviário* da Linha 4 do metrô de São Paulo, envolvendo agentes, usuários e maquinismos. Utilizo dados que venho produzindo através de trabalho de observação participante nos espaços do metrô e conversas com usuários e profissionais, entre agentes, técnicos e membros dos quadros diretores da Companhia do Metrô e da concessionária ViaQuatro. Em diálogo com esses meus interlocutores e com trabalhos de outros autores, faço algumas indicações sobre o problema da vigilância na experiência de automação integral da condução na Linha 4 e em suas repercussões na rede paulista, buscando compreendê-lo também no contexto mais amplo da multiplicação dos cenários de vigilância no contemporâneo a partir sobretudo do advento das tecnologias digitais de comunicação e informação.

NA SALA DE CONTROLE

Logo no início da pesquisa, aprendi que numa linha automática o papel do Centro de Controle Operacional (CCO) se torna particularmente relevante. O CCO é um centro de comando a distância que recebe informação de todo o sistema e envia constantemente relatórios para assegurar a movimentação fluida e ininterrupta dos trens nas vias. Para isso o CCO observa também os fluxos humanos a partir das imagens enviadas pelas câmeras em plataformas, estações e mesmo no interior dos trens, e controla os equipamentos elétricos e eletromecânicos instalados por todo o espaço do metrô. No CCO ficam operadores em seus consoles ou postos de trabalho, que consistem em computadores e comunicadores de vários tipos, e diante de grandes painéis de controle ótico, sob o comando de um supervisor. Na visita que fiz ao CCO da Linha 4 confirmei esse papel maior do CCO numa linha automática que havia aprendido em conversas anteriores com meus interlocutores. Jorge Secall, diretor de operações da ViaQuatro na época, foi o primeiro a me indicar estas questões, aliás numa entrevista muito interessante e definitivamente impulsionadora para a pesquisa.

Jorge me falou do funcionamento "matricial" e "radial" da Linha 4, diferente das outras linhas do metrô, e mesmo de qualquer linha não integralmente automatizada. Os comandos que é preciso fazer circular para o funcionamento do sistema vão do centro à periferia, ou seja, do CCO para a estação, onde estão os agentes e outros supervisores.

Em seguida, ao observar o dia a dia da linha, constataria que é paulatina e parcial a aplicação desse princípio. Como, aliás, esse meu interlocutor e outros assinalariam, inclusive o supervisor do CCO, que tão gentilmente conversou comigo, ao mostrar que uma negociação tem lugar nas conversas com os colegas que estão fazendo trabalho de estação. De toda forma, esse princípio

— da prioridade do CCO nas decisões operacionais — é uma diretiva importante e percebe-se como é determinante para o investimento na vigilância.

Assim, o CCO da Linha 4 concentra mais funções que o CCO que controla as outras linhas do sistema, operadas pela Companhia do Metrô, que não são automáticas – por exemplo, a função de supervisão e controle da manutenção dos trens. Do CCO da Linha 4 pode-se, ainda, injetar um trem na via, enquanto no outro CCO, não imbuído desse papel matricial, recorre-se à agência humana para alcançar o pátio de manobras, inspecionar e liberar o trem.

Como costuma ocorrer nas linhas integralmente automáticas, na Linha 4 há câmeras no interior dos trens. Em geral, apenas as plataformas, num metrô, são alvo desse escrutínio. Assim, em nome da vulnerabilidade dos equipamentos e da reatividade requerida da parte do conjunto dos operadores, vigia-se mais minuciosamente ainda os humanos. Os painéis do CCO mostram, ao lado da representação precisa do caminho dos trens na linha, imagens dos passageiros em lugares sensíveis das plataformas e transferências e durante suas viagens nos trens. Estas últimas, embora já as tivesse visto antes em algumas telas menores em salas técnicas da Companhia do Metrô, me impressionaram particularmente no momento daquela visita ao CCO da Linha 4. Observei os passageiros sentados ou de pé, apoiados nos balaústres, em várias posições e com o olhar vago dos viajantes em ambiente coletivo, alheios à captação de sua imagem. Talvez pela monumentalidade do aparato, de estética muito forte na exposição formidável que proporciona, a intervenção no cotidiano privado das pessoas me pareceu mais contundente.

Os primeiros metrôs do mundo, como o de Londres e o de Nova York, surgiram ainda no final do século dezenove e início do século vinte. Mas foram os metrôs mais jovens, implementados nos anos 1970, como os de São Paulo, o de São Francisco e o do Rio de Janeiro, que trouxeram composições com maior capacidade de carregamento, introduziram sistemas de ajuda à condução dos trens e a supervisão computadorizada a partir do CCO (Alouche, 1990). Nos anos 1980 a automação e a informatização dos metrôs avança e surge o primeiro metrô com condução totalmente automática, o VAL da cidade de Lille, França, um metrô leve, ou seja, de baixa capacidade de carregamento e que atende uma demanda moderada. A década de 1990 e o novo milênio trouxeram as experiências de automatização integral da condução em metrôs pesados, ou seja, de grande capacidade, como as Linhas 1 e 14 do metrô de Paris, a Linha D do metrô de Lyon e a Linha 4-Amarela do metrô de São Paulo. Como indica Alouche (1990), a informática penetra em todos os setores do transporte metroviário.

De fato, como vimos, outros automatismos costumam acompanhar a implementação da condução automática — embora possam ocorrer também independentemente dela —, como a automatização da venda de bilhetes ou dos bloqueios que controlam o ingresso no sistema e a introdução de esteiras e intercomunicadores. O edifício do metrô assim modernizado é por vezes denominado "inteligente", como ocorre com outros ambientes, inclusive as cidades. Nas chamadas "*smart cities*", a gestão de equipamentos e serviços tende a ser feita através de tecnologias de informação e comunicação. Essa gestão requer constante monitoramento de máquinas, pessoas e do próprio

espaço. A cidade inteligente ou tecnológica é, assim, tipicamente vigiada e esquadrinhada. Os efeitos de melhoria dos serviços (como coleta de lixo, informação sobre horários de sistemas de transporte) não se obtêm sem a detecção de eventos, a localização de pessoas e o controle do cotidiano da cidade.

Antoine Picon (s/data: 28) mostra como nas *smart cities*, através desses instrumentos de captura, a informação se torna, ela própria, "acontecimental". Revolvendo a história dessa governança digital das cidades, o autor observa que as primeiras grandes redes informáticas, construídas pela IBM nos Estados Unidos, eram destinadas a detectar situações, virtuais ou reais, de ataques termonucleares da União Soviética durante a Guerra Fria. Foi preparando "esquemas de resposta" a esses possíveis eventos de guerra que começou a prosperar a "simulação informática". Esse aspecto de detecção e intervenção – e, de início, com objetivos bélicos — está na origem da informática e se viu reforçado com a crescente importância do digital.

Nos metrôs, ambientes vigiados desde os seus inícios, a necessidade de detectar e intervir é ainda mais enfatizada com a entrada das tecnologias digitais. O imperativo da gestão dos riscos num contexto tecnológico avançado veio alimentar a aposta na necessidade incontornável da vigilância.

A época em que os metrôs começaram a investir em trens modernos e sinalização mais avançada, no Pós-Guerra, e a introduzir sistemas informatizados de ajuda à condução e supervisão computadorizada no CCO, nos anos 1970, coincide com a do fenômeno que Picon (s/data: 33) chama de "verdadeira fascinação" pelas salas de controle. Trata-se, inclusive, da ocasião de emergência e desenvolvimento da cibernética e de sua aliança com a teoria dos sistemas. A origem desses centros de comando centralizado também é bélica, remontando às *WarRooms* da Segunda Guerra Mundial, de que derivam, por sua vez, a sala de controle da NASA (*National Aeronautics and Space Administration*) e do NORAD (*North AmericanAerospace Defense*). A cidade tecnológica ou inteligente é a sua expansão mais recente.

É fato que minha visita ao CCO da Linha 4-Amarela em nada se assemelhou ao campo dos jogos militares, dada a afabilidade dos operadores que ali me receberam e da camaradagem que me pareceu predominar entre eles, ao menos naquele turno e naquela ocasião. No cotidiano do metrô a extrema variabilidade das atitudes e estilos humanos vai gerando outros cenários, criando relações que não obstam as estipuladas pelos imperativos da gestão tecnológica e empresarial, mas os modificam em alguma medida, como veremos mais adiante.

UM REGIME DE VIGILÂNCIA

Muitos metrôs do mundo já introduziram sistemas de auxílio à condução dos trens que tornam a condução quase totalmente automática. É o caso das outras linhas do metrô de São Paulo e da Linha 1 do Rio de Janeiro. O equipamento embarcado conduz o trem, cabendo ao condutor abrir e fechar as portas e, em alguns casos, dar a partida. É a modalidade de condução Piloto Automático

ou ATO (*Automatic Train Operation*). A condução Manual Livre, em que condutor humano conduz o trem, ainda é utilizada na maioria das linhas do metrô de Nova York, na Linha 2 do metrô do Rio de Janeiro e em geral no pátio de manobras dos metrôs. Na modalidade Manual Controlada, que pode ser usada em período de vale (baixa demanda), o piloto conduz o trem sob a supervisão da máquina, que pode, por exemplo, frear numa emergência Os níveis mais altos de automação são o *Driverless Train Operation* (DTO) e o *Unattended Train Operation* (UTO). Nas duas modalidades a condução é integralmente automática, com o equipamento embarcado conduzindo o trem sob a supervisão do CCO. No DTO conserva-se um agente no trem para emergências e no UTO opera -se sem presença humana a bordo). A Linha 4-Amarela foi preparada para operar na modalidade UTO.

Os usuários com quem conversei até agora não demonstraram em geral medo ou desconfiança em relação à condução do trem pela máquina. Alguns não sabiam que a Linha 4-Amarela funcionava assim e foi nossa conversa que lhes revelou. Por vezes alguém hesitava ou fazia alguma ressalva.

> — É estranho, né? Vou te falar, hoje a tecnologia tá muito... Fala a verdade, hein, tá sem piloto aqui mesmo? — me perguntou um usuário durante uma viagem.
> — Tá sem piloto.
> — Como é que pode? Fazer o quê, né?

Desconfiamos às vezes, mas frequentemente nos acostumamos à presença da tecnologia no nosso cotidiano. Outros autores apontaram este aspecto da relação dos usuários com os trens automáticos (Latour, 1991; Alouche, 2012). Quanto à vigilância, segundo mostram os dados até agora, é difícil a percepção espontânea das desvantagens de ser controlado. Os usuários em geral falam muito em segurança como um bem maior e desejável.

Bruno (2010: 156) cunhou a noção de "vigilância distribuída" para caracterizar os regimes de vigilância da atualidade. A autora aponta que nas sociedades contemporâneas a vigilância diversificou seus "propósitos, funções e significações", exercendo-se em variados setores — como no entretenimento e na prestação de serviços — e visando múltiplos objetos. Pode ocorrer também associada a outros dispositivos que a princípio não se destinariam a esse fim, como é o caso da geolocalização. Essa associação ou mistura, como prefere a autora, gera a multiplicação de objetos, estendendo a vigilância, por exemplo, a consumidores e transeuntes, de tal forma que os suspeitos e perigosos "podem ser todos ou qualquer um".

No caso dos metrôs e sobretudo no contexto das experiência da automatização integral da condução — e especificamente no caso da Linha 4 — os vigiados são, além dos transeuntes nos espaços do metrô, as próprias máquinas e seus primeiros utilizadores, os agentes de operação. À observação dos usuários em fluxo pelos corredores e alheios em sua viagem nos trens em movimento, alia-se a atenção ao funcionamento dos automatismos cada vez mais numerosos e complexos, e dos agentes de estação, cujo trabalho é ao mesmo tempo auxiliado e controlado pelo monitoramento desde a sala de controle.

A vigilância, nesse caso, não é descentralizada ou sem hierarquia — diferente, nesse aspecto, da modalidade distribuída descrita por Bruno, ou da espécie de democratização dos dispositivos que só faz reforçar o controle ao permitir a partilha, de que fala Rodrigues (2012). Na experiência da Linha 4, como se pode esperar dos ambientes dos metrôs e sobretudo no caso da automatização, o controle tende a ser centralizado e hierarquizado, dada a importância assumida pelo CCO. Nesse caso, encontramos um aspecto da vigilância operante no modelo panóptico, vigente a partir do século XIX e característico das sociedades modernas ou disciplinares, em que tipicamente um vigilante observa o comportamento dos indivíduos de uma torre central (Foucault, 1987). Os indivíduos não se encontram confinados, contudo, como na vigilância do tipo panóptico, que se realiza no hospital, na escola e mais caracteristicamente na prisão. De fato, estão confinados apenas provisoriamente nas estações, frequentemente subterrâneas, ao mesmo tempo que constituem uma *população em movimento*, seja em marcha pelo edifício do metrô nos espaços de transferência e acessos, seja conduzidos pelos trens. Não são vigiados pela sua periculosidade, como no sistema panóptico, mas apresentam, em alguma medida, esse aspecto, já que é preciso proteger os artefatos técnicos da violência humana, além de manter a ordem para o sucesso da operação. O agente de segurança nos metrôs tem poder de polícia.

Encontramos nos observatórios do metrô uma combinação de estratégias reminiscentes das disciplinas modernas e outros em consonância com a plasticidade e a diversificação das medidas contemporâneas atualizadas na internet e nas cidades inteligentes. Adequadas aos propósitos desse equipamento coletivo de serviço (Caiafa, 2013), essas estratégias parecerem se justificar sobretudo por dois dos "regimes de legitimação" da vigilância distribuída indicados por Bruno (2010: 157), o da segurança e o da eficiência. Aliás, a noção de eficiência é uma figura crucial, como aponta Hess (2007), nas justificativas para a adoção de tecnologias e para a sua naturalização nas sociedades contemporâneas.

A implementação da Linha 4 fez chegar aos trens — modernos, confortáveis e atraentes, como não é difícil constatar e como afirmam os usuários — a novidade da presença de câmeras e de intercomunicadores, além do projeto de sonorização que permita ao CCO ouvir o som ambiente durante as viagens. Os trens recentemente adquiridos pela Companhia do Metrô para as linhas que opera são igualmente equipados com câmeras.

Embora essas medidas sejam compreensíveis no contexto da operação complexa de um metrô, e sobretudo de uma linha que dispensa o grande guardião das viagens, o condutor, é preciso observar que toda assistência é, em alguma medida, *restritiva*. Como explorei em *Trilhos da cidade* (Caiafa, 2013), quando se orienta o usuário com a sinalização para que se desloque no espaço do metrô, se está ao mesmo tempo direcionando e controlando seu percurso, ou seja, impedindo -o, em alguma medida, de se deslocar. Quando se lhe oferece a assistência do agente, que tem poder de polícia, ou da câmera que tudo observa, se o vigia e controla também.

MONITORAMENTO E PILOTAGEM

Como vários interlocutores me disseram e eu mesma constatei, o CCO da Linha 4 é mais "enxuto" do que o da Companhia do Metrô. Em cada console há um operador, às vezes dois, além do supervisor. O segundo é um auxiliar escalado sobretudo em hora de pico. Vi também que os operadores são bem jovens. Já o supervisor era um pouco mais velho, tendo trabalhado na Companhia do Metrô. Na Linha 4, foi preciso combinar a experiência de profissionais, em geral oriundos do Metrô, e o treinamento de gente nova. A renovação era desejada no contexto da operação privada, que enfatizou o imperativo de produtividade. A população jovem no CCO me pareceu não destoar do ambiente de máquinas e imagens digitais, o que me fez lembrar uma parte da conversa com um profissional que registrei no caderno de campo:

> Conversamos que os mais jovens têm mais facilidade em lidar com novas tecnologias. Observou que explicava a eles, contudo, que não se tratava de vídeo game, que era real. Rimos mas, em seguida, isto me fez pensar, pois de fato as salas de controle têm estratégias comuns com esses jogos, envolvendo as mesmas exigências de um tipo de atenção e uma atividade de pilotagem.

A ênfase no monitoramento a distância caracteriza cada vez mais a operação dos metrôs e, particularmente presente nas linhas automáticas, organiza, como constatei, a operação da Linha 4. Um caso interessante é o da posição especial do supervisor de estação. Aprendi que esse profissional perde parte de sua autoridade no contexto de uma linha automática, tendo constatado este fato tanto na Linha 4 do metrô de São Paulo quanto na Linha 1, também automática, do metrô de Paris.

Na Linha 4, a estrutura matricial e radial determina que as decisões operacionais caibam antes de tudo ao CCO, diferente do que se passa nas outras linhas da rede paulista. O supervisor de estação torna-se sobretudo o chefe local dos agentes. Verifica, por exemplo, quem chegou atrasado, se o agente fez a barba, como está o uniforme. Ele também se ocupa da operação mas, nessa função, se torna antes de tudo um informante do CCO. E quando discordam sobre uma decisão a tomar? Em geral as partes negociam. Parece, portanto, que vai depender da relação que se consiga cultivar no momento e mesmo, certamente, da personalidade das pessoas envolvidas. Um profissional do CCO observou, em conversa comigo:

> Então a gente toma muita decisão compartilhada. Eu... eu, por exemplo, o próprio Console de Passageiros, ele sugere, fala "ó, mas olha, eu tô monitorando aqui e eu tô vendo que não tem uma necessidade tão grande, porque o carregamento não tá assim..." Mas se ainda assim o supervisor [de estação] entender que é uma necessidade, a gente tá aqui pra atender, então a gente vai tomar essa decisão junto.

De toda forma, no tipo de operação vertical tendo à frente a orientação e o comando vindos de uma sala de comando central, como o CCO, esse chefe que fica no campo, na linha, também é vigiado, por mais que possa haver afabilidade no trato entre eles.

Vimos mais acima como se trata, no CCO, da observação de uma *população em movimento*. Acrescentemos que os agentes de estação também fazem parte dessa população, também são

observados nos seus itinerários na linha, quando circulam ou quando se detêm na cabine, em torno dos bloqueios, nas transferências. É fato que estes também vigiam, reportam ao CCO e agem sob a sua orientação.

Monitoramento é, a meu ver, a melhor palavra para caracterizar esse tipo de observação, feita sobretudo a partir do CCO mas também de alguma forma "distribuída" aos agentes na linha. Monitor, em português, é aquele "que dá conselhos, lições, que admoesta" (Ferreira, 1999). Pode ser também o sargento ou auxiliar de oficial que, na Marinha, instrui os subordinados em certa atividade. É, ainda, o monitor de vídeo. O primeiro sentido elencado para "monitorar" no dicionário mencionado, é acompanhar e avaliar dados provindos de aparelhos técnicos. Pode referir-se também a avaliação de "riscos e oportunidades". Os aspectos da intermediação da máquina, do acompanhamento com instrução, da detecção de riscos e intervenção na oportunidade, além da tonalidade de comando militar — evocando a origem bélica das salas de controle — a meu ver cabem como uma luva.

Explorando um pouco mais a questão da associação entre antigas e recentes estratégias de vigilância, notemos, em relação aos usuários, que constituem, apenas momentaneamente, uma *massa*. A inscrição numa massa é uma das características do regime panóptico, que nos controla ao mesmo tempo como indivíduos. Os usuários da Linha 4 são, literalmente, *passageiros*. Não têm um número de matrícula que os fixe na massa, mas sua entrada fica registrada na linha de bloqueio. Outra forma de localizá-los e fixá-los momentaneamente nessa *população em fluxo* são as estatísticas produzidas a partir de sua passagem. Elas constituem parte da própria matéria dos relatórios necessários à operação da linha. Registrados ali e também nas imagens digitais das telas do CCO, tornam-se parte de um *banco de dados*. Nas novas estratégias de controle, como observou Deleuze (1990), as massas se tornaram "amostras, dados, mercados ou 'bancos'". Os agentes na linha também são em alguma medida fixados como bancos de dados.

Não só*monitorar*, mas *pilotar*, agir desde o ponto de observação. Vimos que o CCO modernizado está capacitado a realizar mais operações a distância, como injetar um trem na linha. Constatei, por outro lado, que algumas dessas capacidades podem ser usadas apenas ocasionalmente. É comum que se delegue aos agentes em campo, por exemplo, ligar e desligar uma esteira. No começo do dia pode ser possível mas, nos espaços muito povoados, o agente humano presente no local é mais confiável. Por outro lado, os agentes são também pilotados a distância no contexto das contingências da operação, como vimos no caso do supervisor de estação. Vimos também que se negocia, pois é preciso ponderar quando de trata de uma população humana, mesmo com o crescente investimento nos maquinismos. Permanece, contudo, a aposta que caracteriza esta e outras salas de controle, figuras do advento do digital, qual seja, a de que se pode *pilotar um conjunto de acontecimentos a distância*. Aposta, aliás, que rege a lógica dos vídeo games e, como observa Picon (s/data), é uma característica das chamadas cidades inteligentes.

É interessante observar que, ao mesmo tempo, aspectos da sociabilidade humana podem interromper ocasionalmente a pilotagem. Vimos como a estrutura vertical pode se dobrar em

alguma medida a negociações no caso do supervisor de estação. As próprias máquinas digitais, sofisticadas que são, podem sofrer um embaralhamento, por vezes inexplicável até para os operadores, e a situação demandar que os humanos acorram ao local e tentem achar uma solução. É o caso, por exemplo, de problemas na interface das portas de plataforma com as portas do trem (Caiafa, 2015b), região bastante sensível que, na linha automática, perde o seu guardião mais garantido, o condutor. Todas as plataformas da Linha 4 têm essas portas, como é comum nas linhas automáticas. Nem sempre é possível pilotar de longe.

E, ainda, ponto que abordei em outro trabalho (Caiafa, 2015a), há o fenômeno interessante da presença constante de um agente nos trens da Linha 4, preparada, como observei acima, para funcionar na modalidade "unmanned". De fato, segundo entendi, ele é posto a trabalhar a serviço do CCO para garantir o bom funcionamento da máquina. Não foi possível confiar apenas na pilotagem a distância. Parece que a presença humana questiona os novos modelos de vigilância, mesmo que se insira neles também, como vigilante e vigiado. Numa conversa comigo, alguns agentes de estação disseram que eram "as meninas dos olhos do CCO". Eco, talvez, dos ritornelos do treinamento que receberam, esta frase — dita com uma sinceridade por que lhes sou grata — soou para mim um tanto perturbadora, talvez pela carga poética aliada à atividade pesada da vigilância.

NOTAS

* Professora Titular/Escola de Comunicação-Universidade Federal do Rio de Janeiro. Ph.D., Antropologia, Cornell University. Contato: janicecaiafa@gmail.com.

1. Cf. cidade.ibge.gov.br

2. Cf. http://www.metro.sp.gov.br/metro/institucional/quem-somos/index.aspx. Acesso em: 8 de fevereiro de 2016.

3. As Parcerias Público-Privadas (PPP) são contratos de concessão em que o parceiro privado, além de realizar a operação, faz investimentos em infraestrutura. Estes são amortizados e remunerados pelo aporte de verbas públicas a partir do início efetivo da prestação do serviço.

REFERÊNCIAS

Alouche, P. L. (1987). O transporte metro-ferroviário nas regiões metropolitanas. *Revista dos Transportes Públicos. ANTP*, 10 (38).

Alouche, P. L. (1990). A tecnologia dos metrôs do mundo. *Revista dos Transportes Públicos – ANTP, 12* (49), setembro, 43-51.

Alouche, P. L. (2012). Automação dos metrôs: até que nível chegar? *Revista Ferrovia,* n 6.

Bruno, F. (2010). Mapas de crime: vigilância distribuída e participação na cultura contemporânea. In F. Bruno, M. Kanashiro & R. Firmino (Org.). *Vigilância e Visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina.

Caiafa, J. (2013) *Trilhos da cidade: viajar no metrô do Rio de Janeiro*. Rio de Janeiro: Editora 7Letras.

Caiafa, J. (2014). Dinâmicas da experiência de automatização integral da condução no metrô de Paris. *Contemporânea, 12* (03), setembro-dezembro, 595-613.

Caiafa, J. (2015a). Automação e presença humana na Linha 4-Amarela do metrô de São Paulo. *Galáxia*, n. 29, junho, 83-95.

Caiafa, J. (2015b). Comunicação e sociabilidade no metrô de Paris: aspectos de um regime de interfaces. *E-Compós, 8* (3), 1-17.

Caiafa, J. (2016). O metrô de São Paulo e o problema da rede. *Contemporanea, 14* (2).

David, A. (1995). *RATP. La métamorphose*. Paris: InterEditions.

Deleuze, G. (1990). *Pourparlers.* Paris: Les Éditions de Minuit.

Ferreira, A. B. de H. (1999). *Novo Aurélio Século XXI*. Rio de Janeiro: Nova Fronteira.

Foucault, M. (1987). *Vigiar e punir*. Petrópolis: Vozes.

Hess, D. J. (2007). *Alternative Pathways in Science and Industry: Activism, Innovation, and the Environment in an Era of Globalization*. Cambridge and London: The MIT Press.

Latour, B. (1991) Transférer les projets dans la réalité. In D. Chevallier (Org.). *Savoir faire et pouvoir transmettre: transmission et apprentissage des savoir-faire et des techniques*. Paris: Ed. de la Maison des sciences de l'homme.

Paula, A. S. de. (2015). *Parceria Público-Privada — Linha 4-Amarela — Expectativas e Resultados*. (Relatório), 21ª Semana de Tecnologia Metroferroviária. AEAMESP,.

Picon, A. (s/data). *Smart Cities*. (Coleção Actualités). Éditions B2.

São Paulo não para de crescer. (s/data). Os investimentos na melhoria dos transportes urbanos. [Folheto] Companhia do Metropolitano de São Paulo, Diretoria de Planejamento e Expansão dos Transportes Metropolitanos – DM.

Souza, M. A. A. de. (2015). Território e lugar na metrópole. In A. F. A. Carlos & A. U. Oliveira (Org.). *Geografias de São Paulo: a metrópole do século XXI*. São Paulo: Contexto.

Rodrigues, J. C. (2006). Uma paixão cega pelos meios visuais? In *Comunicação e significado: Escritos Indisciplinares.* Rio de Janeiro: Editora PUC-Rio/Mauad X.

Villoutreix, F. (1990). Modalités d'étude, de conception et d'introduction de systèmes intégrés d'automatismes. 339 f. Tese (Doutorado). École Nationale Supérieure des Mines de Paris.

OBJETOS Y NATIVOS DE LA VIGILANCIA. REFLEXIONES SOBRE LA CONSTRUCCIÓN DE LA VIDEOVIGILANCIA COMO OBJETO ETNOGRÁFICO DESDE UNA INVESTIGACIÓN EN CURSO.

Resumen: El presente trabajo se propone aportar al campo de estudios sobre la videovigilancia, presentando y problematizando algunos avances de una investigación en curso. El uso de sistemas de videovigilancia ha experimentado en las últimas décadas una constante expansión, al punto de incorporarse como elemento cotidiano de la mayoría de los paisajes urbanos latinoamericanos. Aunque incipiente, el campo de estudios locales sobre este fenómeno ya ha producido algunos aportes sustanciales. Comenzaremos ubicando nuestra pregunta por el funcionamiento cotidiano de un sistema de videovigilancia en una línea de acercamientos etnográficos a las salas de monitoreo. De estos estudios recuperaremos el rechazo a la "sobredeterminación técnica" y el interés explícito por la incorporación del "factor humano". Sin embargo, tener en cuenta los discursos, prácticas y perspectiva de los actores, en este caso operadores/as de cámara y otros/as trabajadores/as, no debe llevarnos al extremo opuesto: el olvido del papel fundamental que desempeñan distintos dispositivos tecnológicos en el funcionamiento de la videovigilancia. En diálogo también con etnografías previas, intentaremos desplegar algunas de las consecuencias metodológicas de adoptar una mirada latouriana sobre las redes de agenciamientos sociotécnicos que conforman los "vigilantes electrónicos". Esperamos de esta forma aportar a la discusión de nuevas preguntas de investigación, centrándonos en sus implicancias para la proyección y realización de trabajos de campo que sustenten un acercamiento empírico a la videovigilancia.

Palabras clave: Videovigilancia, Etnografía, Factor humano, Objetos, Vigilantes electrónicos.

MARTÍN JAVIER URTASUN*

Objetos e nativos da vigilância. Reflexões sobre a construção da videovigilância como objeto etnográfico a partir de uma investigação em curso.

Resumo: Este trabalho procura contribuir com o campo de estudos da videovigilância, apresentando e problematizando alguns avanços de uma investigação em curso. A utilização de sistemas de videovigilância têm experimentado nas últimas décadas uma expansão constante, sendo incorporados como elementos cotidianos da maioria das paisagens urbanas da América Latina. Embora incipientes, o campo local de estudos deste fenômeno já produziu algumas contribuições substanciais. Começamos colocando nossa pergunta sobre o desenvolvimento diário de um sistema de videovigilância em relação às linhas de abordagen etnográficas das salas de monitoramento. A partir desses estudos recuperamos a rejeição da "sobredeterminação técnica" e o manifesto interesse em incorporar o "fator humano". No entanto, tendo em mente os discursos, práticas e perspectivas dos atores - neste caso operadores/as de câmera e outros trabalhadores/as - não deve nos levar ao extremo oposto: esquecer o papel fundamental dos diferentes dispositivos tecnológicos na operação da videovigilância. Em diálogo com etnografias anteriores, tentamos implementar algumas orientações metodológicas do enfoque latouriano nas redes de agenciamiento sócio-técnico que integram os "vigilantes eletrônicos". Assim, esperamos contribuir à discussão de novas questões de investigação, nos centrando nas implicações para o planejamento e realização de trabalho de campo que apoie uma abordagem empírica da videovigilância.

Palavras-chave: Videovigilância , Etnografia , Fatores humanos, Objetos , Vigilantes eletrônicos.

Objects and natives of surveillance. Reflexions on video surveillance as an object for ethnographic research from an ongoing investigation.

Abstract: This paper aims to contribute to the video surveillance studies field by presenting and problematizing some advances of an ongoing investigation. The steady growth of video surveillance systems in recent decades has led to them becoming a regular part of Latin American cityscapes. Although the local field of studies of this phenomenon is still incipient, it has already produced some substantial contributions. We begin placing our question for daily operation of a video surveillance system among the ethnographic approaches to monitoring rooms. From these studies we recover the rejection of "technical overdetermination" that leads to the incorporation of the "human factor." However, keeping in mind the speeches, practices and perspectives of the actors - in this case, camera operators and other CCTV workers - should not lead to the opposite extreme: forgetting the fundamental role that different technological devices play on video surveillance systems operation. In dialogue also with previous ethnographies, we try to deploy some of the methodological implications of adopting a Latourian look on socio-technical networks assemblages that make up the "electronic surveillants." By doing so we hope to contribute to the discussion of new research questions, focusing on its implications for planning and conducting fieldwork to underpin an empirical approach to video surveillance.

Keywords: Video surveillance, Ethnography, Human factor, objects, Electronic surveillants.

RECONSTRUYENDO UN HÍBRIDO EN SUS ESTADOS DEL ARTE

El uso de sistemas de videovigilancia ha experimentado en las últimas décadas una constante expansión, al punto de incorporarse como elemento cotidiano de la mayoría de los paisajes urbanos latinoamericanos. En Argentina, el uso de “cámaras de seguridad” para la vigilancia del espacio público fue una de las innovaciones más llamativas en materia de políticas públicas de seguridad durante la última década (Sozzo, 2014), ligada a su vez al creciente interés y protagonismo de los municipios en la materia (Sozzo, 2009; Montagna y Urtasun, 2014) y a sus estrategias electorales (Lío, 2012). Su creación pone en contacto diversos elementos, nuevos y preexistentes, trazando relaciones que se aglutinan en distintos puntos de la trama urbana. Las redes de asociaciones resultantes incluyen operadores/as de cámara, personal técnico y policías, pero también a las propias cámaras, sus enlaces inalámbricos o por fibra óptica, servidores, softwares

e imágenes, involucrando a su vez a más actores como el poder judicial, las empresas que comercializan las cámaras, los gobiernos, las fuerzas policiales, las organizaciones políticas y los medios de comunicación.

Esta primera descripción pone en relieve que "las cámaras de seguridad", metonimia con la que muchas veces se habla del sistema o la red en su conjunto, no son solamente "cámaras". La innovación no se reduce a la introducción de un nuevo componente tecnológico, más o menos transparente y neutral, que se incorpora simplemente como una herramienta más en la "lucha contra el delito". Por el contrario, consideramos a la videovigilancia como una red sociotécnica, capaz de conectar un amplio abanico de materiales y agencias heterogéneas. Ni puramente actor, ni puramente objeto, un sistema de videovigilancia puede ser entendido como el resultado de procesos de hibridación por el que humanos y no humanos se articulan creando un "cuasi objeto" (Domènech y Tirado, 1998).

Este carácter híbrido de la red, usualmente dejado de lado en los discursos públicos y académicos sobre la videovigilancia, será el foco de nuestra atención. Intentaremos desplegar algunos de los interrogantes teóricos y metodológicos que de él se desprenden, tomando los recorridos teóricos y empíricos que conforman nuestra propia investigación en curso sobre un sistema de videovigilancia municipal como escenario concreto en el que plantear estos desafíos. Pero primero nos interesa recuperar algunos elementos de los debates sobre el llamado a una "simetría generalizada", radicalización del principio de simetría propuesto por David Bloor (1998) y reformulado por autores de la llamada "teoría del actor-red", para poder luego volver al cuerpo de investigaciones que conforman el estado del arte sobre la videovigilancia bajo esta particular clave de lectura.

En "Nunca fuimos modernos" Bruno Latour utiliza la metáfora de una constitución moderna para señalar el proyecto nunca acabado de purificación de las instancias de la realidad en dos colectores opuestos, "naturaleza" y "sociedad" (Latour, 2007). Con su llamado a practicar una "simetría generalizada", el autor nos indica la necesidad de abandonar tanto "naturaleza" como "sociedad" en tanto categorías excluyentes fijadas a priori, para dar lugar a lo que de hecho es el producto propio del proyecto moderno: la proliferación de todo tipo de híbridos en los que difícilmente se puedan aislar y repartir entre los pares dicotómicos "determinado / indeterminado", "regular / mutable" o "ley / significado". El precio de perder esta simetría y "ver doble" es alto: se pierden los vínculos y mediaciones que están en el corazón de estas innovaciones, cayendo en un abismo insoluble entre los aspectos previamente "purificados". En "Reensamblar lo social" el autor profundiza y sistematiza su propuesta teórica, identificando las fuentes de incertidumbre que debemos considerar para poder rastrear las múltiples asociaciones que constituyen los híbridos e insistiendo en la necesidad de no saltearse pasos en la descripción de los seres, relaciones y agencias que los hacen posibles (Latour, 2008). La noción de "actor-red" se refiere entonces al resultado, más o menos inestable, de los intentos de traducción y enrolamiento que asocian elementos heterogéneos, sin poder establecerse de antemano quiénes lograrán imponerse o quiénes rechazarán el papel que se les intenta asignar (Callon, 1986). La tarea del analista es,

para estos autores, rechazar el cierre prematuro de las "cajas negras" mediante una descripción pormenorizada de que permita desplegar las controversias y los sustratos comunes que las componen, volviendo rastreable la tarea de ensamblado que llevan adelante los propios actores (Latour, 2008b).

¿Cómo se expresan estas posibilidades y desafíos en los estudios sobre videovigilancia? A pesar de ciertas dificultades para constituirse en un campo con una agenda propia (Arteaga, 2012), las ciencias sociales Latinoamericanas han realizado avances en la investigación y problematización de los sistemas de videovigilancia de la región. Podemos organizarlos en función de los ejes y preguntas en los que se centran: lo evaluativo (medición de eficacia), lo normativo (violación a la privacidad), lo simbólico (construcción de sentidos, mensajes políticos), lo espacial (percepción, producción y control de territorios) y lo cotidiano de su funcionamiento (redes de agenciamientos sociotécnicos) (Lío y Urtasun, 2015). Cada eje posee una diversidad interna de métodos, conceptos y enfoques, y existen estudios que cruzan distintos ejes, por lo que se trata de una división en cierto punto arbitraria. Sin embargo, buena parte de la producción académica puede encasillarse siguiendo esta grilla, a la que podríamos agregar los discursos propios de quienes promueven activamente la videovigilancia, como funcionarios políticos y administrativos, pero también empresarios productores y vendedores de las cámaras y otros componentes tecnológicos.

¿De qué materia están compuestos los "sistemas de videovigilancia"? Aunque no formulen directamente esta pregunta engañosa, los cinco ejes pueden reorganizarse en función de las formas subyacentes en que de hecho la responden. En este sentido los estudios evaluativos son seguramente el ejemplo más claro de naturalización: toman la videovigilancia como una "cuestión de hecho", capaz de ser medida cuantitativamente respecto a su eficacia en la baja de las tasas de delito. Al poner en primer lugar los aspectos técnicos la videovigilancia se asemeja a un objeto natural: obedece regularidades y debería ser considerada de la misma forma calculadora y neutral con la que se planifican los medios adecuados para lograr cierto fin en el mundo externo. Al igual que buena parte de los discurso que promueven la videovigilancia, este tipo de estudios no pone en duda su vínculo necesario con la baja de las tasas de delito, como principal punto a ser estudiado y comprobado. Para los estudios evaluativos la videovigilancia es, ante todo, un dispositivo tecnológico orientado a un fin claro, transparente. No hay nada detrás que considerar, más allá de los efectos concretos que debemos medir para considerar su eficacia.

A esta naturalización podríamos oponer una orientación diametralmente opuesta: aquella que encuadra a la videovigilancia como forma visible de distintas fuerzas sociales subyacentes. Este enfoque se aleja de los discursos institucionales que promueven el uso de cámaras de seguridad para marcar que no se trata de dispositivos transparentes, sino de vehículos que actualizan agencias mucho mayores. Las videovigilancia pasa entonces a ser un ejemplo de profundos cambios epocales o transformaciones globales ("Sociedad de la información", "Sociedad de riesgo", "Modernidad Tardía", "Sociedad de la vigilancia" etc.), registradas por otro lado fundamentalmente en Europa y Estados Unidos, cuyas características son teorizadas por los

máximos referentes de las ciencias sociales. La investigación empírica cumple entonces el rol de importación de conceptos y su aplicación al caso local, ilustrando los desarrollos teóricos previos. Siguiendo la propuesta de Latour (2008) podemos identificar cómo estos discursos operan las típicos movimientos de la "sociología de lo social": el fenómeno particular es subsumido como caso de aplicación de alguna explicación social multipropósito basada en una serie acotada de verdaderas agencias reconocidas por el analista, aun cuando no agreguen capacidad explicativa alguna.

Los ejes orientados a las dimensiones espaciales y simbólicas suelen adoptar como punto de partida no explicitado la creencia en "lo social" como materia que conforma los sistemas de videovigilancia. Es el caso de ciertas investigaciones que adoptan la perspectiva de las Tecnologías de la Información y la Comunicación para pensar las transformaciones en el espacio urbano y las formas en que revolucionan al campo de la seguridad (Firmino y Trevisan, 2012; Firmino y Duarte, 2015), pero, sobre todo, es el peligro de algunos usos de Michel Foucault. Quienes intentan estudiar a la videovigilancia desde las ciencias sociales encuentran en su obra, en particular *Vigilar y castigar* (2008), una referencia casi obligada. Su análisis del panoptismo como dispositivo arquitectónico capaz de maximizar el poder disciplinario sobre quienes son sometidos a una vigilancia constante e inverificable, encuentra todavía ecos en muchos acercamientos contemporáneos a las cámaras de seguridad. Aunque la medida en que la videovigilancia actual puede ser pensada en términos panópticos es tema de debate, encontrando defensores (Simon, 2005; Cameron, 2004; 2002; Gray, 2003), detractores (Koskela, 2003; Lianos, 2003) y múltiples redefiniciones (Bauman y Lyon, 2013), la metáfora panóptica ha logrado cautivar la imaginación por su capacidad de combinar el despliegue de un aparato teórico elegante y sofisticado, junto con la pretensión explícita de relevancia política con fines críticos y emancipatorios. La videovigilancia pasa a ser sinónimo de disciplinamiento y control social, tecnología de gobierno de poblaciones o biopoder, capaz de identificar y marginar a sujetos o poblaciones "peligrosas" para proteger los espacios privilegiados de acumulación del capital. Todos estos efectos de dominación se dan por sentados, relegando la necesidad de investigaciones empíricas en profundidad que indaguen sobre los efectos reales de tales dispositivos, los elementos que los componen y su funcionamiento. Estos usos de la obra de Foucault suelen correr los riesgos más claros de sostener "sociologías críticas" que no sólo movilizan explicaciones sociales superfluas, sino que pretenden verificar su pertinencia a partir de la oposición que despierten entre los actores investigados.

Como señala el propio Latour, que la sociología de lo social no sea capaz de rastrear las nuevas asociaciones y desplegar sus controversias no quiere decir que sus discursos no tengan efectos. De hecho, la movilización de explicaciones sociales generales ha demostrado tener un gran potencial normalizador (Latour, 2008). Desde los lugares que adoptan para acercarse al fenómeno, cada discurso muestra su capacidad de encender debates y polémicas sobre la pertinencia de este tipo de "sistemas", su eficacia y efectos en el delito, su carácter simbólico y su valor electoral, su papel en tanto tecnologías de gobierno, así como las necesidades de regulación o limitación.

Es la perspectiva jurídica la que ha generado las principales críticas públicas a la videovigilancia, operando en ciertas situaciones la presión necesaria para generar nuevas leyes y marcos normativos (Cardoso, 2013). Sin embargo, el interés directo por la actividad política de problematización, enrolamiento y movilización de aliados no debe confundirse con el reconocimiento y despliegue de las distintas fuentes de incertidumbre que atraviesan los vínculos y mediadores propios de un actor-red. De hecho, las denuncias legales suelen sostenerse prescindiendo de la producción de conocimiento empírico sobre la videovigilancia.

Leída en una clave simétrica, buena parte de la bibliografía disponible sobre la videovigilancia oscila entre la naturalización de los aspectos técnicos como "cuestiones de hecho" y su subsunción a mero ejemplo de procesos sociales más amplios. Sin embargo, podemos encontrar en los escasos trabajos que abonan al quinto eje - el funcionamiento cotidiano - algunos aportes a la tarea de abrir estas cajas negras, rastrear los elementos heterogéneos que las componen y desplegar sus relaciones. Podemos presentar estos avances como intentos de rechazar una purificación apresurada de los híbridos en cuestión, deteniéndose en las formas en que "humanos" y "no humanos" se asocian para conformar las complejas redes de agenciamientos sociotécnicos que conforman los "vigilantes electrónicos" (Cardoso, 2011).

UNA TRIBU DE HUMANOS POBLANDO AL DISPOSITIVO

El interés por el desarrollo cotidiano de la tarea de vigilancia y el funcionamiento del dispositivo ha inspirado una incipiente línea de estudios etnográficos en las salas de monitoreo. Más allá de las diferencias entre casos y perspectivas adoptadas, ya desde las primeras etnografías del mundo anglosajón (Norris y Armstrong, 1999, Smith, 2004; Walby, 2005) y entre los trabajos que comienzan a surgir en América Latina (Cardoso, 2010a; Firmino y Trevisan, 2012; Urtasun, 2016) se comparte el reconocimiento de actores, y no solamente "cámaras de seguridad", como parte fundamental de los sistemas de videovigilancia. Actividades que van desde la instalación, mantenimiento, vigilancia y "operación" o "monitoreo" de las cámaras, hasta la interpretación, registro y circulación de las imágenes producidas, muestran que estos sistemas están también compuestos por personas cuyo trabajo es un componente vital, sin el cual los artefactos tecnológicos dejan de tener sentido alguno.

El primer aporte de los estudios etnográficos al despliegue de los híbridos implicados en los "vigilantes electrónicos" va entonces en dirección a estos actores, en una posición que suele condensarse apelando a la idea de incorporar el estudio del "factor humano". Este señalamiento se construye explícitamente como una crítica al "determinismo técnico" o "sobredeterminación técnica" por el cual se naturalizan los elementos "técnicos" como los únicos relevantes del sistema. Estos determinismos, señalan los autores, son defendidos por investigadores tanto como por políticos, empresarios y administradores, pudiendo a su vez sustentar posicionamientos entusiastas o críticos. En todos los casos el punto en común es la creencia en que las cámaras de seguridad, su cantidad y capacidades técnicas, así como en las redes inalámbricas o de fibra

óptica utilizadas para transportar las imágenes, pueden, por sí mismas, explicar los efectos del sistema, los intereses que representa, su éxito o fracaso. Quiénes las vigilan, cómo son seleccionados /as, cómo detectan algo "sospechoso", cuánto cobran o qué formación tienen, se vuelven de esta forma datos irrelevantes.

Frente a esta simplificación, los acercamientos etnográficos a las salas de monitoreo se proponen recuperar la complejidad propia de la vigilancia. Aunque no se descarta el uso de otras técnicas, como la entrevista a informantes clave, la observación directa del trabajo de los y las vigilantes cumple un lugar fundamental. Dada la exposición política y mediática a la que se somete a los y las encargados/as de los sistemas de videovigilancia, sus discursos suelen mostrar un fuerte peso de la imagen institucional que se desea proyectar, omitiendo o distorsionando muchas veces elementos cruciales de la tarea de vigilancia tal como la experimentan otros actores del sistema, en particular los y las operadores/as de cámara. En lugar de movilizar explicaciones sociales basadas en teorías o conceptos "críticos", el o la etnógrafo/a busca lograr distanciarse de la versión institucional mediante un mayor conocimiento empírico del fenómeno. Compartir el trabajo abre la posibilidad a resituar al investigador/a, desplazándose de la típica figura de la visita periodística hacia nuevos vínculos, más cercanos y duraderos. Sobre esta base se pretende seguir a los actores, describir sus prácticas, reconstruir sus relaciones y conflictos.

El estado incipiente de esta línea de investigación y la falta de trabajos en profundidad que sustenten comparaciones limitan aún su productividad (Urtasun, 2014). De todas formas, algunos de los hallazgos producidos pueden ubicarse dentro de las coordenadas previstas por los acercamientos foucaultianos a la videovigilancia, como por ejemplo la racialización de las consideraciones de peligrosidad en función de marcadores físicos (Walby, 2005; Cardoso, 2010a), mientras que otros apuntan a un conjunto de elementos insospechados: el peso del "factor aburrimiento" en la experiencia de operar las cámaras (Smith, 2004), los cruces y reenvíos entre la mirada vigilante y el voyeurismo (Cardoso, 2010b), la tensión que implica la "dilución de la mirada" ante el crecimiento del sistema y la paradoja de los "hechos captados en el acto" (Cardoso, 2012) o el peso de informaciones externas, como las comunicaciones radiales de la policía, como guía para la búsqueda de eventos relevantes (Urtasun, 2016). Al recuperar la perspectiva de quienes trabajan en ellos, los sistemas de videovigilancia dejan de ser maquinarias homogéneas y los dispositivos se vuelven a poblar de conflictos, negociaciones, sentidos, experiencias y prácticas. Combinados, los hallazgos previos facilitan la comprensión de lo difícil que es lograr que efectivamente quienes son contratados/as a tal fin vigilen de forma efectiva las cámaras asignadas, generándose alrededor de su tarea toda una serie de presiones y controles, llegando al monitoreo por cámaras ubicadas en la propia sala de monitoreo (Firmino y Trevisan, 2012; Urtasun, 2012). Al mismo tiempo, una mirada atenta a las formas en que se construyen las habilidades necesarias para "detectar" una situación "sospechosa" nos lleva más acá y más allá de los saberes y técnicas como el "olfato policial" (Garriga Zucal, 2013), atravesando a la práctica de videovigilancia tanto por estereotipos sociales ampliamente difundidos como por las particularidades del medio técnico y discursivo al que deben aplicar. Las descripciones producidas

enriquecen de esta forma nuestro conocimiento de las diversas formas en que se construyen los dispositivos de videovigilancia, abriendo nuevos problemas o resituando y dando cuerpo a viejas inquietudes.

HACER UN LUGAR A LOS "NO HUMANOS" Y RASTREAR SUS ASOCIACIONES

Si bien la recuperación del "factor humano" es un aporte sustantivo, el foco de atención en los seres humanos dentro del dispositivo puede implicar el riesgo de perder nuevamente el carácter híbrido de las asociaciones que componen su objeto, olvidando esta vez prestar atención a los componentes "no humanos" de la red. Esta posibilidad puede ya estar cerrada por las perspectivas y conceptos teóricos con los que el o la investigador/a construye sus preguntas y su objeto, pero puede también expresarse de modos más sutiles. Un retorno reflexivo sobre nuestras primeras prácticas de investigación de campo, realizadas como parte del proceso de escritura de una tesina de grado (Urtasun, 2016), nos devuelve a la inevitable dimensión metodológica que deben adquirir las distintas herramientas conceptuales que nos interesa utilizar, inventar o reconstruir. En particular, cierto logocentrismo a la hora de registrar nuestras experiencias en el campo nos llevó a priorizar lo dicho durante el trabajo por sobre la descripción pormenorizada de las acciones implicadas en la vigilancia o las características particulares de las imágenes que debían ser producidas, vigiladas y "detectadas". Es en este nivel de la práctica cotidiana de investigación, en que se articulan en el quehacer etnográfico técnicas, metodología y enfoque, que se juega la posibilidad de construir descripciones lo suficientemente densas y sensibles para poder efectuar los necesarios desplazamientos de nuestra perspectiva previa como investigadores/as.

Nos interesa por lo tanto enfocarnos en un sesgo paradójico: recuperar el "factor humano" puede significar un nuevo desbalance que vuelva a romper la simetría, en la medida en que se enfatice exclusivamente la acción de los sujetos o, incluso peor, en sus palabras. Porque así como no podemos reducir toda una red de agenciamientos sociotécnicos a un par de artefactos especialmente vistosos, tampoco podemos entender qué es lo que vuelve tan peculiar al trabajo de vigilancia sin considerar las características de los "no humanos" involucrados y su vínculo con los y las trabajadores/as. La utilización de algunos andamiajes provenientes de la "teoría del actor-red" y de la sociología pragmática contemporánea pueden resultar estimulantes, siempre y cuando se les de alguna forma de expresión metodológica sin avasallar las especificidades del objeto de estudio.

Algunos trabajos han avanzado en la caracterización de estos elementos y sus vínculos indisociables con los y las operadores/as de cámara. En este sentido, podemos recuperar la propuesta de Cardoso, quien propone llamar "vigilantes electrónicos" al conjunto de asociaciones entre cámaras, computadoras, enlaces y operadores/as que conforman las unidades mínimas de videovigilancia (Cardoso, 2011). En el sistema de videovigilancia de Río de Janeiro, caso estudiado por el autor, una de las particularidades de estos "vigilantes electrónicos" es la particular distancia que muestran quienes operan las cámaras - ex policías y bomberos jubilados - para con el uso

de las computadoras y otros artefactos con los que deben lidiar todos los días (Cardoso, 2010b). Esta falta de conocimiento tecnológico práctico, compensada supuestamente por sus experiencias como agentes de calle, convertía aquellos elementos que se esperaban funcionaran como simples vehículos de las imágenes y capacidad de control, en mediadores que en ocasiones se negaban a colaborar, gravitando de hecho en el funcionamiento del sistema. Por su parte, los enlaces que componen las redes de conectividad también muestran su capacidad de resistencia, generando caídas del sistema y moldeando la forma en que se expande por la trama urbana (Barrionuevo, 2014).

Como muestran estos ejemplo, una orientación posible es buscar las huellas, más o menos latentes, de conflictos y controversias que pongan a descubierto la complejidad de las asociaciones propuestas, con sus fallas, sus reformulaciones y los nuevos intentos de traducción. Al igual que se ha propuesto para el estudio de otras innovaciones tecnológicas, podemos adoptar sucesivamente distintas perspectivas para trazar los mapas de "programas" y "antiprogramas" movilizados en distintos momentos, enrolando más o menos entidades en función de distintos propósitos (Latour, 1998). Operamos de esta forma sin presuponer fuentes estables e inmóviles de agencia y pasividad, ya que cada nuevo elemento modifica toda la red anterior. Los debates en torno a horizontes cercanos de innovación, particularmente visibles en nuestro caso por la demora en aplicar los últimos paquetes tecnológicos creados e implementados originalmente en Europa y Estados Unidos, pueden ser una lente especialmente fructífera. En particular, la utilización de cámaras con mayor resolución y de software de detección automática de rostros, patentes o hasta situaciones y movimientos sospechosos, es una oportunidad para desplegar "en vivo" las distintas ramificaciones de un cambio tecnológico.

Por otro lado, buena parte de los elementos "no humanos" de la red se encuentran tan sedimentados que su funcionamiento es puesto fuera de cuestión, como algo natural y objetivo con lo que se puede contar. El desafío aquí es mayor, ya que se trata de los componentes centrales de un sistema de videovigilancia, desde la software que permiten el control de las cámaras para la producción, circulación y registro de imágenes, hasta las características de los puestos de vigilancia y la disposición espacial de la propia sala de monitoreo. En este caso, se vuelve crucial un trabajo pormenorizado de observación y registro que evite el sesgo sistemático a favor de los elementos verbales, por sobre otras características de la situación observada.

Incorporar una mirada sobre los "no humanos" puede llevarnos también más allá de la sala de monitoreo. Como mostraba Latour de forma paradigmática en su estudio sobre Pasteur y sus descubrimientos bacteriológicos, los saltos de escala entre lo pequeño y lo grande, lo local y lo general, pueden dejar de pensarse como un salto analítico propio de la violencia teórica de quien investiga, para pasar a ser operaciones que se juegan de forma concreta en los propios ámbitos de estudio (Latour, 2008a). Extendiendo la máxima pragmática de "seguir a los actores", podemos también "seguir a los objetos", reconstruyendo sus formas de circulación y los modos en que se asocian y despliegan sus agencias sobre otros artefactos y seres humanos. Las direcciones de este seguimiento pueden ser múltiples. Como parte de un proceso de búsqueda que atravesamos

en nuestro trabajo de campo actual, proponemos dos "no humanos" que podemos seguir en distintos sentidos. En primer lugar, las cámaras pueden ser objeto de una historia propia, en los que interactúan distintos modelos y artefactos posibles con un conjunto de actores que van desde ingenieros innovadores, productores, informáticos, comerciantes e importadores, compradores y financiadores, a periodistas, investigadores/as y funcionarios políticos, técnicos capaces de instalarlas, vecinxs y sus organizaciones, así como los y las operadores/as que deben utilizarlas cotidianamente y otros consumidores del producto terminado, como policías, instancias judiciales o medios de comunicación y sus audiencias. Se trata de una red infinita de vínculos sin un criterio a priori que pueda limitar su profundización, siendo el despliegue de asociaciones una tarea siempre inconclusa. En segundo lugar, las propias imágenes producidas, "detectadas", registradas, editadas y puestas en circulación - o eliminadas - pueden ser tomadas como un elemento a seguir. Como señalaba Kevin Walby, los productos de la videovigilancia pueden ser abordados como textos que los y las vigilantes "activan", pudiendo incidir en distintos escenarios y escalas temporales "organizando lo social" (2005). Reconstruir los circuitos por los que se desplazan, sus regulaciones y negociaciones, las transformaciones que sufren en el camino y los efectos que generan, parece otra forma productiva de operativizar la mirada sobre la red y asegurarse de captar al menos algunos de los manojos de asociaciones presentes.

A MODO DE CIERRE: DISPOSITIVOS Y REDES DE AGENCIAMIENTOS

Partimos de reconocer el carácter híbrido de las redes de agenciamientos sociotécnicos que conforman los sistemas de videovigilancia, buscando en autores de la teoría del actor-red algunas claves con las que revisitar el estado de la cuestión en las ciencias sociales. Luego nos situamos en la línea de acercamientos etnográficos a las salas de monitoreo, recuperando sus interrogantes tanto sobre el "factor humano" como sobre los no humanos participantes. Creemos que ambos movimientos permiten afinar nuestras preguntas de investigación y nuestras formas de responderlas, apuntando en un mismo sentido: la necesidad de conocer y describir en su complejidad el funcionamiento cotidiano de estas redes. Sus efectos deben buscarse entonces en los modos de hacer trabajo de campo, qué registrar y de qué forma, buscando reflexivamente formas de concretar las tareas complementarias de "seguir a los actores" y "seguir a los objetos". Es en este nivel metodológico, según podemos recuperar de los problemas y limitaciones experimentadas en experiencias de investigación previas, que se juega la posibilidad de construir nuevos conocimientos, más allá de la aplicación de una u otra "gran teoría" al objeto entre manos.

Esto no debe entenderse como una limitación a los estudios de caso, sin interés por la comparación, la generalización o la construcción teórica. Ni siquiera implica descartar las preguntas de raíz foucaultiana por el poder o la dominación. Aunque abrevar al mismo tiempo en el legado foucaultiano y en la "teoría del actor-red" pueda parecer a simple vista una maniobra de un eclecticismo, creemos que ambas perspectivas pueden ser articuladas y potenciadas. Como señalan algunos de sus primeros traductores para el ámbito académico de habla hispana, en

varios de los trabajos seminales de este grupo de autores franceses la deuda con Foucault es explícita (Domènech y Tirado, 1998), reconociendo continuidades en la forma en los estudios de la ciencia y la tecnología reformulan el problema del poder (y del saber) "como si se tratara de un *efecto* de conjuntos de abigarradas y exitosas estrategias para enrolar a otros antes que como una *causa* de tal éxito" (Law, 1998:68). Como señala Latour en un artículo titulado "la tecnología es la sociedad hecha para que dure", el enigma de la dominación y su estabilidad puede aclararse reponiendo los no humanos a las tramas de relaciones que dan forma a nuestras sociedades (Latour, 1998). Desplegar y describir estas tramas hasta la saturación nos permite situar todas las explicaciones dentro de la red, sin necesidad de incluir causas generales externas. Filtrada de esta forma, la noción de dispositivo como trama que producen sujetos, objetos y saberes bajo racionalidades que los atraviesan de formas no homogéneas (Foucault, 1991) se vuelve a poblar de entidades y relaciones que altamente diferenciadas. Nuestro desafío es evitar los atajos teóricos más seductores, para de esta forma comenzar a producir y analizar nuevos hallazgos empíricos.

NOTAS

* CIMeCS, IdIHCS, Conicet - UNLP, Profesor en Sociología y Doctorando del en Ciencias Sociales – UNLP. Contacto: martinjurtasun@gmail.com

REFERENCIAS

Arteaga Botello, N. (2012) "Surveillance Studies: An Agenda for Latin America". En *Surveillance & Society*, *10* (1), 5–17.

Barrionuevo, L. (2014) Gobernar el medio. La video vigilancia policial en la ciudad de Córdoba, 2007 – 2013. Trabajo Final de la Licenciatura en Geografía, Universidad Nacional de Córdoba.

Bauman, S. y Lyon, D. (2013) Vigilancia Líquida. Paidós, Barcelona.

Bloor, D. (1998 [1976]) Conocimiento e Imaginario Social. Gedisa, Barcelona.

Callon, M. (1986) "Algunos elementos para una sociología de la traducción: la domesticación de las vieiras y los pescadores de la bahía de St. Brieuc". En A Juan M. Iranzo; Teresa Gonzales de la Fe y José R. Blanco (coords.). *Sociología de la ciencia y la tecnología*. Madrid: CIS, p.259-282.

Cameron, H. "CCTV and (In)dividuation". En *Surveillance & Society*, 2004, vol. 2, n° 2/3, 136–144.

Cardoso, B. (2010 a) "Todos os Olhos . Videovigilâncias, videovoyeurismos e (re)produção imagética na tecnologia digital". Tesis para la obtención del Doctorado en Ciencias Humanas (Antropología Cultural) Universidad Federal de Río de Janeiro.

Cardoso, B. (2010 b) "Olhares e mediações sociotécnicas: Videovigilâncias e videovoyeurismos".En *DILEMAS: Revista de Estudos de Conflito e Controle Social* - Vol. 3 - no 10 - OUT/NOV/DEZ 2010 - pp. 33-50. Río de Janeiro.

Cardoso, B. (2011) "Vigilantes eletrônicos no Rio de Janeiro: agenciamentos sociotécnicos e pesquisa em tecnologia". En *Configurações* [Online], 8 | 2011. Centro de Investigação em Ciências Sociais.

Cardoso, B. (2012) "The Paradox of Caught-in-the-act Surveillance Scenes: Dilemmas of Police Video Surveillance in Rio de Janeiro". En *Surveillance & Society* 10(1): 51-64.

Cardoso, B. (2013) "Câmeras Legislativas: videovigilância e leis no Rio de Janeiro" En *Revista Brasileira de Ciencias Sociais* Vol. 28 n° 81 fevereiro/2013.

Domènech, M. y Tirado, J. (1998) "Claves para la lectura de textos simétricos". En Domènech, M. y Tirado, J (comps.) Sociología simétrica. Ensayos sobre ciencia, tecnología y sociedad. Gedisa, Barcelona.

Firmino, R. y Trevisan, E. (2012). "Eyes of Glass: Watching the Watchers in the Monitoring of Public Places in Curitiba, Brazil". En *Surveillance & Society*, *10* (1), 28–41.

Firmino, R. y Duarte, F. (2015) "Private video monitoring of public spaces: the construction of new invisible territories". En Urban Studies, 1 – 14.

Foucault, M. (1991). "El juego de Michel Foucault", en Saber y verdad. Ediciones de la Piqueta, Madrid, pp. 127-162.

Foucault, M. (2008 [1975]) Vigilar y Castigar. Siglo XXI Editores, Buenos Aires.

Garriga Zucal, J. (2013) "Usos y representaciones del 'olfato policial' entre los miembros de la policía bonaerense". Dilemas: Revista de Estudos de Conflito e Controle Social - Vol. 6 , No 3, JUL/AGO/SET 2013, pp. 489-509.

Gray, M. (2003) "Urban Surveillance and Panopticism: will we recognize the facial recognition society?". En *Surveillance & Society, 1* (3), 314–330.

Koskela, H. (2003) "'Cam Era' – the contemporary urban Panopticon". En *Surveillance & Society*, 1 (3), 292–313.

Latour, B. (1998 [1991]) "La tecnología es la sociedad hecha para que dure". En Domènech, M. y Tirado, F. (comps.) Sociología simétrica. Ensayos sobre ciencia, tecnología y sociedad. Gedisa, Barcelona.

Latour, B. (2007 [1991]). Nunca Fuimos Modernos: Ensayo de antropología simétrica. Siglo XXI Editores, Buenos Aires.

Latour, B. (2008a [1983]). "Dadme un laboratorio y conquistaré al mundo". Versión Castellana, Ciencia , Tecnología y Sociedad, CTS, OEI.

Latour, B. (2008b [2005]). Reensamblar lo social. Una introducción a la teoría del actor-red. Manantial, Buenos Aires.

Law, J. (1998 [1986]) "Del poder y sus tácticas. Un enfoque desde la sociología de la ciencia". En Domènech, M. y Tirado, J (comps.) Sociología simétrica. Ensayos sobre ciencia, tecnología y sociedad. Gedisa, Barcelona.

Lianos, M. (2003) "Social Control after Foucault". En *Surveillance & Society*, 2003, vol. 1, n° 3, 412–430.

Lio, V. (2012) "El Municipio Vigila. Un análisis comunicacional de los sistemas de monitoreo del espacio público en manos del estado". En *Question* – Vol. 1, N.° 36 (Primavera 2012). Buenos Aires.

Lio, V. y Urtasun, M. (2015) "Devolviendo la mirada. Aportes a la construcción de preguntas de investigación en torno a la videovigilancia" Ponencia presentada en el II Congreso Latinoamericano Delito y Sociedad, Universidad Nacional del Litoral, Santa fé, diciembre 2015.

Montagna, Y. y Urtasun, M. (2014) "Prevención situacional y municipalización de las políticas de seguridad" Ponencia presentada en las VIII Jornadas de Sociología de la UNLP, La Plata, Diciembre 2014.

Norris, C., y Armstrong, G. (1999). "CCTV and the social structuring of surveillance". En *Crime Prevention Studies*, 10, 157–178.

Simon, B. (2005). "The return of panopticism: Supervision, subjection and the new surveillance". En *Surveillance & Society*, *3* (1), 1–20.

Smith, G. (2004) "Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK". En *Surveillance and Society*, 2 (2 / 3): 376-395.

Sozzo, M. (2009) "Gobierno local y prevención del delito en la Argentina". En *Urvio, Revista Latinoamericana de Seguridad Ciudadana*, No 6, FLACSO Sede Ecuador, Quito.

Sozzo, M. (2014) "Delito común, inseguridad y respuestas estatales. Inercia e innovación durante la década kirchnerista a nivel nacional en Argentina". En *Cuestiones de Sociología*, nº 10, 2014. Universidad Nacional de La Plata, Facultad de Humanidades y Ciencias de la Educación.

Urtasun, M. (2012) "Vigilar y prevenir. Procedimientos y marcos interpretativos organizando las tareas de los trabajadores detrás de las cámaras de un sistema de videovigilancia urbana". Ponencia presentada en las VII Jornadas de Sociología de la UNLP. La Plata.

Urtasun, M. (2014) "Superar el punto ciego. La vigilancia en Latinoamérica y sus estudios" En *Cuestiones de Sociología*, nº 10, 2014. Universidad Nacional de La Plata, Facultad de Humanidades y Ciencias de la Educación.

Urtasun, M. (2016) Vigilancia detrás de cámara: Acercamiento etnográfico a un sistema de videovigilancia. Tesis de grado. Universidad Nacional de La Plata. Facultad de Humanidades y Ciencias de la Educación. En Memoria Académica. Recuperado de: http://www.memoria.fahce.unlp.edu.ar/tesis/te.1245/te.1245.pdf

Walby, K. (2005) "How Closed-Circuit Television Surveillance Organizes the Social: An Institutional Ethnography". En *Canadian Journal of Sociology*, 30 (2), 189-214.

MÁS ALLÁ DE LO “SMART”: IMPLICANCIAS SOCIALES DE LAS TECNOLOGÍAS DE VIGILANCIA EN CONTEXTOS URBANOS

Resumen: El surgimiento del concepto de “Smart cities”, asociado al uso de tecnologías de la información y la comunicación orientado a la optimización de la planificación urbana, ha dado pie a una serie de discusiones a nivel global. La ponencia busca comprender tal discusión en el contexto regional, articulándose en base a tres ejes: primeramente, buscará situar la discusión en torno al concepto de “Smart city” como proyecto *modernizador* que, siendo principalmente promovido desde el hemisferio norte, requiere la adopción de nuevas tecnologías. Esto supone poner especial énfasis en la configuración de alianzas público-privadas y desarrollos institucionales para la instalación de la infraestructura requerida para el funcionamiento de “Smart Cities” en Latinoamérica, planteando así la pregunta en torno a la economía política de tales desarrollos. En segundo lugar, la ponencia indagará respecto a las políticas de promoción en torno a tecnologías “Smart” en la ciudad. Finalmente, se discutirá respecto al conocimiento y disposición, por parte de la ciudadanía, a generar datos que alimenten tales plataformas en contextos como el latinoamericano, indagando en las concepciones sobre privacidad que subyacen a tal entrega y gestión de información. Se considera, de esta forma, que la discusión en torno a “Smart Cities” plantea desafíos al menos en tres niveles: económico-políticos, regulatorios y relativos a prácticas sociales, que no han sido debidamente abordados en la región hasta el momento.

Palabras clave: Ciudades inteligentes, Vigilancia, Privacidad.

PATRICIO VELASCO F.*

Além do "Smart": implicações sociais das tecnologias de vigilância em ambientes urbanos

Resumo: O surgimento do conceito de "cidades inteligentes", associado com o uso de tecnologias de informação destinadas a optimizar o planeamento urbano, levou a uma série de discussões sobre um nível global. O documento procura entender tal discussão no contexto regional, articulado em torno de três eixos: em primeiro lugar, ele irá procurar colocar a discussão em torno do conceito de "cidade inteligente" como um projeto modernizador, sendo promovido principalmente do hemisfério norte, que exige a adoção de novas tecnologias. Isso envolve colocar ênfase especial na criação de parcerias público-privadas e desenvolvimentos institucionais para a instalação da infra-estrutura necessária para o funcionamento do "Cidades Inteligentes" na América Latina, aumentando, assim, a questão sobre a economia política de tais desenvolvimentos. En segundo lugar, a ponencia indaga sobre as políticas de promoção em torno de tecnologias "Smart" en la ciudad. Finalmente, discutimos sobre o conhecimento e vontade por parte dos cidadãos, para gerar dados que alimentam tais plataformas em contextos como a América Latina, se aprofundar nos conceitos subjacentes privacidade tal entrega e gestão da informação. Considera-se, assim, a discussão sobre "Cidades Inteligentes" coloca desafios em pelo menos três níveis: práticas sociais econômicos, políticos, regulatórios e relacionados, que não tenham sido devidamente tratados na região até agora.

Palavras-chave: Cidades inteligentes, Vigilancia, Privacidade.

Beyond “Smart”: social implicancies of surveillance technologies in urban settings

Abstract: The emergence of the concept of "Smart cities", associated with the rise of information technologies and its use oriented to urban planning has led to a series of discussions on a global level. The paper seeks to understand such a discussion in the regional context, based upon three axes: first, it will seek to place the discussion around the concept of "Smart city" as a modernizer project that requires the adoption of new technologies, being mainly promoted from the northern hemisphere. This involves putting special emphasis on setting up public-private partnerships and institutional developments for the installation of the required infrastructure for the operation of "Smart Cities" in Latin America, thus raising the question about the political economy of such developments. Second, the paper inquires about the promotion policies around "Smart" technologies in the city. Finally, we discuss about knowledge and willingness on the part of citizens, to generate data that feed such platforms in contexts such as Latin America, delving into the concepts that underlies privacy, such delivery and information management. Thus, it is considered that the discussion on "Smart Cities" poses challenges on at least three levels: economic, political, regulatory and related social practices, which have not been adequately addressed in the region so far.

Keywords: Smart cities, Surveillance, Privacy.

La siguiente ponencia tiene como objetivo discutir el carácter de las denominadas “Smart cities”, poniendo en discusión la lógica que subyace a tales proyectos, la economía-política tras su desarrollo y las estrategias de implementación que han comenzado a desplegarse en distintas latitudes. Se parte de la consideración que la emergencia de las “Smart cities” supone la implementación de tecnologías que permiten la generación y recolección de datos vinculados al desarrollo de la vida urbana de formas anteriormente no verificadas, y que pueden ser comprendidas en el contexto de lo que Bruno ha denominado como vigilancia distribuida (Bruno, 2014). Esto implicaría una serie de desafíos al ordenamiento legal existente en la materia y, sobre todo, una reflexión en torno al nivel de datos que genera la mera habitación en centros urbanos “inteligentes”.

El argumento se estructurará de la siguiente forma. En primer término, se discutirá respecto a la racionalidad de las “Smart cities”. Luego se apuntará a comprender cuál es el trasfondo económico-político de la instalación de tecnologías “Smart”. Finalmente, se expondrán las orientaciones de política pública en la materia, sus implicancias en materia de privacidad y los discursos en torno a ésta[1].

LA RACIONALIDAD TRAS LA PRETENDIDA INTELIGENCIA DE LAS SMART CITIES

Ángel Rama ha dado cuenta de la forma en que las tecnologías configuraron el espacio colonial latinoamericano (Rama, 1984). La tesis de Rama no es otra que la reflexión en torno al modo en que cierto conocimiento opera como condición de posibilidad del ejercicio del poder. En el caso de las ciudades coloniales, el foco estaba en la estabilización y manutención del poder desde la metrópoli imperial, mediante la configuración de un orden espacial (de la grilla) que se correspondía con un orden administrativo (de la palabra). Ambas tecnologías –la grilla y el idioma- fueron entonces capaces de transformar los asentamientos urbanos coloniales en dispositivos de gestión del poder real. La ciudad latinoamericana, de este modo, no surge sino como un engranaje más del proyecto colonizador español.

La independencia de España supuso, por cierto, una reconfiguración del ordenamiento espacial de las ciudades latinoamericanas. Existen casos ejemplares a tales efectos: la reconfiguración de Santiago por Benjamín Vicuña Mackenna en el contexto del primer centenario de la independencia y, por cierto, las reformas propuestas por Sarmiento y Alvear en pos de modernizar Buenos Aires a comienzos del siglo XX. Ambos esfuerzos buscaban poner a las capitales de las nacientes repúblicas a la altura de los tiempos y ello, por cierto, implicaba reconfigurar el espacio urbano. La tarea era dar cuenta que las capitales de las nuevas repúblicas latinoamericanas podían afirmar no sólo su propia independencia, sino también que fuesen capaces de incluir los últimos logros de la civilización en tal proyecto.

Así como la grilla y la palabra habían sido las herramientas de la Colonia, las grandes avenidas y los parques pasaron a constituirse como los principales dispositivos de afirmación de las repúblicas latinoamericanas. El surgimiento de las diagonales de Buenos Aires, así como de los parques de Palermo dan cuenta de ello. Semejante es lo que acontece en Santiago con el Parque Forestal y la canalización de La Cañada. La ciudad pasa a ser ahora un lugar para las masas, en el que es requerido contar con espacios que permitan tanto la exposición de ideas divergentes, como el control (estatal) de las multitudes que las proponen. Siguiendo la tesis de Gorelik, nos hallamos en este punto en un nuevo esfuerzo de lectura, desde América Latina, de los dispositivos civilizatorios existentes en Europa y, en particular, de la herencia de las modificaciones que Haussmann habría implementado en París en la segunda mitad del siglo XIX (Gorelik, 1998).

Mediante la síntesis de la herencia colonial y los esfuerzos modernizadores de principios del siglo XX, el espacio urbano latinoamericano se conforma como uno que integra su herencia colonial en espacios donde la pregunta por la aparición en el espacio público busca ser resuelta mediante la existencia de "espacios civilizatorios". Los parques, por excelencia, dan cuenta de aquel carácter: en tanto lugares donde se pone en tensión los alcances del proceso civilizatorio y la capacidad de hallarse constreñido por la mirada de los otros (Kilminster, 2007). Siguiendo la tesis de Elias, el desarrollo de este tipo de espacios supondría un nuevo estadio en los denominados umbrales de vergüenza con los que participamos en sociedad (Elias, 2000). En buena cuenta, la ciudad cuenta ya con espacios que permiten un ejercicio de autovigilancia y control de los cuerpos (Foucault, 1979).

El saber de otros, tanto como el saber de sí, se encuentra en los orígenes de esta discusión. Y la ciudad, espacio por antonomasia de la concurrencia entre distintos, es vista como el lugar preferente de promoción de comportamientos deseados. Las tecnologías disponibles –ya sea el idioma, la reconfiguración del espacio público, la construcción de carreteras o la "iluminación" de zonas urbanas con WiFi- no hacen sino responder a tales consideraciones desde las herramientas disponibles a cada época. Es posible afirmar, de este modo, que la relación entre tecnologías y ciudad no es nueva, así como la relación entre datos y ciudad tampoco lo es (Van Zoonen, 2016).

El foco en la vigilancia y el control de las masas, ya existente en los albores de la estadística del siglo XIX, adquiere ahora formas diversas. Catalizadas por las tecnologías disponibles y su ubicuidad, la observación de la ciudadanía y sus prácticas no responde a una finalidad nueva, sino, más bien, adquiere distintas modalidades.

Ahora bien, el desarrollo de nuevas tecnologías ha permitido una reconfiguración respecto a qué es lo que se puede conocer (y gestionar) sobre la ciudad. Ello supone, igualmente, repensar cuáles son los mecanismos mediante los cuales es posible disponer de tal conocimiento. Particularmente, la masificación de la denominada "internet de las cosas" ha supuesto, a través de la proliferación de sensores conectados en tiempo real, la posibilidad de surgimiento de una nueva capa de información sobre la ciudad (Dodson, n.d.). Algo semejante sucede con la proliferación de los denominados "wearable devices" –entre los que se cuentan desde Smartphones hasta la posesión de tarjetas con chip RFDI- y la generación de datos a partir de las diversas prácticas de los usuarios.

La proliferación de este tipo de tecnologías ha permitido el surgimiento de un nuevo tipo de discurso modernizador en torno a la ciudad. El foco, esta vez, está puesto en la afirmación de la ciudad como un espacio "inteligente". Lo inteligente supone la superación de lo estúpido, de lo tonto. Como antes lo moderno se superponía a lo tradicional. Ante ello, resulta razonable preguntarse quién podría querer vivir en una ciudad estúpida.

El carácter normativo asociado al despliegue de tecnologías en la ciudad va impreso en la propia denominación de las Smart cities. Se nos presenta lo nuevo no sólo como nuevo, sino igualmente como una instancia de progreso. La premisa es que las tecnologías de la comunicación permitirían una coordinación social sin precedentes en el espacio urbano. La provisión y gestión de servicios públicos se optimizaría: el transporte sería más eficiente, el manejo de residuos y la gestión del tráfico serían sólo algunos de los ámbitos que, en principio, se verían positivamente afectados por la inclusión de tecnologías "Smart". Así, estaríamos cada vez más cerca de la siempre escurridiza etiqueta del "desarrollo".

Por otro lado, el discurso en torno a las tecnologías Smart es capaz de reunir gran parte de las metáforas en torno al progreso tecnológico, la eficiencia y la modernización (sin por ello implicar modernidad). Además, el carácter masivo de las tecnologías que alimentan las tecnologías de Smart cities y su relativo bajo costo de implementación a escala vuelve plausible su extensión hacia territorios catalogados como en vías de desarrollo. De la misma forma, el mecanis-

mo de generación de datos que se articula en una ciudad inteligente dista mucho de los modos de recolección tradicionales de la estadística: ya no es un agente estatal que requiere información a la ciudadanía, es la propia ciudadanía quien genera y difunde información de potencial interés para la gestión de la ciudad.

Poco se dice en las comunicaciones gubernamentales y en la prensa de los eventuales riesgos asociados a la instalación y usos de este tipo de tecnologías. En particular, nos interesa –a nivel estructural- la discusión en torno a la economía política de tales desarrollos; mientras que en una dimensión legal, la consideración sobre la privacidad surge como un aspecto de suma relevancia.

LA ECONOMÍA POLÍTICA TRAS LAS SMART CITIES

La consideración de la ciudad como un espacio público aparece abiertamente puesta en tensión atendiendo a la proliferación de las Smart cities. La razón es simple: la generación de esta nueva capa de datos que llevaría hacia un desarrollo urbano eficiente supone, necesariamente, una inversión considerable. Es requerido desarrollar una infraestructura de datos para cada ciudad: sensores, cableado e "iluminación" con Wi-Fi son sólo algunos de los ámbitos a considerar. A tales efectos se plantea la necesidad de contar con inversión privada para la provisión de bienes públicos. Resulta imperioso, entonces, preguntarse en relación al modo en que los privados participarán de tal proyecto.

Mientras en Europa los planes de desarrollo de tecnologías Smart suponen una intensa articulación y coordinación con el gobierno local, como puede observarse en el caso de Amsterdam, en el *Big South* las inversiones para el desarrollo de ciudades inteligentes no hallan necesariamente un solo modelo de aplicación. Por ejemplo, en India, es conocido el convenio firmado con CISCO Systems para transformar 14 ciudades en Smart cities, llegando a un total 50 billones de dispositivos conectados para 2020 (Kumar, n.d.).

No existe un modelo único de integración de los intereses públicos y privados en torno al desarrollo de tecnologías Smart. En el caso de Corea del Sur se ha intentado desarrollar un plan que supone el desarrollo de una fuerte inversión pública en infraestructura que luego supondrá el desarrollo de servicios y aplicaciones por parte de los privados. Sin embargo, como ha señalado Kim, "there has been no clear definition of smart cities or consistent understanding of the concept among the stakeholders involved. It is simply dificult to build a comprehensive consensus among stakeholders on how 'smart' a smart city has to be" (Kim, 2015: 5). Por otro lado, en el caso de China, se ha observado que el despliegue del proyecto Smart cities ha supuesto una serie de conflictos con la institucionalidad –y el ordenamiento partidario- del gigante asiático: "With regard to people and communities, in China top participants are members of the party. Even if decisions are taken in a very consultative manner with groups in society, and collaboration ranks high, the fact that democracy is not in place puts restrictions on people and communities participation" (Gil & Zheng, 2015: 17).

Las diferentes tensiones existentes en el diseño, planeación y ejecución de las Smart cities puede ser ilustrado siguiendo la analogía propuesta por Kim: mientras la naturaleza de las Smart cities se funda en el concepto de gobernanza, el proceso de planificación actual aún se sostiene en la noción de gobierno (Kim, 2015). Esto supone plantear la pregunta por el rol de la ciudadanía en los procesos de diseño, implementación y evaluación de las Smart cities. Para Stimmel esto puede ser entendido de la siguiente manera: "Because the citizens of the city are now also users, the important role of addressing the societal aspects of planning cannot be underemphasized in planning exercises" (Stimmel, 2015: 122).

En el contexto latinoamericano este tipo de cuestiones pueden ser ampliamente discutidas. Por ejemplo, en 2014 Chile presentó su "Estrategia de ciudad inteligente para el transporte. Chile 2020", en el documento se asume que el tránsito hacia las ciudades inteligentes supondrá la participación de agentes tales como la academia, la ciudadanía, el sector público y el sector privado, sin por ello explicitar cuáles serán los modos específicos de integración de cada uno de estos agentes en el proceso de discusión, planeación, ejecución y evaluación de las políticas propuestas. La inclusión de tales actores se presenta como un cambio positivo, toda vez que: "a pesar de todos los esfuerzos que se han hecho y se harán bajo la lógica sectorial, el Estado no podrá resolver la complejidad de los problemas que surgen en las ciudades. Esta "ceguera cognitiva" nos ha llevado a perder de vista nuestro foco en las personas y el territorio y sobre todo a entender que se requiere, como condición de éxito, la colaboración activa de los diversos actores" (De Transportes, 2014: 16). El problema, sin embargo, es que supone la concurrencia de los diversos agentes en igualdad de condiciones, sin dar efectiva cuenta de las asimetrías existentes en un orden complejo: desde las asimetrías de conocimiento, que las más de las veces son resueltas desde la apelación a criterios técnicos, hasta las asimetrías de capital, donde los agentes inversores cuentan con primacía.

Como ha mostrado la literatura (Carvalho, 2015; Söderström, Paasche, & Klauser, 2014), la lógica tras la configuración de las Smart cities supone afrontar conflictos. No sólo desde el punto de vista de la participación ciudadana sino, igualmente, desde la lógica de integración de los intereses de los agentes privados y su rol en el espacio público. Ante ello, pareciera ser que la negación –o suspensión- del conflicto y las controversias que se verifica en los documentos oficiales supone un diagnóstico incompleto, decisión bastante poco inteligente a fines de desarrollar las mentadas ciudades inteligentes.

En América Latina el discurso en torno a las ciudades inteligentes, y su componente modernizador, ha sido fácilmente instalado en la esfera pública. Pero lo que no ha sido discutido es cuáles serán los modos en que, por ejemplo, se integrará la inversión privada en el modelo de gestión de las Smart cities. Los documentos oficiales, las más de las veces, son declaraciones de buenas intenciones que no dan cuenta efectiva de, por ejemplo, el modelo de propiedad propuesto para las inversiones requeridas. Esto es, no sabemos con certeza si las inversiones serán realizadas con cargo a rentas generales, en base a inversión privada, o si se desarrollarán modelos de

concesiones público-privadas (y cuáles serían las características de estas asociaciones público-privadas). En buena cuenta, la pregunta por quién (o quiénes) serán los *dueños* de las ciudades inteligentes –o al menos, los dueños del capital tras las inversiones requeridas- permanece abierta (Albino y otros, 2015). Ante ello, la consideración por la economía política de tales desarrollos resulta imperiosa, en vistas de conocer cuáles serán los principales intereses que se verán reflejados en las políticas implementadas.

Lo anterior es particularmente sensible en contextos como el chileno, donde las transformaciones neoliberales impulsadas durante la dictadura de Pinochet implicaron un profundo cambio en la comprensión de lo público (Solimano, 2012). La lógica del estado subsidiario, donde el estado sólo actúa como ente subsidiario y se arroga primacía a la acción privada supone, justamente, que la consideración en torno a la economía política de proyectos como el de ciudades inteligentes resulten de suyo controversiales.

Resulta imperioso, bajo la lógica de la gobernanza, que los vínculos e intereses de los diversos actores que conforman el espacio urbano se transparenten. Especialmente en lo referido a la financiación de las estructuras que permitirán la generación y el manejo de los datos que alimentan las Smart cities. Lo anterior ya nos sitúa en el conflicto en torno a la generación de datos para el funcionamiento de las tecnologías Smart y, con mayor relevancia, el debido resguardo sobre la privacidad en tales circunstancias.

VIGILANCIA DISTRIBUIDA Y PRIVACIDAD: EL RETO DE LAS SMART CITIES

Bruno ha dado cuenta de las implicancias que tiene para la vida social el participar de interacciones que pueden ser comprendidas bajo el marco de la vigilancia distribuida. Para la autora, las dinámicas de observación, conocimiento e intervención pueden ser verificadas en distintas instancias sociales, a través de la mutua implicancia de los circuitos de seguridad y control, visibilidad mediática y eficacia informacional (Bruno, 2014). No sería desacertado presentar las tecnologías desarrolladas en el contexto de las Smart cities bajo tal conceptualización. Para van Zoonen, por su parte, el principal problema de las Smart cities se encuentra relacionado con el tipo de datos que están siendo generados y la funciones que tales datos apuntan a satisfacer, sin embargo, esto ocurriría en un contexto en que "there is little attention for 'politics of city data' nor for the question how particular practices of data collection and analysis may have problematic social effects." (Van Zoonen, 2016: 1).

Por el contrario, la semántica de las Smart cities se nutre de un manto de aparente neutralidad, a favor del diseño y ejecución de planes eficientes para la gestión racional de aspectos relevantes de la vida urbana, entre los que se cuentan el transporte, la gestión de la energía, la calidad del aire y, en general, el mantenimiento de la ciudad. Todo ello, sin embargo, oculta los intereses políticos y corporativos que puedan existir tras el desarrollo de ciudades inteligentes y, a mayor abundamiento, podría desplazar el control de la ciudadanía respecto al manejo de sus datos ante la pericia de *expertos*.

Para Taylor, y en el marco de una investigación empírica con habitantes de Amsterdam, "most participants felt ambivalent about the automated collection of data in public space – they understood that the new data technologies could provide for monitoring and surveillance that could potentially make them and their property safer, but at the same time did not feel informed as to what was being used, how it was governed or what their role in giving permission was" (Taylor & Richter, 2016: 3). La generación y manejo de los datos requeridos para el funcionamiento de las Smart cities aparece así como intransparente a los ojos de la ciudadanía. El problema de fondo parece residir en el modo en que las ciudades inteligentes se nutren de los datos generados por sus habitantes: en principio resultaría difícil para la ciudadanía identificar cuándo se está entregando información requerida para el funcionamiento de los mecanismos Smart, ello supone un velo sobre la generación de datos que torna crecientemente más difícil avalar los usos realizados con éstos.

Las nociones de privacidad y resguardo de datos personales parecen todavía principalmente relacionadas a interacciones con pantallas y plataformas mediante el ingreso activo y directo de información personal, tal como dan cuenta las siguientes citas recabadas en el contexto de una investigación empírica sobre privacidad:

> *"Yo uso internet, principalmente redes sociales para informarme, o pa reírme, pero jamás empiezo a ventilar mi vida privada en estas cuestiones.Entonces, mi privacidad de internet realmente no me preocupa tanto porque yo desde el punto de vista de filtrar desde mi casa a mi computador hago una barrera anterior, cachai. Entonces tampoco es como que me vuelva loco con la privacidad"*
> José Ignacio, 36 años.

> *"Creo que [la privacidad] es manejable. Porque en realidad uno puede decidir no entregar información. O tener una cuenta paralela. Yo podría entregar una cuenta paralela, entonces podría enmascarar y no dar mi mail de siempre y dar otra. También uno sabe cuando se está metiendo a páginas que son chantas po."*
> María Eugenia, 46 años.

Tal como se muestra en las citas, el control sobre la privacidad supone el establecimiento de barreras en torno al carácter y cantidad de información que es entregada. Lo anterior es problematizado por las dinámicas propias de las ciudades inteligentes: espacios donde el mero tránsito ya resulta información relevante para quienes gestionan el espacio público. En las interacciones mediadas por pantallas y plataformas es posible tener una cuenta paralela, protegerse en la pseudonímia o en el anonimato. No podemos, sin embargo, desafectarnos de nuestros cuerpos en el tránsito urbano. La reflexión de Taylor & Richter sobre este punto es adecuada, al señalar: *"all day, spatial signatures are embedded in the technologies we use, emitted as we communicate and move around, and signalled by most of our activities. This means that the picture that builds up about us in the course of every day is behavioural, but also spatial in ways that are often opaque to us. But increasingly, it is the spatial aspect of our data that tells the most detailed story about us."* (Taylor & Richter, 2016: 7).

Se ha señalado, en relación a la proliferación de las tecnologías propias de las ciudades inteligentes, que la percepción en torno al riesgo de ciertas tecnologías puede diferir considerablemente de la seguridad efectiva de ciertos dispositivos tecnológicos (Carvalho, 2015; Taylor & Richter,

2016). Lo anterior puede explicarse atendiendo a que lo que se concede informar mediante dispositivos –ya sea tácita o explícitamente- es más bien la propia experiencia de habitación urbana, antes que informaciones o percepciones singulares. Y, toda vez que la experiencia urbana tiene un carácter subjetivo, se sigue entonces la variabilidad en las percepciones de seguridad.

Vale señalar en este punto que, tal como ha señalado van Zoonen, las preocupaciones en torno a la privacidad del público dependen igualmente de quién maneja los datos entregados. Existiría, según los datos recabados, una mayor disposición (al menos entre ciudadanas y ciudadanos europeos) a confiar información con menor recaudo hacia los bancos y organismos de salud. Por contraparte, las compañías de telecomunicación e internet (incluyendo las redes sociales) despiertan mayor desconfianza (van Zoonen, 2016). Lo anterior resulta significativo, especialmente, a la hora de evaluar cuál es el tenor de las corporaciones que se hacen parte de proyectos de Smart cities, donde se ha verificado que compañías como Telefónica han desplegado amplios desarrollos en pos de ciudades inteligentes en la región. Nuevamente, entonces, la cuestión sobre la economía política de las ciudades inteligentes se torna problemática, esta vez desde el prisma de la privacidad.

Ante este contexto no existiría un camino único capaz de hacer frente a las problemáticas que ofrece el desarrollo de las ciudades inteligentes en relación a la privacidad, tal como se ha señalado, *"the choice of smart technologies and the usage of particular (combinations of) data and analytic tools are crucial factors to understand people's privacy concerns in smart cities"* (Van Zoonen, 2016: 7)

HACIA CIUDADES REALMENTE INTELIGENTES

No sería impensable señalar, ante la intrasparencia de los proyectos de Smart cities, los nuevos desafíos que suponen para la privacidad y, con ello, la serie de preguntas que surgen en torno al resguardo de derechos fundamentales, que pueda ser una buena idea seguir viviendo en ciudades *tontas*. Huelga entonces preguntarse: ¿Cómo abordar de buena forma las ventajas comparativas que puede ofrecer la gestión tecnológica de las ciudades?

En primer término es requerido un adecuado planteamiento del problema. Las ciudades son instancias de interacción social eminentemente complejas –la verdadera revolución moderna, diría Weber, ocurre en el surgimiento de éstas. Ello supone, necesariamente, reconocer el conflicto que supone una reconfiguración tecnológica del principal espacio de interacción existente en Occidente.

Respecto a las dudas que surgen en relación a la economía política de las ciudades inteligentes el piso mínimo a exigir, creemos, refiere a la necesidad de transparentar los intereses de los actores participantes en la gestión de este tipo de proyectos. Asumir que existirá una cooperación tácita entre los diversos actores (y que existan actores predeterminados en juego) es un error. Abrir la controversia y reconocer los intereses resulta imperioso. En principio, sin embargo, lo primero que puede demandarse es mayor transparencia en las instancias de negociación y planeación de ciudades inteligentes.

Institucionalmente, además, es imperiosa la actualización de las normativas y directrices que guían el actuar estatal. La adecuada protección de los datos personales pasa, evidentemente, por una normativa que los garantice en forma, lamentablemente no es este el caso en gran parte de los países de la región, donde la normativa sobre privacidad se halla bastante desactualizada en razón de los desarrollos tecnológicos presentes.

En relación a las consideraciones sobre la privacidad y el manejo de datos resultaría importante que las organizaciones de la sociedad civil, así como agentes públicos, desarrollen campañas de concientización respecto al tipo y densidad de datos que los habitantes de las ciudades están generando cotidianamente por su mera participación en el espacio urbano. Todo ello en vistas de generar, luego, efectivas políticas de control sobre los mismos que sean prerrogativa de la ciudadanía.

Finalmente, es necesario reconfigurar la discusión en torno a los datos mismos. El criterio sobre la gestión de información parece ya no ser suficiente en el contexto actual. Se ha postulado, en este sentido, la necesidad de desarrollar lineamientos éticos en torno al manejo de datos (Floridi & Taddeo, 2016; Kitchin, 2016). Ello supone, como señala Kitchin, partir de la siguiente consideración: *"the present reality is that many smart city technologies capture data without consent or notice with respect to such a 'gifting' and are so pervasive that the gifting is compulsory with no alternatives. Moreover, the benefits of 'sharing' data are most often stacked in favour of those capturing the data, especially when they are monetized or shared with third parties and used against individual interests"* (Kitchin, 2016: 12)

NOTAS

* Investigador ONG Derechos Digitales, MSc in Media & Communications, London School of Economics and Political Science. Contacto: patricio@derechosdigitales.org.

1. La discusión en torno a privacidad utilizará discursos recabados en el marco de la investigación "Experiencia y motivaciones de uso de Internet: Usuarios Chilenos frente a la privacidad y la participación ciudadana" (2016), realizada por Gabriel Briceño y José Rioseco para ONG Derechos Digitales.

REFERENCIAS

Albino, V., Berardi, U., Dangelico, R. M., Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, *0* (0), 1–19. Recuperado de: http://doi.org/10.1080/10630732.2014.942092

Bruno, F. (2014). *Máquivas de ver, modos de ser* (p1–194). Editora Meridional.

Carvalho, L. (2015). Smart cities from scratch? A socio-technical perspective. *Cambridge Journal of Regions, Economy and Society*, *8* (1), 43–60. Recuperado de: http://doi.org/10.1093/cjres/rsu010

Subsecretaría de Transportes, Chile. *Estrategia de Ciudad Inteligente para el transporte: Chile 2020* (p1–96).

Dodson, S. (n.d.). The net shapes up to get physical. Retrieved November 4, 2016, from Recuperado de: https://www.theguardian.com/technology/2008/oct/16/internet-of-things-ipv6

Elias, N. (2000). La Sociedad de Los Individuos. Ediciones Península.

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society a: Mathematical, Physical and Engineering Sciences*, *374* (2083), 20160360–5. Recuperado de: http://doi.org/10.1098/rsta.2016.0360

Foucault, M. (1979). *Microfísica del poder*. Ediciones de La Piqueta.

Gil, O., & Zheng, T.-C. (2015). Smart cities thorugh the lenses of public policy: the case of Shanghai. *Revista Española De Ciencia Política*, *38*, 63–84. Recuperado de: http://doi.org/10.2307/781149?ref=search-gateway:f02775af60974cc83435afd1dd7449b1

Gorelik, A. (1998). *La grilla y el parque: espacio público y cultura urbana en Buenos Aires, 1887-1936*. Buenos Aires: Universidad Nacional de Quilmes.

Kilminster, R. (2007). *Norbert Elias* (p1–224). Routledge.

Kim, J. S. (2015). Making smart cities work in the face of conflicts: lessons from practitioners of South Korea's U-City projects. *Town Planning Review*, *86* (5), 561–585. Recuperado de: http://doi.org/10.3828/tpr.2015.33

Kitchin, R. (2016). The ethics of smart cities and urban science: Table1. *Philosophical Transactions of the Royal Society a: Mathematical, Physical and Engineering Sciences*, *374* (2083), 20160115–15. Recuperado de: http://doi.org/10.1098/rsta.2016.0115

Kumar, (n.d.). (22 de November de 2016) CISCO Ready to Digitally Transform 14 Cities in India. Recuperado de: http://www.smartcitiesprojects.com/cisco-ready-to-digitally-transform-14-cities-in-india/

Rama, Á. (1984). *La Ciudad Letrada*. Ediciones del Norte.

Solimano, A. (2012). Chile and the Neoliberal trap: The Post-Pinochet era. New York: Cambridge University Press.

Söderström, O., Paasche, T., & Klauser, F. (2014). Smart cities as corporate storytelling. *City*, *18* (3), 307–320. Recuperado de: http://doi.org/10.1080/13604813.2014.906716

Stimmel, C. L. (2015). Building Smart Cities. *CRC Press*. Recuperado de: http://doi.org/10.1201/b18827

Taylor, L., & Richter, C. (2016). Customers, Users or Citizens? Inclusion, Spatial Data and Governance in the Smart City. *SSRN Electronic Journal*. Recuperado de: http://doi.org/10.2139/ssrn.2792565

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 1–9. Recuperado de: http://doi.org/10.1016/j.giq.2016.06.004

(IN)SEGURANÇA PÚBLICA: CARTOGRAFIA DE RELAÇÕES ENTRE DISPOSITIVOS DE VIGILÂNCIA, POLÍTICAS PÚBLICAS E VIOLÊNCIAS EM ESPAÇOS URBANOS CONTEMPORÂNEOS

Resumo: Este trabalho aborda a associação entre dispositivos de vigilância e produção de segurança pública, concebendo a (in)segurança como resultado de múltiplos elementos que se conectam em redes sociotécnicas. Analisa, assim, algumas correlações existentes entre dispositivos de vigilância, práticas e concepções vigentes de segurança pública referentes ao controle da criminalidade e à prevenção de violências. Os altos investimentos dos órgãos de segurança pública em dispositivos tecnológicos de vigilância para o controle de crime e práticas violentas são resultantes de decisões políticas, além de técnicas, e envolvem a configuração de redes sociotécnicas de atores, exercício de poder e conhecimento. A pesquisa está sendo realizada no Brasil (Rio de Janeiro e Santa Catarina) e na Bélgica (Bruxelas), por meio da cartografia das controvérsias e acompanha algumas controvérsias relacionadas às concepções vigentes de segurança pública e instalação de dispositivos de vigilância quanto à eficiência e à eficácia de sua utilização, à liberação de recursos ou não pelos governos, à definição das áreas a serem monitoradas e aos efeitos que produzem na sociabilidade e modos de subjetivação. Por meio da cartografia das controvérsias, busca-se evidenciar atores, vinculações e agências envolvidos na configuração de jogos de forças, dando visibilidade às associações dos atores e ao que está em disputa, auxiliando na compreensão das práticas contemporâneas de vigilância e dos processos de construção e estabilização das redes sociotécnicas para a produção de segurança. Os resultados do estudo poderão contribuir para avançar na compreensão de temas tão complexos e multifacetados que se desdobram na análise das ações atuais de agências de segurança, demandas de pessoas que circulam nos espaços urbanos pesquisados, bem como na formulação, implementação e avaliação de políticas públicas relacionadas à segurança pública. A pesquisa está sendo realizada com bolsa de pós-doutorado da Research Support Foundation of the State of Rio de Janeiro FAPERJ.

Palavras-chave: Vigilância, Violência, Segurança pública, Cartografia das controvérsias.

IRME SALETE BONAMIGO*
ROSA MARIA LEITE RIBEIRO PEDRO**
LUCAS MELGAÇO***

(In)Seguridad pública: cartografía de relaciones entre dispositivos de vigilancia, política pública y violencias en espacios urbanos contemporáneos

Resumen: En este trabajo se aborda la asociación entre dispositivos de vigilancia y producción de seguridade pública, concebiendo (in)seguridade cómo resultado de muchos elementos que se conectan en redes sócio-técnicas. De esta manera, analiza algunas correlaciones existentes entre dispositivos de vigilancia, prácticas y conceptos actuales de la seguridad pública conectados al control de la delincuencia y la prevención de las violencias. Las grandes inversiones de los órganos de seguridad pública en los dispositivos de vigilancia tecnológica para el control de la delincuencia y de las prácticas violentas son el resultado de decisiones políticas y técnicas, involucran la configuración de redes socio- técnicas de actores, ejercicio del poder y del conocimiento. Mediante la cartografía de las controversias, se busca mostrar actores, vinculaciones y organismos involucrados en la configuración del juego de fuerzas, dando visibilidad a las asociaciones de los actores y lo que está en competición, ayudando en la comprensión de las prácticas contemporáneas de vigilancia y de los procesos de construcción y estabilización de las redes socio-técnicas para la producción de seguridad. Los resultados del estudio puede ayudar a avanzar en la comprensión de cuestiones complejas y variables que se despliegan en el análisis de las acciones actuales de las agencias de seguridad, en las demandas de las personas que se mueven en los espacios urbanos donde se pondrá la investigación, así como la formulación, aplicación y evaluación de políticas públicas relacionadas con la seguridad pública. La investigación está siendo llevada a cabo por medio de la beca Post -Doctoral FAPERJ.

Palabras clave: Vigilancia, Violencia, Seguridad pública, Cartografía.

Public (in)security: cartography of relations between surveillance devices, public policies and violence in contemporary urban spaces

Abstract: This study discusses the association between surveillance devices and public security production devices, producing (in)security as a result of multiple elements that are connected in socio-technical networks. It analyzes, therefore, some correlations between surveillance devices, practices and current concepts of public security related to crime control and prevention of violence. The high investments of public security agencies in technological surveillance devices for crime control and violent practices are the result of technical and political decisions and involve the configuration of socio-technical networks of actors, exercise of power and knowledge. The research is being conducted in Brazil (Rio de Janeiro and Santa Catarina) and Belgium (Brussels), through the method of the cartography of controversies and follows some controversies related to current conceptions of public security and the installation of surveillance devices considering the efficiency and effectiveness of their use, the release of funds or not by governments, the definition of areas to be monitored and the effects that may produce sociability and modes of subjectivity. Through the cartography of controversies, we seek to highlight actors, linkages and agencies involved in the power play, giving visibility to the associations of the actors and which are in dispute, assisting in the understanding of the contemporary practices of surveillance and construction and stabilization processes of socio-technical networks to the production of security. The study results could help in the understanding of complex and multifaceted issues that unfold in the analysis of current security agencies, demands of people moving in the analyzed urban areas, as well as the formulation, implementation and evaluation of public policies related to public security. The research is being conducted with postdoctoral fellowship from FAPERJ.

Keywords: Surveillance, Violence, Public security, Cartography.

INTRODUÇÃO

Em nossa sociedade contemporânea as tecnologias têm sido traduzidas como dotadas de alta potencialidade na contraposição às violências e à insegurança social. Os dispositivos tecnológicos de controle e vigilância, em especial o sistema de videomonitoramento[1], estão sendo cada vez mais utilizados por órgãos de segurança pública. Concebidos como ferramentas de registros de práticas criminais, de investigação policial e de prevenção da criminalidade, os dispositivos tecnológicos de vídeovigilância visam capturar imagens para ampliar a visibilidade em espaços

onde a polícia não está fisicamente presente e para constituir bancos de dados que podem ser consultados a qualquer momento.

Os dispositivos de controle e vigilância colocam em funcionamento uma tecnologia híbrida que pode ser compreendida como uma rede sociotécnica (LATOUR, 2001), composta pela vinculação entre diferentes entidades heterogêneas, híbridas de natureza-cultura, do científico, do político e do tecnológico[2]. O seu desempenho é sustentado por atores humanos e não-humanos (LATOUR, 2006), sendo o controle e a vigilância um efeito dessa rede. No sistema de videomonitoramento, por exemplo, cabe às câmeras captar as imagens no exato momento em que elas acontecem, ao mesmo tempo cabe aos operadores considerar a pessoa da imagem suspeita ou não para acionar policiais (que estão associados às suas armas e viaturas), arquivar imagens em banco de dados, transformar ações em estatísticas. Essas estatísticas atuarão de modo a sustentar decisões tais como o incremento do número de câmeras e/ou de policiamento presencial.

Em uma rede sociotécnica há troca de propriedades entre humanos[3] e não-humanos[4] que estão entrelaçados, denominada por Latour (2001, 216) de delegação, definição que diz respeito à distribuição e à troca contínua entre humanos e não humanos, na qual a atuação dos não humanos transforma a ação humana e pode abranger três deslocamentos: atorial (as câmeras de monitoramento passam a constituir um novo personagem que produz determinados efeitos); espacial (o novo ator ocupa um determinado espaço nas ruas); temporal (as câmeras podem estar presentes o tempo todo e substituir os policias). É necessário considerar também que "os atores se conectam pela tradução[5] [...] eles próprios traduzem a si mesmos e aos demais e, ao mesmo tempo, são traduzidos". (CASTRO; PEDRO, 2013, 354).

É importante analisar que esses dispositivos constituem uma instância de subjetivação coletiva (GUATTARI, 1992), já que sua presença implica na produção ou modificação de modos de perceber, pensar e sentir de indivíduos e grupos. Assim, participam ativamente da "reordenação dos modos de ver e de ser visto" (BRUNO; KANASHIRO; FIRMINO, 2010, 7) e da produção de informações sobre as pessoas e suas ações, produzindo "efeitos de subjetividade e sociabilidade" (CASTRO; PEDRO, 2010, 37).

Este artigo tem como base parte da pesquisa de pós-doutorado em andamento e discute a experiência da instalação de câmeras de videomonitoramento no Brasil, (Chapecó e Rio de Janeiro) e Bélgica (região de Bruxelas). O objetivo é identificar elementos que possibilitem apreender algumas práticas contemporâneas de vigilância e processos de construção e estabilização de redes sociotécnicas para a produção de segurança, articulados às políticas públicas que as legitimam.

MÉTODO

Este artigo se trata de parte da pesquisa de pós-doutorado mais ampla, em andamento, que está sendo realizada no Programa de Pós-graduação em Psicologia na Universidade Federal do Rio de Janeiro (UFRJ), orientada pela profª Rosa Maria Leite Ribeiro Pedro, com período de estágio

na Vrije Universiteit Brussel (VUB) como pesquisadora visitante, orientada pelo prof. Lucas Melgaço. Neste artigo está sendo utilizada como fonte apenas a pesquisa bibliográfica resultante de publicação de resultados de estudos sobre videovigilância realizados em Santa Catarina (Bonamigo, 2007, 2013; Bonamigo & Chaves, 2015), no Rio de Janeiro (Cardoso, 2013; Castro, 2013; Castro & Pedro, 2015) e Bruxelas (Keersmaecker & Debailleul, 2016).

A pesquisa tem seus fundamentos teórico-metodológicos vinculados à Teoria Ator-Rede (TAR), cunhada por Bruno Latour, Michel Callon, John Law, entre outros autores. A TAR contribui na análise de associações heterogêneas, seus mecanismos de consolidação ou transformação, de forma a não as reduzir nem a um ator, nem a uma rede, mas à composição ator-rede que *faz-fazer*, sendo compreendidas como efeitos de conexões entre diversos atores que engendram práticas e discursos. A noção de rede remete a um paradigma ligado a um pensamento das relações, em oposição a um pensamento das essências (Serres, 1968). Por meio da cartografia das controvérsias (Latour, 2000, 2005, 2012; Venturini, 2010) busca-se evidenciar atores, vinculações e agências envolvidas na configuração de jogos de forças, dando visibilidade às associações dos atores e ao que está em disputa, buscando compreender as práticas contemporâneas de vigilância e os processos de construção e estabilização das redes sociotécnicas para a produção de segurança.

EXPERIÊNCIAS DE VIDEOVIGILÂNCIA NA REGIÃO DE BRUXELAS

A pesquisa de Keersmaecker e Debailleul (2016)[6], realizada em 2014 e atualizada em 2016, mapeou a distribuição espacial das câmeras em ruas da região de Bruxelas, analisou relatórios de polícia e de autoridades da cidade em jornais locais e conduziu entrevistas semi-estruturadas com 16 entrevistados (polícia, agentes de segurança que monitoram as câmeras e chefes e autoridades locais e regionais). O objetivo dos autores foi esclarecer os processos e razões que estão por trás da localização do câmeras. Para complementar e verificar a confiabilidade dos dados foi realizado trabalho de campo para a identificação de cada câmera no local de sua instalação. Segundo os autores, a abordagem empírica no estudo do videomoitoramento[7] em Bruxelas foi adotada pela primeira vez.

Em uma análise histórica os autores identificaram que a primeira câmera de vigilância foi instalada pela primeira vez em 1968 pela empresa de transportes públicos STIB / MIVB para monitorar plataformas de metrô e estandes de vendas. Em seguida, em 1990, foram surgindo esporadicamente no espaço público. O Campeonato Europeu de Futebol, em 2000, foi um motivo para a sua instalação nos arredores do estádio de Heysel e simultaneamente foram colocadas no pequeno anel viário que cerca o pentágono (área central de Bruxelas), com a finalidade de regulação do tráfego. Em 2003, o governo regional disponibilizou um orçamento de 1,5 milhões de euros para ajudar os municípios a instalarem os equipamentos em seus próprios territórios. Mas, apesar dos primeiros sistemas de videomonitoramento serem iniciados pelos municípios, o controle foi gradativamente deslocado para as zonas de polícias, sendo unificada em 2000 com

novas salas de controle nas principais estações de polícia.No período mais recente houve uma coordenação mais direta pelo governo, com o planejamento de quatro fases: a instalação de 230 câmeras na área policial de Ixelles, entre 2005 e 2015, com orçamento de 10 milhões de euros, 130 câmeras na área policial de Bruxelas do Norte (6 milhões) e 108 câmeras na área policial de Bruxelas do Sul (previsto término em 2016).

Keersmaecker e Debailleul (2016) avaliam que essas iniciativas de grande escala proporcionaram um salto qualitativo nas tecnologias de vigilância por vídeo, como câmaras inteligentes que detectam comportamentos suspeitos automaticamente por meio da aplicação programada da análise de conteúdo de vídeo (VCA). Além disso, a empresa de transportes públicos STIB / MIVB vai completar a reforma das estações de metrô que abrange uma rede intensa de vigilância por vídeo, totalmente financiada pelo governo da região de Bruxelas capital. Segundo os autores, a empresa de transporte é a maior proprietária na região com 1800 câmeras em edifícios e 4000 em veículos e este número será dobrado quando o metrô estiver totalmente automatizado e implementado.

Os autores ainda descrevem que o videomonitoramento atualmente está muito disperso e as autoridades regionais preferem um sistema centralizado. Há em andamento o estudo para a implementação de uma rede regional pela Brussels Regional Informatics Centre (BRIC). No entanto, autoridades locais entrevistadas por Keersmaecker e Debailleul (2016) não mostraram entusiasmo pela ideia, pelo receio de perder o controle na gestão das “suas” câmeras de videomonitoramento.

Com relação às razões para o desenvolvimento do sistema de vídeovigilância pública em Bruxelas, Keersmaecker e Debailleul (2016) analisam que: (a) é utilizado como um meio de urbanismo defensivo (minimizar os riscos e maximizar o controle, em um quadro jurídico bastante permissivo com inovações tecnológicas e práticas policiais); (b) as câmeras estão concentradas principalmente nos centros de consumo (lojas, lugares turísticos, transportes), bem como nas áreas mais socioeconomicamente desfavorecidas, especialmente se estas áreas têm uma grande população "não-ocidental" e estão localizadas a uma curta distância do centro da cidade. O aumento da vigilância destes dois tipos de espaço em que coexistem pode ser explicado pelo fato de que, num contexto de uma economia globalizada capitalista, aumentou a competição entre cidades e parte da estratégia de uma cidade para atrair capital internacional é tornar o seu ambiente "mais seguro". Os autores avaliam também que a abordagem espacial forneceu uma melhor compreensão da tecnologia do videomonitoramento, pois destacou sua distribuição desigual em todo o território, e mostrou que está destinada a proteger interesses determinados e monitorar grupos sociais específicos.

EXPERIÊNCIAS DE VIDEOVIGILÂNCIA NO RIO DE JANEIRO

Cardoso (2013) identifica a expansão do sistema de videovigilância associada aos Jogos Pan-Americanos de 2007 e aos recursos recebidos pela Secretaria Nacional de Segurança Pública (Senasp), com o objetivo de produzir mais segurança durante o evento internacional. Castro

(2013) refere o uso de câmeras de monitoramento como estratégia privilegiada do SESEG/RJ para a produção de segurança e prevenção de crimes, em 2010. Naquele momento só a favela Santa Marta possuía câmeras, já em 2013 outras comunidades também passaram a ter esses equipamentos instalados, em uma aliança entre poder público e iniciativa privada. A escolha do Rio de Janeiro como sede da Copa do Mundo de 2013 e das Olimpíadas 2016 foi outro fator que multiplicou o investimento em câmeras de vídeo, tanto de capital privado nacional e internacional como de investimento por parte dos três níveis de governo (municipal, estadual e federal). Assim, segundo castro (2013), o crescimento das práticas de vigilância/monitoramento e o aumento do número de câmeras materializaram-se na construção e funcionamento do Centro Integrado de Comando e Controle (CICC).

O CICC está localizado na Praça 11 e é apresentado pela Secretaria de Segurança estadual do Rio de Janeiro, em seu site, como o maior centro de tecnologia de segurança da América Latina. Integra diferentes órgãos do estado, município e governo federal: Polícia Militar, Polícia Civil, Corpo de Bombeiros, Serviço de Atendimento Móvel de Urgência (Samu), Polícia Federal, Polícia Rodoviária Federal, Guarda Municipal, Defesa Civil e Companhia de Engenharia de Tráfego do Rio (Cet-Rio).

Desde 2010 o Rio de Janeiro também conta com o Centro de Operações Rio (COR) que atua no gerenciamento e controle urbano e possui 560 câmeras instaladas por toda a cidade. Segundo Castro (2013, 44), o COR foi construído em quatro meses pela Prefeitura do Rio e procura articular "as informações e ações de, aproximadamente, trinta órgãos públicos e concessionárias integrando imagens de câmeras de transito, mapas de satélite, radares, relatórios meteorológicos etc." Há parceria entre o CICC e o COR.

Castro (2013) analisa que ambos os centros utilizam as câmeras de vídeo, com ações de monitoramento da cidade com diferentes objetivos: o CICC busca promover a segurança por meio do combate ao crime e à violência e o COR visa promover segurança por meio da regulação dos fluxos da cidade, no sentido de garantir a mobilidade mesmo diante de situações de emergência. Para o autor, os dois centros, pela organização em forma de rede e composição heterogênea, colocam em prática formas de governo à distância, com atuações que se distribuem entre vários atores em um exercício sutil de controle e intervenção apenas quando necessário.

EXPERIÊNCIAS DE VIDEOVIGILÂNCIA EM CHAPECÓ

Estudos realizados (Bonamigo, 2007, 2013; Bonamigo & Chaves, 2015) sobre violências, segurança pública e videomonitoramento em Chapecó[8], Santa Catarina, Brasil, acompanharam os movimentos de órgãos públicos e privados que culminaram na instalação de câmeras de monitoramento na cidade. Apesar da consolidação atual dessa tecnologia de vigilância, o seu uso no município é recente e fruto de um processo de elaboração de projeto, mobilização de atores e recursos para a aquisição dos equipamentos, que iniciou com uma câmera experimental em abril de 2005.

Essa primeira experiência não obteve os recursos pretendidos para a aquisição e instalação das câmeras de monitoramento, nem do Estado e nem da iniciativa privada. Houve uma tentativa, por parte de seus articuladores, de apresentação do projeto para financiamento na Secretaria Nacional de Segurança Pública (Senasp), mas não foi aprovado. No entanto, a mobilização não foi em vão, já que foram lançadas as justificativas da importância do monitoramento eletrônico e a legitimação da sua existência ao ser associada à vigilância ao controle de práticas violentas (Bonamigo, 2013). A efetivação do projeto aconteceu seis anos depois, em abril de 2011, por meio de um convênio estabelecido entre o município e o governo do estado de Santa Catarina, que instituiu o Programa Chapecó Segurança Máxima pela Lei nº 5989 (de 26 de abril de 2011) e teve como resultado a instalação de 186 câmeras de monitoramento em diferentes locais da cidade (Prefeitura De Chapecó, 2013).

O sistema de videomonitoramento é uma tecnologia que requer um grande volume de recursos para a sua aquisição e manutenção e cria expectativas de efeitos de segurança. Bonamigo e Chaves (2015) identificaram que a persistência da sensação de insegurança e acontecimentos relacionados a possíveis falhas operacionais e/ou a limites do próprio sistema de monitoramento têm gerado desconfiança da população quanto a eficiência e a eficácia da tecnologia do videomonitoramento, o que tem requerido constantes justificativas de legitimação dessa tecnologia de vigilância por gestores de políticas públicas de segurança.

Outro aspecto evidenciado pela pesquisa é que a vigilância por meio das câmeras de monitoramento, no cotidiano, não se dá de forma linear e total. Há zonas de sombra que impedem a vigilância máxima: as câmeras de vídeo não conseguem atingir todos os lugares e regiões; as tecnologias de segurança também podem ser apreendidas pelas pessoas que se quer controlar, necessitando de inovações permanentes e há uma infinidade de possibilidades de resistir e subverter dispositivos de controle. Com relação aos locais de instalação das câmeras de monitoramento, as regiões e as pessoas são diferentemente concebidas e pensadas no município: há pessoas e espaços protegidos e há pessoas e espaços vigiados.

Outra informação a ser destacado é o Programa Bem-Te-Vi: Segurança por Videomonitoramento em Santa Catarina, lançado em 2012 pela Secretaria de Segurança Pública do estado. Este programa possibilita o acesso concomitante das imagens tanto à Polícia Militar como à Polícia Civil e promove o acesso integrado das imagens entre as diversas cidades monitoradas.

ALGUMAS CONSIDERAÇÕES

O estudo do sistema de videomonitoramento, assim como a localização das câmeras, possibilita apreender modos atuais de gestão das cidades e lógicas das economias políticas locais, ao situar-se no cruzamento de interesses econômicos privados, interesses políticos locais e na legitimação da tecnologia como solução para a (in)segurança pública. As experiências de videomonitoramento descritas torna visíveis práticas contemporâneas de vigilância distribuídas entre os atores, tecidas na composição e estabilização das redes sociotécnicas, traduzidas como produtoras de segurança e articuladas às políticas públicas que as legitimam.

As experiências de videovigilância descritas em três espaços diversos possuem particularidades relacionadas às cidades, estados e países. No entanto é possível realizar algumas análises vinculadas à apreensão das condições que possibilitaram a aquisição e o uso desta tecnologia. Em Bruxelas a emergência das câmeras de monitoramento foi gradativa e houve investimento privado e público, já nas duas cidades brasileiras são recentes. Os eventos internacionais tiveram um papel importante na intensificação do uso da tecnologia, mobilizando interesses e recursos tanto privados como públicos no Rio de Janeiro (Copa do Mundo e Olimpíadas) e em Bruxelas (Campeonato Europeu de Futebol), demandando maior produção de segurança ou pelo menos da "sensação de segurança". Já em Chapeco, houve um período de mobilização para a instalação dos dispositivos de vídeovigilância, iniciado em 2005 e concretizado em 2011, com o investimento de recursos do estado de Santa Catarina e da Secretaria Nacional de Segurança Pública (Senasp), tendo em vista a política nacional de incentivo do uso dessa tecnologia. Os recursos regionais, nacionais e/ou internacionais foram significativos para a instalação de equipamentos nas três cidades descritas, pois a tecnologia requer um grande volume de recursos.

Percebe-se, ainda, o delineamento da tendência de centralização e integração da vídeovigilância tanto de diferentes órgãos como no Rio de Janeiro e Santa Catarina, como de diferentes municípios no caso de Santa Catarina. Mesmo no caso de Bruxelas há movimentos para a centralização do videomonitoramento por meio da ligação das redes das diferentes áreas de polícia com o Porto de Bruxelas, corpo de bombeiros, transporte público e Ministério da Mobilidade. Ainda, todos as experiências descritas foram acompanhadas da produção constante de discursos referentes à eficácia das câmeras de vídeo, associando-as a produção de segurança e a diminuição de práticas violentas.

Para Pedro e Castro (2015), as práticas de vigilância/monitoramento por meio das câmeras de vídeos visando à segurança e a manutenção da ordem parece ser uma política irreversível. Mesmo quando falhas são identificadas, a resposta é a intensificação do uso das próprias câmeras, em uma tentativa de resolver problemas da tecnologia com mais tecnologia. Pedro e Castro (2015, 231) destacam que "embora sua eficácia no combate aos crimes seja discutível, esses dispositivos inegavelmente potencializam a capacidade de vigilância das polícias [...] à distância" o que não necessariamente traduz-se em mais segurança para a população. Ressaltam, assim, a necessidade de se questionar e problematizar no campo das políticas públicas a utilização das câmeras na gestão das cidades. Melgaço (2010, 248) chama a atenção para os efeitos que podem ser provocados por um território vigiado, pois além de não combater o medo pode reforça-lo, constituindo-se em fonte de segurança para alguns, mas de violência para outros.

É importante considerar que "as decisões acerca dos dispositivos tecnológicos de vigilância [...] são tanto políticas, quanto técnicas e, portanto, produzidas por um jogo de forças onde exercício de poder, conhecimento técnico e imprevisibilidade se fazem presentes" (Castro & Pedro, 2010, 59). Afinal, "nossas tecnologias [...] reproduzem e dão corpo ao jogo complexo de vetores técnicos, econômicos e políticos" (Bijker & Law (1997, 7).

NOTAS

* Pós-doutoranda pelo Programa de Pós-graduação em Psicologia na Universidade Federal do Rio de Janeiro (UFRJ), com estágio na Vrije Universiteit Brussel (VUB) como pesquisadora visitante. Professora do Programa Políticas Sociais e Dinâmicas Regionais e do Curso de Psicologia da Universidade Comunitária da Região de Chapecó (Unochapecó), Brasil.

** Professora do Programa de Pós-graduação em Psicologia na Universidade Federal do Rio de Janeiro (UFRJ), Brasil. Membro do Lavits.

*** Professor do Departamento de Criminologia e membro do Grupo de Pesquisa Crime e Sociedade da Vrije Universiteit Brussel, Bélgica. Membro do Lavits.

1. As expressões videovigilância e videomonitoramento são utilizadas neste texto como sinônimos.
2. O princípio de simetria generalizada (LATOUR; WOOLGAR, 1997) nos permite desestabilizar distinções tradicionalmente feitas entre esses elementos, pois propõe tratar de modo igual e nos mesmos termos a natureza e a sociedade. Desse modo, tanto humanos quanto não humanos (objetos, equipamentos, dispositivos tecnológicos, entre outros) constituem-se atores (agentes, actantes) quando produzem efeitos na rede a que estão vinculados e compõem o que Latour (2001) denominou coletivo sociotécnico.
3. Por exemplo: policial militar que faz monitoramento, policial civil que tem acesso às imagens, pessoa que está sendo filmada, etc.
4. Câmeras, equipamentos que arquivam imagens gravadas e demais dispositivos técnicos.
5. A denominação tradução refere-se ao significado linguístico (transposição de uma língua para outra) e ao significado geométrico (transposição de um lugar para outro). O processo de tradução envolve "a interpretação dada pelos construtores de fatos aos seus interesses e aos das pessoas que eles alistam", oferecendo "novas interpretações desses interesses" e canalizando "pessoas para direções diferentes" (LATOUR, 2000, 194).
6. Artigo pulicado em inglês e traduzido pelos autores.
7. Denominados pelos autores de Circuito Fechado de Televisão (CCTV), referindo-se às câmeras utilizadas para monitorar pública espaço pelas autoridades públicas ou pela polícia.
8. Município com população estimada em 209.553 mil habitantes, no ano de 2016.

REFERÊNCIAS

Bruno, F. (2009). Vídeo-vigilância e mobilidade no Brasil. In: Josgrilberg, F., & Lemos, A. *Comunicação e mobilidade: aspectos socioculturais das tecnologias móveis de comunicação no Brasil*. Salvador: EDUFBa.

Bruno, F., Kanashiro, M., & Firmino, R. (Org.) (2010). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina.

Bonamigo, I. S. (2007). *Violências na contemporaneidade: etnografia de redes sociotécnicas na cidade de Chapecó (SC)*. 2007. Tese (Doutorado em Psicologia Social) – Universidade do Estado do Rio de Janeiro (UERJ), Rio de Janeiro, 2007.

Bonamigo, I. S. (2013). Novas tecnologias de vigilância e a gestão de violências. **Fractal,** *Rev. Psicol*. [on-line], v. 25, n. 3, 659-674.

Bonamigo, I. S., & Chaves, L. C. (2015). Sistema de videomonitoramento na segurança pública em Santa Catarina: a experiência de Chapecó e o Programa Bem-te-vi. In: Pimentel, L.O, Zibetti; F.W., & Ziegler Filho, J. A. *Inovações tecnológicas e legislativas em segurança pública*. Ciência Tecnologia e Inovação em Segurança Pública III. Florianópolis: FORMATTO-A Produções Editoriais.

Cardoso, B. V. (2013). Megaeventos esportivos e modernização tecnológica: Planos e discursos sobre o legado em segurança pública. *Horizontes Antropológicos*, Porto Alegre, ano 19, n. 40, 119-148, jul./dez.

Castro, R. B. (2013). *Dispositivos de segurança: performações de governo articuladas às câmeras de vídeo*. Tese (doutorado) – Universidade Federal do Rio de Janeiro, Instituto de Psicologia, Programa de Pós-Graduação em Psicossociologia de Comunidades e Ecologia Social - EICOS,Rio de Janeiro.

Castro, R. B.; Pedro, R. M.L.R. (2010). Redes de vigilância: a experiência da segurança e da visibilidade articulada às câmeras de monitoramento urbano. In: Bruno, F., Kanashiro, M., & Firmino, R. (2010). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Porto Alegre: Sulina.

Castro, R. B.; Pedro, R. M.L.R. (2013). Experiências da vigilância: subjetividade e sociabilidade articuladas ao monitoramento urbano. *Psicol. Soc.* [on-line], v. 25, n. 2, 353-361, 2013.

Deleuze, G., & Guattari, F. (1995). *Mil Platôs. Capitalismo e esquizofrenia*. Rio de Janeiro: Editora 34, 1995.

Latour, B. (2005). *La cartographie des controverses.* Recuperado de `http://www.technologyreview.fr/?id=65` em 03 nov. 2013.

Latour, B. (2000). *Ciência em ação: como seguir cientistas e engenheiros sociedade afora*. São Paulo: UNESP.

Latour, B. (2001). *A esperança de Pandora*. Bauru: EDUSC.

Latour, B. (2006). *Changer de société. Refaire de la sociologie*. Paris: La Découverte, 2006.

Latour, B. (2012). *Reagregando o Social: uma introdução à teoria do Ator-Rede*. Salvador: EDUFBA; Bauru: EDUSC, 2012.

Latour, B, & Woolgar, S. (1997). *A vida de laboratório: a produção dos fatos científicos.* (A. R. Vianna, Trad.). Rio de Janeiro: Relume Dumará, 1997.

Keersmaecker, P., & Debailleul, C. (2016). The spatial distribution of open-street CCTV in the Brussels - Capital Region. *Brussels Studies*, Number 104, October 10th.

Melgaço, L. (2010). Securização urbana: da psicosfera do medo à tecnosfera da Segurança (Tese de doutorado em Geografia). Programa de Pós-Graduação em Geografia Humana, Universidade de São Paulo, São Paulo.

PREFEITURA DE CHAPECÓ (2013). *Segurança Pública: Novas câmeras de monitoramento na Grande Efapi apresentam resultados positivos*. 08 mar. 2013. Recuperado de `http://www.chapeco.sc.gov.br/noticias/2494-seguranca-publica-novas-cameras-de-monitoramento-na-grande-efapi-apresentam-resultados-positivos.html`; em: 25 fev. 2014. Recuperado de `http://www.brusselsstudies.be/`, em 30 out, 2015.

Serres, Michel (1968) apud Musso, (2013). A filosofia da rede. In: PARENTE, André. (org.). *Tramas da rede*. Porto Alegre: Sulina.

Venturini, T. (2010). Diving in magma: How to explore controversies with actor-network theory. *Public understanding of Science* 19.3, 2010: 258-273. Disponível: `http://www.tommasoventurini.it/wp/wp-content/uploads/2011/08/DivingInMagma.pdf`. Acesso em 3 de maio de 2015.

A ÚLTIMA PORTA DO ESTADO. AEROPORTOS, VIGILÂNCIA E CONTROLE

Resumo: Os aeroportos modernos se constituem como a última porta de entrada e saída do Estado, são áreas estratégicas e espaços emblemáticos do moderno mundo globalizado. Um espaço cuja própria configuração física é peculiar, pois tratam-se de fronteiras que não estão localizadas nas bordas dos países, pelo contrário, em geral os aeroportos estão incrustrados no interior do território. São áreas que contam com uma arquitetura genérica, standartizada e internacionalizada na qual diferentes códigos de contato se chocam e que possuem uma moralidade própria. Esse modelo surgiu em meados dos 1970 e se espalhou pelo planeta a partir de então.
Quando foi inaugurado em 1977 o Aeroporto Internacional do Rio de Janeiro, também conhecido como Galeão, era o terceiro desse tipo no mundo e na época foi apresentado como um marco para o Brasil, um símbolo da entrada do país no mundo moderno. Para os militares, uma obra dessa magnitude fortalecia o discurso de progresso, desenvolvimento e modernidade que foi amplamente explorado pela ditadura.
Neste texto, a inauguração do Galeão será o ponto de partida para discutir a história dos aeroportos modernos, bem como os discursos que envolvem a adoção dessas novas tecnologias no interstício entre conforto, segurança, controle e vigilância.

Palavras Chave: Vigilância, Aeroportos, Controle, História.

La última puerta del Estado. Aeropuertos, vigilancia y control

Resumen: Los aeropuertos modernos son la última puerta de entrada y la puerta de salida de los Estados. Son áreas estratégicas y espacios emblemáticos del mundo globalizado moderno. El espacio en el que su propia configuración física es particular, porque son límites que no están ubicados en las fronteras de los países, por el contrario, en general, los aeropuertos están incrustados en el interior del territorio. Estas áreas tienen una arquitectura genérica, estandarizada e internacionalizada en la que chocan diferentes códigos de contacto. Este modelo surgió a mediados de la década de 1970 y se extendió por todo el planeta a partir de entonces.
El Aeropuerto Internacional de Río de Janeiro, también conocido como Galeão, inaugurado en 1977, fue el tercero de su tipo en el mundo. En su inauguración, el Galeão fue presentado como un hito para Brasil, símbolo de la entrada del país en el mundo moderno. Para los militares, un logro de esta magnitud fortaleció el discurso del progreso, el desarrollo y la modernidad que fue ampliamente explorado por la dictadura.
En este texto, la inauguración del Galeão será el punto de partida para discutir la historia de los aeropuertos modernos, así como los discursos que implican la adopción de estas nuevas tecnologías en el intersticio entre comodidad, control y vigilancia.

Palabras clave: Vigilancia, Aeropuertos, Control, Historia.

The State's last door. Airports, surveillance and control

Abstract: The modern airports are the last gateway and exit door from the States. They are strategic areas and emblematic spaces of the modern globalized world. Spaces in which its own physical configuration is singular, because they are borders that are not located in the borders of the countries, on the contrary, in general the airports are installed inside the territory. These areas have a generic, standardized and internationalized architecture in which different codes of contact clash. This model emerged in the mid-1970s and spread throughout the planet thereafter.
The International Airport of Rio de Janeiro, also known as Galeão, that was opening in 1977, was the third of this kind in the world. In its opening the Galeão was presented as a landmark for Brazil, a symbol of the country's entry into the modern world. For the military, a accomplishment with this magnitude strengthened the discourse of progress, development and modernity that was widely explored by the dictatorship.
In this text the opening of the Galeão will be the start point to discuss the history of modern airports, as well as, the discourses that involves the adoption of these new technologies in the interstice between contort, control and surveillance.

Keywords: Surveillance, Airports, Control, History.

LUIZ FILIPE DA SILVA CORREIA

Conhecido também como Galeão, o Aeroporto Internacional do Rio de Janeiro (AIRJ) foi inaugurado oficialmente no dia 20 de janeiro de 1977 após uma série de polêmicas. A obra ficou a cargo da Odebretch, custou mais de 350 milhões de dólares e passou por 6 adiamentos que culminaram em 3 anos de atraso. Para as autoridades, os custos e a demora na conclusão eram motivados pela sofisticação técnica da obra. A ARSA (Aeroportos Rio de Janeiro S.A.), responsável pela administração do novo Galeão, deu as seguintes justificativas para os atrasos:

> Um aeroporto moderno como o AIRJ, que é o mais moderno da América do Sul, é uma obra muito complexa, com muitos equipamentos eletrônicos integrados e seu projeto tem a flexibilidade de adaptar-se às necessidades do tráfego aéreo como uma de suas principais características. (...) Nunca se marcou uma data exata para a inauguração do aeroporto. O que ora se conclui é sua primeira etapa. O marco da operação que se abre com uma solenidade é a sua primeira estação de passageiros, uma das partes vitais do aeroporto. (FSP, 1977)

A solenidade de inauguração, que teve toda pompa e circunstância, foi amplamente coberta pela imprensa e contou com a presença do general Ernesto Geisel, então presidente da Ditadura Civil -Militar. Ele conheceu as instalações e concedeu uma entrevista coletiva no local onde saudou o novo Galeão como uma evolução para o país:

> É o primeiro grande aeroporto que se constrói no Brasil. Representa uma extraordinária evolução em relação ao que nós tínhamos. Com ele, o Brasil está de acordo com o mundo moderno (Veja, 1977).

Por estar "de acordo com o mundo moderno", entenda-se que o Galeão oferecia um nível de conforto, segurança e automação computadorizada que na época eram novidade não apenas no Brasil, mas também na maior parte do mundo. Dentre as "inovações" estavam lojas de presentes, livrarias, cafés, tabacarias, entre outras. Estas lojas além de oferecerem toda sorte de produtos para o consumo dos passageiros, ainda funcionavam como uma fonte de receitas para o AIRJ:

> O coronel Pedro Silva [responsável pelo Galeão] está satisfeito porque as lojas alugadas vão dar mais dinheiro do que se previa. Segundo seu planejamento, além do aluguel fixo por área, o aeroporto obteria uma participação média de 3% sobre o faturamento. A excessiva procura elevou o percentual para algo entre 4% e 5%" (Veja, 1977).

Apesar dos lucros acima do esperado, a ARSA inovou e criou áreas cujo acesso só era permitido mediante ao pagamento de tarifas especiais, como uma das reportagens explicou:

> Para conseguir a melhor receita possível, o aeroporto criou tarifas inéditas. O acesso ao terraço panorâmico custará 5 cruzeiros. Os sanitários terão uma tarifa para custear ao menos o serviço de limpeza (Veja, 1977).

Apesar da estrutura colossal que fazia o Galeão ser comparado a uma cidade, os itens que mais receberam atenção da imprensa períodica foram o elevado grau de automação, os recursos eletrônicos, os computadores e o moderno aparato de segurança. A reportagem do jornal Folha de São Paulo, por exemplo, destacou:

> Mais, uma das melhores novidades é o fato de não haver mais a revista manual de passageiros. A bagagem de mão passara por um dispositivo de raio-X, que indicará a presença de objetos metálicos. Isso evitará a abertura de bolsas, valises e frasqueiras. O passageiro passará por um pórtico, que detectará se ele porta uma arma ou objeto metálico. Em caso positivo, o funcionário do setor usará um bastão magnético que localizará em que

> parte está o objeto. Todo o complexo aeroportuário será vigiado por um sistema de televisão, com monitores, controle remoto e aparelhos de video-tape (FSP, 1977).

A revista Veja, por sua vez, dedicou a capa da edição de 26 de janeiro à inauguração do AIRJ. A reportagem especial recebeu o título de "O Cibernético Galeão" e destacou a infraestrutura automatizada e principalmente os computadores que controlavam o moderno aeroporto:

> A partir de 1 de fevereiro, as 5000 pessoas que forem trabalhar no aeroporto sentirão que, debaixo de tudo, controlando, facilitando ou atrapalhando estará presente o computador, ou melhor, um grupo de computadores. Se tudo correr como planejado, os computadores vão detectar qualquer anormalidade, indicando inclusive o procedimento a ser adotado pela manutenção. Além disso, um onipresente sistema de televisão acompanhará pousos, decolagens e o estacionamento de aviões. Nas salas de controle do aeroporto já circulam com desembaraço certas palavras do vocabulário cibernético. Como "acessar" - ter acesso ao computador, consultá -lo; "reinicializar" - tradução do inglêsrestart , reiniciar (Veja, 1977).

Motivos para desconfiança não faltavam, o sistema de check-in falhou em um dos testes preliminares e uma das esteiras de bagagem controlada por computador sofreu uma pane. E a reportagem prosseguia:

> Os poucos funcionários do aeroporto da ARSA que sabem lidar com computadores se orgulham da importância de sua tarefa. O resto, mesmo não entendendo nada a respeito, se convenceu da fatalidade irreversível de conviver com tantas máquinas e seus códigos. 'A tecnologia é cada vez mais sofisticada e o homem depende cada vez mais dela. Havendo uma falha, pára tudo. Mas isso não é somente aqui, é em todo lugar. Já pensou se quebrasse o computador do Banco do Brasil?', divaga um engenheiro da ARSA (Veja, 1977).

O comentário do engenheiro da ARSA não poderia ser mais preciso e elucidativo. Foi principalmente a partir da segunda metade da década de 1970 que a informática e as tecnologias microeletrônicas começaram a tomar de assalto a vida cotidiana, o imaginário e a cultura, sendo uma novidade não apenas no Brasil mas em todo o mundo. Nesse período, a cibernética era uma das palavras da moda sendo utilizada para reforçar valores de modernidade, sofisticação, conforto, qualidade e eficiência. A tecnologia já era vista como algo irreversível da qual os homens seriam cada vez mais dependentes. Além disso, como a reportagem deixa claro, ela era ainda motivo de orgulho para os poucos funcionários do aeroporto que trabalhavam diretamente com os computadores.

A mesma matéria da Veja aprensentou um quadro onde foram detalhados os computadores em funcionamento no novo Galeão e explicou a função de cada um deles. O controle do estacionamento ficou a cargo da *Texas Instruments*, o gerenciamento das mensagens automáticas, a supervisão e o controle do aeroporto ficaram sob a responsabilidade da *Digital Equipment Corporation*, por fim, tudo o que era relacionado aos passageiros, ficou sob o comando do computador IBM 145. Notemos que, apesar das políticas de valorização da indústria nacional de informática, todos os computadores utilizados no Galeão eram de fabricantes estadunidenses.

Os elevados níveis de informatização e automação renderam ao Galeão a alcunha de Aeroporto Supersônico, um simbolismo que também foi amplamente explorado na época. Nos dias que se seguiram à inauguração, foi comum encontrar nas páginas dos jornais e revistas anúncios de

empresas que além de dar boas vindas ao Galeão tentavam associar suas respectivas imagens com a do "Aeroporto Supersônico".

Para os militares, uma obra dessa magnitude fortalecia o discurso de progresso, desenvolvimento e modernidade que foi amplamente explorado pela ditadura. A presença de Geisel não deixa qualquer dúvida da importância estratégica do aeroporto para o Brasil. A imprensa também fez questão de ressaltar que o novo Galeão era um cartão de visitas para o país.

Pouco mais de um ano após sua inauguração, o Aeroporto Supersônico já tinha apresentado problemas operacionais e falhas no sistema automatizado de bagagens, os computadores IBM 145, no entanto, estavam funcionando perfeitamente. Graças a eles, no dia 18 de fevereiro de 1978, o músico Chico Buarque e o escritor Antônio Callado ficaram detidos por quase 11 horas no Galeão. Eles retornavam de participação no concurso literário internacional da Casa de las Américas, em Havana. As reportagens da época noticiaram o ocorrido da seguinte maneira:

> Chico Buarque e Callado foram "descobertos" pelo moderno computador existente no aeroporto internacional do Rio de Janeiro que tem em seus registros uma lista de quase 20.000 nomes de pessoas que devem ser detidas em caso de desembarque no Brasil (Veja, 1978).

O Galeão foi apenas o terceiro de uma série de Aeroportos Internacionais construídos ou reformados a partir da década de 1970. Nestes aeroportos modernos a arquitetura, os procedimentos, os serviços e o controle eletrônico computadorizado seguiam uma espécie de padrão que foi implementado em várias partes do mundo. Em qualquer parte do mundo o procedimento tornou-se parecido: o passageiro passa pelo escrutínio de modernos dispositivos capazes de enxergar através de roupas, bolsas e malas. Não tendo sido detectado nada suspeito ele é autorizado a prosseguir sua jornada. Quando chega ao seu destino, o viajante ainda terá que passar pelo pente fino das autoridades de emigração e da receita. De fato, durante toda a permanência no perímetro do aeroporto os gestos, os sorrisos e as lágrimas dos passageiros não escapam do olhar atento das câmeras espalhadas estrategicamente por todo o saguão, na cafeteria e na loja de perfumes. Esse modelo que se consolidou nas décadas de 1980 e 1990 foi principalmente o resultado da expansão da aviação civil comercial e da preocupação com a ameaça terrorista.

Mesmo com as frequentes notícias de crise e falências, desde os anos 1970, a aviação civil é um dos setores da economia que mais cresceram em todo o mundo. Esse crescimento aumentou a concorrência e fez com que as companias aéreas e os aeroportos se modernizassem. É importante ressaltar ainda que essa prosperidade no setor não está relacionado apenas ao turismo, mas também às viagens de negócios e ao transporte de mercadorias. Assim, o conjunto dos Aeroportos Internacionais modernos formam uma espécie de rede que tem uma importância estratégica, econômica e geopolítica para os estados e nações.

Não demorou muito para que essas áreas de importância simbólica, econômica e política virassem alvo e objeto de ataque do chamado terrorismo internacional. Embora desde a década de 1930 existam notícias de ataques à bomba em aviões foi só a partir dos anos 1970 quando tornaram-se

frequentes sequestros a aeronaves comerciais que outras medidas de segurança passaram a ser implementadas na aviação civil. Estimasse que até meados dos anos setenta a chance de sucesso em uma tentativa de sequestro de avião era de aproximadamente 76% (Adey, 2003).

No Brasil, ao longo da Ditadura, quase uma dezena de aeronaves foi sequestrada para tirar do país pessoas perseguidas pela Ditadura ou como forma de exigir a libertação de presos políticos. Um desses casos ocorreu em 01 de Julho de 1970, pouco antes do início da construção e reforma do novo Galeão. Quinze minutos após decolar do Rio de Janeiro, com destino à cidade de São Paulo, um avião foi sequestrado por integrantes do Comando Reinaldo Silveira Pimenta, nome dado em homenagem a um militante da Dissidência Estudantil de Niterói, morto em 1969. Eles exigiam a libertação e saída do país de 40 presos políticos. O piloto foi obrigado a retonar para o Rio de Janeiro. Quando pousou no Galeão, o avião foi cercado por tropas da Aeronáutica que cobriram as janelas com espuma, o que impedia a visão de dentro para fora. As tropas arrombaram a porta e invadiram a aeronave e mataram um dos sequestradores, Eiraldo Palha Freire. Os demais – Fernando Palha Freire, Jessie Jane Vieira de Souza e Colombo Vieira de Souza Júnior – foram presos e condenados há mais de 20 anos de prisão.

Em solo, um dos principais atentados envolvendo a aviação civil aconteceu no 30 de maio de 1972, no hall do aeroporto de Lod em Tel-Aviv / Israel. Nesse dia, três integrantes do Exército Vermelho Japonês, organização criada em 1969 e aliada da FPLP (Frente Popular pela Libertação da Palestina), lançaram granadas e atiraram com fuzis contra a multidão. Como resultado, 26 pessoas foram mortas e outra centena foi ferida. Os três integrantes do Exército Vermelho desembarcaram em LOD carregando cases de instrumentos musicais, o que fez com que as autoridades do aeroporto pensassem que se tratavam de músicos japoneses em turne pelo país, de modo que as bagagens não foram revistadas. Mais tarde, membros da FPLP explicaram que escolheram integrantes do Exército Vermelho justamente para despistar as autoridades que só barravam Palestinos. Após o massacre de LOD uma série de medidas foram tomadas para aumentar a segurança nos aeroportos.

Assim, os chamados aeroportos modernos são construídos para facilitar a mobilidade dos passageiros e das bagagens, mas também para garantir a segurança dos vôos e das viagens. E é dentro deste contexto econômico e de segurança que se insere o processo de modernização ocorrido a partir dos anos 1970, e do qual o Galeão fez parte. Esse processo marca não apenas uma mudança ocorrida na aviação civil, mas também expressa profundas transformações na própria sociedade. É a transição da Sociedade Disciplinar para a Sociedade de Controle diagramada por Deleuze no seu *Post-Scriptum sobre as Sociedades de Controle.* Para Deleuze, o que caracteriza as Sociedades de Controle "são as formas ultra-rápidas de controle ao ar livre, que substituem as antigas disicplinas que operavam na duração de um sistema fechado" (Deleuze, 2000). Ao contrário da arquitetura das instituições disciplinares que se fundamentam no confinamento, a arquitetura das sociedades de controle está acentada sob a égide da mobilidade. Mobilidade essa, que é modulada com a ajuda de máquinas cibernéticas e computadores. Ou nas palavras de Deleuze:

> Os confinamentos são moldes, distintas moldagens, mas os controles são uma modulação, como uma moldagem auto-deformante que mudasse continuamente, a cada instante, ou como uma peneira cujas malhas mudassem de um ponto a outro. (...) as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores (Deleuze, 2000).

Mais do que um cartão de visitas, os aeroportos modernos se constituem como a última porta de entrada e saída do Estado, são áreas estratégicas e espaços emblemáticos do moderno mundo globalizado. Um espaço cuja própria configuração física é peculiar, pois tratam-se de fronteiras que não estão localizadas nas bordas dos países, pelo contrário, em geral os aeroportos estão incrustrados no interior do território. São áreas que contam com uma arquitetura genérica, standartizada e internacionalizada na qual diferentes códigos de contato se chocam e que possuem uma moralidade própria. Trata-se de um ambiente carregado de tensão e ansiedade motivados pelos diversos riscos envolvidos.

Dentre as principais funções dos aeroportos modernos estão o controle do fluxo de imigração (tanto legal quando ilegal), o monitoramento do movimento dos cidadãos, a coleta de taxas e impostos, a restrição do tráfico e do contrabando de drogas e armas, impedir a circulação de criminosos procurados e até mesmo o controle de epidemias de doenças.

Portanto, podemos dizer que a principal função dos modernos aeroportos é a de controlar e modular a mobilidade de corpos e objetos a partir de métodos e mecanismos de controle e vigilância que operam de maneira associada e coordenada.

Essa modulacão é feita através de checagens, de instruções sonoras, de proibições, de inspeções, de avisos, entre outros. E pode acontecer tanto em termos de acesso a locais específicos do aeroporto, quanto em termos do monitoramento, seleção, categorização e restrição do fluxo de pessoas. Tais mecanismos servem para discriminar e separar os passageiros em categorias como por exemplo: o turista, o homem de negócios, o oriental, o latino, o imigrante, o árabe e o terrorista, etc.

Outra característica dos Aeroportos modernos é que eles podem ser compreendidos como um microcosmo das tendências de vigilância das sociedades contemporâneas, pois em geral, são neles que as modernas tecnologias de controle fazem sua estreia antes de serem incorporadas a outros espaços públicos. Basta lembrar que ao longo dos anos tornou-se cada vez mais comum o uso de "tecnologias de aeroporto" para garantir a segurança em shows e eventos esportivos.

Em linhas gerais, o modelo que se estabelece a partir da década de 1970 perdura até os dias atuais, mesmo os atentados de 11 de setembro que provocaram uma série de mudanças nos procedimentos de embarque não provocaram grandes alterações nesse padrão apenas intensificaram a tendência à vigilância e ao controle.

Passados quase quarenta anos, os computadores que barraram Chico Buarque no Aeroporto do Galeão não passam de dinossauros extintos. Atualmente está em curso o projeto *Checkpoint of the Future* da International Air Transport Association - IATA, associação das principais companhias

aéreas mundiais. Esse projeto prevê que até 2020 estejam disponíveis os seguintes recursos de segurança para uso nos aeroportos de todo o mundo:

- Processamento remoto das imagens do aeroporto;
- Uso de bancos de dados com informações digitais dos passageiros;
- Coleta em tempo real dos dados e informações sobre os passageiros;
- Diminuição das filas filtrando viajantes frequentes com autenticação biométrica;
- Avançada tecnologia de Raio-X que permite identificar material explosivo dentro de frascos de liquidos;
- Monitoramento de comportamento e análise das expressões faciais.

De acordo com o site do projeto, todos esses recursos poderão ser modulados segundo os interesses dos países que possuírem essa tecnologia. Ou seja, os dados coletados e analisados dos passageiros serão feitos segundo critérios e filtros específicos. E assim é possível ter um pequeno vislumbre das tecnologias que estarão à disposição para controle e vigilância dos espaços públicos em um futuro próximo.

Como tentei mostrar ao longo do texto, através de diversos exemplos históricos, ao mesmo tempo em que são lançadas as tecnologias de vigilância e controle nos aeroportos com a justificativa de aumentar o conforto e a segurança, é importante entender como tais tecnologias são políticas e transmitem valores e discursos oficiais dos Estados.

REFERÊNCIAS

Aaltola, M. (2005). The international airport: the hub-and-spoke pedagogy of the American empire. *Global Networks, 5* (3), 261-278.

Adey, P. (2003). Secured and Sorted Mobilities: Examples from the Airport. *Suveilance & Society, 1* (4), 500-519.

Deleuze, G. (2000). Post-scriptum das sociedades de controle. In G. Deleuze, *Conversações 1972-1990.* Rio de Janeiro: Ed 34.

FSP. (1977, Janeiro 21). Novo Galeão está inaugurado. *Jornal Folha de São Paulo*, p. 8.

FSP. (1977, Janeiro 20). Rio inaugura aeroporto. *Jornal Folha de São Paulo*, p. 6.

Lyon, D. (. (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination.* NY-Londres: Routledge.

Veja. (1977, Janeiro 26). O Cibernético Galeão. *Revista Veja*, pp. 56-63.

Veja. (1978, Fevereiro 18). Pelo Computador. *Revista Veja*, p. 24.

OS OLHARES SOBRE A CIDADE: UMA ABORDAGEM BIBLIOMÉTRICA DA VIGILANCIA NOS ESTUDOS URBANOS

Resumo: Temos vivenciado a partir do final do século XX uma proliferação de estudos sobre vigilância, onde novos autores dedicam-se a analisar os impactos de sistemas de monitoramento na sociedade contemporânea. O tema compreende diversos campos disciplinares devido a sua abordagem crítica, sendo presente desde a filosofia e a sociologia até extrapolar para a esfera do urbanismo. Portanto, a relação entre as novas formas de vigilância e as cidades nos leva a uma sobreposição teórica com os estudos urbanos, cuja interligação temática se deve aos impactos das tecnologias de monitoramento e controle de acessos que permeiam o espaço urbano, bem como as práticas de planejamento e gestão das cidades. A discussão acadêmica nesse campo é feita majoritariamente nos países do norte desenvolvido. Entretanto, as cidades dos países em desenvolvimento têm experimentado uma forte presença das práticas e tecnologias de vigilância, especialmente em decorrência da informatização de tarefas cotidianas, da comunicação móvel e da modernização da gestão urbana. Tal situação nos leva a creditar que está surgindo um maior interesse em estudos sobre vigilância por pesquisadores nessas regiões geográficas. O objetivo deste trabalho é mapear cronológica e geograficamente a produção científica global situada na correlação entre vigilância e estudos urbanos, contribuindo para o entendimento de como essas duas áreas de estudo abordam problemas contemporâneos. As buscas são efetuadas utilizando termos da área de vigilância associados a temas dos estudos urbanos (em português, espanhol e inglês) nas bases dos portais Scielo, Redalyc e Capes, e nos periódicos Urban Studies, Journal of Urban Technologies e Surveillance & Society As unidades de análise utilizadas incluem autoria, procedência geográfica, temas recorrentes e data de publicação (no de 2002 à 2016). A partir dos resultados especula-se sobre a crescente importância dos temas vigilância e cidades para a ciências sociais no período pós-11/9 e pós-Snowden.

Palavras-chaves: Vigilância, Espaço urbano, Monitoramento e controle, Bibliometria.

MARCELA DE MORAES BATISTA*
THIAGO GONÇALVES ROBERTO**
GABRIELA FEDRIZZI VARELA***

Ojos en la ciudad: un enfoque bibliométrico de la vigilancia en los estudios urbanos

Resumen: Desde el final del siglo XX hemos observado un surgimiento de los estudios sobre la vigilancia, donde nuevos autores se están dedicando al análisis de los impactos de los sistemas de monitoreo en la sociedad contemporánea. Dado su enfoque crítico, el tema abarca varias áreas disciplinarias, desde la filosofía y la sociología hasta el campo del urbanismo. Por lo tanto, la afinidad entre las nuevas formas de vigilancia y las ciudades nos lleva a la superposición teórica con los estudios urbanos, cuya interconexión del tema es debido a los impactos de las tecnologías de monitoreo y control de accesos que permean el espacio urbano, así como las prácticas de planeamiento y gestión de las ciudades. El debate académico en ese campo se hace sobre todo en los países desarrollados del norte. Sin embargo, las ciudades de los países en desarrollo están experimentando una presencia cada vez mayor de las prácticas y las tecnologías de vigilancia, sobre todo debido a la digitalización de las tareas diarias, la comunicación móvil e la modernización de la gestión urbana. Este escenario nos lleva a creer que está surgiendo un mayor interés por los estudios de vigilancia por investigadores en estas regiones geográficas. Este documento pretende trazar un mapa cronológico y geográfico de la producción científica mundial enfocada en la correlación entre la vigilancia y los estudios urbanos, lo que contribuye a la comprensión de cómo estos dos campos de estudios se acercan a los problemas contemporáneos. La investigación de los datos se realiza a través de terminologías del área de vigilancia asociadas a las del estudio urbano (en portugués, español e Inglés) en los directorios Scielo, Redalyc y Capes, y en las revistas Urban Studies, Journal of Urban Technologies e Surveillance & Society. Los datos utilizados se referencian con su autoría, procedencia geográfica, temas recurrentes y la fecha de publicación (entre 2002 y 2016). De los resultados se especula la creciente importancia de los temas de vigilancia y ciudades para las ciencias sociales en el período post-9/11 y post-Snowden.

Palabras clave: Vigilancia, Espacio urbano, Monitoreo y control, Bibliometría.

Eyes on the city: a bibliometric approach of surveillance on the urban studies

Abstract: From the beginning of the twentieth century we've been observing an emergence of studies on surveillance, where recent authors are devoted to the analysis of the impacts of the monitoring systems on the contemporary society. Given its critical approach, the subject encompasses several disciplinary areas, being on the original philosophy and sociology discussions and go further to the field of urban issues. Therefore, the affinity between the new surveillance means and the cities brings us to the theoretical superposition with the urban studies, which the subject interconnection is due to the impacts of the monitoring and control technologies that permeates the urban space as well as the urban planning and management practices. The academic debate on the field is mostly made on the developed countries. However, the cities in the developing countries are experiencing an increasing presence of the surveillance practices and technologies, especially due to the digitalization of the daily tasks, the mobile communication e the urban management modernization. This scenario leads us to believe that is emerging the interest in the surveillance studies in this geographical regions. This paper aims to chronologically and geographically map the global scientific production in the correlation between surveillance and urban studies, contributing to the understanding of how these two fields approach the contemporary issues. The searches are made by associated terminologies from the surveillance area and the urban studies (in Portuguese, Spanish and English) on the directories Scielo, Redalyc and Capes, and on the journals Urban Studies, Journal of Urban Technology and Surveillance & Society. The review data are authorship, geographical origin, recurring subjects and publishing date (year from 2002 to 2016). From the results is speculated the growing consideration of the subject matters of surveillance and cities to the social studies on the post-9/11 and post-Snowden period.

Keywords: Surveillance, Urban space, Monitoring and control, Bibliometry.

INTRODUÇÃO

Geoge Orwell no romance 1984 (Nineteen Eighty-four), narra a vida do protagonista sob um regime totalitário no qual os cidadãos vivem vigiados ininterruptamente pelo governo através de sistemas tecnológicos em um modelo panóptico. Porém, ainda que consideremos que hoje vivemos em uma panaceia tecnológica de vigilância ubíqua, o Estado não é o único detentor dos dispositivos de controle, além de que os fins e justificativas no mundo contemporâneo não coincidem com a dimensão do autoritarismo do Grande Irmão. Entretanto, a vigilância está mais

presente do que nunca nos dias de hoje e deve ser analisada como um elemento central para o funcionamento da sociedade em que vivemos.

Atualmente, tecnologias de informação fazem parte do nosso dia-a-dia e compõem uma estrutura de vigilância global da qual é praticamente impossível se manter externo. Por exemplo: câmeras de segurança, bancos de dados, transações bancárias, senhas de acesso, imagens aéreas, dispositivos com GPS, e outros, são algumas das formas de registro das nossas ações. Esses dispositivos onipresentes sevem tanto para o controle e a segurança nacional, envolvidos nos discursos antiterror, e a segurança urbana, mas também são ferramentas de manutenção da modernidade, dentro do paradigma da eterna busca pela eficiência máxima, e aos objetivos capitalistas de otimização do comércio através de estratégias de marketing que pressupõem a utilização de dados pessoais.

Dessa forma, as tecnologias de vigilância compõem o rol de tecnologias de informação que são utilizadas em múltiplos e ubíquos processos cotidianos, inclusive nos governos e órgãos públicos em todas as escalas de domínio, ou seja, do supra-nacional ao municipal. Nesse contexto, a vigilância faz parte da rotina, do controle e da gestão das cidades, especialmente através de dispositivos tecnológicos que permitem a coleta de dados em tempo real para a automatização de sistemas e o auxílio nas tomadas de decisão pelos responsáveis pela administração municipal.

Para um entendimento mais amplo da relação das práticas e infraestruturas da "nova vigilância" e as cidades, é necessário, antes de tudo, compreender a relação dos espaços urbanos com as tecnologias emergentes, bem como as relações urbanas surgidas dentro do paradigma da globalização. A aplicação tecnológica na gestão urbana vem em decorrência desse cenário, onde os dispositivos de vigilância se integram em uma composição tecnológica total.

Diante do exposto, a relação entre o espaço urbano e a vigilância torna-se cada dia mais evidente, para tanto a presente pesquisa propõe a seguinte pergunta norteadora: Como os estudos sobre a vigilância estão sendo realizados e relacionados com o espaço urbano?. Conduzindo ao seguinte objetivo que é mapear cronológica e geograficamente, por meio de uma bibliometria, a produção científica global da correlação entre vigilância e estudos urbanos, contribuindo para o entendimento de como essas duas áreas de estudo abordam os problemas contemporâneos.

REVISÃO DA LITERATURA

A vigilância tem se tornado um elemento fundamental nas sociedades contemporâneas, sendo objeto de estudo de diversos pensadores atuais (LYON, 2004; 2009; 2010; 2013; 2015; MARX, 2002; 2013; MURAKAMI WOOD e outros, 2006; GANDY, 1993; MATHIESEN, 1997; BOGARD, 1996; HAGGERTY; ERICSON, 1996), que têm levantado importantes questões quanto sua natureza e implicações no panorama global e no paradigma tecnológico atual.

O desenvolvimento tecnológico moderno, especialmente o advento das Tecnologias de Informação e Comunicação (TICs), trouxe novas possibilidades de exercício do poder e configuração social (VIRILIO, 1991; CASTELLS, 1999). Os novos padrões de vigilância, então, são dependentes das

TICs para a execução de seus processos, além de funcionarem em uma rede global de troca de informações, envolvendo instituições públicas e privadas.

A prática de rotina da coleta de dados pessoais está presente no dia-a-dia de praticamente qualquer indivíduo em uma sociedade ocidental desenvolvida. Todas as transações eletrônicas são registradas, imagens capturadas em câmeras de circuitos fechados de televisão (CFTV), localizações de GPS (Global Position System) anotadas em sistemas georreferenciados; o nível de pervasividade dos processos de vigilância é integral (LYON, 2013). Entretanto, Bogard (1996) vê o objetivo da vigilância além da omnisciência panóptica, pois acredita que o objetivo final da vigilância não é registrar tudo em tempo real, mas poder prever todas as ações antes que de fato ocorram (BOGARD, 1996).

A vigilância é uma ferramenta de exercício de poder e controle, e, como tal, é esperada a relação desta com o Estado e sua utilização como instrumento de governo. Como argumentou Foucault (1984), os paradigmas de exercício de poder da soberania e da disciplina são formas de gerir a população; são modelos de governo.

Sistemas de vigilância se desenvolveram junto dos estados democráticos e dos direitos dos cidadãos, dessa forma políticas e formas de gestão pública atuais dependem de sofisticados sistemas de vigilância para funcionar e se tornarem cada vez mais eficientes. Esses sistemas baseados no acumulo de informação são utilizados como insumo para a tomada de decisões e o desenho de conclusões sobre assuntos públicos (LYON, 2013).

Com as tecnologias atuais, Estados podem armazenar volumes enormes de informação pessoal dos cidadãos, podendo ser utilizadas para a melhoria do atendimento e individualização das necessidades de cada um. Entretanto, está justamente no uso do poder de vigilância estatal o fantasma orweliano do totalitarismo, da perda de privacidade e do controle total da vida dos indivíduos. Apesar de não haver, empiricamente, uma relação direta entre regimes totalitários e o uso extensivo de tecnologias de informação, não se pode deixar de lado o potencial de autoritarismo que essas práticas carregam, especialmente contra minorias e populações vulneráveis (LYON, 2013).

VIGILÂNCIA, AS TICS E A CIDADE

Com as transformações na sociedade associadas ao avanço da modernidade, as cidades passaram por mudanças profundas nas suas estruturas e dinâmicas. Isso se deu associado a uma aceleração do processo de urbanização, cujo resultado é que que atualmente a maior parte das pessoas no mundo inteiro vivem em cidades (ONU, 2014).

Milton Santos (2014) caracteriza o espaço contemporâneo como o meio técnico-científico-informacional, pois, segundo ele, a construção e reconstrução do espaço se dá com uma participação cada vez maior de técnicas e ciências. A partir do meio natural, o espaço se tornou técnico com a industrialização e partir da Segunda Guerra Mundial adquiriu características cientificas, com o avanço das ciências, e informacional, em consequência da informatização crescente a partir da década de setenta (SANTOS, 2014).

Com o avanço da globalização, as cidades têm se interconectado em escala mundial. Castells descreve o espaço de fluxos como particular das dinâmicas capitalistas globais e em oposição ao "espaço de lugares", aquele que carrega significados e valor local. O espaço de fluxos está conectado às redes globais, ou seja, faz parte da dinâmica globalizada de troca de informações, pessoas, bens e capital (CASTELLS, 1999).

Essa relação das cidades em escala mundial proporciona a troca de informações necessária para a realização da vigilância global, que necessita de uma rede integrada de dados para a análise e cruzamento com a finalidade de coletar, agrupar e classificar pessoas e referências que podem se locomover entre as nações. Além disso, a desigualdade intra-urbana, que ocorre entre as diferentes áreas em relação à integração global e a infraestrutura tecnológica, também tem seu rebatimento em relação às tecnologias de monitoramento, fazendo surgir áreas com presença, escala e qualidade da vigilância global discrepantes em relação umas às outras. Ou seja, são estabelecidas regiões vigiadas e não-vigiadas no território urbano.

Nas últimas décadas houve a invasão das TICs no espaço urbano e a computação se tornou ubíqua e pervasiva, ou seja, atualmente são onipresentes as redes e dispositivos informáticos no ambiente construído e no cotidiano dos habitantes das cidades contemporâneas. Essas ferramentas de comunicação e acesso às redes informacionais estendem as capacidades e sentidos do corpo humano, adicionando, dessa forma, uma nova camada de experiência ao espaço; uma dimensão virtual que conforma, junto com a realidade física, a realidade ampliada (DUARTE; FIRMINO, 2008).

Essa qualidade tecnológica e dimensional garante que a vigilância seja realizada em tempo real, de acordo com os fluxos e registros pessoais efetuados no cotidiano dos atores urbanos. Também viabiliza a vigilância invisível através dos dispositivos em escala reduzida e embutidos nas estruturas urbanas tradicionais, característica essa que se opõe ao modelo disciplinar de Foucault, pois na maior parte das vezes a vigilância passa despercebida, deixando o indivíduo alheio a sua realização.

Neste sentido, Lyon (2004), aponta que após os ataques terroristas a Nova York em 11 de setembro de 2001, a vigilância nas cidades dos países desenvolvidos sofreu um grande aumento sob a justificativa da proteção contra novos atentados. Assim, o anonimato, marca fundamental da vida urbana durante séculos, tem sido posto de lado em favor do escrutínio público através de tecnologias de informação e quanto maiores as complexidades urbanas, mais se desenvolvem tecnologias capazes de garantir o controle social (LYON, 2003).

A vigilância passa a ser cada vez mais significante para o controle governamental dos espaços urbanos nas sociedades conhecidas como da informação e do conhecimento (LYON, 1994).

A vigilância atualmente faz parte da agenda político-administrativa das instituições públicas, incluindo-se as esferas municipais. Os dispositivos e processos de monitoramento, atualmente, fazem parte do aparato tecnológico utilizado pela gestão urbana como forma de administrar o território das cidades em suas relações dinâmicas de fixos e fluxos. A capacidade de coleta e

análise de informações pessoais são necessários em um paradigma de gestão baseado no exame de dados e indicadores em tempo real.

A transformação de ambientes urbanos construídos a partir da infraestrutura de sistemas de vigilância desafia a ideia de anonimato e privacidade. Com um espaço mais vigiado, o olho eletrônico, onipresente, garante uma sensação de segurança e bem-estar em que os serviços públicos passam por um processo de aceleração de suas respostas às demandas populares. Mas essa interação eletrônica transcende todas as barreiras de tempo-espaço e passa a invadir a vida dos sujeitos (GRAHAM; MURAKAMI WOOD, 2006).

Dessa forma, Kayyali (2016) defende que nem sempre as opções tecnologicamente avançadas são a melhor solução para os problemas urbanos, sendo que projetos para a melhora da qualidade de vida dos habitantes são mais eficientes quando há uma intenção de se resolver um problema através da equidade e inclusão social. Kayyali aponta que sistemas tecnológicos de controle de dados são poderosas ferramentas de reprodução da ideologia dominante, tornando-a inútil, senão contraprodutiva, para a resolução dos problemas estruturais das cidades (KAYYALI, 2016).

Já Batty (2013) e Kitchin (2014) ressaltam que sensores e sistemas coletam dados pessoais de cidadãos em tempo integral nas cidades, sendo que toda a informação coletada é armazenada em grandes bancos de dados, ou Big Data. Esse processo pode gerar vantagens à população, ao governo e à iniciativa privada, porém os dados, que são produzidos em larga escala e fornecem os indicadores urbanos de imediato, podem mudar o paradigma do planejamento a longo prazo para uma gestão tecnocrática de cada instante da vida urbana (BATTY, 2013; KITCHIN, 2014).

Chegamos então em um paradigma urbano em que as tecnologias de vigilância estão presentes em todo o território das cidades, sendo utilizados pela gestão pública e pela iniciativa privada para o controle dos espaços públicos e os fluxos intra-urbanos. Apesar de trazer benefícios e resolver pragmaticamente certas adversidades pontuais, o emprego dessas tecnologias tem levado a um governo tecnocrático que não reconhece os problemas em suas origens para então desenvolver uma resposta adequada, simplesmente se contentando com medidas paliativas de gerenciamento imediato das situações críticas. Além disso, questões de discriminação estatística, privatização da gestão pública, invasão da privacidade e cerceamento da livre expressão, são apontamentos importantes para o entendimento das consequências associadas à adoção desse tipo de agenda.

Assim, fica evidente que a relação da vigilância com o espaço urbano é algo cada vez mais concreta e complexa, justificando o desenvolvimento de estudos mais pontuais sobre essa correlação temática e material.

A BIBLIOMETRIA

O artigo trata-se de uma pesquisa de cunho descritivo, com enfoque quantitativo, uma vez que os fatos são observados, registrados analisados sem serem manipulados (GIL, 1999). Tal como citado anteriormente, o objetivo é o mapear cronologicamente e geograficamente a produção

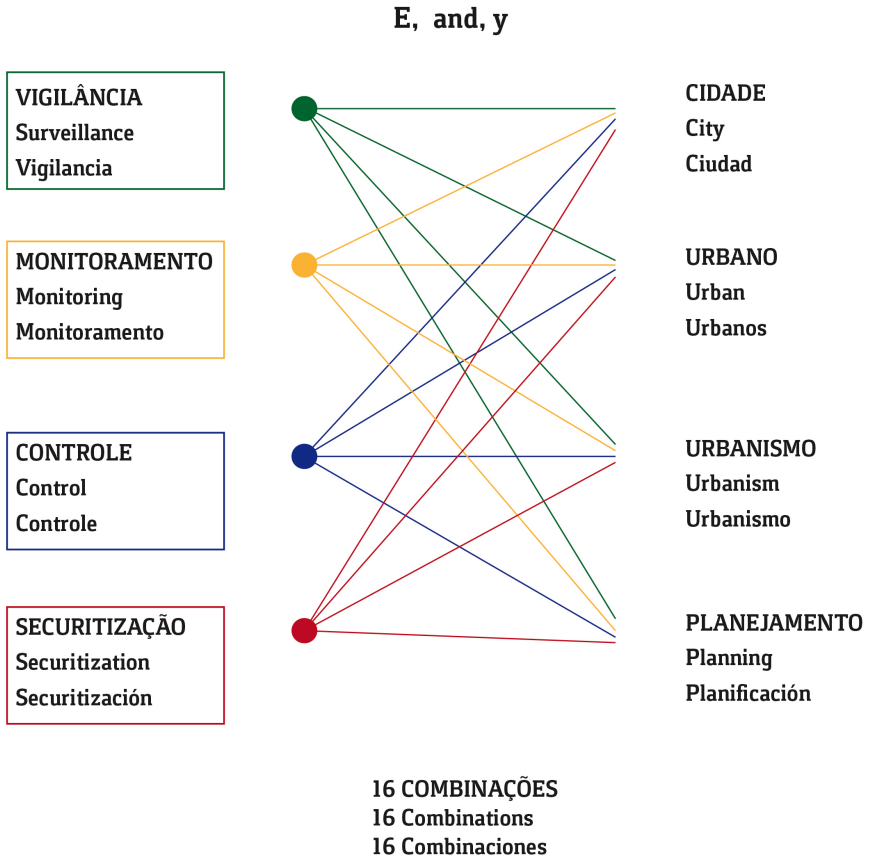
científica global identificada na correlação entre a vigilância e os estudos urbanos, a fim de contribuir para o entendimento de como essas duas áreas de estudo abordam os problemas contemporâneos.

A bibliometria é uma técnica que consiste na medição de índices que apontam a produção e disseminação do conhecimento científico (FONSECA, 1986) podendo ser aplicada em qualquer área do conhecimento (ARAUJO, 2006).

Para atingir o objetivo do trabalho, ele foi organizado em quatro etapas distintas: coleta de dados, análise dos dados, seleção dos trabalhos para análise e representação gráfica dos resultados analisados.

Desta forma, para concretizar a correlação utilizou-se o operador lógico (e, and, y) nas pesquisas efetuadas nos bancos de dados. As palavras-chave escolhidas foram: vigilância, monitoramento, controle, securitização, cidade, urbano, urbanismo e planejamento, associadas conforme a Figura 01.

FIGURA 01
Escolha das Palavras-Chave.



Fonte: Autores (2016).

As buscas foram efetuadas nas bases dos portais Scielo, Redalyc e Capes, e nos periódicos Urban Studies, Journal of Urban Technologies e Surveillance & Society As unidades de análise utilizadas incluem a autoria, procedência geográfica, temas recorrentes, periódicos e data de publicação (no de 2001 à 2016)

A partir dos registros retornados em cada base, os dados foram importados para a tabela referente a sua combinação (ex. vigilância e cidade) possibilitando a organização e visualização dos dados, permitindo uma análise mais eficiente e completa.

Após todos os dados estarem organizados nas, iniciou-se a aplicação dos critérios pré-estabelecidos para a seleção de estudos. Inicialmente, realizou-se a identificação dos artigos repetidos, em seguida, buscou-se descartar os artigos que apesar de ter palavras-chave compatíveis não correspondiam a área de estudo delimitada por este artigo.

A partir da padronização dos dados foi possível gerar gráficos e nuvens de palavras que demonstrassem os resultados encontrados, procurando apresentar um panorama da área de estudo.

O MAPEAMENTO DA PRODUÇÃO CIENTÍFICA

Uma das análises propostas do presente artigo é mapear geograficamente e cronologicamente a produção cientifica global da correlação entre a vigilância e os estudos urbanos. Para isso, foram selecionados, de acordo com os critérios estabelecidos, 81 artigos e a partir destes foram confeccionados gráficos e figuras a fim de facilitar a análise das ocorrências.

A premissa do artigo era de houve uma crescente importância dos temas vigilância e cidades para a ciências sociais no período posterior aos atentados terroristas de 11 de Setembro de 2001 e o caso Snowden (2013). Para verificar a existência de uma relação entre o aumento do terrorismo e a produção científica procurou-se comparar os gráficos gerados por meio de dados extraídos da Global Terrorism Database (GTD) com os resultados da produção obtidos por data.

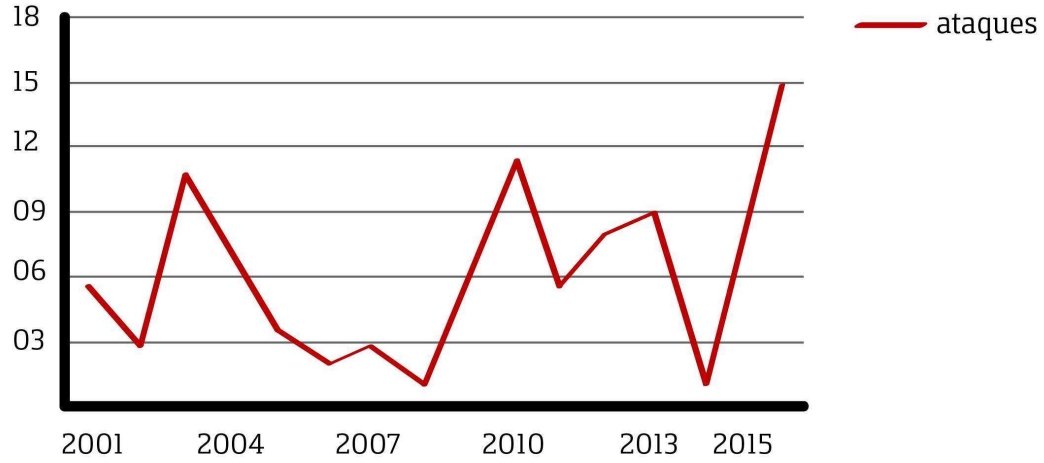
Segundo dados da GTD os anos 2000 já somam o maior total de ações terroristas no mundo, cerca de 70 mil casos. De acordo com o gráfico 01 é possível observar a incidência dos ataques ao longo destes anos e no gráfico 02 como se deu a produção cientifica no mesmo período de tempo. Para a comprovação da hipótese levantada, houve a sobreposição dos dois gráficos.

Primeiramente, é relevante apontar o crescimento do número de estudos a partir de 2010, demonstrando que essa sobreposição temática tem provocado um interesse recente por parte da academia. Este cenário pode ser explicado pelo fato de que esse sombreamento temático é uma ramificação dos estudos de vigilância sobre os estudos urbanos, sendo que o primeiro ainda é relativamente recente enquanto disciplina.

No Gráfico 03 é nítido que a linha cronológica de produção cientifica está diretamente ligada aos incidentes ao longo do tempo. Entretanto, a não se pode constatar o mesmo com a hipótese relacionada ao caso Snowden (2013), conforme o gráfico 02 mostra há uma queda significante da produção após 2013.

GRÁFICO 01

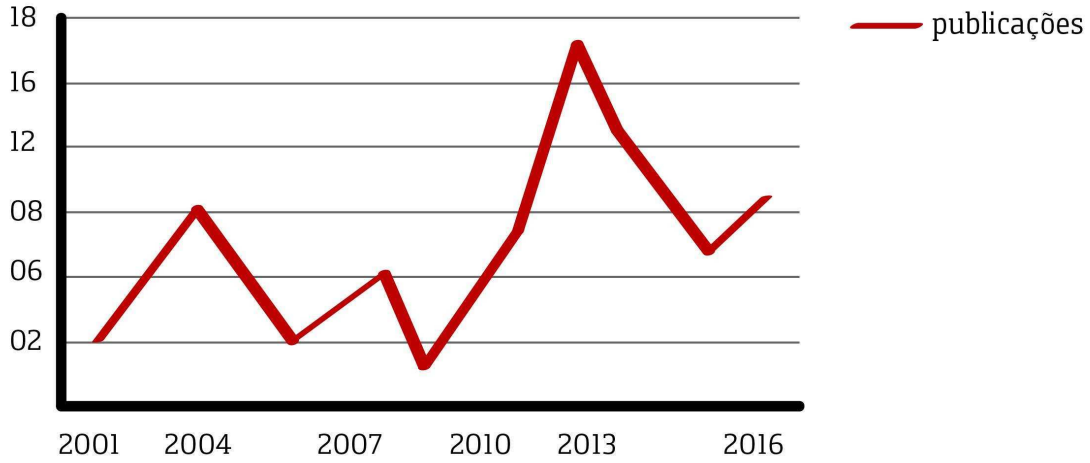
Ataques terroristas a partir de 2001



Fonte: Os autores, com base no GTD (2016).

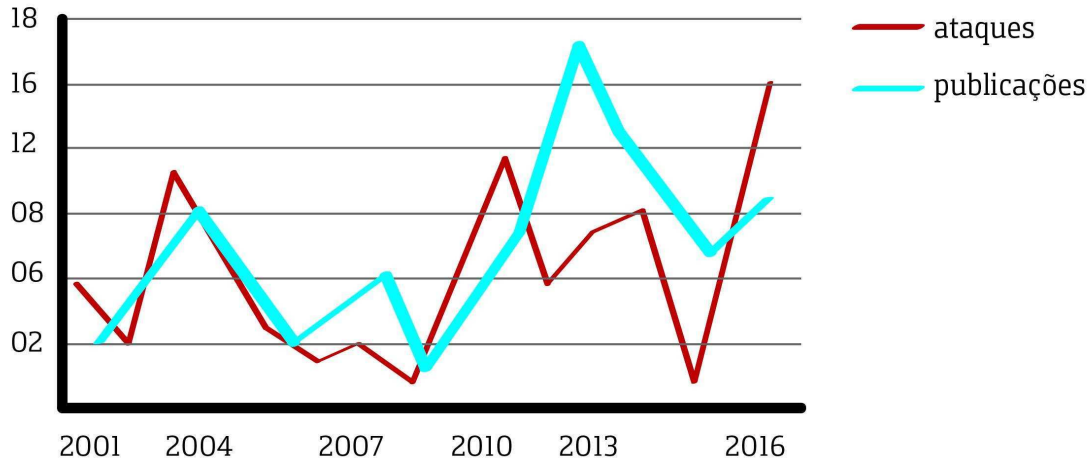
GRÁFICO 02

Publicações Científicas relacionadas aos temas



Fonte: Os autores (2016).

GRÁFICO 03
Sobreposição dos dados



Fonte: Os autores (2016).

Um fator relevante identificado é a correlação da produção científica com atentados terroristas. Este fato pode ser associado ao conceito de "militarismo urbano" de Stephen Graham (2010), pois, para o autor, depois dos ataques terroristas de 11 de setembro de 2001 os sistemas de vigilância passaram a ser implantados nas cidades a partir da esfera militar, prescindindo análises de seus impactos no espaço urbano.

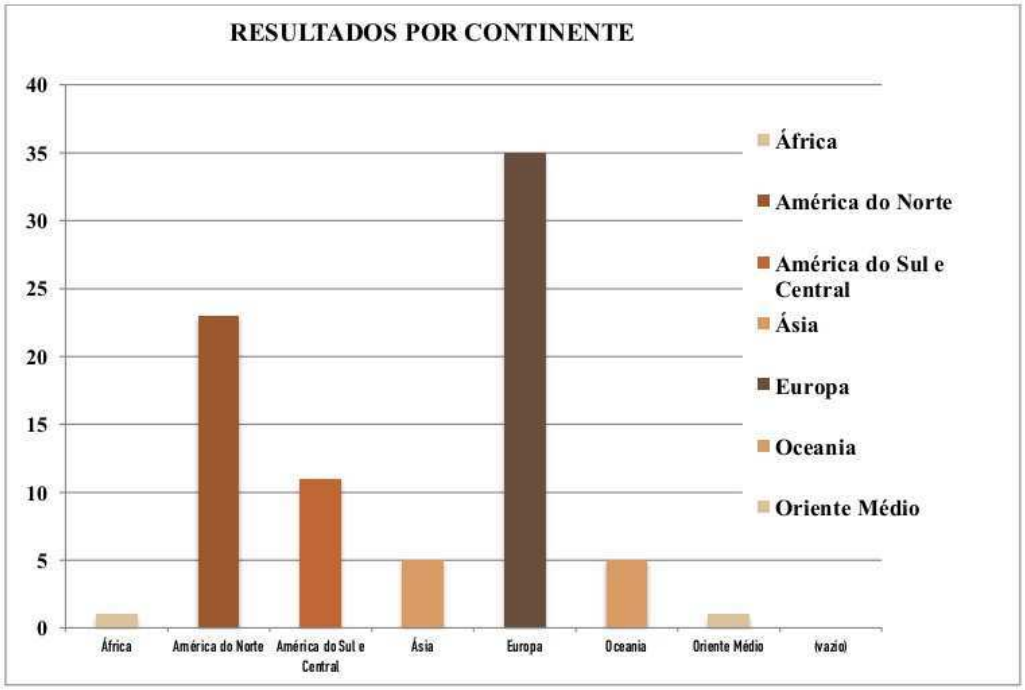
Outro aspecto a ser observado é a diferença do volume de produção por continentes, como mostra o gráfico 04 e a figura 02. Tal diferença pode ser explicada primeiramente, pelo fato de que há uma maior tradição e incentivo às pesquisas e ao debate acadêmico nas universidades europeias e da américa do norte, sendo comprovada pela figura 03, que ilustra os países com maior volume de artigos encontrados no levantamento

Outro fator é a existência, nestes dois continentes, de uma preocupação maior acerca da correlação dos temas, uma vez que eles são alvos frequentes de ataques terroristas e por isso houve nas ultimas décadas um aumento significativo dos sistemas de vigilância nos espaços urbanos. Os países do norte desenvolvidos são frequentemente aqueles que promovem políticas globais de vigilância e controle de fronteiras, além de coleta de informações digitais através de instituições de segurança nacional. Mais especificamente, foi identificada uma dominância dos Estados Unidos e do Reino Unido, países que contam com sistemas de vigilância global e centralizam os discursos de segurança nacional e controle de fronteiras.

Além disso, é também nesses territórios onde houve o desenvolvimento e uma maior penetração das tecnologias digitais, que são fundamentais para a transformação do urbanismo contemporâneo e a adoção de ferramentas tecnológicas na gestão das cidades. Tais tecnologias estão profundamente associadas ao desenvolvimento da vigilância no âmbito urbano e, portanto, ganhou uma maior atenção dos estudiosos das áreas da vigilância e dos estudos urbanos.

GRÁFICO 04

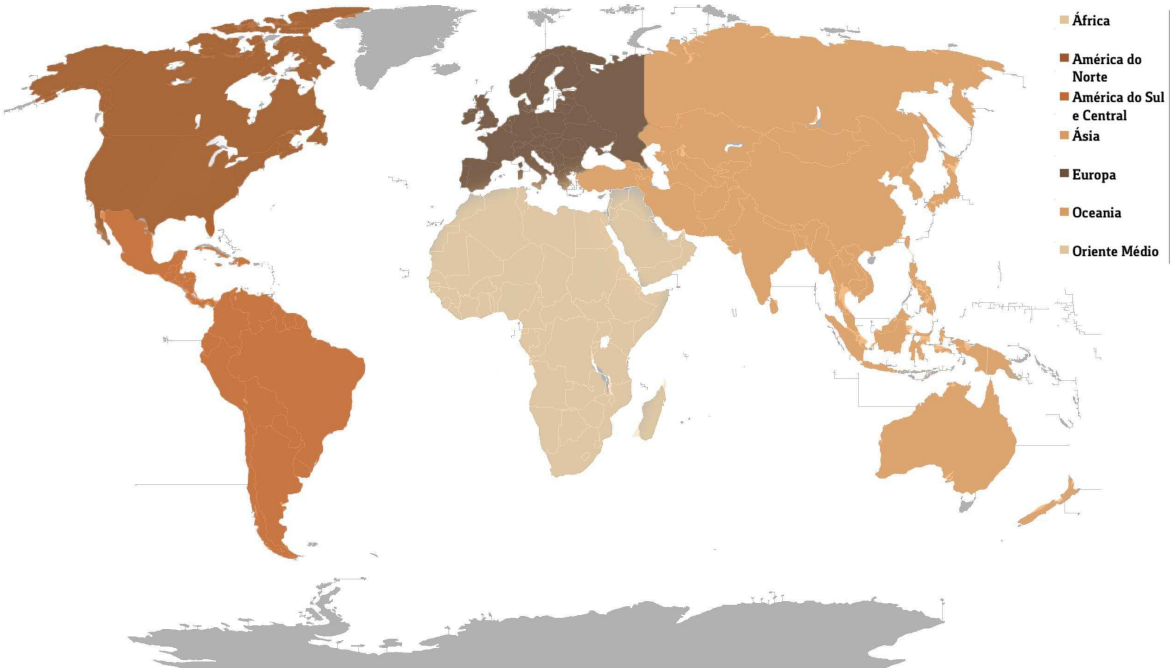
Publicações por Continente



Fonte: Os autores (2016).

FIGURA 02

Publicações por Continente



Fonte: Os autores (2016).

FIGURA 03
Volume de produção por país.

Fonte: Elaborado pelos autores a partir da ferramenta de análise de recorrências textuais worditout

Uma análise das palavras-chave com maior ocorrência, como mostra a figura 04 revela que a palavra *vigilância* é a mais recorrente para a identificação do tema, sobrepondo outras terminologias utilizadas como monitoramento, controle e securitização. Já no que tange os estudos urbanos, a principal unidade de análise, a partir do levantamento das palavras-chave, é o espaço urbano, seguido do termo genérico *urbano.* A partir desses dados sugerimos que há um maior interesse dos pesquisadores na relação da vigilância com o espaço urbano, mais especificamente com a presença de câmeras de vigilância, corroborada pelo destaque do termo *videovigilância.*

FIGURA 04
Palavras-chave.

Fonte: Elaborado pelos autores a partir da ferramenta de análise de recorrências textuais worditout

CONCLUSÃO

A investigação da relação da cidade com a vigilância é uma temática bastante atual e importante para os estudos urbanos e, por esse motivo, tornou-se o objeto desta pesquisa. Todavia, no processo investigativo foi identificada uma relativa baixa produtividade mundial dentro do assunto, que pode ser um dado preocupante, visto que as tecnologias de vigilância estão sendo implantadas no espaço urbano de forma cada vez mais intensiva, seja com o uso do discurso das cidades inteligentes, no combate à violência, na maior eficiência dos serviços públicos e fluxos urbanos, no combate o terrorismo, entre outros usos e discursos.

O crescimento dos sistemas de vigilância, dessa forma, também traz implicações mais complexas para os cidadãos e para o espaço urbano, entre elas está a gradativa perda da liberdade, da privacidade e a discriminação estatística. Gandy (1993) defende que a classificação por meio de dados coletados do cidadão faz parte de um processo que ele chamou "panoptic sort", ou seleção panóptica. Para o autor é uma forma nova de discriminação, no qual são gerados perfis de cidadãos que são considerados ameaças ou indesejados nos espaços urbanos.

Neste sentindo, a produção científica sobre a relação da vigilância e o urbano é uma importante discussão para se construir uma sociedade mais crítica, por questionar de forma holística os impactos da vigilância no espaço, papel este dos cientistas, escritores e pesquisadores que trabalham com vigilância. É fundamental pois a produção cientifica deve enxergar questões para além da ordem política ou mercadológica, ultrapassando o discurso essencialmente positivo e solucionador de todos os problemas presente na promoção dos sistemas de vigilância.

Deve-se salientar ainda que os sistemas de vigilância trazem para o cidadão a sensação de segurança, sendo considerados positivos e desejáveis, o que pode ser um julgamento equivocado, pois não há correlação direta desses sistemas com a redução efetiva da criminalidade ou o fim do terrorismo. Assim, a implantação dessas tecnologias segue um discurso tecnocrático alinhado à ideologia dominante que resulta ineficiente na solução dos problemas urbanos.

Por tais motivos, a baixa produtividade científica na relação da vigilância com o espaço urbano e a dominância dos países centrais na produção acadêmica na área são vistas nesta pesquisa como um dado importante e passível de novas investigações. Este artigo apenas mostrou um cenário, mas é preciso uma análise mais profunda sobre as causas deste fenômeno, abrindo espaço para novos estudos e contribuições acadêmicas.

NOTAS

1. Doutoranda em Gestão Urbana PPGTU/PUCPR, Curitiba – Brasil. Contato: marcelamoraes.b@gmail.com

2. Mestrando em Gestão Urbana PPGTU/PUCPR , Curitiba – Brasil. Contato: thiagogsroberto@gmail.com

3. Mestranda em Gestão Urbana PPGTU/PUCPR, Curitiba – Brasil. Contato: gabifvarela@gmail.com

REFERÊNCIAS

BATTY, (2013). M. Big data, smart cities and city planning. London: Dialogues in Human Geography, v. 3, n. 3, p. 274-279.

BAUMAN, Z. (2001). Confiança e medo na cidade. Tradução de Dentzien, P. Rio de Janeiro: Zahar.

BENTHAM, J.; MILLER, A. PERROT, M. (2008). O panóptico. Organização de Tomaz Tadeu; traduções de Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. Belo Horizonte: Autêntica Editora,

BOGARD, W. (1996). The simulation of surveillance: hypercontrol in telematic societies. Cambridge: Cambridge University Press,

CASTELLS, M. (1999) A sociedade em rede (A era da informação : economia, sociedade e cultura : v. 1). São Paulo: Paz e Terra.

DELEUZE, G. (2013) Conversações (1972-1990). Tradução de Pal Pelbart, P. São Paulo: Editora, 34.

DUARTE, F.; FIRMINO, R. J. (2008). Cidade infiltrada, espaço ampliado: as tecnologias de informação e comunicação e as representações das espacialidades contemporâneas. Disponível em http://www.vitruvius.com.br/revistas/read/arquitextos/08.096/3408. Acesso em 18/04/2016.

FOUCAULT, M. (2013). Vigiar e punir: o nascimento da prisão. Tradução de Ramalhete, R. Rio de Janeiro: Editora Vozes.

FOUCAULT, M. (1984) Microfísica do poder. Organização e tradução de Machado, R. Rio de Janeiro: Edições Graal.

GANDY, O. H. (1993) The panoptic sort: a political economy of personal information. Boulder: Westview Press.

GRAHAM, S. (2004) Excavating the material geographies of cybercities. *In:* GRAHAM, S. The cybercities reader. Londres: Routledge.

GRAHAM, S.; MARVIN, S. (2001) Splintering urbanism: network infrastructures, tecnological mobilities and the urban condition. Londres: Routledge.

GRAHAM, S; WOOD, D. (2003) Digitizing surveillance: categorization, space, inequality. Critical Social Policy, v.23, n. 2, p. 227-248.

HAGGERTY, K. ERICSON, R. (1997). Policing the risk society. Toronto: University of Toronto Press.

KITCHIN, R. (2014). The real-time city? Big data and smart urbanism. GeoJournal, v. 79, n. 1, p. 1-14.

KAYYALI, D. (2016). Cidades inteligentes: conectadas para a injustiça. Disponível em: https://antivigilancia.org/pt/2016/03/cidades-inteligentes-conectadas-para-a-injustica/. Acessado em 24/05/2016.

LYON, D. (2013). The electronic eye: the rise of surveillance society. Cambridge: Polity Press. [E-BOOK]

LYON, D. (2009). Surveillance, power and everyday life. *In:* MANSEL, R. The Oxford handbook of information and communication technolgies. Oxford: Oxford University Press.

LYON, D. (2003). Surveillance technology and surveillance society. *In:* MISA, T.J.; PHILIP, B.; FEENBERG, A. Modernity and technology. Cambridge: MIT Press.

LYON, D. (2002). Everyday surveillance: personal data and social classification. Information, Communication & Society, v.5, n.2, p. 242-257.

MARX, G.T. (2002). What´s new about the "new surveillance"? Classifying for change and continuity. Surveillance & Society, Ontario, v. 1, n. 1, p. 9-29.

MARX, G.T. (2013). An Ethics for the New (and Old) Surveillance. *In*: FLAMMINI, F; SETOLA, R; FRANCESCHETTI, G. Effective Surveillance for Homeland Security: Balancing Technology and Social Issues. Boca Raton: CRC Press.

MURAKAMI WOOD, D. (2006). A report on the surveillance society. Disponível em: https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf. Acessado em 17/03/2016.

SANTOS, M. (2014). A natureza do espaço: técnica e tempo, razão e emoção. São Paulo: Editora da Universidade de São Paulo.

VIRILIO, P. (1993). O espaço crítico. Tradução de Pires, P. R. Rio de Janeiro: Ed. 34.

“EL REALITY DE LA INSEGURIDAD”. TELEVISIÓN, CÁMARAS DE VIGILANCIA Y NUEVOS MODOS DE CONSTRUCCIÓN DE LA NOTICIA POLICIAL AUDIOVISUAL.

Resumen: Esta ponencia presenta los resultados preliminares de un trabajo en curso sobre los nuevos modos de construcción de la noticia policial en la televisión. A partir de un monitoreo de noticieros de aire de la Ciudad de Buenos Aires, se busca dar cuenta de la especificidad de la noticia audiovisual y revisar de qué modo se construyen las noticias sobre el tópico seguridad/inseguridad a partir del uso de las imágenes de las cámaras de seguridad (públicas o privadas). Se analizaron un total de veinte emisiones de noticieros de horario central en canales de aire públicos y privados de la Ciudad de Buenos Aires durante la primera semana de octubre de 2015. El rol de las fuerzas de seguridad y la justicia en la generación de contenido policial para los medios de comunicación está mutando a partir de la emergencia, en estos últimos años, de nuevos modos de producción de noticias. El procedimiento de vinculación entre la policía, la justicia y el periodismo hoy no desaparece, pero ante la imagen negativa de algunas instituciones y las capacidades técnicas que habilitan las nuevas tecnologías las fuentes se diversifican. El acceso a estos registros audiovisuales habilita un nuevo modo de relatar los hechos, una estética de “lo real” que busca invisibilizar las mediaciones y emular en las pantallas “la vida misma”. La noticia policial se construye así desde lo cotidiano, dando espacio a un tipo de información que no se sustenta sin el material provisto por estas nuevas tecnologías. Como resultado, los criterios de veracidad parecen dejar de estar definidos por las fuentes institucionales y pasan a estarlo por la sensación de inmediatez que habilitan las imágenes captadas por estos dispositivos.

Palabras clave: Cámaras de seguridad, Noticia policial, Medios, Televisión.

MERCEDES CALZADO*
YAMILA GÓMEZ**
VANESA LIO***

"O reality da insegurança". Televisão, câmeras de vigilância e novas formas de construção da notícia policial audiovisual.

Resumo: Este artigo apresenta os resultados preliminares de um trabalho em curso sobre os novos modos de construção da notícia policial na televisão. A partir do monitoramento de noticiários da cidade de Buenos Aires, procura explicar a especificidade das notícias audiovisuais e rever a forma como as notícias sobre a segurança/insegurança são construídas a partir do uso de imagens de câmeras de segurança (públicas ou privadas). Foram analisados um total de vinte emissões de canais de noticias públicos e privados de Buenos Aires durante a primeira semana de outubro de 2015. O papel das forças de segurança e da justiça na geração de conteúdo para a mídia tem mudado a partir do surgimento nos últimos anos, de novas formas de produção de notícias. A ligação entre a polícia, a justiça e o jornalismo não desaparece, mas diante a imagem negativa de algumas instituições e pelas capacidades técnicas que permitem as novas tecnologias, as fontes se diversificam. O acesso a essas gravações de vídeo permite uma nova forma de contar os fatos, uma estética do "real" que busca tornar invisível as mediações e imitar nas telas de televisão a "vida mesma". A notícia policial é construída a partir do cotidiano, gerando espaço para um tipo de informação que não é suportado sem o material fornecido por essas novas tecnologias. Como resultado, os critérios de veracidade parecem não estar definidos por fontes institucionais e são definidos pela sensação do imediato que permitem as imagens capturadas por esses dispositivos.

Palavras-chave: Câmeras de segurança, Notícia policial, Media, Televisão.

"The insecurity reality show". TV, surveillance cameras and new ways of building audiovisual police news.

Abstract: This paper presents the preliminary results of an ongoing research on new modes of production of police news on television. From monitoring Buenos Aires' air TV newscasts, it seeks to describe the specificity of audiovisual news and examine how the news about the topic "security/insecurity" are constructed from the use of security cameras images (public or private). We analyzed twenty primetime emissions on the most important public and private TV channels of Buenos Aires city during the first week of October 2015. The role of security forces and justice in the generation of police content for the media is mutating from the emergence, in recent years, of new ways of news production. The linkage between police, justice and journalism does not disappear, but the negative image of some institutions together with technical capabilities that enable new technologies contribute to the diversification of sources. The access to these audiovisual recordings enables a new way to tell facts, by using an aesthetic of "reality" that tends to erase mediations and emulate "real life" on the screens. Police news are built from everyday life events, enabling the emergence of a new type of information that is not supported without the material provided by these new technologies. As a result, the truthfulness criteria is not defined by institutional sources anymore but by the sense of immediacy that images captured by these devices enable.

Key-words: Videocameras, News, Media, Televisión.

INTRODUCCIÓN

Históricamente la noticia policial en Argentina se produjo gracias al estrecho contacto entre periodismo y agencias policiales. La profesionalización del periodismo policial en nuestro país se entiende en gran medida a partir de este vínculo. Tan es así que uno de los primeros periodistas de noticias sobre el mundo criminal es Fray Mocho, quien antes de dedicarse al periodismo se desempeñó como inspector de la Policía Federal. Muchos estudios relatan este vínculo (Caimari, 2004; Saítta, 1998), como así también el modo en que desde mediados de la década del noventa -cuando la noticia policial adquiere un lugar central en los medios gráficos y televisivos de Argentina- las principales fuentes del periodismo en esta materia son las policiales, seguidas de lejos por las agencias judiciales (Martini, 2009).

Pese a que este modo de construir las noticias policiales sigue estando presente, en los últimos años comenzó a surgir una novedad: la información producida gracias a imágenes (no

necesariamente relevantes) de cámaras de seguridad, redes sociales y celulares. El acceso a registros audiovisuales que hasta un tiempo atrás no existían como tales habilita un nuevo modo de relatar los hechos, una estética de "lo real" que busca invisibilizar las mediaciones y emular en las pantallas "la vida misma". En la construcción de estas imágenes como productos mediáticos se pretende una "estética de la objetividad" que, para el caso de las cámaras de seguridad, se funda en la presentación de los videos como evidencia, buscando borrar las marcas que las constituyen como construcciones intencionadas (Gates, 2013).

En términos estéticos, la videovigilancia se transformó en una parte del repertorio cultural contemporáneo (Groombridge, 2002; Bruno y otros, 2012). Así, a partir de su inclusión en las vidas cotidianas surgen nuevas prácticas y discursos en torno a las cámaras de seguridad. La atención a su dimensión política y poética dio lugar a trabajos críticos que buscan demostrar la cualidad ficcional de toda imagen y cuestionar el valor de realidad que se atribuye al material audiovisual surgido de estos dispositivos (Baretto Leblanc, 2010).

La "retórica de la vigilancia" atraviesa no sólo las producción de noticias audiovisuales para televisión y medios gráficos online, sino también la industria fílmica, a partir de la recurrencia a "imágenes falsas de cctv" (Kammerer, 2004). En este sentido, al interés por estudiar la videovigilancia desde perspectivas criminológicas y sociológicas se suman los abordajes que buscan entenderla desde los estudios, artísticos, culturales y de medios.

Algunos trabajos indagan las representaciones mediáticas de la videovigilancia, los significados privilegiados y el rol que la televisión juega en la aceptación por parte del público del uso de estas tecnologías (Hempel, 2006; Kroener, 2013). La tendencia a la espectacularización de la videovigilancia (Arteaga Botello, 2006) adquiere, en el caso argentino, características particulares a partir de su vinculación con la agenda política local: los contenidos de los cctv se vuelven un capital político central en las estrategias comunicacionales a nivel municipal. La estética y las marcas sobre la imagen permiten constatar que las instituciones locales ceden el material a los fines de gestionar el miedo en la población y mostrar un Estado activo frente a la cuestión del delito (Lio, 2012). En este sentido, nuestra pregunta acerca de las fuentes habilita, en el caso de las imágenes de circuitos públicos, una nueva serie de interrogantes acerca de las vinculaciones entre las instituciones a cargo de la vigilancia pública de las ciudades y los productores de noticias de los canales televisivos. Como señalan Norris y otros (2004), al público se le recuerda constantemente de la presencia de las cámaras "a través de unos medios de comunicación locales hambrientos de una noticia impactante que pueda ser dramáticamente visualizada a través del uso de las imágenes grabadas por los cctv" (125). Sin embargo, de acuerdo con Cardoso (2012), el accionar de estos gobiernos conduce a una "paradoja": la construcción de legitimidad a partir de la circulación mediática de materiales que muestren la actuación ejemplar de los sistemas de monitoreo supone la necesidad de "captar en el acto" una mayor cantidad de los mismos hechos que las propias cámaras pretenden disuadir.

Nuestro trabajo se sitúa en el cruce de estas formas de vigilancia y los nuevos modos de construcción de la noticia policial en la televisión. A partir de un monitoreo de noticieros de aire de la Ciudad de Buenos Aires, que forma parte de una investigación más amplia aún en curso, se busca dar cuenta de la especificidad de la noticia audiovisual y revisar de qué modo se construyen las noticias sobre el tópico seguridad/inseguridad a partir del uso de las imágenes de las cámaras de seguridad (públicas o privadas). Para ésto, se analizaron 25 emisiones de noticieros de horario central en canales de aire públicos y privados de la Ciudad de Buenos Aires durante la primera semana de octubre de 2015.

La hipótesis que guía este trabajo es que los criterios de veracidad parecen dejar de estar definidos por las fuentes institucionales y pasan a estarlo por la sensación de inmediatez que habilitan las imágenes captadas por estos dispositivos. De allí a que el rol de las fuerzas de seguridad y la justicia en la generación de contenido policial para los medios de comunicación está mutando a partir de la emergencia, en estos últimos años, de nuevos modos de producción de contenidos. Aunque el procedimiento de vinculación entre la policía, la justicia y el periodismo no desaparece, ante la imagen negativa de algunas instituciones y las capacidades técnicas que habilitan las nuevas tecnologías las fuentes se diversifican. La noticia policial se construye así desde lo cotidiano y le da un lugar a un tipo de información que no existiría sin el material provisto por las nuevas tecnologías.

NOTICIA POLICIAL, TECNOLOGÍAS Y NUEVAS FUENTES DE INFORMACIÓN

Las nuevas tecnologías incorporan un novedoso modo de contar las noticias policiales. Cámaras de seguridad, teléfonos celulares y redes sociales se convierten en fuentes de los relatos sobre la inseguridad urbana. Las noticias en los informativos de aire se tratan como pequeñas historias cuyo anclaje de veracidad se encuentra fuertemente dado por la centralidad de estos dispositivos.

El seguimiento que realizamos en los informativos de aire transmitidos desde la Ciudad de Buenos Aires revelan que en general la información producida desde estos dispositivos es, en principio, poco relevante. No obstante ello, la información generada por las nuevas tecnologías es puesta en un lugar central como resultado de la accesibilidad única de la producción al material. De allí a que los noticieros refuerzan la figura de la primicia en torno a estas imágenes.

Un resultado interesante de este proceso es la dispersión de la agenda tanto al interior de cada informativo como entre las emisiones de los distintos canales. Se busca dar cuenta a los espectadores de un acceso diferencial a las imágenes como una forma de "tener la exclusiva", más que a perseguir la relevancia noticiosa o una agenda temática preexistente.

La noticia titulada "Pirán, la calle de los robos y del miedo" (Telefé Noticias 2a Edición, 6/10/2105) permite ejemplificar esta búsqueda de la primicia. La información se basa en la particularidad de una zona de esta calle en la localidad de Wilde, Provincia de Buenos Aires, y en la dinámica vecinal que se construyó como consecuencia "de los robos y la inseguridad". Mientras se muestran imágenes de las cámaras de seguridad públicas y privadas, se relata la acción de los vecinos

como protagonistas de la noticia: "Los vecinos hicieron todo para evitar los robos, pusieron varias cámaras de seguridad, también pusieron alarmas, pero parece que nada alcanza porque los hechos de inseguridad continúan". Otro ejemplo de la magnificación de casos puntuales es la noticia "Cometen entraderas con tarjetas" (América Noticias, 8/10/2015), presentada por el conductor como "historias de inseguridad en el conurbano bonaerense", que se construyen a partir de un video de unos pocos segundos de duración como única fuente. La búsqueda de "la exclusiva" también se evidencia en la presentación de "hechos insólitos". Ejemplo de esto es la noticia "'Martillo' peligroso como 'bombita'" (Telenueve, 9/10/2015). El video sobre el que se narra la noticia muestra a un hombre -dueño de un auto que fue remolcado por la grúa por estar mal estacionado en la Ciudad de Buenos Aires- que amenaza con un martillo a los empleados de la playa de infractores para retirar su auto sin pagar la multa. La presentación de la noticia se basa en las imágenes de las cámaras de seguridad que registraron el momento, se extiende por más de nueve minutos y repite varias veces el material audiovisual, enfatizando lo "extraño" del hecho y apelando a la categoría de "locura" para explicarlo.

Estas modalidades habilitan, además, la construcción de noticias policiales centrales a partir de hechos que no sólo podrían considerarse poco relevantes en términos de la agenda noticiosa, sino que muchas veces no constituyen delitos sino que se definen en tanto hechos insólitos, extraños, bizarros o fuera de lo común. En relación con esto, se verificó una tematización como noticias policiales y sobre inseguridad de contenidos que comúnmente eran incluidos en la sección "información general".

Esto conduce a otra característica que surgió del monitoreo de los noticieros de televisión: la presentación de información que difícilmente hubiese configurado una noticia sin el acceso a las imágenes que habilitan estos dispositivos. La noticia "Abogado borracho atropelló a agentes de tránsito" (todos los noticieros, 9/10/2015) se construye a partir de la imágenes tomadas por las cámaras de la Policía Metropolitana de la Ciudad de Buenos Aires. Los noticieros de los cinco canales analizados incluyen la noticia y la narran a partir de las imágenes disponibles que intentan mostrar (aunque no queda del todo claro en el registro audiovisual) el momento en que el auto atropella a los agentes de tránsito. Cabe al menos preguntarse si la noticia hubiera tenido el mismo despliegue (o, incluso, si se hubiese construido como noticia) sin las imágenes del hecho. Algo similar sucede con una noticia sobre un robo en un banco de Hurlingham (Telenueve Central y Telefé Noticias, 9/10/2015). Las cámaras de seguridad del municipio registran el momento en que salen los ladrones del banco y a partir de esas imágenes se narra la historia. Se trata, en realidad, de una noticia de un "no robo" dado que, por error, los ladrones se llevaron una bolsa con papeles en lugar del dinero. En este caso, la noticia de policiales es matizada con un tono de humor y alivio porque el robo "salió mal".

Otra noticia interesante de revisar es la titulada "Robos insólitos e increíbles" (América Noticias 2a edición, 8/10/2015). Por un lado, se construye sobre la rareza del hecho y, por otro, no sería posible sin las imágenes. Se trata de personas que quedan registradas en las cámaras de seguridad, en general, de sistemas privados y que roban plantas, perros y cuchas. Lo ubican en una serie y

se vuelven a contar noticias que ya se habían mostrado semanas atrás, retomando hechos de características similares por su "rareza". Estas noticias a partir de pequeños sucesos, de los que hay una imagen filmada, a su vez facilitan la exhibición del robo como algo cotidiano, ubicuo, que puede cometer cualquiera y del cual "todos" somos potenciales "víctimas". En este "reality de la inseguridad", los modos de narrar los hechos desde una "estética de lo real" a partir de las imágenes provistas por las nuevas tecnologías, se vincula con una nueva modalidad que verificamos en el análisis y que denominamos "narración extendida". Esta forma de presentar la noticia habilita la construcción de miedos y riesgos a partir de una "no noticia". Es decir, a pesar de la ausencia de un hecho delictivo particular, se configuran los peligros potenciales a partir de la posibilidad de que determinado hecho suceda. En este sentido, se presenta como un peligro potencial en término de riesgos futuros. Se produce un doble proceso que, por un lado, vuelve realidad los mundos posibles ("Van a seguramente robar a una persona inocente") y, por otro, generaliza esos riesgos identificando al televidente como posible víctima ("Le podría pasar a usted"). Desde lo discursivo, los periodistas destacan la importancia de las cámaras de seguridad, asociándolas a la resolución de los hechos y la prevención, tanto en noticias referidas a hechos delictivos como a anuncios gubernamentales o promesas electorales.

A este uso de las imágenes de las cámaras de seguridad como fuentes de información se suma el recurso a otras tecnologías cotidianas, como los teléfonos celulares. La especificidad de estas imágenes es que tienen una estética particular (desprolija, con cámara en mano, donde partes de la imagen pueden aparecer tapadas con personas u objetos que se cruzan) que da lugar al mismo recurso de relato de "lo real" que comentamos anteriormente: mostrar lo que sucedió "realmente" en el aquí y ahora del hecho noticioso1. Además, son expresión de una modalidad de periodismo que fue creciendo en los últimos años con las posibilidades de estas nuevas tecnologías y dispositivos para la comunicación: el "periodismo ciudadano". Los mismos noticieros piden a los televidentes que les acerquen imágenes tomadas por ellos mismos de los hechos que comunican. Estas imágenes suelen ser fragmentos cortos que se transmiten repetidas veces para enfatizar la importancia de este tipo de testimonio audiovisual2. Muchas veces estos contenidos son viralizados antes por las redes sociales y luego son incorporados a los programas televisivos o a los periódicos digitales. A través de esta modalidad los sujetos sociales se reconstituyen como productores primarios de representaciones mediadas producidas por ellos mismos. Prolifera así la producción por parte de "gente común" de fotos o videos sobre hechos policiales tomadas por cámaras de teléfonos celulares u otros dispositivos (Yar, 2012: 246).

Por otro lado, aparecen las redes sociales como un canal de acceso a las fuentes primarias. En muchos casos, esto permite un acceso inmediato a las declaraciones de los protagonistas de las noticias, mediante el rastreo de sus intervenciones en cuentas o perfiles de Twitter y Facebook. Ante la imposibilidad de contactar a las fuentes de modo inmediato por las vías tradicionales, las redes sociales se convierten en un modo de acceso directo e inmediato. En otros casos, pareciera haber una búsqueda específica sobre un tema o hecho en particular, que posibilita reponer algunas intervenciones de actores involucrados pero no necesariamente famosos. Por

otro lado, este tipo de redes sociales, y particularmente Youtube, permiten viralizar videos tomados por los noticieros y construidos como contenidos del programa, a partir de su reproducción, una tematización determinada y los comentarios o análisis que los periodistas puedan aportar al tema3. Esto da lugar a la inclusión en términos de noticia policial y de inseguridad de hechos sucedidos en otros países, regiones y continentes. Finalmente, en relación con las imágenes, las redes sociales más vinculadas a la circulación de fotografías (como Facebook, Pinterest o Instagram) parecen funcionar como un repositorio de imágenes de archivo y se utilizan como fuentes para ilustrar las noticias policiales con fotografías de los actores involucrados previas al hecho y surgidas de su ámbito "privado".

COMENTARIOS FINALES

Como anticipamos, los resultados parciales que aquí se presentan son producto de la primera etapa de una investigación en curso sobre los nuevos modos de construcción de la noticia policial en la televisión. En este sentido, el monitoreo de noticieros centrales en canales aire de la Ciudad de Buenos Aires nos permitió observar una serie de regularidades en la construcción de información sobre el tópico seguridad/inseguridad y dar cuenta de la especificidad de la noticia audiovisual, tanto en relación con las modalidades de otros medios de comunicación como con las características históricas de este formato televisivo.

Es en este marco que surge la especificidad de las noticias construidas a partir de imágenes de cámaras de seguridad y otras tecnologías de uso cotidiano. La frecuencia con que los videos procedentes de estos dispositivos se incorporaban en las noticias de los informativos analizados nos dio la pista para comenzar a indagar con mayor profundidad en esta característica específica de los contenidos audiovisuales. Así surge nuestra observación de que las nuevas tecnologías, en especial las cámaras de seguridad, los teléfonos celulares y las redes sociales, se incorporan como fuente de información de noticias (fundamentalmente pero no sólo) policiales. Esto nos conduce a plantear como hipótesis que la expansión en el uso de este tipo de tecnologías está transformando las rutinas de los medios televisivos en la producción de contenido. El acceso a un nuevo tipo de registro audiovisual permite construir noticias sobre hechos que, en principio, no serían noticiables de no contar con las imágenes. A esto se suma que la "estética de la vigilancia" habilita un registro discursivo con una pretensión de "realidad", que busca invisibilizar las mediaciones y presentar los hechos tal y como suceden.

Sin embargo, no pretendemos decir que la disponibilidad de estas imágenes implique por sí misma y necesariamente su inclusión en la agenda de los canales y programas de noticias. Entendemos que esta nueva forma de construcción de información policial y sobre inseguridad es parte de otros procesos sociales y culturales más amplios, que se vinculan con la producción de noticias pero también con las demandas de las audiencias.

En este sentido, el análisis en paralelo que en el marco de este proyecto hicimos de los noticieros de la Ciudad Autónoma de Buenos Aires y de la Ciudad de Córdoba nos permitió observar que

esta nueva modalidad y estas nuevas fuentes sólo se verificaban en el caso de CABA, mientras que en Córdoba los informativos mantenían las modalidades y formatos más tradicionales.

Así, en principio, pareciera que los contextos geográficos, socio-políticos y culturales tuvieran una incidencia en los tipos de contenidos y en los modos de producción privilegiados por las empresas de medios. Al respecto, las próximas etapas de la investigación, que estarán enfocadas en las instancias de producción de noticias y de recepción de la información en las audiencias televisivas, nos permitirán ahondar en las características observadas a partir del análisis de los contenidos y corroborar de qué modo ingresan las nuevas tecnologías de la vigilancia a las rutinas periodísticas.

NOTAS

* IIGG-FSOC-UBA/CONICET, Licenciada en Comunicación, Magíster en Investigación y Doctora en Ciencias Sociales (Universidad de Buenos Aires). Contacto: calzadom@gmail.com.

** FSOC-UBA, Licenciada en Comunicación, doctoranda en Ciencias Sociales (Universidad de Buenos Aires). Contacto: yamilagomez@gmail.com.

*** CIMeCS-IdIHCS (UNLP/CONICET), Licenciada en Comunicación, Magíster en Comunicación Pública y Política y Doctoranda en Ciencias Sociales (Universidad de Buenos Aires). Contacto: vanesa.lio@gmail.com

1. "Fariña esposado y desmejorado", se titula una noticia presentada en América Noticias (6/10/2015) que ejemplifica este proceso. En ella utilizan una imagen de celular del programa Intrusos, donde uno de sus movileros realiza una serie de preguntas a Leonardo Fariña en el pasillo de Tribunales en el momento en que se encuentra declarando en un juicio por calumnias. La información dista de ser novedosa y quien lo reporta es un periodista de espectáculos. Pese a ello, la existencia de la "imagen" promueve por sí misma la novedad ya que no hay datos recientes sobre la causa, únicamente la figura de un personaje mediático en la pantalla televisiva.

2. La noticia "Casi lincha a un motochorro" (Telenueve Central, 5/10/2015) se presenta con imágenes tomadas con un celular, que son la fuente principal que inicia la noticia. Luego el noticiero complementa la información con un móvil desde el lugar del hecho y entrevistas a vecinos, pero las imágenes del momento en que "capturan" al "motochorro" se repiten varias veces y son el elemento central de la noticia.

3. En la noticia "Mandan videomensaje a otra banda" (Telenueve, 6/10/2015) la búsqueda de la primicia se refleja en la presentación de una noticia basada en un video casero subido a las redes sociales por una supuesta banda delictiva. El noticiero construye un modo de revisar mensajes entre supuestas bandas criminales a partir de un video que no posee más datos que los que brinda el audiovisual por sí mismo. De alguna manera es como si el espectador desde las imágenes espiara el accionar de las bandas delictivas. Otro tipo de uso de las redes sociales se puede ver en la noticia "¿Avisan o no avisan?" (Telenoche, 6/10/2015) que informa sobre una supuesta amenaza de masacre de un estudiante en la Facultad de Diseño y Urbanismo de la Universidad de Buenos Aires. El mensaje amenazante es retratado gracias a las imágenes tomadas de capturas de pantallas de las redes sociales y de mensajes leídos por los periodistas también desde Facebook que darían cuenta de la existencia de un sujeto que amenaza con ejecutar una masacre.

REFERENCIAS

Arteaga Botello, N. (2006). Vigilancia y control social de la violencia en México. *Capítulo Criminológico*, *34* (1), 34–54.

Bruno, F., Barreto, P., & Szafir, M. (2012). Artistic Presentation Surveillance Aesthetics in Latin America: Work in Progress. *Surveillance & Society*, *10* (1), 83–89.

Caimari, L. (2004). *Apenas un delincuente. Crimen, castigo y cultura en la Argentina, 1880-1995.* Buenos Aires: Siglo XXI.

Cardoso, B. D. V. (2012). The Paradox of Caught-in-the-act Surveillance Scenes: Dilemmas of Police Video Surveillance in Rio de Janeiro. *Surveillance & Society*, *10* (1), 51–64.

Gates, K. (2013). The cultural labor of surveillance: video forensics, computational objectivity, and the production of visual evidence. *Social Semiotics*, *23* (2), 242–261.

Groombridge, N. (2002). Crime control or crime culture TV? *Surveillance & Society*, *1* (1), 30–46.

Hempel, L. (2006). In the eye of the beholder? Representations of video surveillance in German public television. *Surveillance & Society*, *4* (1/2), 85–100.

Kammerer, D. (2004). Video Surveillance in Hollywood Movies. *Surveillance & Society*, *2* (2/3), 464–473.

Kroener, I. (2013). "Caught on Camera": The media representation of video surveillance in relation to the 2005 London Underground bombings. *Surveillance & Society*, *11* , 121–133.

Leblanc, P. B. (2010). From Closed-circuit Television to the Open Network of Live Cinema. *Surveillance & Society*, *7* (2), 102–114.

Lio, V. (2012). El Municipio Vigila. Un análisis comunicacional de los sistemas de monitoreo del espacio público en manos del Estado. *Question*, *1* (36), 221–233.

Martini, S. y Pereira, M. (2009). *La irrupción del delito en la vida cotidiana. Relatos de la comunicación política*. Buenos Aires: Biblos.

Norris, C., Mccahill, M., & Wood, D. (2004). Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society*, *2* (2/3), 110–135.

Saítta, S. (1998). *Regueros de Tinta. El diario Crítica en la década de 1920.* Buenos Aires: Sudamericana.

Yar, M. (2012) "Crime, media and the will-to- representation: Reconsidering relationships in the new media age". *Crime, media, culture*, 8 (3), 245-260.

ESCENAS DE LA VIDA COTIDIANA. ACTORES, DISCURSOS Y REPRESENTACIONES EN TORNO A LA VIDEOVIGILANCIA PÚBLICA EN UN MUNICIPIO BONAERENSE.

Resumen: Esta ponencia se centra en la videovigilancia gubernamental de espacios públicos en ciudades argentinas, a partir de una indagación acerca del rol que cumplen las cámaras de seguridad en la dinámica local de un municipio bonaerense. Se presentan resultados parciales de un trabajo en curso que se propone describir el entramado existente en relación con estos sistemas de monitoreo del espacio público, a través de la identificación de los actores y del seguimiento de las interacciones que se dan entre ellos. A partir de una serie de entrevistas en profundidad realizadas a actores vinculados de modos diversos con el funcionamiento de la videovigilancia en un municipio de la Provincia de Buenos Aires, se analizan y problematizan discursos políticos, empresarios, mediáticos y ciudadanos. En los últimos años la tecnología se fue incorporando cada vez con mayor cotidianidad a la vida en las ciudades y la colocación de cámaras de vigilancia en el espacio público es un ejemplo de este proceso, que comenzó en Argentina en 2008 y se expandió velozmente a partir de la implementación del Plan de Seguridad Ciudadana del gobierno nacional en 2009. En este escenario, los discursos en circulación ponen de manifiesto el valor simbólico de estos dispositivos técnicos en la búsqueda de disminución del sentimiento de inseguridad. Las cámaras modifican los modos de interacción en el espacio público, al tiempo que las imágenes han ganado espacio en los medios de comunicación en una búsqueda por suplir la falta de evidencia empírica sobre su efectividad en la reducción del delito.

Palabras clave: Cámaras de seguridad, Noticia policial, Medios, Televisión.

VANESA LIO*

Cenas da vida cotidiana. Atores, discursos e representações sobre videovigilância pública em um município na província de Buenos Aires.

Resumo: Este artigo centra-se na vigilância do governo dos espaços públicos nas cidades da Argentina, a partir de um inquérito sobre o papel desempenhado pelas câmeras de segurança nas dinâmicas locais de um município na província de Buenos Aires. São apresentados resultados parciais de um trabalho em andamento que visa descrever o quadro existente em relação a estes sistemas de monitoramento do espaço público, através da identificação de atores e acompanhamento das interações que ocorrem entre eles. A partir de uma série de entrevistas em profundidade com atuantes ligados, de várias maneiras, à operação de vigilância de vídeo em um município na província de Buenos Aires, analisa-se discursos políticos, empresários da mídia e cidadãos. Nos últimos anos, a tecnologia foi incorporada cada vez mais na vida em grandes cidades e a colocação de câmeras de vigilância no espaço público é um exemplo deste processo que começou na Argentina em 2008 e rapidamente se expandiu a partir da implementação do Plano de Segurança Pública do governo nacional em 2009. Neste cenário, discursos em circulação realçaram o valor simbólico desses dispositivos técnicos em busca da diminuição da sensação de insegurança. As câmeras alteram os modos de interação no espaço público enquanto as imagens ganham espaço na mídia em uma missão para suprir a falta de evidências sobre sua eficácia na redução da criminalidade.

Palavras-chave: Câmeras de segurança, Espaço público, Atores, Imagens.

Scenes of everyday life. Actors, discourses and representations about public video surveillance in a Buenos Aires municipality.

Abstract: From an inquiry into the role played by video cameras in the local dynamics of a Buenos Aires municipality, this paper focuses on government surveillance of public spaces in Argentinean cities. We present partial results of an ongoing work aimed at describing the existing framework of monitoring systems of public space through the identification of the actors and their interactions. From a series of in-depth interviews with the actors involved, we analyzed politicians, businessmen, media and public speeches linked with the video surveillance system working in a municipality in the Province of Buenos Aires. In recent years this technology was increasingly incorporated to everyday life, for example by the use of surveillance cameras in public spaces. In Argentina this process began in 2008 and quickly expanded from the implementation of a national public politic on security in 2009. In this scenario, outstanding speeches highlight the symbolic value of these technical devices in the search of decreasing the fear of crime. The cameras have changed the ways of interaction in the public space, while images have gained space in the media which looks forward to supplement the lack of empirical evidence on their effectiveness in reducing crime.

Key-words: Videocameras, Public space, Actors, Images.

INTRODUCCIÓN

En los últimos años la tecnología se fue incorporando cada vez con mayor cotidianidad a la vida en las ciudades. La colocación de cámaras de vigilancia en el espacio público es ejemplo de este proceso, que comenzó en Argentina en 2008 y se expandió velozmente a partir de la implementación del Plan de Seguridad Ciudadana del gobierno nacional en 2009, en el marco de consolidación de la inseguridad como uno de los principales problemas públicos (Kessler, 2009) y del ascenso de las políticas de prevención situacional del delito (Sozzo, 2009). Así, la instalación de circuitos cerrados de televisión (CCTV) para vigilancia, históricamente restringida al ámbito privado, se desplazó hacia al sector público.

Ante este escenario, discursos académicos, políticos y ciudadanos sobre estas tecnologías comienzan a circular con mayor frecuencia en la esfera pública. En los estudios que vinculan ciencia, tecnología y sociedad, la puesta en marcha de estos nuevos modos de vigilancia contribuyó a la emergencia de un campo específico de investigación, que en el mundo anglosajón se manifestó

a partir de diversos enfoques teóricos y metodológicos que confluyen en los "surveillance studies" (Lyon, 2002; Ball y Haggerty, 2005). En América Latina, un interés similar por estos temas de investigación comenzó a surgir en los últimos años (Arteaga Botello, 2012).

Estos debates en el plano internacional dan cuenta de una serie de dimensiones estudiadas de la videovigilancia, que se expresan en distintos interrogantes que guían estos trabajos de investigación: lo normativo y su relación con la violación de otros derechos, como la privacidad y la protección de datos personales; lo evaluativo, en vinculación a la medición de la eficacia y eficiencia; lo simbólico, a partir de la circulación de sentidos en torno a la videovigilancia; lo espacial, a partir de la percepción y productividad en las tramas urbanas; y el funcionamiento de los centros de monitoreo, con una mirada etnográfica que se enfoca en la tarea de vigilancia (Lio y Urtasun, 2016).

Algunas de estas discusiones académicas se vinculan estrechamente con preguntas que surgen en la esfera pública acerca de la utilización de las cámaras de seguridad para monitoreo de los espacios urbanos. ¿Existe un conflicto de intereses entre las demandas de seguridad que abogan por la utilización de estas tecnologías y las luchas en defensa de la privacidad? ¿Hay una preocupación por esta dimensión que se exprese en los discursos públicos? ¿Son los sistemas de videovigilancia defendidos o detractados? ¿Son considerados mayormente eficaces o ineficaces? Y, en todo caso, ¿en qué reside su eficacia? ¿Sus efectos deseados apuntan a la reducción del delito o se apoyan en su valor simbólico para disminuir la sensación de inseguridad y el temor al crimen? En este último caso, ¿cómo repercuten los discursos y las imágenes que circulan a través de los medios de comunicación? Por último, ¿cómo inciden la presencia de las cámaras y los discursos que circulan en torno a ellas en los modos en que los actores se representan el espacio urbano y la forma en que piensan su relación con la ciudad y el barrio?[1].

Si bien el presente trabajo no pretende de ningún modo responder a todos estas preguntas, estos interrogantes funcionan como disparadores para empezar a explorar los modos en que los distintos actores se posicionan respecto de la videovigilancia del espacio público, qué funciones le atribuyen a las cámaras de seguridad y en qué medida modifican sus percepciones y representaciones sobre la ciudad y el delito[2].

Para esto, se trabaja en el nivel discursivo a partir de una serie de entrevistas en profundidad realizadas a actores vinculados de modos diversos con el funcionamiento de la videovigilancia en el municipio de Tigre (Provincia de Buenos Aires). Se analizan y problematizan discursos en circulación, buscando dar cuenta de las representaciones que atraviesan la justificación o rechazo de la utilización de las cámaras de seguridad para el monitoreo urbano. Entre los entrevistados del ámbito político local se incluyó a los responsables en materia de seguridad y monitoreo público del gobierno local, así como a concejales oficialistas y de oposición. Respecto del sector empresario, se entrevistaron referentes de compañías proveedoras del servicio, como también de la cámara empresaria que nuclea a las compañías del sector. Para obtener representación de organizaciones del tercer sector, se entrevistaron miembros de organizaciones no gubernamentales

o asociaciones civiles que hayan tenido una intervención pública en relación a la cuestión en estudio. Finalmente, se realizaron entrevistas a residentes del partido de Tigre, a fin de incorporar los posicionamientos ciudadanos acerca de la utilización de estas técnicas de monitoreo urbano, con diversidad en cuanto a edad (tomando población adulta de entre 18 y 70 años) y sexo. Se seleccionaron tres zonas con características socioeconómicas bien diferenciadas, tomando como premisa que sean lugares alcanzados por el sistema de monitoreo municipal. Las entrevistas se orientaron a identificar los principales posicionamientos y debates surgidos en torno a esta temática. Para ello, se utilizó un guión flexible que se adecuó a cada uno de los grupos de actores pero que se organizó en torno a dimensiones comunes: formas de conceptualizar esta tecnología, funciones atribuidas a los dispositivos, relación con el espacio a partir de la presencia de las cámaras, opinión sobre la videovigilancia (incluyendo cuestiones como la utilidad de las cámaras, los costos y la eficiencia de los sistemas, la privacidad y los derechos en juego), conocimiento de las políticas públicas y la legislación específica.

Partimos de la hipótesis de que los roles específicos de los actores implican diversos modos de entender las tecnologías y, por lo tanto, difieren también las funciones que se atribuye a la videovigilancia del espacio público, las formas de justificarla o detractarla. Al mismo tiempo, la presencia de las cámaras de seguridad modifica los modos en que los actores describen los espacios urbanos como seguros o inseguros: mientras que previo al uso de los cctv, todo el espacio era definido como "seguro" y algunos lugares bien delimitados se consideraban "inseguros" de acuerdo a ciertas condiciones particulares; actualmente, la visión de un peligro cuya característica es la ubicuidad y la aleatoriedad (Kessler, 2011) conduce a una definición del todo como "inseguro", siendo algunos lugares definidos como "seguros" a partir de control que se opera sobre ellos.

VIDEOVIGILANCIA Y GOBIERNO LOCAL

La extensión de estos sistemas de videovigilancia en la Provincia de Buenos Aires ha encontrado su mayor impulso a partir de la creación y puesta en marcha en abril de 2009 del Programa Integral de Protección Ciudadana (PIPC), surgido de un convenio de cooperación firmado por la Jefatura de Gabinete de Ministros de la Nación y el Ministerio de Justicia y Seguridad de la Provincia de Buenos Aires. A partir de la suscripción de convenios de adhesión con los gobiernos locales, el programa consistió en la asignación de recursos nacionales no reintegrables a diversos municipios bonaerenses destinados a incorporar tecnología en materia de seguridad, dotar de mayor capacidad operativa a las fuerzas policiales, incentivar la participación ciudadana y conformar redes para la prevención de delitos[3].

Ahora bien, el municipio de Tigre fue pionero en la implementación de la videovigilancia del espacio público en Argentina y su sistema de monitoreo fue incluso previo al lanzamiento del PIPC. El programa municipal denominado "Sistema de monitoreo por GPS y cámaras de control de tránsito" fue inaugurado a principios de 2008, producto de un convenio de colaboración con

la Universidad Tecnológica Nacional, Facultad Regional General Pacheco (UTN-FRGP), destinado al apoyo tecnológico y técnico, que fue convalidado por el decreto municipal 2399/07 y por la ordenanza 2865/08. Sin embargo, la vinculación con el PIPC se evidencia en la figura de su precursor. A pocos días de haber asumido su primer mandato como Intendente del municipio de Tigre (por entonces, como referente local del Frente para la Victoria), Sergio Massa firmó el convenio con la UTN-FRGP el 26 de diciembre de 2007, dando el puntapié inicial de lo que se convertiría en su "caballito de batalla" en las intervenciones en materia de seguridad: la utilización de las tecnologías para la prevención, con especial énfasis en las cámaras de seguridad. Algunos meses más tarde, habiendo tomando una licencia en su cargo de Intendente entre julio de 2008 y julio de 2009 para desempeñarse como Jefe de Gabinete de Ministros de la entonces presidenta Cristina Fernández de Kirchner, fue el mismo Massa quien tuvo a su cargo el diseño y la ejecución del PIPC. Esto fue incluso interpretado en las lecturas mediáticas como un intento por replicar en otros distritos bonaerenses la fórmula por él implementada en Tigre (Galvani, Ríos y Cañaveral, 2015). Esta modalidad de la "exportación del modelo"[4] en seguridad es recurrente en los discursos de los funcionarios municipales y en las propias comunicaciones institucionales del gobierno local, que dan difusión a recorridas de intendentes y secretarios de seguridad de otras localidades por el Centro de Operaciones Tigre (COT) y a visitas de los referentes de Tigre a otras ciudades y provincias del país.

Tigre es un municipio de 360 km^2 y algo más de 376 mil habitantes[5], ubicado en la región norte del conurbano bonaerense. Es una de las ciudades más monitoreadas del país, y también de las más fragmentadas. El 60 por ciento de su territorio está ocupado por countries, barrios cerrados y complejos urbanos de altos ingresos en los que sólo vive el 10 por ciento de la población. Por otro lado, aunque más del 90 por ciento de las viviendas cuenta con buenas condiciones de habitabilidad, un 47 por ciento de los hogares no tiene gas y el 83 por ciento no cuenta con cloacas (Zuazo, 2015).

Desde 2007, el municipio es gobernado por el partido liderado por Sergio Massa (hasta las elecciones de 2011, el Frente Todos por Tigre, versión local del FPV; desde 2013, el Frente Renovador, que consolidó su fuerza como partido de oposición al gobierno nacional en los últimos años y fue la tercera fuerza en las elecciones presidenciales de 2015). Si bien hoy el gobierno es conducido por Julio Zamora, Massa continúa siendo el referente a nivel local, lo cual se refleja tanto en los discursos mediáticos como en las entrevistas realizadas a políticos, funcionarios y residentes locales. Desde 2009, la conformación del Honorable Concejo Deliberante (HCD) es favorable a la gestión de gobierno y hoy cuenta con una mayoría oficialista con 15 de 24 concejales del Frente Renovador.

El sistema integral que hoy el municipio denomina "Alerta Tigre" se financia con el 50 por ciento de los fondos recaudados mensualmente en concepto de una contribución al sistema de "protección ciudadana" que se incluye en la tasa municipal. En este sistema confluyen las fuerzas de seguridad locales y los móviles municipales del COT, el Sistema de Emergencias Tigre (SET), bomberos, defensa civil, un área de tránsito inteligente y una central meteorológica. Dependiente de la

Secretaría de Protección Ciudadana municipal, presenta como su principal objetivo "fortalecer la prevención de delitos, accidentes de tránsito y siniestros en general". Cuenta, de acuerdo a información provista por el propio municipio, con 1.500 cámaras, monitoreadas las 24 horas por 300 operadores civiles, y 42 móviles propios, conducidos por un policía retirado y uno en actividad, cuyo objetivo es "reforzar los patrullajes" de la policía. Además, los colectivos de líneas locales cuentan con GPS y botones anti-pánico. Estos dispositivos de emergencia fueron también instalados en jardines de infantes y escuelas del municipio, y el municipio distribuye dispositivos de alerta especiales para las mujeres víctimas de la violencia de género. El plan fue redefinido Alerta Tigre 2.0 a partir de la incorporación del uso de nuevas tecnologías y redes sociales. Por un lado, se incluye a los comercios a través de los dispositivos utilizados para compras con tarjeta de débito y crédito, que se utilizan como botones de pánico. Por otro, posibilita a los vecinos contactarse de manera directa con el COT a través de un teléfono celular o una computadora, pudiéndose realizar denuncias vía mensaje de texto, online, por sistema WAP desde celulares y mediante las redes sociales Twitter y Facebook.

Por último, Tigre cuenta con una red de líderes barriales que se vinculan directamente al COT y un acuerdo con la cámara del sector que le permitió integrar los 400 puntos fijos del sistema de vigilancia privado, haciendo confluir todas las imágenes en el mismo centro de monitoreo. Todos estos elementos han convertido a Tigre en el municipio más vigilado del país y en pionero en la aplicación de tecnologías para la seguridad.

ACTORES, DISCURSOS Y ENTRAMADOS

La extensión de la videovigilancia en el espacio público pareciera conducir, en principio, a una disputa de intereses en los derechos a la seguridad y a la privacidad. De acuerdo con Edwards (2005), "las víctimas potenciales (…) prefieren sacrificar un grado de su privacidad personal por un grado de protección personal" (93). En el contexto argentino, las imágenes de las cámaras de seguridad están alcanzadas por la protección constitucional del artículo 19 que refiere a los derechos a la privacidad e intimidad, en tanto su texto menciona no sólo la esfera doméstica y familiar sino otros "aspectos de la personalidad espiritual y física de las personas tales como la integridad corporal o la imagen". Por otro lado, de acuerdo con la definición de la Dirección Nacional de Datos Personales (DNPDP), las imágenes de la videovigilancia constituyen datos personales dado que el material fotográfico o fílmico permite identificar o hacer identificable a una persona. Así se señala tanto desde trabajos académicos (Cejas y González, 2015; Parrili, 2011) como desde posturas críticas de organizaciones no gubernamentales y asociaciones civiles (como la Fundación Vía Libre, el Centro de Estudios Legales y Sociales o la Asociación por los Derechos Civiles), que cuestionan que no está claro qué información se recopila, qué pasa con ella, cómo se procesa y quién tiene acceso (Cejas y González, 2015).

Algunos de estos aspectos están regulados por normativas con distintos alcances institucionales y geográficos. La disposición 10/2015 de la DNPDP establece una serie de principios que deben

aplicarse a la videovigilancia en el territorio argentino y que otorgan o no el carácter de licitud a los sistemas: consentimiento, respeto de la finalidad, calidad del dato, seguridad y confidencialidad, ejercicio de los derechos del titular del dato, inscripción y manual de tratamiento de datos[6].

En el ámbito de la Provincia de Buenos Aires, el marco regulatorio está establecido por los convenios que, como mencionamos, forman parte del PIPC. Dos normas de alcance provincial refieren a la temática[7] pero no hay legislación que regule la utilización y el funcionamiento de los sistemas de videovigilancia públicos. En el contexto local del municipio que estudiamos, las ordenanzas municipales convalidan las decisiones tomadas por el Poder Ejecutivo, para el establecimiento inicial del sistema y para modificaciones sucesivas relativas al alcance, el financiamiento y las tecnologías utilizadas.

La cuestión normativa aparece también como una preocupación del sector empresario, que aboga por reglamentaciones de estos sistemas no desde la perspectiva de la defensa de los derechos civiles sino en relación al funcionamiento técnico, las habilitaciones para ingresar al negocio y las características del personal. La visión orientada al mercado y que busca asegurar ciertas condiciones que beneficien sus propias posibilidades de negocio es matizada por el discurso del avance tecnológico constante que les permite colocarse en el papel de "expertos", a quienes los sectores políticos deben acudir para "evitar y corregir las distorsiones" generadas por la multiplicidad de regímenes locales. Se establece así una vinculación con ciertos sectores del ámbito político, principalmente funcionarios municipales pero también representantes de poder legislativo, a quienes los empresarios acusan de "no comprender adecuadamente el sector" o no contar con "los conocimientos técnicos específicos", que los conducen a proponer normas que luego son "inviables" en la práctica.

Ahora bien, nos preguntamos si la cuestión relativa a la regulación de la videovigilancia y este conflicto con los derechos a la privacidad y la intimidad aparece como un problema en los discursos de los ciudadanos. Por un lado, si bien en los primeros años posteriores a la implementación de los sistemas de videovigilancia en Argentina, algunas voces alimentaron desde los medios un debate relativo al uso de cámaras de seguridad en el espacio público, desde perspectivas críticas que las asociaban a la idea del panóptico de Bentham (Foucault, 2002) o al Gran Hermano de George Orwell, este tipo de enfoques fueron disminuyendo con el pasar de los años. Por otro lado, en los diálogos con los habitantes de nuestro municipio en estudio, se evidencia en principio un desconocimiento de los marcos regulatorios de este tipo de sistemas. Al preguntar específicamente por la relación con la privacidad, aparece cierta coincidencia respecto de la definición de "lo público" como ámbito donde todos los actos privados se convierten en algo público y, por ende, no existiría conflicto aparente con la observación operada por terceros. Este tipo de discurso se complementa con un argumento referido a la responsabilidad y publicidad de las acciones propias. En este sentido, "quien no tiene nada que ocultar no tiene motivo para preocuparse por la mirada ajena".

Mientras algunos actores consideran estas perspectivas críticas como "marginales", otros sugieren

que se trata de "un debate saldado". Argumentos de este tipo aparecen repetidamente entre los discursos de los empresarios y de los políticos. En el ámbito legislativo, los debates y conflictos surgidos en torno a la colocación o no de las cámaras de seguridad se narran como una instancia del pasado. Esto no implica, sin embargo, que no existan posturas que cuestionen el uso estos dispositivos para la prevención del delito. Ahora bien, las críticas al sistema de monitoreo no se fundan en la potencial amenaza que pueden representar para la privacidad, sino en fallas de su funcionamiento. Concejales de los partidos opositores a la gestión municipal y ciudadanos no del todo de acuerdo con los lineamientos definidos por el actual Intendente ponen en duda que "el sistema funcione como se quiere hacer creer". Es decir, las críticas se fundan en que "muchas cámaras están dañadas y no graban", en la existencia de áreas del partido que se encuentran "desprotegidas" y en el "accionar negligente" de los empleados municipales que se mueven en los móviles del COT. En este sentido, las críticas van dirigidas más al funcionamiento práctico de estos sistemas que a un cuestionamiento de la decisión política de su utilización. Un concejal opositor expresó sintéticamente: "No todo lo que brilla es oro. Es más para la galería, para la vidriera que realmente pare la seguridad interna". Paradójicamente, la cuestión de "la vidriera" es también un aspecto central para propia gestión municipal en relación con la videovigilancia, tema que retomaremos en breve.

Por su parte, los vecinos del municipio han instaurado a partir de sus prácticas una modalidad de intervención en relación a los sistemas de videovigilancia. Por medio del HCD presentan pedidos específicos para la colocación de cámaras de seguridad en un lugar definido del municipio, fundados en el "aumento de los hechos delictivos" en su barrio, en la "falta de control policial y de iluminación". En relación con esto, otro legislador de la oposición narró: "No hay pedidos para que saquen cámaras, los vecinos no se quejan por las cámaras. Son todos pedidos para que pongan cámaras o pedidos de mayor control policial, pero las cámaras tienen que funcionar". Estos pedidos ingresan al HCD y son girados a la comisión de Seguridad, que discute cada caso y decide si someterlo o no al tratamiento en el plenario. En ese ámbito, los pedidos pueden convertirse en una ordenanza o recomendación del HCD al ejecutivo municipal.

La pregunta que sigue es ¿por qué los vecinos piden cámaras de seguridad? Surge así la dimensión de la efectividad de la videovigilancia que nos conduce incluso hasta la definición de estos sistemas de monitoreo. En el caso argentino, la falta de un diagnóstico previo de las características del problema delictivo que se pretende enfrentar con el uso de cámaras de seguridad y la inexistencia de una evaluación pertinente de su funcionamiento ha conducido a definir a la videovigilancia como una medida de cuasi-prevención situacional-ambiental (Sozzo, 2014). Se asume una pretensión de generalidad, que equivale a vigilar toda la ciudad, en lugar de plantear su colocación para el tratamiento de delitos puntuales en ambientes o situaciones particulares. La falta de diagnóstico y evaluación redunda en la falta de estadísticas y datos empíricos que justifiquen su utilización y puedan mostrar su efectividad en la reducción del delito. Mientras estudios evaluativos en el ámbito internacional han demostrado el débil impacto de los CCTV en el comportamiento de las tasas delictivas (Welsh y Farrington, 2009; Hempel y Töpfer, 2004;

Sperber, Seck y Johnson, 2013; Armitage, 2002; Medina Ariza, 2010; Waples, Gill y Fisher, 2009, entre otros), en Argentina este tipo de análisis son directamente inexistentes.

El vínculo entre el masivo crecimiento de la videovigilancia y su efectividad se redefine, entonces, a partir de su valor simbólico. Los sistemas de monitoreo muestran una productividad en tanto mensaje político: la gestión necesita mostrarse activa ante la cuestión del delito y el Estado se posiciona como dador de una marco de protección a los ciudadanos a partir de este tipo de políticas (Norris, Mc Cahill y Wood, 2004). La decisión de instalar cámaras de seguridad no se funda en un diagnóstico previo pasado en los índices delictivos, sino que resulta de la convergencia de intereses expresados por actores políticos y económicos (Frois, 2011).

Ante la falta de estadísticas que justifiquen su utilización, los políticos utilizan los casos exitosos para mostrar la efectividad de estos dispositivos en la reducción del delito. En el caso de Tigre, la identificación de la gestión local y del referente Sergio Massa con las cámaras de seguridad no es casual. Quienes conducen su equipo de prensa definen que necesitan "comunicar seguridad". Para mostrarlo, especifican: "Desde hace siete años, tengo que lograr que dos veces por semana 'las cámaras de seguridad de Tigre' salgan en los medios" (Zuazo, 2015). El objetivo de ubicar a las cámaras como protagonistas permitió construir un discurso en torno a estos dispositivos de seguridad que, atravesado por determinismo en torno a las tecnologías, inviste a la videovigilancia de un poder total: "Las cámaras atrapan delincuentes" y "las cámaras logran justicia", se fundamenta desde la propia gestión. Las cámaras, en síntesis, permiten reducir el sentimiento de inseguridad.

Los medios de comunicación emergen, en este sentido, como un actor fundamental e inevitable de estos procesos. "Dar las imágenes a los medios" es parte de una estrategia de la propia gestión, para nada casual ni improvisada (Lio, 2012). El objetivo –y la condición para ceder las imágenes– es que se "muestre la efectividad de las cámaras" a partir de hechos concretos en los que "se previenen delitos o se agarran delincuentes".

Este modo de mostrar los resultados y construir la eficacia de la videovigilancia introduce, de acuerdo con Cardoso (2012), una "paradoja" detrás de los "hechos captados en el acto" por las cámaras. El reemplazo de los modos estadísticos de objetivar los resultados por la construcción de una legitimidad que se sustenta en la reproducción de imágenes que muestren su actuación ejemplar conduce a la necesidad de producir constantemente ese tipo de ejemplos visibles de para qué sirven las cámaras. Ahora bien, si la efectividad atribuida a las cámaras para disuadir la violencia y el delito reduce también la cantidad de hechos a ser "captados en el acto", la cuestión de qué mostrar para justificar la presencia de las cámaras y capitalizar el rédito político aparece como un problema estructural de su exposición mediática.

Más allá de esta cuestión central para los gobiernos, lo cierto es que la relación se funda en una mutua conveniencia. Los medios acceden a materiales únicos que les permiten construir noticias impactantes, dramáticamente visualizadas a través del uso de las imágenes grabadas por el CCTV (Norris, Maccahill y Wood, 2004), desde una estética de la objetividad que pretende presentar

los hechos como "reales" (Gates, 2013). Los gobiernos, por su parte, saben que la televisión juega un rol decisivo en la aceptación pública y en la implementación de estas tecnologías de vigilancia (Hempel, 2006).

La naturaleza retórica de los discursos y prácticas en torno a la implementación de la video vigilancia subsume a un segundo plano el debate público acerca de sus consecuencias. Como resultado, la percepción que la gente tiene de las ventajas y la eficacia de la videovigilancia está basado en un "meta-discurso", más que en una conciencia directa de los efectos que estas tecnologías pueden tener sobre la propia seguridad (Frois, 2011). Así, la discusión del uso actual del CCTV está sujeta a su presentación mediática y el material visual de las cámaras aparece como una prueba de su eficiencia (Hempel, 2006).

En los discursos ciudadanos de nuestro municipio de estudio es recurrente la mención a los "casos mediáticos" que justifican, de algún modo, la posición a favor de la videovigilancia del espacio público y que fundan las demandas por la colocación de más cámaras de seguridad que mencionamos anteriormente. El sentimiento de mayor protección y seguridad que habilitan los dispositivos está dado por la sensación de control permanente sobre ciertos espacios urbanos. Esto genera una modificación en ciertas dinámicas cotidianas, como elegir los recorridos en función del conocimiento del lugar donde están estos dispositivos o esperar el colectivo en la parada que está monitoreada. En este sentido, la presencia de las cámaras repercute en los modos en que los actores se representan el espacio urbano y la forma en que vivencian su propio barrio. Y, al mismo tiempo, como plantea Zurawski (2007), el apoyo o no al uso de la videovigilancia se vincula a la experiencia espacial, que es construida a partir del cruce entre el sentimiento de inseguridad, el conocimiento del espacio y su cercanía afectiva.

PALABRAS FINALES

En relación con la gestión pública de la seguridad, la contribución o no de estos dispositivos a la disminución del temor percibido se presenta como un interrogante central. Señala Bruno Latour (1992) que los objetos desempeñan una función central para estabilizar relaciones sociales por definición fluctuantes. Ciertos dispositivos, como las cámaras de seguridad, permiten delegar en un tercero, ya sea un objeto o una persona, parte de la gestión de la inseguridad. Ahora bien, estos elementos pueden tanto contribuir a lograr una mayor sensación de seguridad como incrementar el temor al recordar en forma constante la existencia de peligros (Kessler, 2011).

En este trabajo, partimos de la identificación de una serie de actores que intervienen en el debate público respecto de la videovigilancia y en las prácticas relativas a su implementación en el ámbito local de un municipio de la Provincia de Buenos Aires. Así, los cruces discursivos y las vinculaciones entre políticos (concejales y funcionarios), empresarios (proveedores del servicio y cámaras del sector), asociaciones civiles, vecinos del municipio y medios de comunicación empiezan a delinear un entramado que da cuenta de la complejidad del fenómeno.

Por un lado, se observó que las intervenciones de los actores y las relaciones puestas en juego entre ellos ponen de manifiesto el valor simbólico de estos dispositivos técnicos en la disminución del sentimiento de inseguridad. El discurso político oficial se sostiene en la necesidad de introducir constantemente nuevas herramientas tecnológicas en la gestión de la seguridad y, especialmente, aumentar el número de cámaras: "Cuantos más ojos vigilando tengamos, más seguros estaremos". Los ciudadanos, por su parte, instituyen una serie de dinámicas para solicitar la colocación de estos dispositivos en sus barrios.

En un municipio donde la vigilancia del espacio público creció de manera exponencial en poco tiempo y donde las cámaras de seguridad se convirtieron, en términos discursivos, en casi un sinónimo de la gestión actual, la videovigilancia fue transformando algunas formas de interacción y circulación por el espacio público. Esta expansión del monitoreo urbano no se debió a una evidencia empírica de su efectividad en la prevención del delito, sino que una nueva "eficacia mediática" aparece como la base argumental de los discursos que defienden su uso.

Si, por un lado, el avance de los sistemas de videovigilancia en áreas públicas se justifica en que es una respuesta política diseñada para dar una solución rápida un fenómeno subjetivo (Frois, 2011), en la construcción de las imágenes de las cámaras de seguridad como producto mediático se juega un elemento nodal de la demostración de su "éxito".

Así, la pregunta por los problemas que representa para la privacidad y la intimidad, que nos ocupa en la tarea investigativa, pareciera estar siendo desplazada paulatinamente de los debates públicos, y la "medición" de la efectividad se redefine a partir de nuevos parámetros. En los discursos analizados para este trabajo, se observó que la eficacia de estos sistemas no se vincula a la reducción del delito en términos estadísticos si no a la posibilidad de mostrar (o construir) mediáticamente para qué sirven las cámaras. La inversión de los gobiernos locales se justifica, de este modo, en el rédito político que obtienen a partir de mostrarse activos frente a la cuestión de la inseguridad.

NOTAS

* Becaria doctoral del Consejo Nacional de Investigaciones Científicas y Técnicas en CIMeCS-IdIHCS (UNLP /CONICET). Licenciada en Ciencias de la Comunicación, Magíster en Comunicación Pública y Política, Doctoranda en Ciencias Sociales (Universidad de Buenos Aires). Contacto: vanesa.lio@gmail.com

1. Respecto de la última dimensión de análisis de la videovigilancia, referida a lo cotidiano del funcionamiento de la tarea de monitoreo, podrían plantearse otras preguntas acerca, por ejemplo, de cómo se describe a los vigiladores en el imaginario social, qué se conoce de ellos, quiénes son y qué lugar se atribuye a su trabajo. Sin embargo, decidimos dejar de lado esta serie de preguntas ya que no se vinculan con los hallazgos que esta ponencia presenta.

2. La ponencia es parte de un trabajo más amplio que realizo en el marco de mi tesis de doctorado. A partir del supuesto inicial de que la videovigilancia se constituye como una controversia (Latour, 2008; Venturini,

2009), el objetivo es describir el entramado existente en relación con estos sistemas de monitoreo del espacio público, identificando a los actores y siguiendo sus interacciones, utilizando como marco la Teoría del Actor-Red (Latour, 2008; Callon, 1998).

3. Para más información sobre el Programa Integral de Protección Ciudadana, véase Galvani, Ríos y Cañaveral (2015).

4. Se utilizan comillas para referir a frases o términos que fueron empleados por los entrevistados.

5. De acuerdo a los datos del Censo 2010 del Instituto Nacional de Estadísticas y Censos.

6. Para más detalles sobre los principios, consultar la disposición 10/2015 de la DNPDP, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243335/norma.htm.

7. La ley 14.050 establece la instalación de obligatoria de cámaras de video en la salida de los boliches bailables y la 14.172 introduce al Código Procesal Penal de la Provincia de Buenos Aires un capítulo destinado a las filmaciones y grabaciones que posibilita que los videos de las cámaras de seguridad sean utilizados como prueba en los procesos judiciales.

REFERENCIAS

Armitage, R. (2002). To CCTV of Not to CCTV: a review of current research into the effectiveness of CCTV systems in reducing crime. *Nacro. Comunity Safety Practice Briefing*, 1–8.

Arteaga Botello, N. (2012). Surveillance Studies: An Agenda for Latin America. *Surveillance & Society*, *10* (1), 5–17.

Ball, K., y Haggerty, K. D. (2005). Editorial: Doing Surveillance Studies. *Surveillance & Society*, *3* (2/3), 129–138.

Callon, M. (1998). El proceso de construcción de la sociedad . El estudio de la tecnología como herramienta para el análisis sociológico. In M. Domènech & F. Tirado (Eds.), *Sociología simétrica. Ensayos sobre ciencia, tecnología y sociedad.* Barcelona: Gedisa.

Cardoso, B. D. V. (2012). The Paradox of Caught-in-the-act Surveillance Scenes: Dilemmas of Police Video Surveillance in Rio de Janeiro. *Surveillance & Society*, *10* (1), 51–64.

Cejas, E. y González, C. C. (2015). Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales. In *15° Simposio Argentino de Informática y Derecho* (pp. 174–184). Ciudad Autónoma de Buenos Aires.

Edwards, L. (2005). Switching off the surveillance society? Legal regulation of CCTV in the United Kingdom. In S. Nouwt, B. R. de Vries, & C. Pries (Eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (pp. 91–114). La Haya: TMC Asser Press.

Foucault, M. (2002). *Vigilar y castigar. Nacimiento de la prision.* (1ª ed.). Buenos Aires: Siglo XXI Editores.

Frois, C. (2011). Video SurVeillance in Portugal: Political Rhetoric at the Center of a Technological Project. *Social Analysis*, *55* (3), 35–53.

Galvani, M., Rios, A., y Cañaveral, L. (2015). *Seguridad, policía y gobiernos locales: el Programa Integral de Protección Ciudadana*. Ciudad Autónoma de Buenos Aires: CLACSO.

Gates, K. (2013). The cultural labor of surveillance: video forensics, computational objectivity, and the production of visual evidence. *Social Semiotics*, *23* (2), 242–261.

Hempel, L. (2006). In the eye of the beholder? Representations of video surveillance in German public television. *Surveillance & Society*, *4* (1/2), 85–100.

Hempel, L., y Töpfer, E. (2004). *CCTV in Europe. Final report* (No. 15). Berlin, Alemania.

Kessler, G. (2009). *El sentimiento de inseguridad. Sociología del temor al delito.* Buenos Aires: Paidós.

Kessler, G. (2011). La extensión del setimiento de inseguridad en América Latina: Relatos, acciones y políticas en el caso argentino. *Revista de Sociologia E Politica*, *19* (40), 83–97.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. Bijker & J. Law (Eds.), *Shaping Technology* (pp. 225–258). Cambridge: MIT Press.

Latour, B. (2008). *Reensamblar lo social. Una introduccion a la teoria del actor-red.* Buenos Aires: Manantial.

Lio, V. (2012). El Municipio Vigila. Un análisis comunicacional de los sistemas de monitoreo del espacio público en manos del Estado. *Question*, *1* (36), 221–233.

Lio, V. y Urtasun, M. (2016). Devolviendo la mirada. Interrogantes y claves de lectura para la investigación de la videovigilancia. *Delito y Sociedad*, 41, en prensa.

Lyon, D. (2002). Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society*, *1* (1), 1–7.

Medina Ariza, J. (2010). Políticas de seguridad ciudadana en el contexto urbano y prevención comunitaria. La experiencia anglosajona. *Revista Electrónica de Ciencia penal y Criminología*, 12 (2).

Norris, C., Mccahill, M., y Wood, D. (2004). Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society*, *2* (2/3), 110–135.

Parrilli, R. (2011). *Los sistemas de video vigilancia, el derecho a la privacidad, la imagen y la protección de datos personales*. Buenos Aires: La Ley.

Sozzo, M. (2009). Gobierno local y prevención del delito en la Argentina. *Urvio, Revista Latinoamericana de Seguridad Ciudadana*, (6), 58–73.

Sozzo, M. (2014). Delito común, inseguridad y respuestas estatales: Inercia e innovacion durante la década kirchnerista a nivel nacional en Argentina. *Cuestiones de Sociologia*, (10).

Sperber, S., Seck, M., y Johnston, E. (2013). *Surveille Deliverable 2.3: Paper by local authorities end-users* (Vol. 6).

Venturini, T. (2009). Diving in magma: how to explore controversies with actor-network theory. *Public Understanding of Science*, *19* (3), 258–273.

Waples, S., Gill, M. y Fisher, P. (2009). Does CCTV displace crime?. *Criminology & Criminal Justice*, 9 (2), 207-224.

Welsh, B. y Farrington, D. (2009). Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis. *Justice Quarterly*, 26 (4), 716-745.

Zuazo, N. (2015), *Guerras de Internet*. Ciudad Autónoma de Buenos Aires: Debate.

Zurawski, N. (2007). Video Surveillance and Everyday Life. Assessments of Closed-Circuit Television and the Cartography of Socio-Spatial Imaginations. *International Criminal Justice Review,* 17 (4), 269-288.

EJE 3

IDENTIFICACIÓN Y BIOMETRÍA

A RICOS ENRIQUECIDOS, PUEBLOS VIGILADOS: BIOMETRÍA, SEGURIDAD Y EVASIÓN FISCAL

Resumen: Mientras los organismos multilaterales parecen ser incapaces de utilizar los avances tecnológicos para identificar y culpar a los responsables del fraude fiscal mundial -estimado en un mínimo de 130.000 millones de euros por año (Zucman, 2015)-, los mismos organismos han promovido en varios Estados el empadronamiento biográfico y biológico de más del 15% de la humanidad -por primera vez en su historia-, en función de ahorros fiscales de resultados discretos o desconocidos. La creación de grandes bases de datos poblacionales biométricas -a veces ilegalmente-, en función de crear perfilados para fines sociales, comerciales, policiales y/o militares, ha aumentado el control empresarial y estatal sobre sus ciudadanos, y el poder de ciertos países sobre otros. De manera que, mientras los ultra ricos fortalecen su opacidad y derecho de presunción de inocencia -e incluso son premiados por sus ilegalismos-, las mayorías poblacionales debemos transparentar cada día más nuestra vida, entregando copia de nuestra biología y biografía -nuestra *zoe* y *bio* (Agamben, 1998)- al Estado.

Este trabajo, enmarcado en el proyecto de investigación "La Promesa Represiva" (FSOC-UBA), apunta a reflexionar desde la óptica de biopoder de Foucault y Agamben, cómo estas prácticas redefinen la ciudadanía y el estado de derecho en el mundo y el caso de Argentina, así como también plantean la idea de autodeterminación informativa ya no como un derecho acotado a una perspectiva individual/liberal, sino ligado al derecho de los pueblos.

Palabras Clave: Biometría, Seguridad, Impuestos, Biopoder, Argentina.

ANDRÉS PÉREZ ESQUIVEL*

Os ricos enriquecem, os povos são vigiados: biometria, segurança e evasão fiscal

Resumo: Embora as agências multilaterais parecem incapazes de usar os avanços tecnológicos para identificar e culpar aos responsáveis da evasão fiscal global -estimada em um mínimo de 130.000 milhões de euros por ano (Zucman, 2015)-, as mesmas agências têm promovido em vários estados o registo biográfico e biológico de mais do 15% da humanidade -pela primeira vez em sua história-, com a finalidade de obter poupanças fiscais discretas ou desconhecidas. A criação de grandes bases de dados biométricos da população -por vezes, de forma ilegal- a fim de criar perfis sociais, comerciais, policiais e / ou militares, tem aumentado o controle das corporações e do Estado sobre seus cidadãos, e o poder de certos países sobre outros. Assim, enquanto os ultra-ricos reforçam a sua opacidade e direito de presunção de inocência -e até são recompensados por seus ilegalismos-, as maiorias populacionais devem ser cada dia mais transparentes, entregando uma cópia da nossa biologia e biografia -nossa zoe e bio (Agamben, 1998)- ao Estado.

Este papel, enquadrado no projecto de investigação "A Promesa repressiva" (FSOC-UBA), tem como objetivo refletir a partir da perspectiva do biopoder de Foucault e Agamben, como essas práticas redefinem a relação entre cidadania e o Estado de Direito no mundo e no caso da Argentina, e como levantam a idéia de autodeterminação informativa não mais como um direito delimitada a uma perspetiva liberal/individual, mas ligado ao direito dos povos.

Palavras Chave: Biometría, Segurança, Tributação, Biopoder, Argentina.

While the rich enrich, peoples get surveilled: biometrics, security and tax evation

Abstract: While multilateral agencies seem to be unable to use technological advances to identify and blame those responsible for global tax fraud -estimated at a minimum of 130 billion euros per year (Zucman, 2015)-, the same agencies have promoted in several states the biographical and biological registration of more than 15% of humanity -for the first time in its history-, to achieve discrete or unknown fiscal savings. The creation of large biometric population databases -sometimes illegally- in order to create profiles for social, commercial, police and / or military purposes, has increased business and state control over its citizens, and the power of certain countries over others. So while the ultra rich strengthen their opacity and right of presumption of innocence -and are even rewarded for their illegality-, the majorities of the population must make our life more transparent, delivering a copy of our biology and biography -our zoe and bio (Agamben, 1998)- to the State.

This work, framed in the research project "The Promise of Repression" (FSOC-UBA), aims to reflect from the perspective of Bio-Power of Foucault and Agamben, how these practices redefine citizenship and the rule of law in the world and the case of Argentina, as well as raising the idea of informational self-determination, no longer as a right limited to the individual / liberal perspective, but linked to the right of peoples.

Keywords: Biometry, Security, Taxes, Bio-power, Argentina.

EL FRAUDE DE LOS RICOS Y EL INTERCAMBIO AUTOMATIZADO DE INFORMACIÓN

El poder y los recursos están cada día en menos manos. La economía mundo ha trabajado para que el 0,7% más rico de la población mundial concentre más del 45,6% (Credit Suisse Research Institute, 2016) de la riqueza global, y el caso de los Panama Papers[1] ha vuelto a mostrar que los paraísos fiscales están en el meollo de las actuales crisis financieras, presupuestarias y democráticas, al ofrecer a los más poderosos la posibiliad de robarles a sus gobiernos, provocando un problema para todo el mundo, y en especial a los países periféricos.

En materia de fraude fiscal ligado al secreto bancario, tenemos estimaciones de máxima como las de James Henry, de *Tax Justice Network*, que calculan una riqueza offshore fuera del control tributario de entre 21 y 32 billones de dólares (BBC, 2012). Y también estimaciones de mínima críticas a las de Henry, como las de Gabriel Zucman (2015), autor del libro *"La riqueza escondida de las naciones"*, que dice que en 2013 había 5,8 billones de euros guardados offshore en paraísos

fiscales. Y como el 80% de ellos no estaban declarados, calcula que como mínimo indiscutible *"el fraude de los ultrarricos cuesta cada año 130.000 millones de euros a los Estados del mundo entero"*.

En abril de 2009, la OCDE, comisionada por el G20 para luchar contra el fraude fiscal, consideró poco realista el Intercambio Automatizado De Información (IADI) y propuso el *intercambio a pedido* (Zucman, 2015). O sea, que un Estado deba aportar pruebas para realizar un pedido de cooperación a los bancos para que levanten el secreto bancario. Algo en la práctica imposible excepto que se obtenga la información a través de filtraciones al filo de la ilegalidad como el caso *Panama Papers*. Esta actitud cambió declarativamente con la aprobación del *Common Reporting Standard* (CRS) de 2014 y la promesa de iniciar el intercambio automatizado obligatorio desde el año 2017, aunque sin claras amenazas de sanciones que materialicen la supuesta voluntad.

Henry cree que en vez de los paises ricos de la OCDE, el tema lo debería desarrollar la comisión tributaria de la ONU, que ha sido reducida a tres empleados y un presupuesto de sólo 400.000 dólares (El País, 2014). Para Zucman (2015), basado en registros parciales ya existentes, el *objetivo central* es crear un *registro internacional* indicando quien posee los títulos financieros en circulación, las acciones, las obligaciones, y las partes de los fondos de inversión de todo el mundo, de manera que se deje de confiar en la palabra de los bancos. Tarea para la cual considera al Fondo Monetario Internacional (FMI) como la organización mejor posicionada para hacerlo ya que, una vez creado, podría garantizar el acceso a todas las agencias fiscales del mundo.

Sin embargo, lejos de crear un padrón mundial de ricos y el manejo de sus riquezas, para preservar la soberanía fiscal de los Estados, los organismos internacionales han estado enfocándose en la ineficiencia y corrupción estatal como el principal problema de los países periféricos.

EL FRAUDE DE LOS ESTADOS Y LOS PROGRAMAS DE IDENTIFICACIÓN BIOMÉTRICA

Hay mucha y preocupante corrupción entorno al financiamiento internacional que involucra a gobiernos de Estados prestados como también a organismos prestadores. Del lado de los organismos ya nos encontramos que el halcón del Pentágono, Paul Wolfowitz, tuvo que renunciar a la presidencia del Banco Mundial (BM) por actos de corrupción en 2007. Que en 2008 Wikileaks develó informes internos de corrupción en sus programas, y que el mismo BM reconoció en 2009 que no protegía bien sus fondos de la corrupción interna.

Por el lado del FMI, también nos encontramos a los tres últimos directores, Rato (El País, 2015), Strauss-Kahn (Telesur, 2016) y Lagarde, investigados por escándalos de corrupción, con el primero actualmente detenido y la última recientemente condenada pero no sancionada debido a su *"reputación internacional"* (Infobae, 2016: 2).

Dentro de los condicionamientos de transparencia y eficiencia que hacen estos organismos para otorgar financiamiento a un Estado, se incluyen Programas de Transferencia Condicionada (PTC) con campañas de identificación digital y gobierno electrónico. Si bien en casos como África y Asia estos programas facilitaron el acceso directo a servicios a mucha gente que antes no lo

tenía, los mismos han venido acompañados de aspectos innecesarios y desmedidos como la extracción de datos biográficos exhaustivos (personales y filiales) y biológicos únicos (huellas, rostro, iris, etc.) de la población, como una de las condiciones para las transferencias.

Mientras países como Francia consideraron un riesgo para la seguridad nacional la creación de una base nacional biométrica centralizada de sus ciudadanos y la declararon inconstitucional por afectar desproporcionadamente el derecho a la privacidad (Le Monde Diplomatique, 2012)[2], el BM (2016) celebró la implementación del programa AADHAAR del gobierno de la India, sin aprobación del parlamento[3], junto a una empresa privada norteamericana/francesa, que ya casi reune en una sola base a sus 1300 millones de ciudadanos -un 15% de la población mundial-.

En la presentación del Informe sobre Desarrollo Mundial 2016 *"Dividendos Digitales"*, el economista jefe del Banco Mundial, Kaushik Basu, dijo que estimaban *"un ahorro de 1000 millones de dólares por año al reducir la corrupción y fuga del gobierno Indio. Es una ayuda para las cuentas fiscales. Es una ayuda para proveer otros servicios de utilidad"* (The Economic Times, 2016: 2). Un optimismo que contrasta con los números globales de la evasión fiscal de ese país en paraísos fiscales, estimada en 500.000 millones de dólares (BBC, 2016), y con los infructíferos planes de amnistía y descuentos del actual gobierno para repatriar dinero a cambio de no iniciar acciones legales. En efecto, en 2015 sólo 700 personas se plegaron a la amnistía pagando 364 millones en impuestos (Reuters, 2016).

Con el mismo énfasis, el Banco Mundial y la República de Francia elaboraron un *Manual de Identidad Digital* (2014) para incentivar a los gobiernos africanos a aplicar estos programas. Partiendo de la idea de que los límites y el contenido de la privacidad varia permanentemente en espacio y tiempo, en su manual definen a la privacidad como *"la habilidad de individuos o grupos de liberarse a sí mismos, o la información sobre ellos mismos, de ser observados y, por tanto controlar que información revelan a otros"* (BM y RF, 2014: 38). Significando, en otras palabras, que para el caso africano no consideran a la privacidad como un derecho a proteger por el Estado, sino como una destreza que *"si no es atendida correctamente desde el inicio, puede poner en riesgo el exito del programa"* (BM y RF, 2014: 38).

El nombre, la historia personal, el sentido de pertenencia a lugares y apego a las personas, ideas y valores hacen a la identidad un proceso de transformación continua. Superponer estos aspectos para diferentes propósitos los convierte en instrumentos de identificación, que ahora incluyen sistemas digitales. Estos *identificadores*, usados para la *identificación* son los mejores proxies para la *identidad*, pero no son sinónimos (Lyon, 2009).

El Banco Mundial asimila identidad con identificador y promueve la identificación masiva arguyendo que *"la falta de identidad impide que las personas pobres puedan ejercer sus derechos humanos y democráticos básicos"* (BM, 2016: 17), por eso considera que *"el objetivo de un programa de identidad nacional debe ser el atribuir una identidad por persona de por vida para todo tipo de necesidad"* (BM, 2014: 7), y que esa identidad *"tiene que ser móbil, transaccional, interoperable, portatil y social, además de ser segura"* (BM, 2014: 1). De esta manera, *"lo fundamental no es la*

tarjeta de identidad, sino los datos de identidad, los que pueden ser aprovechados mediante su almacenamiento en varios medios, dependiendo de las necesidades y presupuestos" (BM, 2014: 33).

De la mano de esta lucha por la eficiencia y la transparencia, aparece entonces un importante conglomerado de empresas privadas que Lyon (2009) llama *"card cartels"*, que implementan estos registros poblacionales masivos, o promueven tarjetas de identificación electrónica (con chip RFID) que permiten hacer trazabilidad de la rutina de movimientos y consumos de la población. O que incluso fomentan la creación de registros de ADN con fines securitarios.

Generalmente estos sistemas replican y a veces exacerban las desigualdades y las injusticias del lugar donde se implementan, y lo hacen de maneras sutiles sin que necesariamente haya una intención por parte de sus promotores. Las identificaciones que uno no elige, sino que son infladas y lanzadas por otros, son el punto de inicio de la vigilancia (Lyon, 2009).

Paradójicamente, este mismo BM que incentiva la expansión de los logros de Costa Rica, Kenia, Nigeria e India, entre otros, señaló en su último informe anual, "*Dividendos Digitales"* (2016), que esto podría no ser tan beneficioso porque, *"en ausencia de instituciones responsables, las inversiones del sector público en tecnologías digitales amplifican la voz de las élites, lo cual puede derivar en la captura de políticas y en un mayor control del Estado"* (BM, 2016: 3), fortaleciendo así el *"riesgo de que los Estados y las empresas puedan valerse de las tecnologías digitales para ejercer control sobre los ciudadanos y no para empoderarlos"* (BM, 2016: 5).

Si tenemos en cuenta que el mismo BM (2012) ya había alertado que los programas de transferencia condicionada podían tener repercusiones en el sistema democrático, al ser factible de ser *"motivados y dirigidos estratégicamente para el clientelismo y la compra de votos"* (BM, 2012: 21); y que además proporcionó evidencia empírica del caso *Familias en Acción* de Colombia, concluyendo que *"la participación política y las opiniones políticas son sensibles a las transferencias dirigidas"* (BM, 2012: 20). No hace falta ir muy lejos para imaginar los riesgos que implica para las democracias la combinación de sistemas de identificación altamente invasivos, el uso de *big data* y la transferencia automatizada de beneficios, en el caso de que un gobierno se vea tentado de regular comportamientos de ciertos sectores sociales para distintos fines.

Entre esos riesgos, tampoco se pueden obviar los grandes intereses económicos y securitarios que hay detrás de la promoción de estas tecnologías. Por un lado están las instituciones bancarias que incorporan grandes masas poblacionales en sus carteras de clientes, y por otro, potencias militares que consideran un recurso estratégico las tecnologías biométricas y celebran convenios (públicos y/o secretos) de acceso a estas bases para crear *"watch lists"* (o listas de observación) y poder expulsar de sus territorios personas que sean identificadas con cierto perfil de peligrosidad, o para atacarlos en el exterior.

Como ejemplo tenemos la base EURODAC que registra obligatoriamente la biometría de todos los solicitantes de refugio en Europa y la guarda por diez años, de manera que si son rechazados en un país son rechazados en el resto. Hasta 2012 ya había medio millón de rechazos (Jones, 2013).

También EEUU, que está estrenando un nuevo sistema de reconocimiento facial de 1000 millones de dólares, ya cuenta con la segunda base de datos biométricos más grande del mundo compuesta de 548 millones de rostros. Hasta el momento el FBI envió a las policías 9303 *posibles candidatos* (Markowitz, 2016) a culpabilidad, pero no se sabe cuantos ni como fueron abordados.

Estas formas de vigilancia y control no se limitan al sector público, también se encuentran en expansión servicios privados como *World-Check*[4]*,* que crea *"watch lists"* arbitrarias y confidenciales para que bancos, empleadores y gobiernos puedan realizar consultas de perfiles de peligrosidad antes de tomar alguna decisión sobre una persona.

Todas estas prácticas no sólo se encuentran en contradicción con la plena vigencia de los derechos humanos, violando convenciones y normativas nacionales, sino que también están redefiniendo el vínculo entre el Estado y la ciudadanía. Cuando el Estado ya no cree lo que dices o en la tarjeta de identidad que él mismo otorga ya que, además de *quién eres,* ahora también exige que demuestres *qué eres* si quieres ejercer tus derechos; el resultado es la consolidación de un Estado desconfiado y poseedor de un poder inmenso e inédito, y una ciudadanía más vulnerable a posibles abusos de poder. Esto nos obliga a replantear el problema del principal-agente, de quién debe servir a quién, y por lo tanto los principios que rigen las democracias formales actuales. Basta ver cómo la Corte Suprema de la India tuvo que aclarar en cuatro oportunidades que estaba prohibida la negación de servicios básicos, de derechos básicos, a los ciudadanos que no tuviesen la tarjeta AADHAAR (TOI, 2015), y como tuvo que impedir que esos datos puedan ser entregados a las agencias policiales (The Hindu, 2014); para dimensionar que, lejos de ser una abstracción, ésta redefinición del vínculo Estado/Ciudadanía es y será una de las pujas centrales por la redistribución de poder a nivel intra e internacional, y la aplicación -o no aplicación- de la biometría con una finalidad y no otra, va circunscribiendo quienes son los más afectados.

EL CASO DE ARGENTINA

El contraste internacional entre la creciente opacidad de los ultraricos, y el que vuelve a las mayorías poblacionales cada vez más transparentes y vulnerables, se puede ver con claridad en un contexto nacional y latinoamericano como el caso de Argentina.

En el año 2012, la Administración Federal de Ingresos Públicos (AFIP), inició una demanda judicial contra el HSBC de Suiza por ayudar a evadir impuestos a 4040 personas físicas y jurídicas de Argentina (Infonews, 2015). A principios del año 2016 el HSBC se negó a brindar información diciendo que los fundamentos no eran sólidos y pidiendo que se demuestre *cómo, cuando y donde fue el delito para brindar los datos de sus clientes* (La Nación, 2016 a). En 2013 la Unidad de Información Financiera (UIF) también había multado por más 5 millones al banco HSBC por no haber reportado operaciones sospechosas de lavado de dinero (Infobae, 2013). Pero de la mano del nuevo gobierno de la coalición *Cambiemos*, las autoridades de la UIF que denunciaron al HSBC fueron removidas y reemplazadas por una ex abogada de HSBC y un ex empleado del FMI (Página/12a, 2016).

El recientemente asumido Presidente argentino, Mauricio Macri, es un millonario hijo de familia millonaria, y fue uno de los pocos presidentes del mundo involucrados en el caso de *Panama Papers.* Con el correr de los meses las causas judiciales que lo imputaron a raíz de esa investigación periodística, fueron avanzando y comprobando relaciones del Presidente con 50 sociedades offshore con sedes en Nueva York, Panamá, Suiza, Bahamas, entre otras (Página/12b, 2016).

En paralelo con el avance de estas investigaciones judiciales, el gobierno presentó una ley de blanqueo de capitales con diversos beneficios para los evasores y, luego de ser aprobada por el Congreso, el Poder Judicial imputó por abuso de autoridad al Presidente, al Jefe de Gabinete y al Ministro de Economía, debido a que por decreto reglamentario[5] eliminaron la expresa prohibición de la Ley que impedía la inclusión de familiares de funcionarios públicos en el blanqueo(La Nación b, 2016).

El Centro de Investigación y Prevención de la Criminalidad Económica (CIPCE, 2016) alertó al Grupo de Acción Financiera Internacional (GAFI) sobre *"el desmantelamiento del sistema"* en el país, y sobre como el gobierno alienta una *"amnistía"*, y pidió que el GAFI intime al Poder Ejecutivo Nacional Argentino, sin una respuesta del organismo hasta la fecha.

Por otro lado, el actual gobierno heredó del anterior una polémica Base Nacional de Datos Biométricos (SIBIOS) de todos los argentinos, creada por decreto para uso de todas las fuerzas policiales y de seguridad, sin ningún mecanismo de control normado. También heredó el Sistema Único de Boleto Electrónico (SUBE), cuya tarjeta con chip RFID se implementó[6] asociado de manera obligatoria con el Documento Nacional de Identidad (DNI) y el domicilio de los usuarios, conformando una base nacional de datos de movilidad y microconsumo comercial de la ciudadanía casi en tiempo real, que a su vez ha probado ser vulnerable a filtraciones (La Nación, 2012).

A esto también debemos agregar que Argentina fue el primer país requerir huellas y fotografías digitales de manera obligatoria para poder realizar vuelos aéreos (Aeropuertos Argentina 2000, 2005). La extracción obligatoria de datos biométricos por parte de la AFIP para que las nuevas generaciones estén habilitadas para obtener un trabajo formal (Clarín, 2010). Y el registro biométrico obligatorio de los jubilados si es que quieren cobrar su jubilación (Infobae, 2014).

En 2014, cuando el gobierno del *Frente para la Victoria* (FPV) quiso implementar por decreto un DNI electrónico con chip RFID[7], ocho organismos de derechos humanos hicieron una campaña alertando sobre los peligros de la iniciativa diciendo que *"el Estado argentino está creando llaves maestras a la vida de todos los ciudadanos que permiten su vigilancia y control en tiempo real y que, como si fuera poco, también se han mostrado vulnerables. Sin dudas esto representa un serio perjuicio para la seguridad democrática sea que esté en manos de un gobierno democrático, autoritario, o que sea filtrada por empresas u organizaciones criminales de cualquier tipo"* (Asociación Pensamiento Penal, 2014: 13). Finalmente la implementación del DNI-e fue suspendida por lo que el riesgo continúa latente.

Todas estas medidas mencionadas violan el derecho a la privacidad que establecen el art. 19 de la Constitución Nacional, el art. 11 de la Convención Americana de Derechos Humanos y el art.

12 de la Declaración Universal de Derechos Humanos; y por lo tanto sólo podrían ser aprobadas por una ley que especifique la necesidad excepcional de limitar un derecho en pos de otro, bajo ciertos resguardos y controles que garanticen el buen uso de la información. Nada de esto sucedió.

Por lo tanto, estas medidas representan un cambio ilegítimo e inconstitucional de paradigma en el abordaje de las políticas de seguridad, que se traslada desde la perspectiva *preventiva* hacia una de tipo *anticipatoria*, esto es, obtener la mayor cantidad de información sobre la mayor cantidad de gente posible para abordarlos en caso de que en algún momento de sus vidas decidan volverse "malos", o las autoridades decidan que no han dejado de ser suficientemente "buenos".

Hoy, con esta capacidad técnica instalada de mecanismos securitarios de poder (Foucault, 2006) y los dispositivos policiales con sus tradicionales mecanismos disciplinarios selectivos (Foucault, 2006), ciertos grupos poblacionales se vuelven más propensos a ser perfilados que otros. Como indica Lyon (2009), son muchos los casos que demuestran que el estigma de la pobreza es exacerbado por su creciente asociación con la criminalidad, la que es racionalizada por la necesidad de reducir reclamos de fraude y vinculada al crimen por el uso de métodos convencionales asociados con infractores de la ley. A este proceso de criminalización también debemos sumarle los riesgos de la selectividad automatizada, porque algunas diferencias tribiales en los criterios de reconocimiento algorítmico, pueden de hecho tener una implicancia política (ética) importante dentro de un abanico de prácticas de vigilancia socio-técnicas (Introna en Lyon, 2009).

En el caso argentino podemos mencionar el reciente programa *Barrios Seguros*, implementado por el Ministerio de Seguridad de la Nación, mediante el cual la Policía Federal Argentina, se encuentra hoy realizando controles biométricos a quienes ingresan y egresan de "Villas Miseria" de la Ciudad Autónoma de Buenos Aires, ejerciendo una criminalización de la pobreza en el presente pero también con el potencial riesgo de que esos controles generen nuevos registros, nuevas listas de seguimiento de personas consideradas peligrosas o potencialmente peligrosas.

Como si este escenario fuera poco, también comenzaron a avanzar proyectos legislativos de diversos sectores políticos para crear padrones genéticos con fines de seguridad.

En la sesión del día 03 de julio de 2013 de la Honorable Cámara de Diputados de la Nación, en la que se creó un registro de huellas genéticas de violadores, la Diputada Patricia Bullrich, actual Ministra de Seguridad de la Nación, dijo lo siguiente: *"Así como la Argentina fue pionera en cuanto al suministro de datos personales que ayudaron a la identificación de los delitos con las huellas digitales* [en referencia al sistema dactilográfico creado por el argentino Juan Vucetich]*, hoy estamos generando un avance similar pensando en las posibilidades que existen en este mundo en que vivimos.*
Por eso, generar este avance implica que a partir de este registro de datos genéticos podamos pensar que de manera rápida se extienda esta herramienta de prueba tan importante, que ya está siendo utilizada aunque no está del todo legislada, en una gran cantidad de delitos para ayudar a esclarecerlos. De modo que no utilizaríamos esta herramienta del ADN para un tipo específico de delito sino que sería la herramienta de identificación del siglo XXI, así como la huella dactilar lo fue en el siglo XX".

En esa misma sesión otro diputado[8] destacó su proyecto para crear un registro de ADN de toda la población nacional con fines de seguridad: *"Personalmente, presenté siete proyectos en contra de los violadores. El primero, propone el registro de ADN, pero de todos los argentinos. Una forma de prevenir las violaciones es que todos los argentinos sepan que están identificados. De la misma forma que todos estamos identificados a través de las huellas digitales, hoy la tecnología nos permite estar identificados a través del ADN".*

Un proyecto similar a este estuvo muy cerca de ser tratado en una sesión legislativa a fines del año 2015. La Legislatura de la Provincia de Buenos Aires, la más poblada del país con 15 millones de habitantes, dió tres dictámenes favorables y puso en el orden del día de la sesión un proyecto de ley del FPV[9],para crear un banco genético de todos los habitantes con fines de seguridad pública. Si bien finalmente no fue tratado en sesión, logró abrirse paso (La Nación, 2015) sentando un grave precedente.

AUTODETERMINACIÓN INFORMATIVA DE LOS PUEBLOS

El derecho fundamental a la autodeterminación informativa, a su vez parte del derecho a la privacidad, consiste en el poder que tienen los ciudadanos de ejercer control sobre su información personal que se encuentra en manos de agencias estatales y privadas, y especialmente qué información puede ser revelada a otros. La traducción procesal de este derecho sustantivo es el conocido recurso de *habeas data*, mediante el cual se puede exigir la supresión o modificación de datos personales.

El actual proceso de recolección masiva de datos biometricos representa un desafío para el esquema clásico de protección de datos personales desde una perspectiva individual liberal. En las últimas décadas el debate principal giró entorno a la necesidad de reforzar los marcos legales y las partidas presupuestarias para obtener organismos estatales de protección de datos personales, que puedan ejercer un control autónomo y autárquico sobre los registros públicos y privados de datos, y sea capaz de poner límites al intercambio de información de las agencias de seguridad, así como exigir mecanimos auditables de control de los mismos.

Sin embargo, cuando el presente nos muestra que la biología de pueblos enteros, de miles de millones de humanos, puede ser copiada y almacenada en un disco rígido, el derecho de autodeterminación informativa ya no resulta circunscribible al derecho a la privacidad como vínculo entre el ciudadano y su Estado, sino que también involucra aspectos del plano de la seguridad nacional, y el derecho internacional de los pueblos.

De esta manera, a las identidades sociales que están en permanente tensión con las identidades que los estados imponen o pretenden imponer, también le debemos agregar la creciente tensión entre las identidades que ciertos estados nación, o bloques regionales, pretenden imponer sobre otras naciones y sus ciudadanos, étnias, y grupos poblacionales sin Estado. Uno de los ejemplos más claros es el papel preponderante que juegan las tecnologías biométricas, no sólo en la

consolidación de la representación de ciertos inmigrantes y refugiados como peligrosos, sino en la consolidación de la capacidad técnica de poder anticiparse a su posible expulsión, constante monitoreo y/o persecución.

El proceso social disperso y desorganizado que se expande día a día, que Nikolas Rose (2000) llama la *securitización de la identidad*, nos requiere a todos probar la legitimidad de nuestra identidad para poder ejercitar la libertad. Mientras la razón gubernamental liberal respeta y garantiza ciertas libertades, también consume libertad porque está obligado a establecer limitaciones, controles, coerciones, etc. Se aplica así una política pública que extrae nuestros datos biológicos únicos, sometiendo la vida al mando de la política. Y este biopoder convierte al Hombre moderno en un animal en cuya política está cuestionada su propia vida de ser viviente.

Por eso Agamben (2006) plantea que así como el Estado-nación cede sus funciones económicas y socio-culturales a las fuerzas globales de la economía de mercado, lo mismo sucede con la técnicas biopolíticas. La vida se divide en Zoé (mera vida biológica en relación con todos los seres vivos) y Bíos (forma histórico-cultural de vivir propia de un individuo o grupo), y la consecuencia de considerar al hombre como mera vida biológica, es que ésta puede ser separada de todo contexto social, político, cultural, y tratada como medio (no como fin en sí), como residuo, como objeto de experimentación; incluso puede ser aniquilada sin puniciones. Así es como Agamben identifica que los "desechos humanos planetarios", la zoé generada por el capitalismo global, son los emigrantes, refugiados, mendigos, desocupados, etc., ante los que el Estado-nación debe abordar como guardián de la ley.

Por estos motivos plantea que la tesis foucaultiana debe ser corregida sobre la base de que lo decisivo no es que la vida natural o simplemente biológica se convierta en objeto de los cálculos y de las previsiones del poder estatal, sino que *"el espacio de la nuda vida que estaba situada originariamente al margen del órden jurídico, va coincidiendo de manera progresiva con el espacio político, de forma que exclusión e inclusión, externo e interno, bíos y zoé, derecho y hecho, entran en una zona de irreductible indiferenciación"* (Agamben, 2006: 19).

La invocación al miedo, la amenaza del terror, pasó a convertirse en la herramienta permanente a la que los Estados pueden apelar para resolver conflictos nacionales e internacionales con la promesa de la protección negativa de la vida natural. Una herramienta biopolítica que suele invocar la suspensión de la norma para conservar la ley, y a la violencia jurídica que conserva el derecho, para "normalizar" una jurisdicción de la soberanía. O en otras palabras, se consolida una biopolítica capaz de hacer emerger el terror constitutivo del poder soberano, y de afianzarlo como terrorismo de Estado dentro de su propio ordenamiento.

CONCLUSIONES

Así como la mundialización financiera no se reduce a la evasión fiscal, tampoco el accionar

estatal se reduce a actos de corrupción con fondos de ayuda internacional. Sin embargo, con Suiza como la cabeza garante del secreto bancario del circuito internacional de especialización de paraísos fiscales, estamos viviendo máximos históricos de fraude fiscal.

Al mismo tiempo que los Estados pierden de mínima 130.000 millones de euros por año, los programas de organismos internacionales hacen que ahorren unos pocos miles, al precio de crear grandes bases de datos poblacionales -a veces ilegalmente- que aumentan el control estatal y empresarial sobre sus ciudadanos, y el poder de ciertos países sobre otros.

Hay un claro contraste entre dos procesos que se están profundizando en simultáneo y espejados, uno que deja a los pocos ultraricos cada vez más opacos y poderosos, y otro que deja al resto de la humanidad cada vez más transparente, empobrecida y vulnerable frente a los Estados y diversos agentes de poder.

De esta manera la *Elite Gobal* (Bauman, 2008b), libre de moverse por todo el mundo buscando maximizar sus ganancias, y con recursos suficientes para crear y financiar ejércitos privados; fortalece su derecho de presunción de inocencia. Mientras tanto, *los condenados a ser locales* (Bauman, 2008b) van perdiendo cada vez más el control sobre sus vidas y se vuelven cada día más sospechosos hasta que demuestren su inocencia, conforme avanzan las políticas de contraterrorismo y contrainsurgencia, y se van expandiendo las tecnologías de vigilancia para el actuar policial cotidiano.

A diferencia de sus antepasados modernos de la era de la construcción de la nación, *"esta elite global no tiene ninguna misión que cumplir; no necesitan ni pretenden ganar adeptos… no se sienten obligados a asumir responsabilidades… no tiene la ambición de administrar, y la construcción del orden no figura en su agenda"* (Bauman, 2008a: 285-286).

En el mercado como biopolítica, el Estado debe limitarse a mantener el orden, y los superricos no se asumen como generadores de desorden, sino como los garantes del orden de mercado. Entonces, bajo el reino de los mecanismos neutros de intercambio, los super ricos se afirman a sí mismos como cuerpos de *"cuentas claras"*, con inclinaciones dignas de confianza, que no requieren de un control incisivo.

Más allá de si existe o no correlación cuantificable entre el proceso de enriquecimiento de los ultra-ricos, y el de vigilancia de grandes masas poblacionales en función de ahorros fiscales y la seguridad pública. Resulta interesante para esta investigación profundizar en el análisis de la construcción de los regímenes de verdad[10] (Foucault, 1979) que permiten que ciertas tecnologías no sean aplicadas para los delitos de mayores montos, con capacidad de afectar seriamente la economia de un país; y sí sean aplicadas y profundizadas en función de registros anticipatorios de grandes masas poblacionales, en el marco de un debate moral vinculado a la falta de transparencia y a un eficientismo utilitarista polifuncional.

Con esta intención, vale la pena analizar el vínculo entre la creciente opacidad de los ultra ricos y el creciente discurso de *la transparencia* como valor central de la democracia. Como dice

Jaquelin Best (2005), la palabra transparencia contiene poderosas asociaciones de arraigo moral y político: honestidad, inocencia, franqueza. Pero los aires democráticos de la *promesa de transparencia* -no necesariamente coincidente con el derecho de acceso a información- tienen sus límites:

En primer lugar, sobrevalorar la transparencia puede hacer creer que la información por sí misma puede resolver nuestros problemas. Así es como se solicita y se brinda información personal de los ciudadanos sin prestar atención a los principios de necesidad, finalidad, proporcionalidad, racionalidad, etc.; bajo e lema de *tenemos que obtenerla/entregarla porque algún día resultará necesaria*.

En segundo lugar, la transparencia suele apuntar a un sólo lado. Aquellos que usan el lenguaje de la transparencia generalmente tratan al gobierno como el principal culpable, cuando usualmente los mercados y los privados comparten las culpas. De la misma manera, a veces los Estados exigen información como si fueran ellos los que tuviesen derechos ante una población que tiene la obligación de brindar su información, cuando se supone que es a la inversa.

Tercero, la transparencia es política. Mientras parece ser una estrategia neutral, simplemente dirigida a revelar información, para que la comunicación sea transparente todos debemos hablar el mismo lenguaje y contar con las herramientas apropiadas para analizar y auditar la información. También puede ser fuertemente intervencionista, cómo en el caso de las exigencias internacionales de la Organización Internacional de Aviación Civil (OIAC) para confeccionar los pasaportes con datos biométricos que, una vez acatados por la principales potencias debieron ser acatados por el resto del mundo, para no ser acusados de no querer cooperar y/o de tener algo que esconder.

Cuarto, la transparencia es frecuentemente monolítica. Los defensores de la transparencia casi invariablemente buscan estandarizar la prácticas para hacerlas fácilmente cuantificables y comparables. En términos de la economía internacional esto frecuentemente significa hacer que las economías de varios países se parezcan entre sí, y en términos de seguridad internacional, esto significa el intercambio estandarizado de información entre agencias de seguridad para la creación de bases compartidas, aún cuando estos estándares o el intercambio choquen con las normativas locales.

Finalmente, la promesa de la transparencia asume que se pueden eliminar todas las incertidumbres en nuestros sistemas políticos y económicos, como una solución perfecta libre de política. Pero la incertidumbre y la política son una parte inevitable de la realidad y de las políticas públicas.

La recuperación de la política y la aceptación de la incertidumbre como contrapuesta a la *promesa de la transparencia*, colabora en el análisis de su régimen de verdad. Por un lado nos permite identificar un Estado sometido a la gubernamentalidad liberal (Foucault, 2006) cumpliendo un papel de guardian de la ley, pero al mismo tiempo ayuda a entenderlo como una arena glocal de disputas en torno a la protección de derechos y su amplificación en función de des/democratizar la democracia. Así como también, a verlo como un actor capaz de des/equilibrar la balanza de

relaciones de poder en el orden nacional e internacional, no sólo a través de poderes fácticos públicos y privados sino también en el plano de los organismos supranacionales con capacidad de incidir e in/visibilizar estos nuevos procesos de redistribución de poder.

NOTAS

* Licenciado en Sociología de la Universidad de Buenos Aires. Maestrando en Políticas Públicas y Gerenciamiento del Desarrollo (UNSAM/GU). Investigador de la Facultad de Ciencias Sociales de la UBA. Miembro de la Red Latinoamericana de Estudios de Vigilancia, Tecnología y Sociedad (LAVITS). Contacto: advocare@-prontonmail.ch

1. International Consortium of Investigative Journalism: https://panamapapers.icij.org/

2. Normativa. Décision n° 2012-652 DC du 22 mars 2012. Loi relative a la protection de l'identité. Recuperado de http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/-download/2012652DCccc_652dc.pdf

3. Finalmente el Parlamento de la India aprobó una Ley para legalizar el programa en el año 2016, luego de que la extracción masiva de información ya estaba concluida casi en su totalidad (The Hindu, 2016).

4. Thomson Reuters World-Check. Recuperado de https://www.thomsonreuters.com/en/products-services/risk-management-solutions/customer-and-third-party-risk/thomson-reuters-world-check.html

5. Decreto PEN Nº 1206/16

6. Si bien luego de unos años se habilitó el uso anómino de la misma, quienes la usan de esta forma pierden beneficios monetarios.

7. Anuncio oficial del gobierno nacional argentino sobre los DNI electrónicos. Recuperado de https://www.youtube.com/watch?v=3pA5PbTPGYU

8. El Diputado Nacional por la Provincia de Salta, Alfredo Horacio Olmedo.

9. Expediente D- 373/14-15- 0 / LPBA.

10. Se entiende por régimen de verdad a los tipos de discurso que las sociedades aceptan y hacen funcionar como verdaderos, a los mecanismos y las instancias que le permiten distinguir los enunciados verdaderos o falsos, la manera en que se sanciona a unos y otros; las técnicas y los procedimientos que son valorados para la obtención de la verdad; y el estatuto de aquéllos que tienen la función de decir lo que funciona como verdadero.

REFERENCIAS

Aeropuertos Argentina 2000 (2005) *Presentaron el nuevo Sistema de Identificación Aeroportuaria*. Recuperado de http://www.aa2000.com.ar/news.aspx?idnoticia=31&group=prensa

Agamben, G. 1998 (2006). *Homo Sacer. El poder soberano y la nuda vida.* España: Giulio Einaudi.

Asociación Pensamiento Penal (2014). *El DNI electrónico viola nuestros derechos.* Recuperado de http://www.pensamientopenal.org.ar/dni/comunicado.pdf

Tax havens: Super-rich 'hiding' at least $21tn (22 de julio de 2012). *BBC*. Recuperado de http://www.bbc.com/news/business-18944097

India tax evasion amnesty uncovers hidden billions (1ro de octubre de 2016). BBC. Recuperado dehttp://www.bbc.com/news/world-asia-india-37530290

Banco Mundial (2012). *Conditional Cash Transfers, PoliticalParticipation, and Voting Behavior*. Policy Research Working Paper Nº 6215. Impact Evaluation Series Nº 66.

Banco Mundial y República de Francia (2014). *Digital Identity Toolkit. A Guide for Stakeholders in África*.

Banco Mundial (2016). *Dividendos Digitales. Informe sobre Desarrollo Mundial.*

Bauman, Z. 2002 (2008a). *La sociedad sitiada*. México: Fondo de Cultura Económica.

Bauman, Z. 2007 (2008b). *Tiempos Líquidos*. México D.F.: Tusquets.

Best, J. (17 de marzo de 2005) *The Limits of transparency*. New York Times. Recuperado de http://www.nytimes.com/2005/03/17/opinion/the-limits-of-transparency.html?_r=0

CIPCE (2016). *CIPCE alerta al GAFI sobre las medidas del Estado argentino en materia de lavado de dinero*. Recuperado de http://www.cipce.org.ar/articulo/cipce-alerta-al-gafi-sobre-medidas-del-estado-argentino-materia-lavado-dinero

CUIT, con foto y huellas dactilares (29 de mayo de 2010). *Clarín*. Recuperado de http://www.clarin.com/politica/CUIT-foto-huellas-dactilares_0_270572979.html

Credit Suisse Research Institute (2016). *Credit Suisse Wealth Report 2016.* Recuperado de https://www.credit-suisse.com/us/en/about-us/research/research-institute/news-and-videos/articles/news-and-expertise/2016/11/en/the-global-wealth-report-2016.html

Rodrigo Rato, acusado de fraude fiscal, blanqueo y alzamiento de bienes (16 de abril de 2015). *El País*. Recuperado de http://politica.elpais.com/politica/2015/04/16/actualidad/1429195780_456210.html

Foucault, M. 1977-78 (2006). *Seguridad, territorio y población.* Argentina: Fondo de Cultura Económica.

Foucault, M. (1979): *Verdad y Poder*, Entrevista con M. Fontana en Rev. L'Arc, nº 70 especial, págs. 16-26, en Foucault, M.: *Microfísica del Poder.* Madrid: La Piqueta.

La UIF aplicó una multa a HSBC Argentina por 5,4 millones de pesos (11 de junio de 2013). *Infobae*. Recuperado de http://www.infobae.com/2013/06/11/715031-la-uif-aplico-una-multa-hsbc-argentina-54-millones-pesos/

Jubilados y pensionados deberán registrar sus huellas digitales para cobrar (30 de diciembre de 2014). *Infobae*. Recuperado de http://www.infobae.com/2014/12/30/1617992-jubilados-y-pensionados-deberan-registrar-sus-huellas-digitales-cobrar/

La insólita excusa para no sentenciar a la presidente del FMI tras ser declarada culpable durante un juicio en Francia (19 de diciembre de 2016). *Infobae*. Recuperado de http://www.infobae.com/america/mundo/2016/12/19/christine-lagarde-la-excusa-para-no-condenar-a-la-presidente-del-fmi-tras-ser-declarada-culpable-durante-un-juicio-en-francia/

HSBC: las lista de las cuentas ilegales que analiza la justicia (14 de abril de 2015). *Infonews*. Recuperado de http://www.infonews.com/nota/194490/hsbc-la-lista-de-las-cuentas-ilegales-que

India launches new tax evasion amnesty scheme to unearth unaccounted cash (28 de noviembre de 2016). *Reuters*. Recuperado de http://www.reuters.com/article/us-india-modi-corruption-tax-idUSKBN13N194

Jones, C. (2013) *11 years of EURODAC* (Statewatch analysis Nº 235). Recuperado de http://www.statewatch.org/analyses/no-235-eurodac.pdf

En medio de la polémica, más demanda de la SUBE (29 de enero de 2012). *La Nación*. Recuperado de http://www.lanacion.com.ar/1444308-en-medio-de-la-polemica-mas-demanda-de-la-sube

Crearían un banco genético de todos los bonaerenses (15 de septiembre de 2015). *La Nación*. Recuperado de http://www.lanacion.com.ar/1827910-crearian-un-banco-genetico-de-todos-los-bonaerenses

Niegan a la Justicia Argentina datos sobre cuentas en Suiza (16 de marzo de 2016). *La Nación* a. Recuperado de http://www.lanacion.com.ar/1880105-niegan-a-la-justicia-argentina-datos-sobre-cuentas-en-suiza

Imputan a Macri, Peña y Prat-Gay por permitir que familiares de funcionarios entren al blanqueo (13 de diciembre de 2016). *La Nación b*. Recuperado de http://www.lanacion.com.ar/1966512-imputan-a-macri-pena-y-prat-gay-por-permitir-que-familiares-de-funcionarios-entren-al-blanqueo

La nouvelle carte d'identité biométrique jugée inconstitutionnelle (23 de marzo de 2012). *Le Monde Diplomatique*. Recuperado de http://www.lemonde.fr/societe/article/2012/03/23/la-nouvelle-carte-d-identite-biometrique-jugee-inconstitutionnelle_1674721_3224.html

Los ricos de Latinoamérica se han llevado su dinero fuera (4 de agosto de 2014). *El País*. Recuperado de http://elpais.com/elpais/2014/08/04/planeta_futuro/1407154193_141507.html

Lyon, D. (2009). *Identifying citizens, ID cards as suveillance*. United Kingdom: Polity.

Markowitz, E. (5 de abril de 2016). The FBI Now Has The Largest Biometric Database In The World. Will It Lead To More Surveillance?. *International Business Times*. Recuperado de http://www.ibtimes.com/fbi-now-has-largest-biometric-database-world-will-it-lead-more-surveillance-2345062

Abogada del HSBC y un ex técnico del FMI (19 de enero de 2016). *Página/12 a*. Recuperado de https://www.pagina12.com.ar/diario/economia/2-290621-2016-01-19.html

Los Macri en busca del paraíso (26 de diciembre de 2016). *Página/12 b*. Recuperado de https://www.pagina12.com.ar/10779-los-macri-en-busca-del-parais

Rose, N. (2000). “Government and control” en *Brit. J. Criminol*. N.º 40, p 321-329. Recuperado de https://www.uio.no/studier/emner/jus/ikrs/KRIM4001/h10/undervisningsmateriale/Artikkel_rose.pdf

Exdirector del FMI involucrado en casos de Panama Papers (6 de abril de 2016). *Telesur*. Recuperado de http://www.telesurtv.net/news/Exdirector-del-FMI-involucrado-en-casos-de-Panama-Papers-20160406-0020.html

Aadhaar ID saving Indian govt about $1 billion per annum: World Bank (14 de enero de 2016). *The Economic Times*. Recuperado de http://articles.economictimes.indiatimes.com/2016-01-14/news/69765565_1_world-bank-group-aadhaar-identification-system

Withdraw notifications making Aadhaar mandatory, Supreme Court tells Centre (24 de marzo de 2014). *The Hindu*. Recuperado de http://www.thehindu.com/news/national/withdraw-notifications-making-aadhaar-mandatory-supreme-court-tells-centre/article5826461.ece

Parliament passes Aadhaar Bill amid acrimonious debates (17 de marzo de 2016). *The Hindu*. Recuperado de http://www.thehindu.com/news/national/parliament-passes-aadhaar-bill-amid-acrimonious-debates/article8361992.ece

Supreme Court allows linking Aadhaar with PDS and LPG subsidies (12 de agosto de 2015). *The Times Of India*. Recuperado de http://timesofindia.indiatimes.com/india/Supreme-Court-allows-linking-Aadhaar-with-PDS-and-LPG-subsidies/articleshow/48444953.cms

Zucman, G. (2015). *La riqueza escondida de las naciones*. Buenos Aires: Siglo XXI.

TECNOLOGIA E PUNIÇÃO: O MONITORAMENTO ELETRÔNICO DE PRESOS NO BRASIL

Resumo: A expansão do sistema carcerário brasileiro e as atuais invocações à segurança fomentam a importação de novas tecnologias penais. Em 2010, o monitoramento eletrônico de indivíduos condenados pelo sistema de justiça criminal foi aprovado pela primeira vez no Brasil. As administrações estaduais passaram a contratar empresas privadas voltadas ao desenvolvimento de tornozeleiras eletrônicas rastreadas via satélite. De acordo com os legisladores, o propósito da medida seria favorecer a superação da calamitosa situação do sistema prisional no país, marcado pela superlotação, condições insuportáveis de vida e episódios de violência extrema. Entretanto, passados mais de 6 anos da autorização do monitoramento eletrônico no país, as taxas de encarceramento seguem em pleno crescimento, concomitantemente à expansão das tecnologias de rastreamento em meio aberto. Atualmente, cerca de 20 mil pessoas são submetidas ao chamado "controle telemático" empregado pelo sistema penal brasileiro. Este trabalho apresenta o processo de implementação do monitoramento eletrônico de presos no Brasil, bem como sua atual aplicação. São analisados os impactos sociais da medida, destacando-se as conexões entre as tecnologias de vigilância e as novas formas de se pensar e exercer o poder de punir. São discutidos alguns dos efeitos do controle eletrônico sobre a vida de pessoas monitoradas, por meio de dados coletados em entrevistas e observação participante. A partir disso, apresenta-se algumas das formas pelas quais as assim chamadas "facções criminosas" têm agenciado os dispositivos de rastreamento de presos e presas na cidade de São Paulo.

Palavras chave: Monitoramento eletrônico, Punição, Dispositivo, Neoliberalismo.

RICARDO URQUIZAS CAMPELLO*

Tecnología y punición: la vigilancia electrónica de presos en Brasil

Resumen: La expansión del sistema penitenciario brasileño y las actuales invocaciones a la seguridad fomentan la importación de nuevas tecnologías penales. En 2010, la vigilancia electrónica de personas condenadas por el sistema de justicia criminal fue aprobada por primera vez en Brasil. Las administraciones estaduales empezaron a contratar empresas privadas encargadas de desarrollar tobilleras electrónicas rastreadas por satélites. Según los legisladores, la finalidad de la medida sería favorecer la superación de la calamitosa situación del sistema carcelario en el país, marcado por la superpoblación, condiciones insoportables de vida e episodios de violencia extrema. Entretanto, más de 6 años después de la autorización de monitoreo electrónico en Brasil, los índices de encarcelamiento siguen en pleno crecimiento, concomitantemente a la expansión de las tecnologías de seguimiento en régimen abierto. Hoy, cerca de 20 mil personas son sometidas al llamado control telemático empleado por la justicia criminal brasileña. Este artículo presenta el proceso de implementación del monitoreo electrónico en Brasil, así como su aplicación actual. Son analizados algunos de los impactos sociales de la medida, destacando-se las conexiones entre las tecnologías de vigilancia y las nuevas formas de se pensar y ejercer el poder de punir. Son discutidos algunos de los efectos del control electrónico sobre la vida de personas monitoreadas, por medio de datos colectados en entrevistas y observación participante. A partir de ahí, presenta-se algunos de los modos por los cuales las denominadas "facciones criminales" agencian los dispositivos de rastreo de presos y presas en São Paulo.

Palabras clave: Vigilancia electrónica, Punición, Dispositivo, Neoliberalismo.

Technology and punishment: the electronic monitoring of prisoners in Brazil

Abstract: The expansion of the Brazilian prison system and the current demands for security foster the importation of new penal technologies. In 2010, the electronic monitoring of individuals condemned by the criminal justice was approved for the first time in Brazil. The local administrations started to hire private companies charged to develop electronic anklets tagged by satellite. According to legislators, the objective of the measure was to permit the overcoming of the dreadful situation of the Brazilian prison system, marked by the overpopulation, unbearable conditions of life and episodes of extreme violence. Nonetheless, more than 6 years after the authorization of the electronic monitoring, the incarceration rates are still growing, simultaneously with the increasing of the tagging technologies. Currently, nearly 20 thousand people are subjected to the so-called telematic control employed by the Brazilian penal system. This wok presents the implementation process of the electronic monitoring in Brazil, as well as its current enforcement. Some of the social impacts of the measure are analyzed, highlighting the connexions between surveillance technologies and the new ways of thinking and exercising the power to punish. Some of the effects of the electronic control on the lives of monitored people are discussed by data collected in interviews and participant observation. From that, some of the ways in which the so-called 'criminal factions' are managing the tagging *dispositifs* in São Paulo are presented.

Key words: Electronic monitoring, Punishment, Dispositive, Neo-liberalism.

INTRODUÇÃO

Maio de 2007

Senado Brasileiro, Sala das Sessões

> A prisão deixou de ser o controle perfeito. É ultrapassado porque ainda é estabelecido em espaço rígido. O limite territorial determinado pelo cárcere não é mais um aspecto positivo do controle penal, mas um inconveniente, haja vista que é insustentável para o Estado manter aprisionadas as inúmeras pessoas condenadas. Alguns países, a exemplo dos Estados Unidos da América, França e Portugal, já utilizam o monitoramento de condenado, exigindo-se o uso de pulseira ou tornozeleira eletrônica como forma de controle das pessoas submetidas ao regime aberto. (...) O controle eletrônico surge para superar as limitações das penitenciárias, podendo ser universalizado. (...) É preciso que criemos sistemas que não tenham os inconvenientes do cárcere, tais como a impossibilidade de expansão rápida e custo muito elevado. Sala das Sessões, Senador Magno Malta. (Brasil, 2007).

Novembro de 2012

Spacecom Monitoramento Ltda.

> O Sistema de Acompanhamento de Custódia 24 Horas (SAC24) é uma solução completa de hardware e software para monitoramento eletrônico de sentenciados concebido e desenvolvido pela *Spacecom*. (...) O juiz, ao determinar o monitoramento de um indivíduo, pode estabelecer áreas geográficas de inclusão ou exclusão. Caso o sentenciado saia da área de inclusão determinada, o sistema SAC24 gerará um alarme on-line à unidade prisional responsável pelo seu acompanhamento. (...) Os dispositivos estão equipados com sistemas contra fraudes e caso sejam abertos ou quebrados, no mesmo instante, sinais de alarme serão enviados para a unidade prisional e para a central de monitoramento responsável, alertando as autoridades. Perda de sinal de satélites GPS serão alarmados ao sentenciado, para que ele possa providenciar a alteração da sua posição. Caso o sentenciado tente se deslocar sem o sinal de satélites GPS, os dispositivos contam com um detector interno de movimento que gera um alarme para a unidade prisional e para a central de monitoramento responsável, indicando a tentativa de deslocamento sem o registro de posição geográfica. (...) A partir das informações geradas no sistema, a unidade prisional pode solicitar a expedição de mandados de prisão e assim que forem recapturados esses sentenciados, serão recolhidos em unidades prisionais de regime fechado (Spacecom, 2016).

Outubro de 2015

Centro de Progressão Penitenciária de Franco da Rocha, São Paulo

> Todos os dias da semana, Gustavo acorda às 6h, na cela 29 da galeria térrea do "Castelinho", como é conhecido o Centro de Progressão Penitenciária (CPP) de Franco da Rocha, situado na região metropolitana de São Paulo, onde o rapaz cumpre pena em regime semiaberto. Antes de sair para trabalhar, certifica-se de que a bateria de sua Unidade Portátil de Rastreamento (UPR) está devidamente carregada. Junto à tornozeleira acoplada ao seu corpo 24 horas por dia, a UPR compõe o sistema de monitoramento eletrônico que controla sua permanência no interior de uma*zona de circulação*, durante suas saídas diárias para realização de trabalho externo. O equipamento emite as informações relativas à sua localização para a Central de Monitoramento, via GPS, cujos sinais são transmitidos em tempo real através da rede de satélites que integra o sistema. O mais tardar, às 22h, Gustavo é esperado de volta ao Centro de Progressão Penitenciária. Aos domingos, impedido de deixar a unidade, toma dois comprimidos de ansiolítico e dorme em sua cela (Registro de campo elaborado em 20 de setembro de 2015).

Nos fragmentos acima, apresentamos três componentes de um mesmo dispositivo. O primeiro texto foi extraído da justificativa do Projeto de Lei do Senado Federal, PLS 175/2007, que culminou com a aprovação do monitoramento eletrônico de presos e presas no Brasil, no ano de 2010. Trata-se de uma das principais procedências jurídicas da Lei Federal 12.258/10, que autoriza o controle eletrônico de pessoas condenadas no país.

O segundo excerto encontra-se disponível no sítio eletrônico da empresa *Spacecom Monitoramento*, compondo a página de apresentação de seu sistema de rastreamento: SAC24. A *Spacecom* é a principal empresa brasileira fornecedora produtos e serviços de controle eletrônico penal, detendo 90% dos contratos firmados com as secretarias estaduais de justiça criminal e administração penitenciária ao redor do país.

Por fim, o terceiro fragmento foi produzido a partir de conversas realizadas em trabalho de campo, junto a Gustavo, preso em regime semiaberto no Centro de Progressão Penitenciária de Franco da Rocha e monitorado diariamente em suas saídas para realização de trabalho externo.

Estado, mercado e sujeito. São essas as três principais pontas a partir das quais se busca analisar, neste texto, a constituição dos dispositivos de monitoramento eletrônico de pessoas condenadas ou processadas pela justiça criminal no Brasil. Três vértices de um triângulo técnico-político conectado às atuais transmutações nos modos pelos quais o poder de punir é exercido e racionalizado.

ACOPLAMENTOS

Em junho de 2010, o chamado monitoramento telemático[1] de pessoas condenadas criminalmente foi legalmente autorizado pela primeira vez no Brasil, por meio da Lei Federal nº 12.258, que alterou a Lei de Execuções Penais (7.210/1984). O texto definiu que em casos de saída temporária no regime semiaberto de cumprimento de pena, ou na aplicação de prisão domiciliar, o juiz poderá determinar a "utilização de equipamento de vigilância indireta pelo condenado" (caput). Via de regra, a modalidade passou a ser executada mediante o uso de tornozeleiras eletrônicas rastreadas via sistema de posicionamento global (GPS) e rede de comunicação celular (GPRS). Violações tais como a remoção do aparelho ou afastamento das zonas pré-determinadas como *áreas de inclusão* acarretariam na regressão do regime, revogação da saída temporária, revogação da prisão domiciliar ou advertência (Art. 146-C).

Menos de um ano depois da aprovação do monitoramento eletrônico de sentenciados no país, as possibilidades de aplicação da medida foram ampliadas para fiscalização de liberdade provisória, concedida a indivíduos que aguardam julgamento. Autorizada em maio de 2011, a chamada nova Lei das Cautelares (Lei Federal nº 12.403) alterou o Código de Processo Penal, prevendo no inciso IX do Artigo 319, a "monitoração eletrônica" como medida cautelar, podendo ser aplicada de maneira cumulativa com demais medidas cautelares, tais como a "proibição de acesso ou frequência a determinados lugares" (Art. 319, inciso II) e "recolhimento domiciliar no período noturno ou nos dias de folga" (Art. 319, inciso V).

Desse modo, o controle eletrônico pode ser aplicado no Brasil como forma de fiscalização do cumprimento de pena no regime semiaberto e prisão domiciliar, ou para controle de medidas processuais, determinadas antes da sentença condenatória.

De maneira geral, os discursos de operadores de justiça criminal e gestão penitenciária que justificam o uso de sistemas de controle eletrônico para supervisão penal enfatizam o propósito de redução da superpopulação carcerária do país, bem como a economia de recursos propiciada pela medida, quando comparada à pena de detenção. Desde os primeiros projetos de lei que visavam a autorização do monitoramento, as finalidades apregoadas à medida referem-se à possibilidade de substituição do cárcere pelo rastreamento em meio aberto.

Entretanto, o acompanhamento dos dados penitenciários indica que a medida não tem apresentado impactos no sentido de contribuir para a redução da quantidade de pessoas encarceradas. O

Sistema Integrado de Informações Penitenciárias do Departamento Penitenciário Nacional (DEPEN), aponta que em 2009 a população carcerária brasileira era de 469.546 indivíduos (DEPEN, 2016). Já em junho de 2014, cerca de quatro anos após a promulgação da lei que autorizou o controle eletrônico de condenados no país, os dados do InfoPen apontam para um total de 607.731 pessoas encarceradas (DEPEN, 2017), perfazendo a quarta maior população prisional do planeta. A quantidade absoluta de presos não parou de crescer e a taxa de indivíduos trancados nas unidades prisionais brasileiras relativamente à população total do país apenas aumentou. Se em junho de 2009 havia cerca de 248 presos por 100 mil habitantes no Brasil, em junho de 2014 essa taxa chegou a mais de 299.

Simultaneamente, os programas de monitoramento eletrônico se desenvolveram rapidamente no país. Em dezembro de 2015, cinco anos após a aprovação da medida, cerca de 18.172 pessoas já estavam monitoradas no Brasil, de acordo com o DEPEN. O país já possui centrais de monitoramento instaladas em 19 Unidades da Federação, sendo que em 17 delas os serviços encontram-se implementados e em 2 unidades estão em fase de testes.

A evolução da política de monitoramento remoto, concomitante ao incremento da população carcerária, indica um processo já avançado de dilatação do sistema penal brasileiro, marcado pelo duplo movimento de *ampliação* e *intensificação* de controles punitivos. De um lado, a profusão de medidas penais em meio aberto no Brasil, ao contrário de favorecer um suposto processo de desencarceramento, tem submetido indivíduos que cometeram pequenas infrações, cuja insignificância não justificaria a prisão, a uma supervisão penal além-muros, conectada ao que Loïc Wacquant (2001) chama de "expansão horizontal do sistema penal" – cresce a população submetida à tutela penal em meio aberto, simultaneamente ao incremento da população encarcerada. De outro lado e no mesmo sentido, os dispositivos de rastreamento telemático conferem um controle suplementar, georreferenciado e ininterrupto sobre os deslocamentos de indivíduos em regimes aberto e semiaberto, intensificando a supervisão sobre eles exercida.

Anunciado como ferramenta de redução da calamitosa situação carcerária brasileira, o controle eletrônico de indivíduos condenados ou processados pela justiça criminal no país tem sido empregado como técnica adjacente à prisão, estabelecendo com o cárcere relações de conexão e complementaridade. Mais do que um substituto, o monitoramento remoto é *anexado* à instituição prisional, estendendo seus limites para além dos muros e conferindo novos horizontes às estratégias de controle punitivo, mediante a modulação paradoxal da liberdade monitorada.

Desse modo, a aplicação do rastreamento de presos e presas estabelece novos aspectos e dinâmicas às práticas de controle penal, vinculadas às atuais transfigurações do *panoptismo* e concebidas por uma nova arquitetura da vigilância. Não se trata de mera reprodução da máquina benthamiana de inspeção intramuros, cujo olhar supervisor partia de um ponto fixo e central (Bentham, 2008; Foucault, 1987). Os novos dispositivos de controle expressam alguns dos aspectos de uma sociedade ordenada por sistemas de gerenciamento e detecção de fluxos, que extrapolam os espaços de confinamento, compondo tecnologias de vigilância a céu aberto.

ANEXOS VIRTUAIS

Desenvolvido pela empresa *Spacecom Monitoramento*, o Sistema de Acompanhamento de Custódia 24 horas (SAC24), é hoje o principal mecanismo utilizado para monitoramento eletrônico de pessoas condenadas ou processadas no Brasil, tendo sido adotado em 17 diferentes estados. Com a recente expansão do mercado de sistemas eletrônicos de controle penal no país, a *Spacecom* cresceu 296% entre 2011 e o fim de 2015, detendo quase a totalidade dos contratos estabelecidos com as administrações penitenciárias estaduais (Sanches, Souto e Dantas, 2016).

O SAC24 é composto por uma tornozeleira eletrônica e um software de monitoramento instalado em uma central. A tornozeleira permanece 24 horas por dia acoplada ao corpo da pessoa monitorada, emitindo sinais de localização via GPS e GPRS. O aparelho é à prova d'água e revestido por fibra ótica para que se detectem possíveis danos ou tentativas de rompimento. As informações de geoposicionamento são transmitidas aos servidores da *Spacecom* e disponibilizadas em interface web às Centrais de Monitoramento geridas pelas secretarias estaduais de administração penitenciária e justiça criminal. Todas as centrais devem contar com servidores da *Spacecom* que prestam auxílio técnico e serviços de manutenção do sistema. A empresa possui, ainda, uma central instalada na cidade de Curitiba, no Paraná, de onde são prestados os serviços de apoio às centrais estaduais espalhadas pelo país. Informações sobre a identidade do indivíduo monitorado, crime cometido e regime de cumprimento de pena ou medida processual são restritas às centrais estaduais.

O software do sistema possibilita a visualização, em tempo real, dos trajetos percorridos pelos indivíduos monitorados. O aplicativo permite a criação de *áreas de inclusão*, no interior das quais a pessoa monitorada deve permanecer, e *áreas de exclusão* que não devem ser penetradas. O SAC24 prevê o acionamento de alarmes digitais no software, caso sejam detectados afastamentos das *áreas de inclusão*, infiltração em *áreas de exclusão*, danos ao aparelho, rompimentos ou descarga de bateria. Cada ocorrência emite um alerta à central, especificando-se o tipo de violação. A pessoa monitorada, por sua vez, é alertada por meio de alarmes sonoros, luminosos e vibratórios emitidos pelo aparelho. Problemas técnicos e descumprimentos das condições fixadas em decisão judicial – tais como recolhimento domiciliar noturno e em finais de semana ou proibição de acesso a determinados lugares – podem gerar relatórios que deverão ser reportados ao juiz, que decidirá sobre a manutenção da medida ou regressão ao regime fechado.

Desse modo, os nexos entre as práticas de rastreamento penal e a prisão propriamente dita são reafirmados mediante a ameaça de regressão de regime. O confinamento permanece como horizonte a ser evitado e condição de aplicação do controle eletrônico em meio aberto, já que é a iminência ou a virtualidade do cárcere que deve garantir o cumprimento das regras impostas judicialmente, relativas ao itinerário e *zonas de circulação* do indivíduo monitorado. É nesse sentido, portanto, que o monitoramento telemático figura como *anexo virtual* – dispositivo inserido no complexo maquínico formatado pelo sistema penal, gravitando em torno de seu eixo principal constituído pela prisão-prédio, fixada como possibilidade permanente.

Entretanto, a transposição e redefinição dos procedimentos de controle punitivo para além dos limites institucionais extravasa os modelos austeros e já arcaicos de castigo e correção de desvios em espaços murados. A ultrapassagem do aparelhamento disciplinar é efetivada, em grande medida, por um movimento de desterritorialização das técnicas de vigilância (Bogard, 2006). Todavia, a efetivação das práticas de monitoramento remoto opera e exige a reterritorialização da supervisão penal no interior de perímetros pré-programados. O controle passa a ser exercido sobre pontos móveis que percorrem circuitos relativamente flexíveis cuja constrição espacial é detalhadamente modulável e programável para cada caso em particular. O alvo de inspeção é circulatório e é precisamente a sua circulação que se torna objeto de governo.

De maneira correlata, os novos inspetores caracterizam-se pelo hibridismo das parcerias público -privadas, exigindo-se um trabalho conjunto e compartilhado entre as agências penitenciárias do Estado e a estrutura tecnocrática fornecida pela iniciativa privada. O mercado da punição entra em cena como parceiro indispensável ao governo dos trajetos. Com ele, a demanda e necessidade de ampliação do público consumidor da pena é introjetada como condição de desenvolvimento e sustentação de uma indústria do castigo em ascensão. O impulso ao mercado de sistemas eletrônicos de controle do crime depende, nessa medida, da produção de condenados em larga escala.

O CARCEREIRO DE SI MESMO E O CORPO MARCADO

Em 2012, Gustavo[2] foi enquadrado no Art. 33, §4º, da Lei 11.343/2006, após ter sido flagrado com êxtase e cocaína em uma boate na região central de São Paulo, por agentes do Departamento Estadual de Prevenção e Repressão ao Narcotráfico (DENARC). Condenado a 5 anos e 10 meses de prisão, com regime inicial fechado, hoje ele trafega entre o *dentro* e o *fora* dos muros prisionais, portando a tornozeleira que compõe o Sistema de Acompanhamento de Custódia 24 horas, desenvolvido pela *Spacecom*.

O acompanhamento que realizei durante as saídas monitoradas de Gustavo para a realização de trabalho externo, bem como as conversas durante os encontros com meu interlocutor, permitem delinear algumas considerações a respeito dos processos de subjetivação implicados pelo monitoramento eletrônico como técnica de controle penal. De um lado, a experiência de Gustavo é analisada como ponto de incidência e componente de uma tecnologia de poder – ponto vivo, biológico, corpóreo, conectado aos elementos técnicos e viabilizando a conformação de um *agenciamento maquínico* (Deleuze & Guattari, 2014).[3] De outro, sua trajetória de institucionalização e rastreamento é tomada como fio condutor para a compreensão de novas estratégias de *condução das condutas* (Foucault, 2008) e as racionalidades às quais obedecem e retroalimentam.

Nossas conversas evidenciaram pouco a pouco o desespero de Gustavo diante da alternância entre os efeitos do encarceramento e a sensação de perseguição contínua provocada pelo monitoramento remoto. Ao lado da experiência carcerária, as saídas rastreadas pareciam operar decisivamente no processo produtivo de sua aflição. *"Eu tô na rua, mas eu tô preso, monitorado,*

parece que tem um guarda do meu lado o tempo todo, em toda a esquina, me olhando em cada canto. Tô no meu limite", afirma. Não é fortuito, portanto, que Gustavo recorra semanalmente a psicofármacos, mesmo sem diagnóstico clínico.

Os efeitos produzidos pela contínua e ininterrupta sensação de vigilância e controle suscitam a presença do vigia onde quer que ele esteja. "*Um guarda na entrada do meu trabalho, outro na porta do banheiro, outro na rua e outro dentro minha casa*". O olhar vigilante se acopla ao seu corpo e converte-se em parâmetro para a condução individual de sua própria conduta, conectando o monitoramento eletrônico às atuais práticas de vigilância empregadas em nome das liberdades de escolha e expressões da individualidade (Lyon, 2006: 6).

Gustavo torna-se o gestor de sua própria pena, tal como aspira o paradigma neoliberal da responsabilização individual. O sujeito neoliberal, produtor e consumidor das escolhas que faz, deve assumir os riscos e responsabilidades de suas atitudes, balanceando sua liberdade com a segurança de uma conduta correta na execução penal. O chamado criminoso passa a ser "subjetivado como sujeito livre, autônomo e racional" (Hamann, 2012) que avalia a incerteza dos riscos de ter que pagar um preço na forma de regressão de regime diante dos possíveis benefícios do descumprimento das condições judicialmente impostas.

Nessa chave, o vigia confunde-se com o vigiado, fazendo do sentenciado uma espécie de *carcereiro de si mesmo*. Eis o modelo panóptico reconfigurado e redimensionado a níveis impensáveis à distopia benthamiana. Do lado de dentro dos muros institucionais, Gustavo tranquiliza-se por meio de pílulas psiquiátricas, substâncias que amenizam a dor e o sofrimento decorrentes da própria dinâmica de funcionamento da máquina penal, mas também os efeitos encarceradores que, curioso notar, são produto de uma pretensa liberdade, constantemente rastreada.

Outras questões reiteradas durante os encontros com Gustavo levantaram referem-se à marca atada ao corpo mediante a fixação de um equipamento que remete infalivelmente à prisão e à condição de prisioneiro. "*Sinto muita vergonha de mostrar o aparelho. Mesmo perto de casa, nas saidinhas,*[4] *sempre fico de calça*", dizia. Em conversas que realizamos com algumas mulheres submetidas ao monitoramento eletrônico durante as saídas do Centro de Progressão Penitenciária do Butantã, situado também na cidade de São Paulo, o *corpo marcado* também fora objeto de discussão e destaque. Não raro foram os depoimentos sobre os efeitos da visibilidade da 'pulseira' que chagava a atrair policiais e agentes de segurança privada nos bairros e estabelecimentos comerciais em que freqüentavam.

Por outro lado, alguns depoimentos colhidos em unidades prisionais da capital paulista indicaram diferentes usos e agenciamentos dessa mesma visibilidade, operados por integrantes das assim chamadas "facções criminosas". Conforme me foi relatado, os membros do Primeiro Comando da Capital (PCC) determinaram que aqueles que pertenciam ao grupo utilizariam a tornozeleira na perna direita, enquanto os membros da "oposição", colocariam o aparelho na perna esquerda. Dessa maneira, o equipamento seria uma forma de autoidentificação e afirmação da identidade

no interior de um grupo específico.

Mais do que um estigma, instrumento social de aniquilação da identidade (Goffman, 2013), o *corpo marcado* sinaliza a produção ativa de identidades específicas, associadas, nesse caso, a grupos considerados criminosos que disputam o controle econômico e político de espaços prisionais e territórios urbanos em diversas partes do Brasil.

Dessa maneira, a análise dos efeitos políticos e dos processos de subjetivação produzidos por novos dispositivos de controle e monitoramento exige um olhar específico que atente para as formas pelas quais indivíduos e populações, inseridos nos mais diversos contextos sociais, se adéquam e se ajustam às metamorfoses da máquina penal.

NOTAS

* Doutorando no Programa de Pós-Graduação em Sociologia da Universidade de São Paulo (PPGS-USP). Mestre em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Correio eletrônico: campello.ricardo@gmail.com

1. A comunicação telemática reúne tecnologias de transmissão de dados à distância possibilitadas pela interconexão entre os recursos disponibilizados pelas telecomunicações, a informática e a engenharia eletrônica (Telematics.com, 2016).

2. Nome fictício.

3. Em Deleuze e Guattari, "jamais uma máquina é simplesmente técnica. Ao contrário, ela só é técnica como máquina social, tomando homens e mulheres em suas engrenagens, ou, antes, tendo homens e mulheres dentre suas engrenagens, não menos que coisas, estruturas, metais, matérias. O que faz máquina, falando propriamente, são as conexões" (Deleuze & Guattari, 2014: 147).

4. São chamadas de "saidinhas" as saídas temporárias no regime semiaberto em ocasiões de comemorações de final de ano, dia das mães, dia das crianças, páscoa e dia dos pais.

REFERÊNCIAS

BENTHAM, J. (2008). *O Panóptico*. Belo Horizonte, Brasil: Autêntica Editora.

BOGARD, W. (2006) Surveillance assemblages and lines of light. En D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond*. (pp. 97-122). Portland, United States of America: Willian Publishing.

BRASIL. (2007) *Projeto de Lei No175 de 2007*. Brasília, Brasil: Senado Federal.

DELEUZE, G., y GUATTARI, F. (2014). *Kafka: por uma literatura menor*. Belo Horizonte, Brasil: Autêntica Editora.

DEPEN. (2016). *Sistema Integrado de Informações Penitenciárias*. Recuperado de: http://www.justica.gov.br/noticias/mj-divulgara-novo-relatorio-do-infopen-nesta-terca-feira/relatorio-depen-versao-web.pdf

FOUCAULT, M. (1987). *Vigiar e punir: nascimento da prisão*. Petrópolis, Brasil: Vozes. (2008). *Nascimento da biopolítica*. São Paulo, Brasil: Martins Fontes.

GOFFMAN, E. (2013). *Manicômios, prisões e conventos*. São Paulo, Brasil: Perspectiva.

HAMANN, T. (2012). Neoliberalismo, governamentalidade e ética. *Revista Ecopolítica*, 3, 99-133.

LYON, D. (2006). The Search for Surveillance Theories. En D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond* (pp. 3-20). Portland, United States of America: Willian Publishing.

SPACECOM. (2016). *Sistema SAC24.* Recuperado de: http://spacecom.com.br

SANCHES, M., SOUTO, L., y DANTAS, T. (2016). *Uso de tornozeleiras eletrônicas dispara e mercado cresce quase 300%*. Recuperado de: http://oglobo.globo.com/brasil/uso-de-tornozeleiras-eletronicas-dispara-mercado-cresce-quase-300-19637514

TELEMATICS.COM (2016). *Welcome to Telematics.com.* Recuperado de: http://www.telematics.com/

WACQUANT, L. (2001). *As prisões da miséria*. Rio de Janeiro, Brasil: Jorge Zahar.

EJE 4

LA SEDUCCIÓN DEL NÚMERO: DECISIONES BASADAS EN ALGORITMOS Y BIG DATA

SEGURANÇA PREDITIVA? A INCORPORAÇÃO DE TÉCNICAS DE MINERAÇÃO DE DADOS E PERFILIZAÇÃO EM CONFLITOS INTERNACIONAIS COM DRONES PELOS EUA E EM PRÁTICAS DE VIGILÂNCIA PELA POLICIA MILITAR DO ESTADO DE SÃO PAULO

Resumo: Com o desenvolvimento de novas tecnologias de comunicação, processamento e gerenciamento de dados, cada vez mais o acesso privilegiado à informação torna-se central para as estratégias de segurança pública e internacional. Um exemplo disso são os Drones, cuja capacidade de coleta massiva de dados, e associação à técnicas de perfilização geográfica, tem autorizado assassinatos extrajudiciais no exterior. De modo semelhante, o governo do estado de São Paulo tem implementado um sistema de vigilância que potencialmente permite prisões e autuações antecipativas. Nosso objetivo apresentar a ascensão desse novo tipo de paradigma militar e de segurança pública, que provisoriamente podemos definir como "segurança preditiva". Debateremos algumas hipóteses de problematização desse dispositivo forma de governamentalidade, à luz dos Estudos de Vigilância, dos Estudos sociais da Ciência e da Tecnologia e em certa medida da Sociologia da Punição. Assim, a tônica geral da nossa problematização é que esse dispositivo de "segurança" se orienta a legitimar práticas excessivas em ambientes de guerra, e em contextos urbanos da guerra global ao terror. No entanto, como concluiremos, um estudo mais detalhado exigirá a compreensão de como se estruturam os algoritmos que sustentam esse dispositivo e práticas.

Palavras Chave: Big data, Vigilância, Drones, Detecta, Segurança preditiva.

ALCIDES EDUARDO DOS REIS PERON*

Seguridad Predictiva? La incorporacion tecnicas de Minería de datos y Perfilizacion em Conflictos Internacionales com Drones por los EE.UU. y em practicas de Vigilancia por la Policia Militar de São Paulo

Resumen: Con el desarrollo de nuevas tecnologías de la comunicación, procesamiento y gestión de datos, cada vez más el acceso privilegiado a la información es central para las estrategias de seguridad pública e internacionales. Un ejemplo son los aviones no tripulados (drones), cuya capacidad de recogida de datos en masa, asociado a técnicas de perfilizacion geográfica, ha autorizado a las ejecuciones extrajudiciales. Del mismo modo, el gobierno del estado de Sao Paulo se ha implementado un sistema de vigilancia que potencialmente permite a las detenciones y multas a futuro, el Detecta. Nuestro objetivo es presentar el surgimiento de este nuevo tipo de paradigma de seguridad militar y pública, al cual podemos definir provisionalmente como "seguridad predictiva." Vamos a discutir algunas hipótesis que cuestionan esta forma el dispositivo de gubernamentalidad, a la luz de los estudios de vigilancia, estudios sociales de la ciencia y la tecnología, y en cierta medida, la sociología del castigo. De este modo, el tono general de nuestra problemática es que este dispositivo "seguridad" está orientada a legitimar prácticas excesivas en los entornos de guerra, y los contextos urbanos de la guerra global contra el terrorismo. Sin embargo, como vamos concluir, un estudio más detallado requerirá una comprensión de cómo se estructuran los algoritmos que apoyan este dispositivo y prácticas.

Palabras Clave: Big data, Vigilancia, Drones, Detecta, Seguridad preditiva.

Predictive Security? The incorporation of Data Minning and Profiling techniques in International Conflicts with Drones by the U.S. and Surveillance Practices by São Paulo's Military Police

Abstract: From the development of new communication, process and data management Technologies, the privileged access to information increasingly becomes central to the public and international security strategies. One example is the Drone warfare, whose massive data collection, and association to profiling techniques, is "legitimizing" extrajudicial killings overseas. Similarly, the government of São Paulo is implementing a surveillance system that potentially allows anticipative imprisonments. Our objective then is to present the ascension on this new military and public security paradigm, which provisionally we could name as "Predictive security". We will debate, then, some hypothesis of this dispositive and new form of governmentality through the Surveillance Studies, Social Studies of Science and Technology and in certain way, Sociology of the Punishment. The general tone of our problematics is the idea that this dispositive of security seeks to legitimize excessive practices in war and urban global war on terrorism environments. However, as we will conclude, a more detailed study will demand th comprehension of the development and controversies around the algorithms that sustains this practices.

Key-Words: Big data, Surveillance, Drones, Detecta, Predictive security.

INTRODUÇÃO

Com o desenvolvimento de novas tecnologias de comunicação, processamento e gerenciamento de dados, cada vez mais o acesso privilegiado à informação torna-se central para as estratégias de segurança pública e internacional. Um exemplo disso é o emprego de Drones Militares armados, como peça chave para a estratégia estadunidense de combate ao terrorismo no Oriente Médio. De modo semelhante, o governo do estado de São Paulo contratou da empresa *Microsoft* um sistema de vigilância que permite o processamento de imagens através das câmeras de monitoramento, recolhendo dados e informações que podem substanciar prisões e autuações antes mesmo que se consubstancie um crime.

Em ambos os casos, observamos a constituição de um novo conceito, que provisoriamente podemos nomear como de "Segurança Preditiva", apoiada em dispositivos de vigilância associados à técnicas de automatização do processamento de dados. Assim, nosso objetivo aqui é apresentar

uma proposta de trabalho que explore a identidade entre uma ascendente prática militar e de segurança pública. Buscaremos, assim, apresentar algumas hipóteses de problematização à luz dos Estudos de Vigilância, dos Estudos sociais da Ciência e da Tecnologia, e em certa medida da Sociologia da Punição. A tônica geral da nossa problematização é que essa forma de "segurança" se orienta a legitimar práticas excessivas em ambientes de guerra, e em contextos urbanos de guerra ao terror, no entanto, como observaremos, paulatinamente elas estariam fundamentando no campo da segurança pública, algo que suscitará algumas hipóteses.

DRONES, *TOTAL INFORMATIONAL AWARENES*, E ASSASSINATOS EXTRAJUDICIAIS

Desde 2004 a Força Aérea estadunidense (USAF) e a Agência Central de Inteligência (CIA) vem conduzindo operações de Assassinatos Extrajudiciais com Drones armados, como ações de contra insurgência em países como Paquistão, Iêmen e Somália. Por si só, esses atos já se caracterizam ilegais, uma vez que atentam contra a soberania de países não implicados formalmente em nenhum conflito, atuando contra pessoas não diretamente engajadas em conflitos armados, como explica Alston (2010).

Priorizando esse tipo de tecnologia, o *DoD* então orquestra a transição dos antigos sistemas de comando e controle em sistemas de Comando, Controle, Computação, Comunicação, Informação, Vigilância e Reconhecimento, denominado C4IRS. Os conflitos agora se centrariam na obtenção de informações e reconhecimento das posições inimigas, através de uma sorte de instrumentos conectados em rede – tudo isso realizado à distância, denominando-se como *Network Centric Warfare* (Cebrowsky, 2000) – permitindo a partir de várias unidades agindo em rede, ações cirúrgicas e rápidas – base da doutrina de *Shock and Awe* (rapidez e reconhecimento) (Albert e Hayes, 2003).

Nesse contexto, a RAM ao introduzir as TICs como uma nova base tecnológica dos armamentos dá a possibilidade para o surgimento, por um lado, de uma nova doutrina de operações militares na qual o acesso a informação passa ser a determinante para o seu sucesso, mas por outro lado, também cria uma nova dimensão de atuação das Forças Armadas em que o controle a disseminação e a destruição da informação tornam-se a dinâmica própria das operações. Emerge então uma nova modalidade de conflito, a "guerra informacional". Bellamy (2001:61) faz uso de uma definição ampla para compreender a Guerra Centrada em Rede: dividida em três partes distintas, a guerra informacional é uma "administração da percepção", quando a informação é a mensagem; ela é destruição de sistemas, quando a informação é um meio; e por fim, ela é exploração da informação, quando esta é o alvo.

Assim, em um determinado momento, como expõe Bellamy (2001), caracterizado por uma Guerra de Comando e Controle (C^2 Warfare) a intenção é o desenvolvimento de operações militares no contexto de C4ISR, capazes de destruir a infra-estrutura de C^2 do inimigo por meio de equipamentos eletrônicos, garantindo a primazia no combate. Por sua vez a *Software Warfare* seria um combate travado no campo de fluxo de dados computacionais com o objetivo

de atingir as capacidades inimigas, neutralizando-as e assim alcançando uma supremacia no combate físico.

A informação, então, torna-se o meio e o fim de grande parte das operações militares, seja pelo seu controle, seja pela posse de informações privilegiadas para elaborar o reconhecimento do território, antevendo-se aos ataques inimigos, e tornando mais precisos.

Sabemos que os Assassinatos Extrajudiciais realizados com Drones se organizam de duas formas. Em primeiro lugar, através de Assassinatos Seletivos (*Targeted Killing*), em que as operações estariam orientadas para eliminar alvos muito específicos, e fariam uso de oficiais de inteligência em campo, bem como de dados coletados a partir da triagem de imagens realizadas pelos Drones, obtidos com rastreamento de celulares, dentre outros. Nesse caso, sabe-se o nome e a localização dos sujeitos, e como descreve O'Connel (2009) existem advogados e especialistas em direito internacional e de guerra presentes durante a autorização dos ataques, que julgam se as provas existentes seriam suficientes para realizar ataques que culminem na eliminação de suspeitos.

Um outro método seria o de Assassinatos por Assinatura de Calor (*Signature Killing*). Nesse caso, como expõe Chamayou (2013), a visualização de "alvos" através das câmeras infravermelho, identificando os corpos enquanto sinais de calor, formam arquivos de imagens, que cruzadas com informações sobre geolocalização, dados telefônicos a partir do rastreamento de "chips", constroem o que é chamado de padrões de vida, ou de comportamento. Essas são informações que podem ser cruzadas para compor os padrões considerados "suspeitos", e com isso legitimar o assassinato de alvos à distância. Segundo Chamayou (2013: 72-73), a análise dos padrões de vida ocorre a partir de uma fusão entre a análise de conexões e geoespacial, uma cartografia conjunta do social, em um local e num espaço temporal. Nesse sentido, assim que um alvo potencial é designado, se inicia uma investigação sobre ele. Recolhem-se dados telefônicos e de outras ordens, que passam a ser associados ao o movimento registrado pela leitura de calor das câmeras do *VANT*. Criam-se, assim, pontos nodulares destinados a construir um diagrama que compõe um arquivo sobre o seu padrão de vida e sua estrutura de relacionamentos.

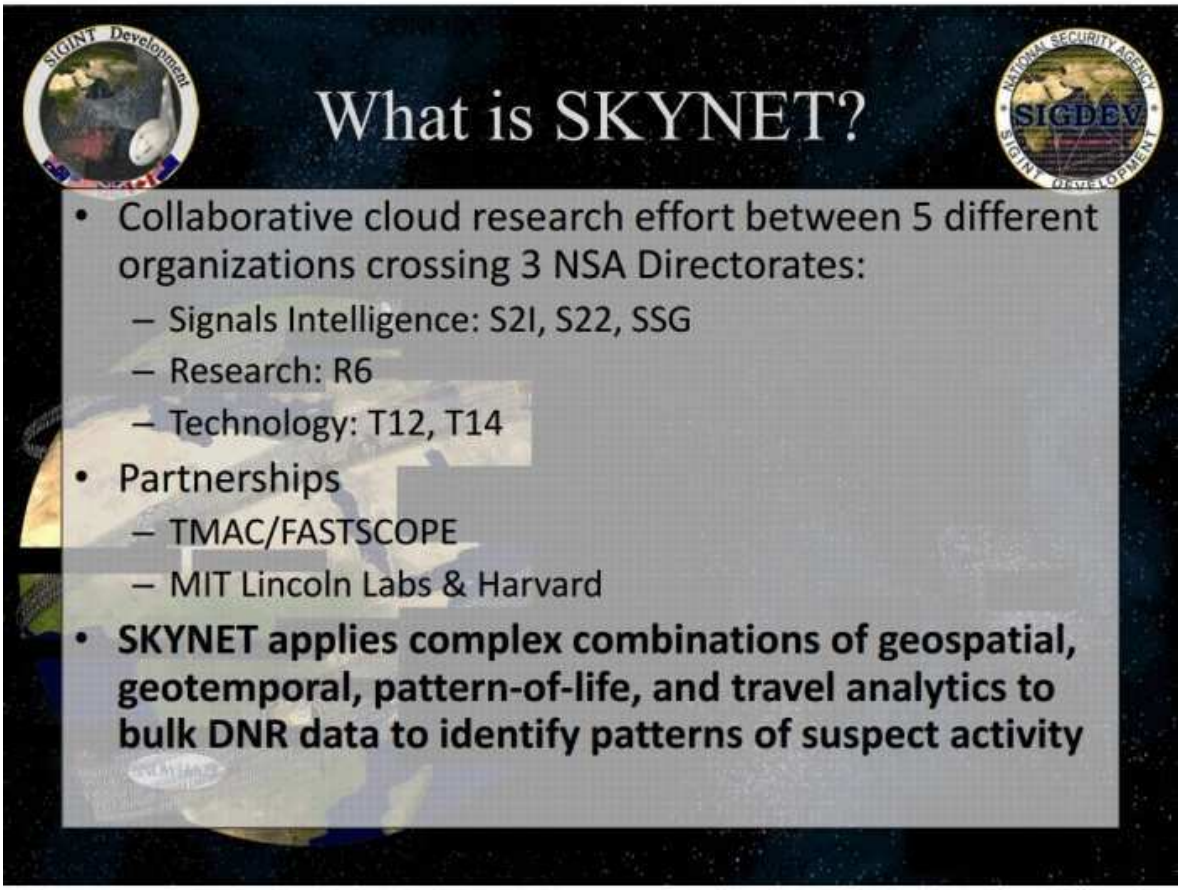
Nesse mesmo período, a *National Security Agency* (NSA), passa a incorporar novos dispositivos de vigilância massiva de dados, tornando-se um dispositivo fundamental de inteligência para a realização de operações militares "encobertas". A atividade central da NSA seria coletar informações de indivíduos de forma massiva, possibilitando aos líderes militares, políticos, e tomadores de decisão, o reconhecimento dos potenciais inimigos e ameaças, suas ações e planos, de forma a tomarem decisões preventivas adequadas (NSA, 2016).

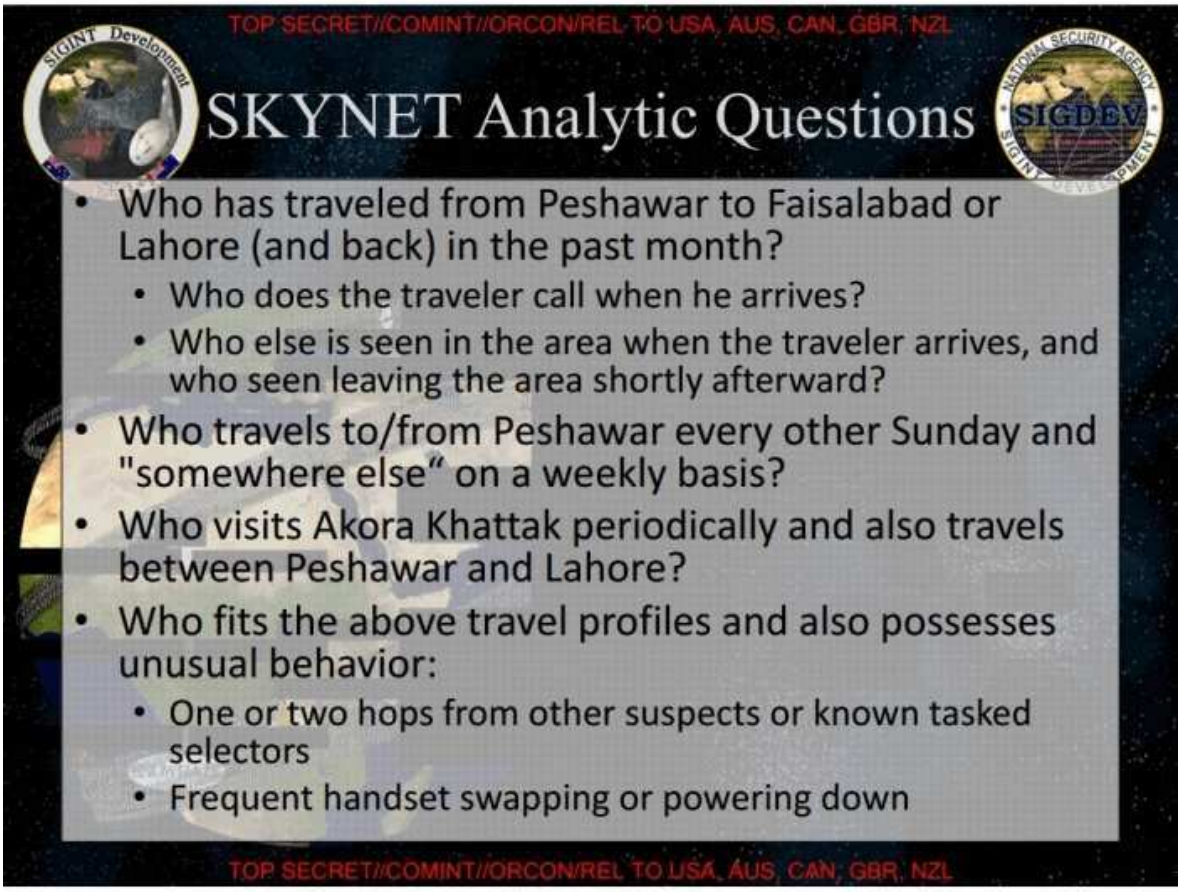
É nesse espírito que se desenvolve o *Total Information Awarness Program* (Mack, Beeb & Wenzel, 2002), pela DARPA, que visa a construção de arquitetura, processos e tecnologias com vias a permitir a coleta e triagem massiva de informações e dados. Não tarda para que militares a agentes de inteligência desenvolvam técnicas e conceitos que permitam o uso desses dados para a operacionalização de suas missões. Com a coleta massiva de dados, e triagem algorítmica, um exemplo pode ser o conceito operacional que Força Aérea dos EUA desenvolve a partir de então,

é o *Predictive Battlespace Awereness*, que pode ser entendido como "(...) o conhecimento do ambiente operacional que permite o comandante e seu pessoal antecipar corretamente condições futuras, acessar condições em mudança, estabelecer prioridades, e explorar oportunidades emergentes enquanto mitiga o impacto de ações adversárias não esperadas" (Piccerillo & Brumaugh, 2004)

Em um recente "vazamento" de informações sobre como se operam esses Assassinatos por Assinatura, a agência de jornalismo investigativo *The Intercept* (2015) revelou que um sistema desenvolvido para o cruzamento de dados obtidos pelos Drones, *Skynet*, é capaz de angariar dados para a construção de padrões de vida a partir de dados produzidos por redes sociais. Essas informações seriam cruzadas tanto com as imagens, como com os padrões de movimento dos alvos, construindo assim padrões aparentemente suspeitos. As imagens abaixo, extraída de documentos oficiais da Agência de Segurança Nacional (*NSA*), revelam brevemente as intenções desse sistema, e as dinâmicas mapeadas.

FIGURA 1:
Slides explicativos dos métodos do sistema Skynet





Fonte: The Intercept (2015)

Assim, os Drones que foram desenvolvidos exclusivamente para vigilância e monitoramento para a USAF e CIA, no momento que são armados, se integram a uma extensa cadeia de comunicação, constituída por pessoas, instrumentos e instituições. Nesse âmbito, são desenvolvidos sistemas capazes de coletar e cruzar dados massivos sobre o comportamento das pessoas observadas. A despeito do caráter panóptico dos drones, monitorando de forma constante e persistente regiões do globo, disciplinando o corpo social a funcionar de maneira ordenada e útil, a adoção de técnicas de mineração de dados (*data minning*) e perfilização (*profiling*), permitem uma nova forma de visualizar os alvos, não apenas mirando o indivíduo, mas como atesta Kanashiro (2016), olha para o fluxo de dados e metadados produzidos por eles. De certa forma, esses metadados, aliados a uma forma de visualização, monitoramento e eliminação, têm potencial de autorizar e manifestar ações preditivas, assumindo o status de evidências de comportamentos suspeitos, até mesmo culpados.

Não seria exagero afirmar, assim, que se inaugura uma prática de segurança, que tem em um saber estatístico-punitivo, o principal pilar para fundamentar ataques e Assassinatos Extrajudiciais. A essa prática, fundamentada por uma sorte de conceitos operacionais maturados da RAM,

podemos denominar como "dispositivo de segurança preditiva", o qual se caracterizaria por um conjunto heterogêneo de práticas, instrumentos e saberes orientados a detectar comportamentos discrepantes e "nocivos", e perfilá-los de forma a atualizar o risco potencial do sujeito, possivelmente autorizando (ou ao menos legitimando) sanções preemptivas. O elemento central dessa prática, ao nosso ver, está na relação temporal e estruturante com as ideias de prevenção e preempção. Enquanto no primeiro caso, o ato se dá como uma precaução diante de uma hipótese de ação de uma outra parte, o segundo se organiza em torno de provas, evidencias "sólidas" que sustentem uma ação antecipatória – legal e prevista na normativa internacional, em alguns casos. No entanto, em ambas as situações, a produção de justificativas para a realização dos atos se organiza a partir do olhar sobre as experiências passadas, evidencias estáticas e opacas, como discursos, movimentos táticos e políticos: O olhar sobre o passado se torna a justificativa presente para os ataques. De modo distinto, o saber estatístico-punitivo olha para o passado e para presente para a conformação das hipóteses de futuro, transformando riscos hipotéticos em "sólidas" evidencias que sustentam os ataques antecipativos: É o olhar assertivo para um futuro certo que condiciona as ações presentes.

Não à toa, o saber preditivo está em perfeita consonância com as ações supostamente "preemptivas" estadunidenses no imediato pós 11 de setembro, contra Estados e organizações inimigas, ampliando descomunalmente o seu escopo de projeção de poder.

O DETECA E O DISPOSITIVO DE POLICIAMENTO PREDITIVO

Em um outro contexto, em setembro de 2014, aparentemente apartado da dimensão internacional e de guerra, o governador de São Paulo, Geraldo Alkmin, anuncia uma parceria com a *Microsoft* e a cidade de Nova Iorque para contratação de um sistema de monitoramento e análise de dados para auxílio das operações policiais do Estado de São Paulo. Denominado Detecta, o sistema é uma adaptação do *Domain Awareness System,* da polícia de Nova Iorque, profundamente imerso em um discurso de emprego de alta tecnologia para combate aos problemas de segurança pública da cidade e do estado (Geraldo, 2014). Segundo a PRODESP, o Detecta seria um sistema baseado em um "complexo algoritmo de processamento e em regras de negócios parametrizáveis" que permitiria "uma correlação das bases de dados com as informações dos sensores e assim emitir alertas" (Beraldo, 2015: 34).

Via de regra, o Detecta possui tanto as funcionalidades de sistemas de leitura imagética algorítimica que permitem a produção de dois tipos de alertas, os "Inteligentes" e os "Analíticos", bem como a funcionalidade coleta massiva de dados, construindo bases de dados de geo-referenciamento para o policiamento preditivo. Aqui, nos interessam os "Alertas analíticos", os quais baseiam-se em perfis de comportamentos "suspeitos" desenvolvidos pela Polícia Militar em parceria com a PRODESP, para o reconhecimento de condutas através das câmeras. De acordo com a Secretaria de Segurança Pública, a intenção é ampliar o leque de perfis compreendidos como suspeitos para além de atividades relacionadas ao transito, cruzando informações de bancos de dados de outras instituições, como o Fotocrim (Secretaria, 2015a).

No que tange a segunda funcionalidade desse sistema, observa-se a sua capacidade de produzir estatísticas e modelos sobre ocorrências e grupos de indivíduos, a partir de sistemas de mineração de dados e perfilização geográfica (*geo-profiling*). Nesse sentido, a intenção do governo paulista é que o sistema passe a munir a PM paulista com dados e informações para o estímulo do que entendem por "Consciência Situacional". Ao cruzar os dados do Registro Digital de Ocorrência (RDO), Detram, Chamados 190 e Fotocrim, a ideia é que isso permita a construção de estatísticas sobre ocorrências, bem como a perfilização de condutas criminosas em regiões específicas capaz de subsidiar uma prática de policiamento preditivo na PM paulista (Secretaria 2015b).

Essa é uma prerrogativa inédita para as práticas policiais, antecipar as autuações e prisões com base em mineração de dados e perfilização de condutas criminosas, legitimando ações preditivas de contenção de manifestações, e de prisão de "perfis" considerados perigosos para determinadas regiões. Ao depositar fé em um sistema que reproduz perfis de periculosidade, travestindo-o enquanto automatizado, ainda que haja um esperado aumento da eficiência policial, abre-se margem para a desenho de uma espécie de saber-poder, que subsidia e garante maior capacidade de controle e gestão sobre grandes fluxos, e fluxos específicos de indivíduos nos ambientes urbanos.

Todavia, conforme um relatório desenvolvido pelo Tribunal de Contas do Estado (TCE), que almejava verificar se de fato o Detecta cumpria a sua função (automatizar o processo de vídeo monitoramento dos espaços públicos, se garante a confiabilidade e a segurança das informações, resultados nas atividades de planejamento, prevenção e investigação policial) conclui que, todas as capacidades previstas, alertas, sistemas estatísticos, não são e nem estão operacionais, por inúmeros motivos (Beraldo, 2015). Mais adiante, exprime também que, devido a uma série de problemas de ordem técnica, com o Detecta "corre-se o risco de que as informações disponibilizadas no banco de dados possam ser utilizadas para outros fins que não o de segurança pública" (Beraldo, 2015: 74). Ou seja, a rigor, o Detecta mantém apenas o sistema de coleta de *feeds*, e seu compartilhamento destes com o *DAS*.

Desse modo, é fundamental que compreendamos que os discursos sobre policiamento e segurança preditiva, os algorítimos para a triagem dos dados, que embasam o Detecta, são desenvolvidos e gestados em países como os EUA e Inglaterra, tanto por autoridades policiais, como por empresas como *Microsoft* e *Cisco*, que provem essa capacidade. Sobre isso, o chefe do Departamento de Polícia de Lincoln, Nebraska, Tom Casady, em sua reflexão sobre sistemas informacionais, afirma que ao se associarem uma série de informações que vão desde histórico de crimes, idade, raça, status de imigração, habitação, renda, à sistemas mapas, há uma melhor e mais clara visualização da relação entre pobreza, renda e criminalidade, antes legada unicamente à uma "literatura criminal" (Casady, 2011).

Conforme os departamentos de polícia adotam sistemas de gestão massiva de dados e registros, a sua capacidade de agrupar e analisar dados sobre crime e desordem se amplia muito. Ainda que esse movimento possa ser entendido como uma mera forma de "mapeamento", muito comum em investigações criminais ao longo dos últimos anos, a sua particularidade reside na possibilidade

de construir modelos estatísticos e de geo-referenciamento, a partir de análise massiva de dados públicos, e seu cruzamento com plataformas de dados criminais, capazes de classificar grupos de indivíduos, e apontar padrões de criminalidade futura. Nesse sentido, essa nova forma de olhar e gerir a criminalidade ganha uma nova notação, Policiamento Preditivo (*predictive policing*), cuja definição tem sido objeto de debate entre departamentos de polícia, e de empresas transnacionais de gestão de infra-estruturas de informação e comunicação.

Ainda que o conceito de policiamento preditivo esteja em disputa, é possível que identifiquemos várias nuances nas definições já apresentadas. Os departamentos de polícia estadunidenses, em parceria com o *National Institute of Justice* compreenderam de forma ampla esse procedimento, o definindo como uma "estratégica policial que usa a coleta de dados de diferentes fontes, e análises avançadas, usando os resultados para informar-se, antecipar-se, prever e responder de maneira mais efetiva ao crime futuro" (Pearsall, 2010). Da mesma forma, a *RAND Corporation* define a prática como: "Aplicação de técnicas analíticas para identificar potenciais alvos para a intervenção policial e prevenção de crimes, ou solução de crimes passados a partir de predições estatísticas" (Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Holywood, J. S., 2013).

Na esteira dessas definições, empresas que provêm os serviços de *cloud based analysis*, como a *Microsoft*, integrando infra-estruturas de monitoramento à sistemas de mineração algorítimica de dados, e perfilização geográfica a partir de plataformas de dados criminais, também buscam imprimir a uma visão positiva dessa nova forma de policiamento. Responsável pelo desenvolvimento do *Domain Awarenes System* (*DAS*) para cidade de Nova Iorque, a *Microsoft* defende que o policiamento preditivo deriva de um novo arranjo possibilitado pelas novas tecnologias de análise e armazenamento em nuvem, considerando, evidentemente, a perspectiva de redução de custos em conjunto com uma maior eficiência das ações policiais no "combate ao crime" (Arthur, 2015). De maneira objetiva, a *Microsoft* explica que, os sistemas de computação em nuvem conectariam todos os departamentos de inteligência policial, para a construção de padrões históricos de criminalidade, e com isso projetar tendências futuras de criminalidade por região (Bhandari, 2016).

A rigor, as plataformas computacionais que substanciam esse tipo de prática, se caracterizam por sistemas complexos de coleta massiva de dados, orientados por algorítimos de busca, classificação, seleção, agrupamento e cruzamento de informações. Em geral o processo pode ser descrito em duas fases: a de mineração e cruzamento de dados (*data minning*), e de perfilização geográfica (*geographical profilling*). Em um primeiro momento são triadas informações geralmente públicas, como números de identidade, imagens e fotos, placas de carro, residência, formação, cor, idade, dentre outros, e a depender do sistema e do contexto, invocam-se dados privados, como dados telefônicos, bancários, ficha criminal, etc. Os sistemas são abastecidos, ainda, com informações e dados criminais geo-referenciados, permitindo a criação dos chamados mapas de densidade, que permitem aos agentes de segurança visualizarem incidentes ocorridos no passado, bem como fluxos e espaços de circulação dos cidadãos e "criminosos". No momento em que os algorítimos desenvolvidos para essa prática estabelecem a classificação desses dados

e o "nexo" possível entre eles, é possível o início de um processo de análise geoespacial que "(...) caracteriza as localizações associadas com os eventos passados e cria um modelo que incorpora fatores ambientais associados estatisticamente com incidentes passados (...) que pode ser usado para identificar localizações similares aonde incidentes futuros podem ocorrer" (McCue, 2011: 04).

É nesse último momento que se verifica a prática de perfilização geográfica, que com base em algoritmos, permite priorizar indivíduos em longas listas de suspeitos. Nessa técnica, modelos computacionais articulados por uma série de algoritmos que analisam uma determinada localização geográfica, padrões de comportamento de "delinquentes", ou grupos de pessoas, considerando informações como data, horário, características estéticas, de comportamento, para verificar a probabilidade voltar a agir ou circular no local.

Em países marcados tanto por atentados terroristas, bem como atos violentos cometidos por indivíduos portando armas pesadas, as formas de policiamento preditivo caem como uma luva para os agentes de segurança pública. O *DAS*, nesse sentido, é declaradamente um dispositivo de contraterrorismo, elaborado mediante a um discurso emergencial, orienta-se a prever e deter a preparação e ataques terroristas, sendo sumariamente aproveitado para conter manifestações, e crimes menores (NYPD, 2009:02). Desse modo, gestado em comum por empresas de telecomunicações e departamentos policiais estadunidenses, e alinhado a uma promessa de maior eficiência em prover segurança à redução de custos oriunda de parcerias público-privadas, o *DAS* e as técnicas de policiamento preditivo, curiosamente, encontram ressonância nos discursos que conformam os sistemas de gestão e controle da segurança pública no Brasil, o que, *a priori*, nos leva a elaborar algumas problematizações.

Nesse sentido, o Detecta, bem como o *DAS* e o *Pred Pol,* tal como os dispositivos preconizados por Foucault (1996), se organizam a partir de um conjunto heterogêneo de saberes e elementos discursivos e materiais, orientados para responder a uma urgência, nesse caso, a necessidade de punições antecipativas. Assim, o saber que nos referimos aqui, que confere autoridade a essa prática é o que se manifesta na perfilização de condutas normais ou anormais, desejáveis ou indesejáveis, a partir de critérios quantitativos, permitindo a classificação de grandes massas de indivíduos como suspeitos, ou propensos ao crime a partir de indícios estatísticos. De certa forma, esses saberes e dispositivos sustentam uma forma de governamentalidade, no mesmo sentido proposto por Foucault (2008), que tem na possibilidade de punição antecipatória – similar a dos ataques preemptivos – uma nova forma de gerir a segurança pública.

A esse respeito, a partir do discurso proclamado por instituições militares estadunidenses, pelas empresas de telecomunicações, departamentos de polícia e segurança pública, é possível apresentar uma problematização acerca do modo como as "predições" assumem o estatuto de verdade futura no momento de elaboração das operações, transformando aquilo que seria um risco potencial, em um risco real, diante das "abordagens preditivas" (Bruno, 2016). Em outras palavras, diante desse estatuto de verdade que as estatísticas preditivas assumem, definindo

níveis de periculosidade em condutas desviantes, como Lianos e Gouglas (2000) irão sustentar, é o risco que se configura como o registro cultural central das práticas punitivas, e não o crime.

Em uma perspectiva mais centrada nos algorítmos, que aprofunda a problematização acima, Josh Scannel (2016: 03), discorrendo sobre o *DAS* irá afirmar que "os softwares de predição de crimes, não tem nada a ver com prevenção de crime". Ao invés disso, os algoritmos que baseiam esses sistemas apenas "matematizam" uma estética policial discriminatória, organizando a cidade em torno de percepções irreais, ou uma "reorganização da ontologia na computação" (Scannel, 2016: 03). O algoritmo seria, portanto, um objeto político, uma junção de forças que se imprimem no social como uma espécie de "governança algorítmica". O autor defende que esses algorítimos preditivos, ao pretenderem reduzir a "bagunça do contexto social em uma computação enxuta" (Scannel, 2016: 08) em uma decisão estética e simplista, acabam por eliminar o social da sociabilidade. Como resultado, produzem uma "fantasia refinada da cidade", a *smart city*, que mascara um Estado carcerário, cuja agência humana na tomada de decisão sobre a "culpabilidade" dos sujeitos, é suprimida por uma governança algorítimica.

Autores como Keith Guzik (2009), Sara Degli Espositi (2014) e José van Dijck (2014), ao contentrarem -se naquilo que chamam Datavigilância, discutem o papel das novas técnicas de processamento de dados em nuvem, como mineração de dados (*Data Minning*) e perfilização algorítmica (*Profiling*)[1], enquanto intensificadores do processo de controle social e discriminação. Por sua vez, Henrique Parra (2016), Fernanda Bruno (2016), Marta Kanashiro (2016), dentre outros, tem buscado, discutir o a relação entre instrumentos de "Big Data" no incremento e intensificação dos sistemas contemporâneos de vigilância e governamentalidade no Brasil. Inaugura-se uma prática, que tem na técnica de processamento algorítimico, o principal pilar para erigir uma nova forma de governamentalidade.

Sobre isso, Antoinette Rouvroy e Thomas Berns (2010), descrevem essas técnicas como um novo saber-poder estatístico, que originados em um fenômeno contemporâneo de registros sistemáticos e "digitalização da vida própria", e apoiadas em dispositivos de detecção, classificação e avaliação antecipatória dos comportamentos humanos, consagram uma forma específica de governamentalidade algorítmica. Ela se caracteriza pela capacidade em interpretar os dados registrados, a partir de critérios de normalidade ou anormalidade, interesse ou indiferença, prevendo, orientando e prevenindo certos tipos de comportamentos. Em geral, seria "um poder que reside nos algoritmos de correlação estatística, articulado para um "controle" ou mais ainda, uma antecipação de um novo tipo" (Rouvroy et Berns, 2010: 88-89).

Portanto, a segurança preditiva, em contexto de gestão de conflitos e da segurança pública em ambientes urbanos, possui uma profunda identidade com os processos que caracterizariam uma "governamentalidade algorítmica", o que lança luzes para um debate mais aprofundado, seja a partir de uma aproximação com a Sociologia da Punição, ou dos Estudos Críticos de segurança Internacional.

CONCLUSÕES PRELIMINARES

Ao observarmos práticas tão semelhantes, em contextos tão distintos, organizadas pelos mesmos pilares, torna-se elementar traçar não apenas um conceito que as exprima em um bojo comum, mas fundamentalmente, um paralelo histórico entre elas. Nesse sentido, o trabalho de Stephen Graham (2006) nos esclarece que diversas tecnologias, projetos, técnicas e doutrinas desenvolvidas no âmbito da RAM tinham por objetivo não apenas uma maior eficiência e capacidade de camuflagem dos armamentos e das operações militares, mas em grande medida, também, o desenvolvimento de dispositivos de vigilância, rastreamento e monitoramento para a gestão da segurança pública. Esses dispositivos e técnicas seriam fundamentais para o projeto estadunidense de "império global" (Graham, 2006: 263), organizando as operações militares também em ambientes urbanos complexos, sejam nos grandes centros urbanos dos países centrais, ou periféricos.

No entanto, ainda que as novas dimensões estadunidenses do militarismo respondam pelo ímpeto de aplicação dessas novas técnicas e produção desse novo saber, é fundamental destacar o discurso privado em seu entorno. É fulcral o papel da *Microsoft* na profusão de um discurso de maior eficiência das ações policiais, pois ele entra em consonância com o discurso de autoridades, respaldando a introdução e aplicação desses sistemas de vigilância em ambientes urbanos. Algumas de nossas primeiras observações a esse respeito, com algumas entrevistas realizadas, é que boa parte dos gestores e responsáveis pelo Detecta enxergam as práticas, os saberes produzidos apenas como um tipo de negócio, abstrato, neutro e imparcial, reforçando a ideia de uma racionalidade econômica, técnica e não política governando a implementação desse sistema.

De acordo com Alvarez (2002: 693), essa busca por centrar o indivíduo, em sua composição biológica e mental, enquanto sujeito do crime, excluindo quaisquer determinações sócio-culturais, teve uma ampla e positiva recepção no Brasil no início do século XX, e permanecem até hoje como característica estruturante do pensamento criminológico brasileiro. De acordo com o autor, o pensamento jurídico daquele período compreendeu as novas teorias criminológicas a partir do seu potencial de controle social, mas principalmente, como estabelecer formas diferenciadas de tratamento jurídico-penal para determinados segmentos da população, o que garante um "tratamento desigual para os desiguais" (Alvarez, 2002: 696).

Em ambos os casos, os "dispositivos de segurança/policiamento preditivo" potencialmente autorizariam ações preemptivas das autoridades, conformando uma governança centrada nos algoritmos, esquadrinhando e classificando aqueles que potencialmente podem ou não circular, ou podem ou não viver. A problemática no caso dos Drones é que os estudos apresentados tanto pela *New American Foundation*, *Bureau of Investigative Journalism*, demonstram a falha dessas técnicas, uma vez que elas tem sido responsáveis por uma descomunal desproporcionalidade nas mortes de civis e "contrainsurgentes". Considerando que o relatório do TCE demonstra a ineficácia "*a priori*" do Detecta, nos parece que um dispositivo gerido em um contexto de "guerra global ao terror", reforçará o uso arbitrário de violência, legitimando e aprofundando práticas punitivas excludentes. Assim, uma compreensão devidamente crítica dos dispositivos e formas

de governança da segurança preditiva, requer uma aproximação que compreenda, problematize a trajetória política dos algoritmos que fundamentam o seu saber elementar. Talvez uma aproximação entre os Estudos Sociais da Ciência e da Tecnologia, os Estudos de Segurança Crítica Internacional e Sociologia da Punição consigam revelar os elementos políticos, sociais e controvérsias no processo de desenvolvimento dos algoritmos e consequentemente da segurança preditiva.

NOTAS

* Doutor em Política Científica e Tecnológica pela Unicamp, e Pesquisador do GAPI (Grupo de análise de Políticas de Inovação)

1. A mineração de dados pode ser entendida como, a aplicação de tecnologias e técnicas de bancos de dados (como de analise estatística e modelização) a fim de descobrir estruturas ocultas e sutis relações entre dados, e inferir regras que permitem a previsão de resultados futuros. Por sua vez, perfilização algorítimica é entendida como a inferência de presença de características observáveis num dado indivíduo, ou de características não observáveis, atuais ou futuras (Rouvroy et Berns, 2010: 91-92).

REFERÊNCIAS

ALBERTS, D. S; HAYES, R. E. (2003) Power to the Edge: Comand… Control… in the Information Age. Washington, D.C.: DoD Command and Control Research Program, 2003.

Alston, Philip (2010) Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions. United Nations Human Rights Council. Disponível em:http://www.refworld.org/docid/4c07635c2.html. Acesso em 02/07/2014.

Alvarez, M. C. (2002). A Criminologia no Brasil ou como Tratar Desigualmente os Desiguais. *Dados, Revista de Ciências Sociais*, 45(4), 677-704.

Arthur, K. (2015) Supporting Law enforcement resources with predictive policing. *Microsoft Government*. Disponível em: https://enterprise.microsoft.com/en-us/industries/government/supporting-law-enforcement-resources-with-predictive-policing/.

Bellamy, C. (2001). What is information warfare? In R. Matthews & J. Treddenick (orgs.) *Managing the revolution in military affairs*, (pp. 56-75). New York: Palgrave.

Beraldo, S. E. (2015). Relatório de Fiscalização de Natureza Operacional Solução de Consciência Situacional – DAS "Detecta". *Tribunal de Contas da União*. Processo n. 17.941/026/2015.

Bhandari, P. (2016) Predictive Policing: The future of law enforcement. *Microsoft State and Local Government*. Disponível em https://enterprise.microsoft.com/en-us/industries/government/predictive-policing-the-future-of-law-enforcement/.

Bruno, F. (2016). Rastrear, Classificar, Performar. *Ciência e Cultura*. 68(1), 34-38.

Casady, T. (2011). Police Legitimacy and Predictive Policing. *Geography Public Safety*. 2(4). 01-03.

Cebrowsky, A. K. (2000). Military responses to the informational age**.** *The RUSI Journal,* 145(5), 25-29.

Chamayou, G. (2013). *Théorie du drone*. Paris: La Fabrique.

Dicjk, J. V. (2014). Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society*, 2(12), 197-208.

Espositi, S. D. (2014). When Big Data Meets Dataveillance: The hidden side of analytics. *Surveillance & Society*, 2(12), 209-225.

Foucault, M. (2008) Segurança, Território e População: Curso no Collège de France (1977-1978). São Paulo: Martins Fontes.

Geraldo 45. (2014) Detecta: Tecnologia Contra o Crime. *Youtube*. Disponível em: https://www.youtube.com/watch?v=KcUH7_-usTs. Acessado em 09/07/2016.

Graham, S. (2006). Surveillance, Urbanization and the "US Revolution in Military Affairs". In D. Lyon (Org.) *Theorizing Surveillance: The Panopticon and Beyond* (247-269). Portland: Willian Publishing.

Guzik, K. (2009). Discrimination by Design: predictive data mining as security practice in the United States' 'war on terrorism'. *Surveillance & Society*. 1(7), 1-17.

Kanashiro, M. (2016) Apresentação: Vigiar e Resistir: a constituição de práticas e saberes em torno da informação. *Ciência e Cultura*. 68(1), 20-24.

Lianos, M; Goulas, M. (2000) Dangerization and the End of Deviance: The institutional Environment. In: British Journal of Criminology. N. 40. Pp. 261-278.

Mack, G; Beeb, B & Wenzel G. (2002). Total Information Awerness Program (TIA), System Description Document (SDD). *Darpa: Information Awerness Office*.

McCue, C. (2011). Proactive Policing: Using Geographic Analysis to Fight Crime. *Geography Public Safety*. 2(4). 03-05.

National security Agency (2016) What We do. Disponível em:https://www.nsa.gov/what-we-do/.

NYPD (2009) DAS: Public Security Privacy Guidelines. Disponível em:http://www.nyc.gov/html/nypd/html/crime_prevention/counterterrorism.shtml

O'Connel, M. E. (2009) Unlawful Killing with Combat Drones: A case Study of Pakistan 2004-2009. *Legal Studies Research Paper*. 6 de Novembro. 09-43.

Parra, H. (2016) Abertura e Controle na governamentalidade algorítimica. *Ciência e Cultura*. 68(1). 39-42.

Pearsall, B. (2010) Predictive Policing: The Future of Law Enforcement? *NIJ Journal*. N. 266. 16-19.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Holywood, J. S. (2013) Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. *Rand Corporation Safety and Justice Program*.

Piccerillo, R. A. & Brumbaugh, D. A. (2004). Predictive Battlespace Awareness: Linking Intelligence, Surveillance and Recoinassance Operations to Effects Based Operations. *2004 Command and Control Research and Technology Symposium: The Power of Information Age Concepts and Technologies*. The Pentagon: Recoinassance Directorate

Air and Space Operations.

Rouvroy, A. et Berns, T. (2010). Le nouveau Pouvoir Statistique: ou quand le controle s'exerce sur un réel normé, docile et sans événement car constitué de corps “numériques”... *Multitudes*, 40, 88-103.

Scannel, J. (2016). What Can an Algorithm Do? *DIS Magazine*. 1-9.

Secretaria de Segurança Pública de São Paulo. (2015a) Alexandre de Moraes Explica o Funcionamento do Detecta. *Notícias*. Disponível em: http://www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=36199. Acessado em: 10/02/2016.

Secretaria de Segurança Pública de São Paulo. (2015b). Secretaría lança cinturão eletrônico de monitoramento do Detecta em todo litoral de SP. *Notícias*. Disponível em: http://www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=36669.

The Intercept. Skynet: Applying Advanced Cloud-based Behaviour Analytics. (2015) *Documents*. Disponível em: https://theintercept.com/document/2015/05/08/skynet-applying-advanced-cloud-based-behavior-analytics/.

DATOS, ALGORITMOS, NEUTRALIDAD DE LA RED Y SOCIEDADES DE CONTROL

Resumen: La presente ponencia tiene como objetivo analizar la dinámica de la continua modulación de los datos tanto al momento de ser 'donados' por los usuarios como operando posteriormente sobre ellos dentro de la problemática económica y de control del concepto/principio de Neutralidad de la Red. Para ello se analizan, problematizan y se ponen en diálogo las teorías y conceptos de la Sociedad de Control (Deleuze), Individuación (Simondon), Normalización Informacional (Rodríguez) y Gubernamentabilidad Algorítmica (Rouvroy y Berns) entendiendo que tanto las acciones de los usuarios como los datos que ellos brindan directa e indirectamente entran, dentro del marco del neoliberalismo como grilla de inteligibilidad, en nuevas lógicas de producción de predicciones, horizontes de posibilidad, prácticas y hasta nuevos regímenes de saber-poder en el capitalismo cognitivo-informacional actual. La relevancia de la ponencia está en analizar un factor clave en las problemáticas y perspectivas de la actual coyuntura capitalista, donde el aumento exponencial de la penetración de las tecnologías digitales representa nuevos desafíos y potencialidades.Las conclusiones parciales y abiertas de este trabajo nos permiten pensar como el proceso de producción de poder en base a los datos, si bien representa nuevas lógicas y planteos en las lógicas de las relaciones de poder, no es un proceso acabado ni unilineal sino que representa, expresa y se encauza en diversas luchas y resistencias materializadas en batallas en constante tensión por parte de los diversos actores involucrados en un panorama abierto y cambiante.

Palabras clave: Neutralidad de la red, Datos, Sociedad de control.

MARTÍN ARIEL GENDLER*

Dados, Algoritmos, a neutralidade da rede e as Sociedades de Controle

Resumo: Este trabalho tem por objetivo analisar a dinâmica do modulação contínua dos dados no momento da 'doados' pelos usuários e também operando posteriormente sobre eles dentro dos problemas económicos e controle conceito / princípio da neutralidade da rede. Para este fim, analisar, problematizar e colocar em teorias de diálogo e conceitos sociedade de controle (Deleuze), individuação (Simondon), Normalização informativos (Rodriguez) e governamentabilidade Algorithmic (Rouvroy e Berns) entendimento de que ambas as ações do usuário como os dados que fornecem, directa e indirectamente abrangida pelo quadro do neoliberalismo como grade de inteligibilidade em novas previsões de produção lógica, os horizontes de possibilidade, práticas e aos novos regimes de conhecimento e poder no capitalismo cognitivo-informacional hoje. A relevância do trabalho é analisar um fator chave para os problemas e as perspectivas da situação capitalista atual onde o aumento exponencial da penetração das tecnologias digitais representa novos desafios e potencialidades. Conclusões parciais e abertas deste estudo permitem-nos a pensar como o processo de produção de poder com base nos dados, mas representa uma nova lógica e planteos na lógica das relações de poder, não é um processo acabado ou unilinear mas representa , expressa e canalizado em várias lutas e resistências incorporadas em batalhas em constante tensão pelas várias partes interessadas em uma paisagem aberta e em mudança.

Palavras-chave: Neutralidade da rede, Dados, Sociedade de controle.

Data, Algorithms, Network Neutrality and Societies of Control

Abstract: This paper aims to analyze the dynamics of continuous modulation of the data at the time of 'be donated' by users and also operating later on them within the economic and control problematic of the concept / principle of Net Neutrality. To this end, we analyze, problematize and put into dialogue the theories and concepts of Control Society (Deleuze), individuation (Simondon), Informational Normalization (Rodriguez) and Algorithmic Governmentability (Rouvroy and Berns) understanding that both user actions as the data that they provide directly and indirectly fall within the framework of neoliberalism as grid of intelligibility in new logic of production predictions, horizons of possibility, practices and new regimes of knowledge and power in the current cognitive-informational capitalism. The relevance of the paper is to analyze a key factor in the problems and prospects of the current capitalist situation where the exponential increase in the penetration of digital technologies represents new challenges and potentials. Partial and open conclusions of this study allow us to think how the process of power production based on the data is not a finished or unilinear process but represents expressed a new logic and problematics in the logic of power relations materialized in fights and battles in constant tension by the various stakeholders in an open and changing scene.

Keywords: Net neutrality, Data, Surveillance society.

INTRODUCCIÓN

A partir de la década de los 70, las tecnologías de la información y de la comunicación fueron una posible vía de salida de los problemas económicos presentados por las sociedades *welfaristas* en articulación con el naciente proceso de globalización actual y la imposición y/o adopción del neoliberalismo para dirimir y planificar políticas sociales, económicas y culturales.

Estos procesos de cambio conllevan (y expresan) a su vez una crisis de las instituciones disciplinarias y de los planteos y estrategias biopolíticas existentes materializados en diversos procesos de cambios tanto de factores productivos, de gubernamentalidad y de los dispositivos y tecnologías de poder que obran de mecanismos para su instalación y ejercicio (Foucault, 2007; Rouvroy e Berns, 2015), del saber-poder que reviste la época y a sus vidas y cuerpos humanos (Sibilia, 2005), o también expresado como un cambio de las sociedades disciplinarias a las sociedades de control (Deleuze, 1991) o de seguridad (Foucault, 2006), entre otras.

En esta dinámica de expansión tecnológica, los datos personales de los individuos, en relación a los postulados y prácticas neoliberales, cada vez más pasan a ser el foco de la producción de

saber-poder así como de la producción de sujetos y sus disposiciones para la acción, configurando un tipo de gubernamentalidad específica denominada como *algorítmica* (Rouvroy e Berns, 2015) que permite modular, intervenir y orientar los procesos de individuación (Simondon, 2016) individual y colectiva.

La presente ponencia tiene como objetivo el analizar y problematizar los puntos anteriormente mencionados en conjunción con la problemática de la Neutralidad de la Red, la cuál se ha trabajado en producciones anteriores (Gendler, 2015) acerca de cómo las acciones (y reglamentaciones) de diversas empresas y Estados respecto a los flujos de datos que circulan suponen el poder conocer y utilizar esos datos de contenido y tráfico, insertándolos en la lógica antes descripta.

CONDICIONES DE POSIBILIDAD: DE LA FÁBRICA AL SMARTPHONE

De la disciplina al neoliberalismo.

Siguiendo a Foucault (1996) y a Sibilia (2005), los cambios en las configuraciones del saber-poder de finales del siglo VIII comenzaron a establecer un cierto dominio y producción sobre la vida denominada como la "estatización de lo biológico".

Se intentaba configurar los cuerpos y poblaciones de la sociedad industrial para beneficio de los mecanismos de producción y de ordenamiento social de la misma: cuerpos moldeados por las instituciones disciplinarias de forma tal de potenciar sus factores productivos y poblaciones que hagan propios los postulados biopolíticos *normales*.[1]

Durante el siglo XX, el avance de los postulados y saberes neoliberales creados en la década de 1930 como posible forma de respuesta a la crisis internacional del capitalismo (aunque poco efectivos en un contexto de amplio intervencionismo Estatal) comenzarían a configurar otros modos de organización de los cuerpos, poblaciones y relaciones de poder teniendo amplia difusión y centralidad, especialmente tras la década de los 70's.

Siguiendo a Foucault (2007), la doctrina neoliberal buscó desarrollar su propia utopía incorporando el trabajo a la teoría económica y postulándolo como una conducta económica racionalizada. En este sentido, el trabajador pasa a ser conceptualizado como una "máquina" productora flujos de salarios cuya idoneidad y capacidad estaría dada por los diversos capitales (entendidos como todo lo que puede ser plausible de ser una fuente de ingresos futuros) que configuran su capital humano, indisociable de su poseedor. De este modo, el sujeto es caracterizado como un "empresario de sí", como una "unidad-empresa" que pasa a componer una sociedad compuesta de unidades -empresas diversas. Como empresario de sí mismo, el individuo dispone de un capital humano genético-heredado fijo pero también de otro adquirido, el cuál puede continuar incrementándose mediante el consumo (para producir su propia satisfacción) y mediante la toma de diversos riesgos e inversiones que le permitan generar este incremento para continuar desarrollándose

y desarrollar de esta manera una "vida digna de ser vivida" y no solamente una "mera vida" (Costa y Rodríguez, 2010).

De este modo, se apunta a generalizar la forma económica del mercado, tanto funcionando este como principio de inteligibilidad de desciframiento de las relaciones sociales y comportamientos individuales como también en forma de una "grilla" que permita supervisar la actividad goburnamental en una crítica permanente al poder político en torno a sus costos y utilidades. Esta *grilla de inteligibilidad* permite realizar y producir una economización de todo el campo social, político y cultural incorporando una lógica de utilitaridad económica a diversos elementos que anteriormente estaban por fuera.

Esto implica un cambio en las concepciones y producciones respecto a la criminalidad y la vigilancia. El criminal ya no será visto como un sujeto que debe ser castigado por sus rasgos morales o antropológicos, sino que la lógica se amplía a todo el espectro social, a "cualquier persona" que intentando tomar un riesgo en pos del incremento de su capital humano generó una externalidad negativa en otro/s o cuyo riesgo era excesivo para los parámetros de normalidad vigente (Foucault, 2007). Este cambio en las configuraciones de saber-poder es fruto tanto de la lógica y práctica individualista del empresario de sí mismo, como de una descentralización de los procesos de producción y sujeción de los sujetos (Sibilia, 2005) en detrimento de los Estados Nación y a favor de la proliferación de empresas y actores del sector privado.[2]

De las tecnologías

Siguiendo a Tiqqun (2016) la cibernética[3] nace con el objetivo de constituirse en una nueva tecnología de gobierno donde se analogan comportamientos de los seres humanos, de los animales y de las máquinas y cuya propuesta es interdisciplinar.

Según uno de sus principales ideólogos Abraham Moles, el principal objetivo de esta corriente filosófico-teórica estaría resumida en la siguiente proclama: "Concebimos que una sociedad global, un Estado, puedan encontrarse regulados de tal suerte que estén protegidos contra todos los accidentes del devenir (…) Es el ideal de una sociedad estable traducido por medio de mecanismos sociales objetivamente controlables" (Moles, citado en Tiqqun, 2016: 33).

Así, se intenta generar un *orden predecibley estable* que permita ser *conducido* evitando los diversos ruidos u obstáculos en su desarrollo.

Serán las diversas máquinas y desarrollos tecnológicos los que permitan vehiculizar la concreción de estas formulaciones al ser elementos de cálculo racional que permitan *superar los límites de la capacidad humana* (la cuál puede generar desorden cuando se ve propasada), permitir una retroalimentación de forma eficaz y continua y al ser elementos de predicción y control de cuerpos y comportamientos individuales y colectivos. Para ello, el concepto de "*información*", sustento vital de las tecnologías maquínicas y entendido como sustancia y flujo activo emitido

que modifica a un receptor pasivo, será vital a fin de alimentar, retroalimentar y constituir una red similar a la red neuronal del cerebro humano (Tiqqun, 2016).[4]

La crisis de 1973 dio el puntapié inicial para pensar nuevas respuestas y formas de salida a la misma, imponiéndose la hipótesis y los postulados neoliberales con las TIC como los principales vehículos materiales de su expansión y materialización, y como **mecanismos vitales** para asegurar la libre y veloz transferencia de flujos financieros y de información a nivel mundial (Gendler, 2016) en el marco de la avanzada del proyecto globalizador de tinte neoliberal y para generar diversos procesos y mecanismos que permitan la gubernamentalidad y conducción de las conductas.

De Controles y Terrores

La conjunción de los postulados neoliberales y cibernéticos y la proliferación de las tecnologías digitales como medio y expresión de estos cambios también incluyen la llamada "crisis de las disciplinas" (Foucault, 1978; Deleuze, 1991) en beneficio de "nuevas fuerzas que están golpeando la puerta. Son las sociedades de control las que están reemplazando a las sociedades disciplinarias" (Deleuze, 1991: 1).

Se corta así la secuencia de la sociedad disciplinaria donde siempre se "estaba empezando de nuevo" en función de unas sociedades de control donde "nunca se termina nada", donde

> (...) los encierros son moldes, módulos distintos, pero los controles son modulaciones, como un molde autodeformante que cambiaría continuamente (...) [y donde] el control es a corto plazo y de rotación rápida, pero también contínuo e ilimitado, mientras que la disciplina era de larga duración, infinita y discontinua (Deleuze, 1991: 1-3).

Estas modulaciones que referencia Deleuze pueden ser definidas desde la teoría de la individuación de Simondon (2015a, 2015b y 2016).

Para este autor, el individuo es un "teatro de individuaciones", un estado metaestable[5] de un proceso contínuo y cambiante de *ontogénesis*, de transformación denominado *individuación* que no es otra cosa que el proceso en el cuál el ser *deviene en ser*. En este proceso, estos estados metaestables están en continua tensión desde una realidad pre-individual que deviene, vía procesos de trasducción, en diversos metaestados (físico, viviente, psíquico, colectivo, que conservan las tensiones iniciales) gracias a la tensión constante y creciente entre el individuo y el medio traducida como "resonancia interna". Esta tensión genera unas ciertas energías potenciales (que constituyen la metaestabilidad) que están en íntima relación con su estructura y que son plausibles de ser ordenadas (*in-formadas*) por una tensión de información que se incorpore al sistema y genere nuevos estados metaestables.

Si bien la información *in-forma*, no es una sustancia que pueda ser emitida sobre un receptor pasivo (como postulaba la cibernética), sino que es el resultado de sus propios procesos de transformación meta-estables y que permite generar estados de metaestabilidad.

Simondon postula dos procesos claves dentro del proceso de ampliación y devenir de los estados metaestables de la individuación. Por un lado, el proceso de **trasducción** el cuál supone que el campo esté en un equilibrio metaestable que encierre una energía potencial que puede ser liberada por el surgimiento de una nueva estructura operando de cierta forma como una "reacción en cadena", la cuál es generada tanto por las energías potenciales generadas por la tensión de la resonancia interna del individuo como por cierta tensión de información externa[67].

El otro proceso clave es el de la **modulación,** el cuál se puede definir como un proceso que "se obtiene al 'domesticar' la propagación trasductiva, controlándola y alimentándola permitiendo trabajar en condiciones regulares (…) el modulador está decidiendo según la incidencia de información. Se gobierna instante por instante el régimen de transformación de energía potencial". (Simondon, 2016: 149-150). Así como en la trasducción hay un cambio permanente (solo detenido por el *recovery time*), en la modulación se controlan y regularizan las energías potenciales difusas que generan estos cambios. Se controla (o intenta controlar) así el régimen de cambio de metaestado de la energía potencial.

Por tanto, volviendo con Deleuze la modulación como *molde deformante y constante* no solo reemplaza al "moldeado" de la disciplina sino que implica un cierto *control y conducción* de los estados metaestables de la individuación al operar para organizar sus energías potenciales en un sentido y no en otro, en parte inhibiendo el factor de impredisibilidad de la ampliación trasductiva en el teatro de individuaciones.

En este escenario, la expansión de estas máquinas informáticas permitirá que esta modulación constante se ejerza por fuera de los espacios de encierro, "al aire libre y en todo momento", a todos los "hijos de vecino" (plausibles de ser criminales en su acción de tomar riesgos para incrementar su capital humano) en su circulación (Foucault, 2006).

Las sociedades de control expresan la conjunción del saber-poder neoliberal y cibernético en función de un nuevo tipo de gubernamentalidad, la cuál es ejercida por las sociedades de control como "máquinas extractoras de información" (Rodríguez, 2008), como también en la elaboración de nuevos índices estadísticos, en base a esta información extraída, que permitan generar e ir modificando las curvas de normalidad con la que se juzgue y produzca a los sujetos.

Cabe destacar dos elementos que complementan esta argumentación:

Rodríguez (2008) advierte que "conviene descartar de antemano toda teoría que intente formular la novedad de la vigilancia contemporánea en términos de creación de "sujetos estadísticos de información", pues tal cuestión es tan vieja como la vigilancia misma" (Rodríguez, 2008: 2). Esto pone en cuestión diversos análisis donde el control y la vigilancia solo se aplican por vía de estas informaciones extraídas, ya que, la estadística como forma de control biopolítico también era aplicable a las sociedades disciplinarias.

Por eso el autor esgrime el concepto de "normalización informacional" como forma de dar cuenta de la articulación de varios procesos que configuran las sociedades de control. Así, se aborda la

centralidad del miedo y de la exclusión[8] como mecanismos de gubernamentalidad que permitan justificar muchas de las tecnologías, regulaciones legales y prácticas implementadas, y asegurar su legitimación. Se puede observar como diversos énfasis sobre el "terror" causado e incentivado por diversos grupos (en un espectro que va desde grupos "terroristas" a delincuentes ordinarios) son la punta de lanza para implementar diversas legislaciones[9], para incentivar la instalación de cámaras de vigilancia y otros dispositivos que permitan monitorear e identificar en todo tiempo y lugar las acciones de individuos y grupos (Alcántara, 2009), y para permitir extender el concepto de "seguridad" al establecer un Estado de Seguridad donde el estado de excepción se vuelve regla y donde

> (...) la seguridad que está en cuestión hoy no apunta a prevenir los actos de terrorismo sino a establecer una nueva relación con los hombres, que es la de un control generalizado y sin límites (...) al Estado de seguridad le interesa que los permanezcan en la incertidumbre sobre aquello que los amenaza (Agamben, 2015: 1-3).

Es en parte por vía de esta incertidumbre y por la aceptación de todo mecanismo (y tecnología) que pueda asegurar la seguridad de los individuos que estos aceptan diversas acciones de "extracción de información" que violen su privacidad personal y la de sus relaciones y que acepten sin mayores miramientos diversas herramientas tanto técnicas como legales que lo aseguren.[10]

El segundo elemento que cabe destacar es que, en concordancia con los postulados neoliberales de toma de riesgos, son los sujetos los que "deben buscar" las actividades y mecanismos (que suelen estar ubicados en la intersección entre prácticas del control de sí y tecnologías de gobierno) que les permitan realizar este incremento de capital humano, y no, como en la sociedad disciplinaria, que simplemente "lo reciban". (Costa y Rodríguez, 2010)

Tanto el "terror", como el deseo y acción de mejora individual en clave de la grilla de inteligilibilidad económica, como la disponibilidad de una gran variedad de mecanismos, objetos y tecnologías fruto de la descentralización de lo biológico y la apertura del juego a iniciativas privadas en función de la producción de consumidores, son factores claves para poder comprender la gubernamentalidad de las sociedades de control[11].

LA GUBERNAMENTALIDAD ALGORITMICA

Para analizar la gubernamentalidad de las sociedades de control enfocaremos en las plataformas de redes sociales como espacios tecnológicos privilegiados para la comunicación, interrelación y la constitución de los sujetos en nuestras sociedades contemporáneas.[12][13]

Siguiendo a Rodríguez (2015) podemos ver como el sujeto se construye en parte en estas redes sociales vía la exhibición de su interioridad e intimidad configurando una imagen teatral que permita establecer comunicación e interrelación con otros. El problema aquí es que en estas redes sociales todo lo que es compartido por el sujeto en la conformación de su "si mismo" queda registrado y es plausible de ser almacenado, procesado y utilizado, y por otro lado, la misma

"naturaleza" de estas plataformas es vivir de estos aspectos internos que son visibilizados. Es decir, la intimidad y los datos proporcionados son el motor de funcionamiento de las redes sociales.

Aquí debemos detenernos en analizar lo que Deleuze llama como "dividual".

Siguiendo a Rodríguez (2015),

> (...) dividual es todo aquello que constituye a los individuos no como individuos sino como especies duplicadas o partes de si mismos compartidas por otras regiones dividuales relacionadas con individuos. (...) Esta definición se ajusta a los modos de subjetivación en las redes sociales, modos que alteran la relación entre lo individual y lo colectivo (Rodríguez, 2015: 62).[14]

Vemos de este modo que estas plataformas de redes sociales son escenarios digitales claves para la interrelación y para esta "dividualidad", tornándose espacios privilegiados de lo transindividual (en términos simondonianos)[15]

El tema está en los datos que son "cedidos" de forma directa o indirecta[16] por los individuos en estos espacios para permitir tanto la producción de su "sí mismo", como para poder interrelacionarse con los otros y los usos que se hacen de estos datos.[17]

Así, la descentralización y la apertura al juego de diversos actores privados (Sibilia, 2005) quienes son los principales impulsores y desarrolladores de estas plataformas que sirven de vehículo de la comunicación y de espacio de dividualización (y de conformación del sí mismo) transindividual por excelencia centran su actividad en (la recolección, almacenamiento y uso de) los *datos* y permiten que se hable ya no de una vigilancia "a secas" (*surveillance*) sino de una *dataveillance*[18].

Rouvroy e Berns (2015) denominan a esta gubernamentalidad como *algorítmica*, refiriéndose a

> (...) un cierto tipo de racionalidad (a)normativa, o (a)política que reposa sobre la recolección, agregación y análisis automatizado de datos en cantidades masivas, de modo de modelizar, anticipar y afectar por anticipado, comportamientos posibles(...) la gubernamentalidad algorítmica no produce cualquier subjetivación, sino una que crea modelos de comportamiento (perfiles) supraindividuales a base de datos infraindividuales (Rouvroy e Berns, 2015: 42).

Se pone el foco tanto en los datos cedidos y recolectados como en las nuevas modalidades de modelado de lo real a partir de algoritmos "autodidactas", que se modifican según los nuevos datos recibidos. Así se reordenan las prácticas estadísticas modernas y se da pie a la emergencia de nuevas formas de control y vigilancia.

Para que este proceso pueda tener lugar, se da una triple operación respecto a los datos.[19]

La *primera operación* es la colecta de una cantidad masiva de datos "no clasificados" para la creación de "almacenes de datos". Estos datos disponibles son fruto de diversas fuentes y son recolectados por diversos actores con diversos fines[20]. Los individuos comparten *libremente* sus datos, los cuáles son conservados en "almacenes", datos accesibles a todo momento desde cualquier parte.

Se postula así que "un dato no es más que una señal expurgada de toda significación propia y de esta manera parecen ser objetivos al ser heterogéneos, poco intencionados, poco subjetivos. ¡Tales datos no pueden mentir! " (Rouvroy e Berns, 2015: 39)[21]

La *segundao peración* remite al tratamiento automatizado (algorítmico) de los datos recolectados y producción del conocimiento para hacer "emerger" correlaciones entre ellos[22]. Aquí todo parece realizarse de forma automática y neutral, por ende se abona la construcción de un saber-poder "reflejo de la realidad" y sin intervención humana ya que esas correlaciones y las producciones fruto de las mismas parecieran seguir un "orden espontáneo" basado en la realidad pero no diseñado por ella y por tanto objetivo[23].

La *tercera* operación refiere a una acción sobre el comportamiento de los individuos vía la creación y aplicación de perfiles predeterminados surgidos en base a las correlaciones algorítmicas del punto 2.

Se hace hincapié que al ser estos perfiles creados en base a un tratamiento automatizado (y por ende "no intencional") de datos que operan como "reflejo de la realidad", la normalización que implica la aplicación de estos perfiles es cuasi "espontánea, surge de la realidad y no de patrones morales o políticos". Asimismo, esta es "más democrática" al colocar a todo el mundo "en pie de igualdad" ya que no tiene en cuenta la clase, las ideologías, etc. sino meramente los datos frutos de la intimidad y acciones de los individuos. De este modo, no solo se abre la posibilidad de generar diversas disposiciones para la acción de los individuos al transformar su entorno con la excusa de que este pasa a estar "personalizado", sino que también en la misma operación se logra obturar tanto las desigualdades y luchas sociales que convergen en la trayectoria individual y social de un individuo como también las diversas intencionalidades e intereses que hay detrás del diseño y justificación de la creación de las tecnologías (Feenberg, 2005).

Asimismo, se hace hincapié que el mismo sistema algorítmico no es plausible de ser "derrotado" por una falla en la producción de su sistema de perfiles estandarizados ya que esta servirá para continuar mejorando y perfeccionando los algoritmos de producción de perfiles y subjetividades. Así, la gubernamentalidad algorítmica parece estar más centrada en el futuro que en el presente, en las propensiones y disposiciones para la acción más que en las acciones mismas (si bien se nutre de ellas).[24]

Respecto a este "sueño democrático" de una sociedad cuya normalización esté basada en "la realidad misma", los autores comentan que "nuestros comportamientos nunca han sido tan conducidos, observados, registrados, clasificados y evaluados (...) la "inofensividad" del gobierno algorítmico es apenas aparente, crea la realidad al mismo tiempo que la registra." (Rouvroy e Berns, 2015: 48).[25]

Se afirma así que esta gubernamentalidad algorítmica devalúa la política al "no haber nada que decidir", y por tanto ataca a las instituciones y al debate público ya que estos solo podrían "interferir" con la realidad creada en base "a la misma realidad".[26]

En clave de la teoría simondoniana, los autores refieren a que este tipo de gubernamentalidad logra dificultar u obstruir el proceso de individuación transindividual (co-individuación) redoblando los procesos de individuación singular (conducidos), al ontologizar las relaciones.

Debemos recordar que la centralidad del planteo simondoniano de la información no está en ésta como *sustancia* emisora sino en que ella es una tensión metaestable que requiere que el receptor también esté en un estado de metaestabilidad para poder ambos en conjunción ser parte del proceso de individuación.[27]

Esto permite analizar que estos datos "extraídos" así como los algoritmos que los procesan y los perfiles producidos también son tensiones que están en continua metaestabilidad y cambio siendo producidos por y ayudando a producir los diversos procesos de individuación tanto individual como colectiva no en sentido (solo) de dar forma para conducir conductas, sino también en ayudar a mantener la metaestabilidad de los propios individuos receptores[28] en su individuación.

Esta puede ser una clave para permitir desgranar ese carácter "neutral y automático" de los datos ya que ellos mismos al estar en continua individuación metaestable no son hechos, sino procesos y son plausibles de recibir también información que modifique sus energías potenciales propias.[29]

En este sentido, la dividualidad permitida y fomentada en los espacios transindividuales digitales es tanto causa y producto de estos procesos.

DE REDES Y NEUTRALIDADES

Todo este recorrido nos lleva ahora a analizar uno de los principales campos de batalla actuales: la Neutralidad de la Red.

Este término/concepto es definido como un principio técnico que establece que todos los contenidos que circulan por Internet deben recibir tratos igualitarios, manteniéndose las redes abiertas a la libre circulación de información, la cuál no debe discriminarse según origen, uso o aplicación.

El carácter abierto de la definición de "no discriminación" ha abierto la ventana para diversas posiciones por parte de múltiples actores en las batallas tanto por su implementación o su eliminación como por la apropiación de su significado.[30]

Resumiendo las principales problemáticas que la Neutralidad de la Red representa (Gendler, 2015):

1) Existe una **problemática económica** que apunta a los beneficios económicos generados por diversas empresas, principalmente los ISP[31] fruto de la violación de la neutralidad al discriminar y/o intervenir el flujo de datos. Aquí podemos encontrar diversos convenios comerciales que impliquen recortar el ancho de banda hacia ciertas páginas o servidores

por ser de la competencia o de un servicio "ilegal" (Torrents u otro intercambio P2P), el generar "vías rápidas de acceso" a ciertas páginas o aplicaciones propias del ISP o de empresas que tengan negocios con el, recortar el ancho de banda en general de los usuarios que suelan hacer un uso intensivo de su servicio, brindar menor ancho de banda del contratado, crear aplicaciones "gratuitas" (que no consuman datos) dentro de la contratación de un servicio (Zero Rating), entre otras.

2) Existe una **problemática de control** referida al almacenamiento, procesamiento, uso y/o comercialización tanto de los datos de tráfico[32] como de contenido[33] de esos flujos de datos respectivos a información personal y geo-localizada de los usuarios. Esto lo realizarían tanto ISP como diversas empresas o incluso diversos Estados por vías legales o meramente ejecutivas.

La mayoría de los enfoques abocados al tema focalizan en la problemática económica cuasi ignorando la problemática de control. Esto es llamativo y preocupante, ya que esta identificación y recolección de datos antes mencionada justamente representa una "discriminación" a los flujos de datos que "deben circular libres".

Estos flujos de datos (tanto los personales como de las acciones y relaciones de los usuarios) sufren una *triple discriminación* al ser identificados, observados y analizados (según tráfico y contenido), al ser duplicados y almacenados para efectuar los procesos de correlación algorítmica y de producción de perfiles antes descriptos, y al ser plausibles de ser interceptados para reducir, ampliar o modificar su flujo dependiendo de la intencionalidad de la acción/interacción.[34]

Sin embargo, en los diversos debates y legislaciones al respecto, la problemática de control muchas veces es ignorada o hasta legitimada siendo ambos casos, por omisión o acción (Alcántara, 2011), una forma de complementar los procesos de la gubernamentalidad algorítmica.

Una legalización y aceptación de la Neutralidad de la Red (que no tiene en cuenta estas problemáticas) legitima y habilita la extracción de los datos, la correlación algorítmica y la producción de los perfiles ya que se entiende que no hay discriminación porque "no hay ninguna interferencia" en la realización de las acciones de los usuarios en Internet sin tener en cuenta que no es necesario reducir o recortar el flujo de los datos para estar cometiendo una "discriminación" de los mismos (al identificarlos, almacenarlos, etc.).

Si bien muchas legislaciones reglamentan la Neutralidad de la Red en su clave económica, también reglamentan el almacenamiento de datos por un tiempo determinado y su uso por parte de cualquier área estatal o privada en pos de la "seguridad nacional" (Gendler, 2015)[35]. Otras, si bien no reglamentan este aspecto, al no decir nada sobre el mismo dan pie a que se realice.

La creación de estos perfiles personalizados (metaestables y perfeccionables y que van modificando las disposiciones de acción de los individuos en su construcción de "si mismos"), habilitado por estas legislaciones, también supone una violación del principio de "no discriminación" de la Neutralidad de la Red al ponderar ciertas informaciones, publicaciones, productos, eventos, etc. por sobre otras, muchas veces directamente ocultando estas últimas. De este modo, estas

legislaciones "bien intencionadas" como también muchos de los activistas "pro neutralidad de la red", defienden (sin saberlo) los procesos de modulación de la individualización y de conducción de conductas de esta gubernamentalidad algorítmica.

Al poner única o mayormente el foco sobre que los tráficos de datos en la acción de los usuarios *no sean recortados, ampliados o impedidos* por diversos intereses comerciales y/o estatales, se deja vía libre a que estas plataformas informáticas puedan violar ese concepto/principio defendido, en base a esta producción de perfiles automatizada que, justamente, *recortan, amplían o impiden* el acceso a cierta información, etc. por sobre otra generando y conduciendo disposiciones para la acción.

REFLEXIONANDO Y CONCLUYENDO PARCIALMENTE

Cabe a todo esto el reflexionar como, a pesar de que las problemáticas respectivas al control y la privacidad están actualmente en foco[36], la dinámica de apropiación, correlación y utilización de los datos personales y de actividad de los usuarios que sustenta esta gubernamentalidad algorítmica no solo continúa sin casi ser interpelada, sino que incluso (como es el caso de la Neutralidad de la Red) aún parece no haber recibido la importancia que amerita o que, peor, se utiliza como forma de reglamentar y legislar estos procesos en pos de defender la "seguridad y la soberanía nacional"[37].

A pesar de que estos temas estén visibilizados, estos procesos de extracción de datos, los cuáles son constituyentes de la dinámica de funcionamiento de la gran mayoría de las redes sociales y otros de la Web 2.0, son aceptados de todos modos por los individuos para poder participar en los diversos espacios transindividuales digitales a pesar de saber los riesgos que eso implica.

Aquí se puede ver la importancia de la grilla de inteligibilidad neoliberal del "empresario de sí mismo" ya que este sabe que para poder participar en estos espacios deberá "correr el riesgo" de que sus datos, producciones y acciones sean monitoreados, intervenidos y utilizados en pos de crear perfiles personalizados que recorten su espectro de acción futuro, pero que sin *embargo parece ser un riesgo que está dispuesto a correr* para continuar ampliando su capital humano en pos de su goce y de construir una "vida digna de ser vivida".

Estas configuraciones neoliberales junto a las problemáticas de la "seguridad" son factores clave para entender la instalación de diversos mecanismos de seguridad, registro y videovigilancia que complementan los datos obtenidos de forma "online"[38].

Podemos apreciar que el problema es tanto que el sujeto y su proceso de individualización (el cuál es modulado) parezca quedar excluido de esta problemática al postular esta gubernamentalidad como "surgida de la propia realidad y por tanto sin influencia de factores morales o políticos" (como si la realidad y las acciones de los sujetos no fueran morales y políticas) como también que los propios individuos participen en esta lógica de producción del gobierno de sus conductas *de forma voluntaria* y cuasi acrítica so riesgo de no poder correr el riesgo de incrementar su capital humano y de "quedar fuera" de este espacio de dividualidad transindividual digital.[39]

Sin embargo, podemos decir que

> Lejos de ser omnipotente, el biopoder tiene grietas a través de las cuales las fuerzas vitales logran infiltrarse y reaccionar. Aunque la vida esté sometida a cálculos explícitos y otros controles, eso no significa que haya sido capturada íntegramente por técnicas capaces de dominarla y moldearla sin fisuras (Sibilia, 2005: 216).

Si bien muchas organizaciones y colectivos parecieran haber "caído en la trampa" al cuestionar solo una parte de la problemática sin hacer fondo al asunto, algunas otras sí problematizan estos temas e intentan desarrollar diversas herramientas (mayormente informáticas) y nuevos conocimientos de saber-poder para hacer frente a la conducción de conductas automatizada y basada en algoritmos. Estas "nuevas armas" postuladas por Deleuze están siendo inventadas continuamente, porque justamente para poder enfrentar y dar una resistencia que sea realmente eficaz a estos procesos de gubernamentalidad algorítmica cambiantes y mutantes, es necesario que estas nuevas armas (y los actores que las desarrollan y utilizan/cen) también continúen sus procesos de concretización y de individuación en pos de los combates presentes y futuros.

NOTAS

* IIGG-CONICET-FSOC-UBA. Licenciado en Sociología, docente y doctorando en Ciencias Sociales – Universidad de Buenos Aires, Argentina. Becario doctoral del CONICET. martin.gendler@gmail.com

1. La elaboración y ejecución de las biopolíticas fueron viables gracias a la acumulación de conocimientos basados en la observación y el examen y la capacidad de realizar un procesamiento centralizado de esa información (vía la estadística y la demografía) para eliminar el azar y poder planificar y mejorar los cuerpos y poblaciones para hacerlos más útiles al capitalismo.

2. Esto habla asimismo de un cambio del moldeo y del disciplinamiento de cuerpos a la *conducción de conductas* (que circulan) materializada en la producción de diversas "posibilidades de acción" en relación directa al concepto de gobierno o gubernamentalidad: *"técnicas y procedimientos destinados a dirigir las conductas de los hombres"* (Foucault, 1980: 125).

3. Cabe destacar que este término deriva del griego *kybernesis* "acción de pilotar una nave", y en sentido figurado, "acción de dirigir, de gobernar".

4. Será el impulso de estos postulados un factor sumamente importante dentro de los desarrollos tecnológicos que generarán lo que hoy día conocemos como Internet por parte de sectores universitarios y militares en los EEUU como forma o mecanismo de poder mantener comunicaciones descentradas ante un potencial ataque nuclear soviético.

5. Entendido como un estado cuya continua tensión genera una "*imposibilidad del ser continuar viviendo sin cambiar de estado*" (Simondon, 2015ª: 504)

6. Principalmente en la fase psíquico-colectiva donde el individuo psíquico requiere de las relaciones con otros individuos para resolver las tensiones de su estado de metaestabilidad individual, en lo que se denomina como transindividualidad.

7. Cabe destacar que esta propagación trasductiva tiene el obstáculo de que existe cierto "*recovery time*" en el cuál ninguna incidencia de información es eficaz. Este *recovery time* varía dependiendo de los niveles de la individuación y de la estructura en que se lleva a cabo, siendo el de las neuronas casi imperceptible pero el de los hechos psicosociales de larga duración. En este sentido que "todo es posible" pero no en cualquier cosa, en cualquier momento y de cualquier manera (Simondon, 2016).

8. Los otros elementos que complementan a la Normalización Informacional son el accionar e influencia de los Mass Media (ocupando el espacio de normalización antes biopolítico y disciplinar de una forma más difusa), la modulación y "materialidad" de la información (ya explicados) y la desaparición de la distinción "público-privado" en concordancia con la crisis de los lugares de encierro y de las nuevas prácticas "al aire libre".

9. Como la ley USA PATRIOT de los EEUU en 2006, la cuál brinda de poderes extraordinarios al Estado como a sus diversas agencias de seguridad para la detención y procesamiento de individuos y colectivos sin juicio previo. Cabe destacar que esta ley sirvió de inspiración a las leyes "antiterroristas" aprobadas y aplicadas en numerosos países.

10. En este sentido, el 'terror' se vuelve tanto una tensión de información que participa en la modulación de los estados metaestables como también una forma de mantener y conducir esta metaestabilidad.

11. Donde pareciera que el individuo tiene libertad de elegir (y consumir) un tipo de conducta cuasi pre-producida que será conducida para satisfacer su goce y formular esa 'vida digna de ser vivida'.

12. Cabe destacar que estas plataformas de redes sociales son la forma hegemónica actual que toman diversos procesos de comunicación "a través de dispositivos tecnológicos-digitales". En este sentido, la producción de tecnologías "cada vez más pequeñas y accesibles" parece tender hacia la "facilitación" del uso de estas plataformas (y de las consecuencias que veremos a continuación).

13. Asimismo, debemos hacer referencia que gran parte de la "Web 2.0" funciona con las lógicas que se describirán a continuación, no solo las plataformas de redes sociales que son su caso más evidente.

14. La traducción es propia.

15. "*Para Simondon, la relación que el hombre mantiene con sus máquinas asume la forma de una trasducción o, mejor dicho, la trasducción en el nivel humano, psíquico y colectivo, supone necesariamente la proliferación de elemento, objetos y sistemas técnicos, entre ellos las máquinas*" (Rodríguez, 2007).

16. La cesión *directa* de los datos remite a todo llenado de formulario necesario para la construcción de un perfil por parte de los sujetos. La cesión *indirecta*** remite tanto a los datos obtenidos de las acciones de los individuos (la "huella digital") como también a todo dato obtenido por estas plataformas gracias a la vinculación de diversos dispositivos por parte no del sujeto sino de los sujetos con los que este se relaciona. Es decir que si bien un individuo puede desplegar diversas estrategias para no brindar sus datos personales, si otra persona que utiliza estas plataformas los tiene ya abre la ventana a su apropiación indirecta.

17. Siguiendo a Zuazo (2015) "*Somos constantes donadores de datos. El problema es que los datos que vamos cediendo a nuestro paso no quedan dentro del objeto que estamos utilizando (celular, tablet, PC). Tampoco se dispersan en el Eter o en la red ni en esa nube mágica donde las empresas nos hacen creer que se almacena la información. Cada rastro digital queda en manos de empresas, en sus granjas de servidores (...) Nuestras huellas son el oro de esas corporaciones* " (p. 261).

18. Vigilancia basada en los datos.

19. Cabe destacar que en cada una de sus etapas parece obturarse el lugar del sujeto y su intencionalidad en pos de considerar a estos datos como "datos concretos de la realidad" que construyen perfiles "emancipados de todo tipo de carácter decisional".

20. El estado los recolecta con fines de seguridad, las empresas privadas con fines de publicidad y marketing y personalización de productos, etc.

21. Traducción propia.

22. Este sería el proceso de conformación de la producción algorítmica de correlaciones de datos denominado como *Big Data*.

23. Parafraseando a Hayek (2008).

24. Zuazo (2015) llega a una conclusión similar al analizar que el objetivo de Google, Facebook y otras plataformas de redes sociales parece ser el predecir con el mayor grado de exactitud los comportamientos, consumos, gustos y deseos de los usuarios. A este "predecir", podemos agregarle "producir" y sobre todo "conducir".

25. Traducción propia.

26. Dicho de otro modo, en este punto es donde se podrían ver concretados los sueños utopistas neoliberales y cibernéticos de postular una sociedad capitaneada en base a su propia "espontaneidad y libre circulación sin interferencias políticas" al postular que no se trata de "gobernar lo real, sino en base a lo real".

27. En este sentido los datos (y los perfiles producidos algorítmicamente en base a ellos) "*sólo será* [n] *información, siguiendo a Simondon, cuando además de manifestar un estado produce o desencadena determinadas operaciones*" (Blanco y Rodríguez, 2015: 112).

28. Quien recordemos, son los "protagonistas" del par emisor-receptor a diferencia de lo planteado por la cibernética.

29. Asimismo, es válido retomar el plateo de Simondon (2007) acerca de que la técnica (y sus productos) es una extensión de lo humano al igual que lo estético-artístico, pero por su carácter subyugado por el trabajo esta apreciación muchas veces no suele evidenciarse dando como resultado que "lo técnico" aparezca como algo separado y cuasi "ajeno" a lo humano.

30. De aquí se pueden enunciar interpretaciones pro neutralidad de la red entendida como un mecanismo que permite el libre mercado (al estar restringida la intervención estatal y la formación de monopolios), otros argumentos pro neutralidad en pos de sostener las "potencialidades democráticas primigenias" del Internet de los primeros desarrollos y otras que están en contra de la neutralidad de la red entendiéndola a si misma como una intervención que afecta el "libre desenvolvimiento" de los actores en el mercado, entre otros argumentos minoritarios.

31. Proveedores de servicio de Internet, por sus siglas en inglés.

32. Entendidos como el "dónde, quien y cuándo" de los flujos de datos.

33. Entendidos como el "qué" y el "porqué" de los flujos de datos.

34. Si bien esta última discriminación también puede vincularse con la problemática económica en función de intereses monopólicos de las empresas o de "violaciones" a los derechos de autor para justificar este recorte u obstrucción del tráfico, estamos pensando más bien en recortar u obstruir los flujos de datos tendientes a realizar prácticas alternativas o de resistencia que puedan ser vistas como "riesgosas" para la "seguridad" de empresas u naciones (y por supuesto de su propiedad privada).

35. El caso ejemplar es el Marco Civil de Internet de Brasil aprobado en 2014 cuyos artículos 13, 15 y 19 estipulan claramente la obligatoriedad del almacenamiento de los datos por parte de los ISP y proveedores de contenidos de Internet que operen en Brasil.

36. Más luego de las "revelaciones" de Edward Snowden en 2013.

37. La cuál cabría preguntarse si realmente se defiende o si también se habilita a que diversos sectores previamente desplazados o excluidos de este ejercicio del poder algorítmico puedan entrar en juego (Gendler, 2015).

38. Los cuáles también son complementados por una serie de malwares que permiten extraer datos de las actividades y "huellas" de los usuarios como también de su actividad digital offline por medio de backdoors y otros.

39. No hay que olvidar que los regimenes de metaestabilidad del proceso de individuación no solo son mantenidos por el individuo, sino también impulsados por él. (Simondon, 2015b).

REFERÊNCIAS

Agamben, G. (23 de diciembre de 2015). De l'Etat de droit à l'Etat de sécurité, *Le Monde*, (en español: http://artilleriainmanente.blogspot.com.ar/2015/12/giorgio-agamben-delestado-de-derecho.html)

Alcántara, J. (2009). *La Sociedad de Control: privacidad, propiedad intelectual y el futuro de la libertad.* Barcelona: El Cobre ediciones.

Alcántara, J. (2011). *La Neutralidad de la Red y por qué es una pésima idea acabar con ella.* Biblioteca de las Indias, Sociedad Cooperativa del Arte de las Cosas. E-book recuperado de http://www.versvs.net/wp-content/libros/la-neutralidad-de-la-red/jose-alcantara-la-neutralidad-de-la-red.pdf

Blanco, J. y Rodríguez, P. (2015). Sobre la fuerza y actualidad de la teoría simondoniana de la información. En J. Blanco, D. Parente, y P. Rodríguez (coordinadores) *Amar a las máquinas: cultura y técnica en Gilbert Simondon* (pp). Buenos Aires: Prometeo.

Costa, F. y Rodríguez, P. (2010). La vida como información, el cuerpo como señal de ajuste: los deslizamientos del biopoder en el marco de la gubernamentalidad neoliberal. En V. Lemm (ed.) *Michel Foucault: Neoliberalismo y Biopolítica* (pp), Santiago de Chile: Editorial Universitaria de la Universidad Diego Portales.

Deleuze, G. (1991). "Posdata a las sociedades de control" (varias ediciones). Recuperado de http://www.fundacion.uocra.org/documentos/recursos/articulos/Posdata-sobre-las-sociedades-de-control.pdf

Feenberg, A. (Junio de 2005). Teoría Crítica de la tecnología. *Revista CTS*, 2(5),109-123. Recuperado de http://www.scielo.org.ar/pdf/cts/v2n5/v2n5a07.pdf

Foucault, M. (1978). *La société disciplinaire en crise*. Recuperado de http://llibertaire.free.fr/MFoucault113.htm

Foucault, M. (1980). Du gouvernement des vivants. En *Dits et Ecrits 1954-1988* (pp. 125-129), Tomo IV, Gallimard: Paris.

Foucault, M. (1996). Clase del 17 de marzo de 1976. En *Genealogía del racismo*, Buenos Aires: Altamira [edición más reciente: (2001). *Hay que defender la sociedad.* Curso en el Collège de France (1975-1976). Buenos Aires: Fondo de Cultura Económica].

Foucault, M. (2006). *Seguridad, territorio, población. Curso en el Collège de France.* Buenos Aires: Fondo de Cultura Económica.

Foucault, M. (2007). *Nacimiento de la biopolítica. Curso en el Collège de France.* Buenos Aires: FCE.

Gendler, M. (Julio/Diciembre de 2015). ¿Qué es la Neutralidad de la Red? Peligros y potencialidades. *Revista Hipertextos*, 2(4). Recuperado de http://revistahipertextos.org/wp-content/uploads/2015/12/Qu%C3%A9-es-la-Neutralidad-de-la-Red-Mart%C3%ADn-Gendler.pdf

Gendler, M. (2016). Globalización y tecnologías digitales: Un estado de situación. *Revista Unidad Sociológica,* 2(6). Recuperado de http://unidadsociologica.com.ar/UnidadSociologica64.pdf

Hayek, F. (2008). *El camino de la servidumbre*. Edición electrónica en español de Liberty Fund. Recuperado de http://biblioteca.libertyfund.org/sites/default/files/camino-de-servidumbre-libro-electronico.pdf

Rodríguez, P. (2007) Prólogo. El modo de existencia de una filosofía nueva. En G. Simondon. *El modo de existencia de los objetos técnicos* (pp). Buenos Aires: Prometeo.

Rodríguez, P. (2008). ¿Qué son las sociedades de control? *Sociedad*, 27. Recuperado de http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9son-las-sociedades-de-control.pdf

Rodríguez, P. (2015) Espetáculo do Dividual: Tecnologias do eu e vigilancia distribuída nas redes sociais. *ECOPOS,* 18(2), 57- 68. Recuperado de https://revistas.ufrj.br/index.php/eco_pos/article/view/2680/2249

Rouvroy, A e Berns, T. (2015). Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? *Revista ECOPOS,* 18(2), 36-56. Recuperado de https://revistas.ufrj.br/index.php/eco_pos/article/view/2662/2251

Sibilia, P. (2005). Biopoder. En *El hombre postorgánico. Cuerpo, subjetividad y tecnologías digitales* (pp.). Buenos Aires: Editorial Fondo de Cultura Económica.

Simondon, G. (2007). *El modo de existencia de los objetos técnicos*. Buenos Aires: Prometeo.

Simondon, G. (2015a). Forma, información, potenciales. En *La individuación a luz de las nociones de forma y de información* (pp), Buenos Aires: Cactus.

Simondon, G. (2015b). Introducción. En *La individuación a la luz de las nociones de forma y de información* (pp), Buenos Aires: Cactus.

Simondon, G. (2016). La amplificación en los procesos de información. En *Comunicación e información* (pp), Buenos Aires: Cactus.

Tiqqun. (2016). *La hipótesis cibernética*. Buenos Aires: Hekht Libros.

Zuazo, N. (2015). *Guerras de Internet: un viaje al centro de la red para entender como afecta tu vida*. Buenos Aires: Debate.

EJE 5

NUEVOS DESAFÍOS EN LA PROTECCIÓN DE DATOS PERSONALES

INTELLIGENCE CHALLENGES IN LATIN AMERICA AND PROSPECTS FOR REFORM: A COMPARATIVE MATRIX ON DEMOCRATIC GOVERNANCE

Abstract: For many reasons, the classic debate between security and civil liberties has been reopened in recent times - 9/11 attack of Twin Towers and subsequent reforms of intelligence, coupled with technological advances and leaks from Snowden who revealed the existence of a massive wiretapping program-. This is particularly important in Latin America where remains a considerable authoritarian legacy in the intelligence agencies which are still going under a democratization process that is partial, discontinuous, belated and reactive to crisis. The paper presents shortcomings and obstacles to democratize intelligence sector in Latin America: a confusion between legal, and a structural and cultural reform; unsuitability of civil management; politicization; weak management capacity of secret expenditures; access and lack of control over sensitive technologies, among others. In order to this, the paper, based on Peter Gill (2016), presents a matrix with a number of dimensions to assess the degree of democratization and the level of accountability of intelligence services, with particular attention to the context of Latin America.

Keywords: intelligence, Democratization, Matrix.

Desafíos y perspectivas de reforma de inteligencia en América Latina: una matriz comparativa sobre gobernabilidad democrática[1]

Resumen: Por diversas razones, el clásico debate entre seguridad y libertades civiles se ha reabierto en los últimos tiempos -atentado del 9/11 a las Torres Gemelas y las subsecuentes reformas de inteligencia, sumados a los avances tecnológicos y las filtraciones de Snowden quien reveló la existencia de un programa de espionaje electrónico masivo-. Ello cobra especial relevancia en América Latina donde subsiste un pesado legado autoritario en los organismos de inteligencia que aún se encuentran, en muchos casos de manera parcial, discontinua, tardía, reactiva ante episodios de crisis, en proceso de democratización. La ponencia plantea falencias y obstáculos para democratizar el sector de inteligencia en América Latina: confusión entre una mera reforma legal y una estructural y cultural; falta de idoneidad de la conducción civil; politización; escasa capacidad de gestión de gastos secretos; acceso y falta de control sobre tecnologías sensibles, entre otros. En orden a lo anterior, la ponencia, basada en Peter Gill (2016), presenta una matriz con una serie de dimensiones para evaluar el grado de democratización y el nivel de rendición de cuentas de los servicios de inteligencia, con particular atención del contexto de América Latina.

Palabras clave: Inteligencia, Democratización, Matriz.

Desafios e perspetivas para a reforma de inteligência na América Latina: Uma matriz comparativa sobre a governação democrática

Resumo: Por várias razões, o debate clássico entre segurança e liberdades civis foi reaberto nos últimos tempos- atentado 11/9 às Torres Gêmeas e subsequentes reformas da inteligência, juntamente com os avanços tecnológicos e vazamentos Snowden que revelaram a existência um programa de masivo de escutas telefônicas. Isto é particularmente importante na América Latina, onde continua a haver um legado autoritário nas agências de inteligência que ainda estão no processo de democratização, em muitos casos parcialmente, descontínuo, e como reação tardia a episódios de crise. O artigo apresenta deficiências e obstáculos para democratizar o setor de inteligência na América Latina: uma confusão entre reforma jurídica e um estrutural e cultural; inadequação da gestão civil; politização; fraca capacidade de gestão dos gastos secretos; de acesso e falta de controle sobre tecnologias sensíveis, entre outros. Com este objetivo, o papel, com base em Peter Gill (2016), apresenta uma matriz com um número de dimensões para avaliar o grau de democratização e o nível de accountability dos serviços de inteligência, com particular atenção para o contexto da América Latina.

Palavras chave: Inteligência, Democratização, Matriz.

ALEJANDRA OTAMENDI*
EDUARDO E. ESTÉVEZ**

INTRODUCTION

Today at the international level there is a strong debate concerning the powers and practice of intelligence services. On the one hand, they seem not be able to prevent attacks such as the one against Charlie Hebdo in Paris. On the other hand, the level of intrusion of intelligence in the lives of citizens and their associated political uses facilitated by technological developments in the information age have generated a strong shock following the unveiled by Julian Assange (Wikileaks) and Edward Snowden. Indeed, "the publication of 'leaked' internal Intelligence and National Security Agency (NSA) documents since June 2013 has detailed governments' attempts to achieve total surveillance of the Internet and other communications" (Andregg & Peter Gill, 2014: 490). As a reaction to this crisis and debate, the USA Freedom Act (2 June 2015) replaced the so-called Patriot Act (Eskens et al, 2015).

Also, some authors argue that intelligence communities are still governed by obsolete doctrines or intelligence paradigms such as those based on international relations realism, and that they still work under assumptions more typical of the Cold War thanattuned to the currentconflicts and international setting (Sheptycki, 2008; Coyne et al, 2014). Given this, a new doctrine based on human securityhas been proposed instead, offering alternatives to the application of power and of military action, even more relevant in the presence of non-state actors and networks threats (Sheptycki, 2008). In addition, in the context of the post-modern information age, the proliferation of information and the availability of new investigative tools, make the role of intelligence professionals more irrelevant for decision-making, limited to techniques for obtaining secret information, without sophisticated analysis (Coyne et al, 2014). After the end of the Cold War and before the attacks of 9/11, many voices advocated, "a massive slashing of intelligence budgets" and even the abolition of intelligence services by merging their functions into other government agencies (Schreier, 2007: 25). As stated by Coyne et al (2014: 65) "Now may be an appropriate time for the intelligence profession to re-examine and fundamentally challenge the underlying assumptions that underpin intelligence theory and practice."

In this international and sectoral context, the debate on the use of intelligence in Latin America where the intelligence structures still respond to authoritarian legacies of military dictatorships, is even more pressing (Andregg and Gill, 2014). Indeed, intelligence agencies are still in the process of democratization, in many cases partially, discontinuous, late and reactive to episodes of crisis, remaining as "authoritarian enclaves" (Estevez, 2015). Thus, numerous episodes occur where intelligence agents appear involved in cases of political and corporate espionage, rather than providing services for national security in still fragile democracies.

However, these problems appear not only in countries in Latin America where they "must often deal with enduring legacies of repressive intelligence and security agencies", but even in mature democracies (Born & Jensen, 2007: 257). In a more general vein, the classic debate between security and civil liberties has been reopened. Indeed, there is a renewed tension between "the relative value placed on the community's collective need for security on the one hand, and

individual rights and freedoms on the other hand" (Caparini, 2007:3). However, "reductions in rights and freedoms do not make for greater security; they make for less democratic societies in which the possibilities of abuse and harm by the state or vengeful populations are increased" (Gill, 2007). Thus, the challenge of vigorous control, oversight and review of state security intelligence activities is renewed in every democratic society (Caparini, 2007; Gill, 2007).

Taking into account these tensions at international and regional levels, but also the large resources they consume, the frequent political scandals they generate and the lack of productivity they achieve, the question of the need for state intelligence activities in Latin America arises. Given that question, this paper reviews, first, the remaining challenges of democratization processes of intelligence in Latin America as "authoritarian enclaves" of civil-military dictatorships in the region, but also general difficulties found in the intelligence sector. Second, the need for control and oversight mechanisms of intelligence services in Latin America. Finally, a matrix with dimensions to evaluate the degree of the democratization process and the level of accountability of intelligence services is introduced.

Challenges and difficulties to democratize intelligence sector in Latin America

From new institutionalism and path dependence perspectives, it could be argued that each historical moment of a country has its counterpart in the security and intelligence structure. This in turn is conditioned by its strategic context, history, political culture, traditions and legacies (Brandão, 2010, Bruneau and Boraz, 2007; Coates, 2013; Estevez, 2014a, Markowitz, 2011; Piedra Cobo, 2012; Ravndal, 2009; Zegart, 1999).

In the case of intelligence services, there is a consensus that one of the main challenges of new democracies is to leave behind agencies dedicated to monitor and operate domestically against inhabitants, to collaborate with or become instruments of repression for military regimes, and to commit abuses and violations of human rights such as extra-legal detention, torture, and extra-legal executions. In fact, through 'political policing', "intelligence services in repressive regimes are often a key means of maintaining power", that could also be used as such in transitional democracies (Caparini, 2007: 21). However, even when structures are modifiedin democratic regimes, the legacies of authoritarian regimes affect the way intelligence is performed in such countries (Marques Kuele et al, 2015).

The omnipresence of intelligence surveillance on society was well established in the case of Peru (see Basombrío and Rospigliosi, 2006: 245-251), but also in the case of Mexico as revealed after the declassification of the archive of the Interior Ministry containing intelligence reports generated by the "General Department of Political and Social Investigations" and the "Federal Security Department" during the 1947-1985 period, which showed the immense amount of mundane information on almost all sectors of society (Padilla and Walker, 2013: 4).

However, the challenges that intelligence poses to democracy are not restricted to new democracies. Indeed, "the intelligence sector's unique characteristics –expertise in surveillance, capacity to

carry out covert operations, control of sensitive information, and functioning behind a veil of secrecy– may serve to undermine democratic governance and the fundamental rights and liberties of citizens" (Caparini, 2007:3). In fact, the imperative for secrecy "can be abused and may lead to inefficiency, unauthorized actions, or the misuse or politicization of intelligence agencies", violating ethical principles, evading political control, and even becoming "a threat to the society and political system they are meant to serve" (Born & Jensen, 2007: 257).

Although "intelligence and security services are key components of any state, providing independent analysis of information relevant to the external and internal security of state and society and the protection of vital national interests", in a democratic state, security as a value must coexist and compete with other values such as respect for civil rights, free speech, the rule of law, checks and balances, and other democratic values (Caparini, 2007:3). Thus, "a trade-off between these diverging interests" has to be found in a manner that is politically and legally sound (Schreier, 2007:34). In fact, secrecy as a core aspect of the definition of intelligence for some authors clashes with the democratic principle of transparency (Crosston, 2016).

Thus, in democracy, the functions and activities of security intelligence must be subject to mechanisms of "control and oversight in the interests of effectiveness, efficiency, legality, propriety and respect for rights" (Andregg & Gill, 2014: 489). In transitional democracies, many of these mechanisms may not only be enforced, but even created as part of a democratization process. However, the dynamics of democratization of intelligence in Latin American countries has not been homogeneous, with variations in the formulas used, timing, and the results achieved, conditioned by particular legacies, historical circumstances and strategic environments (Estevez, 2014a).

One frequentpath to democratize the sector is the building of a new regulatory framework adequate to a democratic concept of intelligence, which ideally should be based on a broad consensus in order to grant legitimacy. However, regulatory reform is not enough. In fact, while the basis for legality is a legal framework for intelligence services, "legitimacy can, however, only be achieved if democratic control of intelligence services is perceived to work and the value of accurate knowledge and unbiased intelligence is recognized as a condition of good governance in the globalized world" (Schreier, 2007: 26). In this sense, legality and legitimacy are both important for any democracy, but particularly in transitional democracies where intelligence services were used against civil society during authoritarian regimes.

Thus, as part of the reform process, intelligence agencies should have examined their organization - structure, functions, procedures and staff - as a means to adjust and improve their performance to assist democratically elected decision-makers. However, at this point in history, it is evident that in the new democracies intelligence services are not going to democratize or reform themselves, even with a new law passed by legislators with a consensus. Rather than legislation, it is the internalization of democratic "political values and ideas within the political culture, especially among the political elite, that provides the most essential indicator of democratic governance of the (internal) security sphere" (Lustgarten, 2003: 326 quoted in Caparini, 2007:17).

Indeed, policymakers of a democratic government are an integral part of the intelligence cycle, they are the "alpha" and "omega" of the cycle: they are the customers that require intelligence services and they are the final recipients of products made by the agencies (Matei and Bruneau, 2011b: 660). Thus, when democratization of intelligence is promoted, the responsibility of policymakers to implement changes resulting from the new democratic legislation comprises not only changes in the structure, but also in the culture and practices of the intelligence services. However, as noted by Professor Robert Jervis (2007: vii), and except few examples (Cepik and Ambros, 2012 for the case of Brazil; Morales, 2016 for El Salvador; Basombrío and Rospigliosi, 2006 for Peru; Estévez, 2015 for Argentina, among others), this relationship has enjoyed little attention despite its important role on the way to the democratization of intelligence in new democracies.

In this section, some other difficulties that affect the democratic governance of the intelligence sector are identified (based on Estévez, 2015). One is to consider, as stated before, that the enactment of democratic legislation alone means that changes will occur in practice. Another is to assume that a civilian leadership of the intelligence sector ensures its functioning according to the new legislation. In this regard, it is important to bear in mind the weight of professional bureaucracies against a mere formal civilian chief. Another mistake from the political sphere is to issue dual or mixed messages on what is expected from the intelligence services. In these cases, when uncertain, the bureaucracy of the sector continues to reproduce illegal practices of authoritarian rule. More specific shortcomings of management that may be mentioned include having poor ability to control and manage secret expenditures; lack of access and lack of control over sensitive technologies; and lack of ability to deal with crisis when an intelligence scandal emerge.

However, one of the most important challenges in a democratization process is the trend towards politicization, that is, the temptation to make partisan political use of the state intelligence apparatus. This can occur in two ways: down, i.e., political authorities require intelligence professionals the products they want or need for domestic politics becoming a “political police” (Matei and Bruneau, 2011b: 663). Andupward, in this case the intelligence professionals voluntarily provide products that they know or infer that policymakers want on domestic issues, with the risk of producing ‘intelligence to please’ and “ignoring danger signals that the policy is misguided” (Caparini, 2007:7).

This trend is particularly serious for Latin American countries, since it does not only mitigate the efforts to reform, but also reproduces flawed intelligence practices from the authoritarian legacies. As Maldonado (2009: 55) argues, "even countries with stronger institutions cannot get rid of this evil", as verified cases of politicization could be found in Argentina and Brazil, but also in countries like Ecuador, Colombia, Peru and Venezuela. At a subnational level, Margaría and Schnyder (2014) while studying the case of Santiago del Estero province of Argentina, agree that the police intelligence service rather than a mere instrument of politics, is a constitutive element that has taken part in the development of the political order, even in democracy.

Apart from the trends of politicization, Matei and Bruneau find a serious reluctance on the part of policymakers to get involved with intelligence reform issues, what leads to “incomplete or hasty fixes to improve intelligence efficiency and ensure accountability” (Swenson, 2015:4). In order to understand

this unwillingness, Peruvian experts Basombrío and Rospigliosi (2006:248) suggest that what the politicians think about intelligence as an unavoidable order should be analyzed. According to them, politicians tend to believe that: *i*) the intelligence services should be in the hands of the military because they are those who know such matter, the intelligence professionals; *ii*) the intelligence services always spy on politicians and all kinds of people and institutions in any government. Therefore, every government should use that to their own advantage; and that *iii*) intelligence services must conduct 'psychosocial' procedures operating covertly and with secret funds. However, as the authors point out, it is wrong, essentially undemocratic and often illegal. Thus, these beliefs are an obvious obstacle to develop intelligence sector policies as public policy in a democracy.

However, not everything depends on the Executive branch. As part of the regulatory reform of intelligence, legislative oversight committees have grown in number in the region. Some cases include the establishment of a special oversight committee to carry out investigations into the abuses, corruption, human rights violations or breach of the legislation (Gomez de la Torre, 2013). Nevertheless, in heavily presidential systems, such as those seen in Latin America, the activity of parliamentary control is relatively weak in any subject, including the exercise of control over the intelligence services. Some experiences indicate that the media may also appear as a monitoring tool more effective than formal mechanisms, as an alternative or complementary to the formal mechanisms (Matei, 2014; Shiraz, 2015).

Even when national specific laws or regulations are not in place, an ethical sensibility by intelligence professionals and internal oversight should determine what choices are to be made regarding intelligence activities (Gill, 2007). In addition, international standards such as international human rights covenants, conventions, and treaties "could be effective moral and even legal substitutes for national guidelines" (Swenson, 2015:6). Thus, a legal framework, effective oversight and an ethical identity are "critical if democracy is to survive the corrosive effects of intelligence agencies turning on the peoples who create and empower them" (Andregg & Gill, 2014: 495).

As part of an ethical approach, a debate on the scope of secrecy, whose derivations make the legitimacy of intelligence, is also taking place. One of the good practices identified by the United Nations Human Rights Council (A/HRC/14/46, 2010: 6) states that

> The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address.

However, this does not always happen because intelligence agents often continue with the inertia of Cold War conflicts and they do not direct their activities to current security requirements. As Crosston points out, "national security interests are combined with domestic consolidation priorities, and softened by the mitigating factors of foreign policy, relationship legacies, and culture" (Crosston, 2016: 128). Thus, it is also part of a democratic intelligence system to reflect local priorities and the general well-being.

Democratization of Intelligence Matrix for Latin America

As noted by Gill (2016) intelligence systems are usually developed by two factors: scandals and democratization processes (Piedra Cobo, 2011). As for the latter, it should be noted that not only occur in countries that went through general recent democratic transitions as they could be in Latin America, Africa, and Eastern Europe, but democratic governance of intelligence is still very young, even in old democracies (Gill, 2016: 5). Therefore, their study is useful for both oldest democracies where setbacks can occur, as well as lessons for new democracies.

To describe and explain the processes of democratization of intelligence is difficult, particularly for secrecy and suspicion prevailing in that domain. However, this secrecy and suspicion makes its study more necessary (Gill, 2016). Indeed, being intelligence a central role of the state, it must be studied especially in a democracy where transparency, access to information, individual rights to privacy and accountability in general are its pillars. In this sense, there seems to be a shared opinion by certain authors that studies of this nature should be of qualitative type since it cannot be analyzed from a quantitative approach because neither large databases are not accessible nor they exist (Gill, 2016). Davies and Gustafson (2013) go beyond pointing out that the quantitative is impractical, especially when there is no agreement in the measurement of certain concepts. In addition, Gill (2016) indicates that since political culture is central to understanding an intelligence system, what is required is a qualitative approach that takes into account the views of experts from different countries to allow comparative analyzes.

In this regard, Davies and Gustafson (2013:7) emphasize that intelligence is a particularly suitable topic for comparative analysis because the intelligence services should resolve similar problems: to obtain information, to understand meanings, and to ensure it reaches the people and places that need it as part of the so-called "intelligence cycle".However, these functions are performed differently, in part because of the "culture of intelligence". In other words, given the need to perform similar functions and knowledge requirements, intelligence services work differently depending on the context, history and legacies (structural conditions), but also on human agency, that is, the ability to act creatively in these structures, even by modifying them.

At this point, this paper seeks to contribute by introducing a matrix of dimensions to consider in a qualitative comparative study of the democratization process of intelligence, particularly in the Latin American context. As Andregg and Gill point out, “democracy requires that security and intelligence activities are subject to control and oversight in the interests of effectiveness, efficiency, legality, propriety and respect for rights” (Andregg & Gill, 2014: 489). Thus, in a broad sense, democratic control and accountability of an intelligence service include the assessment of the legality, ethics, proportionality and propriety for its activities and objectives (Caparini, 2007:9; Schreier, 2007:38).

According to Barreiro and Rivera (2011), accountability should be done through horizontal controls (internal management), vertical controls (public sphere), and crossed controls mixing both previous types. Regarding horizontal accountability, it includes restraints of state institutions

by other equal state institutions such as "public agencies and the three branches of government (executive, legislative and judiciary)". Then vertical accountability refers to "relations among those unequal in power, such as "the hierarchical relationship between senior officials (principals) and their subordinates (agents) within a state institution" as well as the "efforts of citizens, the media and civil society organizations to keep public officials acting in accordance with good standards". A third type of accountability refers to "the role of international actors, such as foreign governments, intergovernmental organizations and international non-governmental organizations in holding a state institutional actor to account" (Caparini, 2007:9). Taking into account all the actors involved, some authors highlight that democratic control of intelligence services should be perceived as an "oversight community" (Gill 2007:213) or "multi-level system of governance", that include "mechanisms at the level of the intelligence agencies themselves, the executive, parliament, courts and the general public and even international organizations who set standards for intelligence oversight."

In order to clarify the different roles of each actor, many authors distinguish between control and oversight functions: "control" over agencies is exercised by the elected civilian officials from the executive branch. Thus, to conduct some activities such as interception of calls, an authorization by elected officials is required (Gill, 2016). This refers to what is known in Latin America as "political governance" by elected authorities. Since it "includes the power to manage and direct an intelligence service" (Eskel et al, 2015:7), two types can be identified. First, political control or executive control that refers "to the direction provided by a Minister through the issuance of guidelines and through monitoring the activities of an agency", and second "administrative control" that refers to the "internal supervision and management of the intelligence agency as a bureaucratic institution (...) its internal rules and regulations" (Caparini, 2007:8). In this regard, "the entity exercising control could also exercise internal oversight", what "cannot be considered to be substitutes for external and independent oversight" (Eskens et al, 2015:7).

Indeed, 'oversight' is in general external, but it could also be internal since it refers to the ways an intelligence service is accountable before the public and the government. In fact, 'oversight' means supervision and watchful care, and in general, it implies the review of legality and of effectiveness of intelligence. In this sense, it is not the request for prior authorization, but oversees what has already been done (Gill, 2016). As noted before, oversight could be internal,performed by the responsible minister, or external, which can include parliamentary oversight, judicial oversight, and economic and financial oversight (Eskens et al, 2015:8; Gomez de la Torre Rotta and Medrano Carmona, 2015). It can also refer to oversight performed by civil society, companies and the media.

Regarding legislative oversight, it tends to examine both efficacy and propriety of intelligence activities, for example, by supervising the accomplishment of the intelligence objectives, but also "whether intelligence activities are being conducted in accordance with the law" (Caparini, 2007:9). For doing so, a standard for oversight national intelligence services is that these

parliamentarian commissions have enough resources in terms of equipment and staff, and more important in terms of access to information and technical expertise (Eskens et al, 2015).

In the case of judicial oversight, the focus is on the propriety of intelligence activities in general, and the respect of rights and civil liberties of citizens in particular (Caparini, 2007; Gómez de la Torre, 2013: 26). Some authors also refer to economic and financial oversight, what includes norms, procedures and organs of the intelligence services that can make accountable the use of their budget and expenditures (Gomez de la Torre Rotta and Medrano Carmona, 2015). Finally, public oversight, due to its limited access to information, tends to focus on propriety issues rather than efficacy issues. Indeed, the media and the public cannot examine whether the intelligence service has achieved its goals if there is no available information about them (Caparini, 2007).

In order to test whether these mechanisms of control and oversight are in place in Latin American countries, following Gill's own scheme (2016), a matrix with eight dimensions were included(Caparini, 2007; Schreier, 2007). The first dimension considers legislation. As mentioned in the second section of this paper, the UN Human Rights Council (A/HRC/14/46, 2010) identifies as a good practice that the mandates, threats and interests of national security are narrowly and precisely defined in a publicly available law. Born and Jensen (2007:264) also suggest that a comprehensive legal framework should include the protection of human rights, particularly regarding "special powers of intelligence services to interfere with private communication and property"; "the proportionality and authorization by law; (...) the relations between the services (...) as well as the status of intelligence employees and the use of public funds", among other issues. Meanwhile, Gómez de la Torre (2013) in his comparative research study of the intelligence legal framework of Peru, Ecuador, Chile, Argentina, Brazil, Colombia, Mexico and Spain, pointed out five dimensions of democratic control to be analyzed: internal and external control and oversight mechanisms; staff professionalization mechanisms; organic dependence of intelligence bodies; and access to information mechanisms. Thus, a comprehensive and up-to-date intelligence legal framework is important, not only because of its legal impact, but also because it means "the embodiment of the democratic will of the people" represented by elected parliamentarians (Born and Jensen, 2007:264).

The second dimension refers to the use of financial resources and has a particular focus on secret budget. Indeed, the weak control over large amounts of secret budgets and their special powers to obtain information make intelligence services a powerful state actor in the shadow, even after a democratic reform. This dimension is related to financial and economic oversight already explained (Gómez de la Torre, 2013). The third dimension refers to political control, a key aspect of democratic governance of intelligence services. As it was detailed in the first section of this paper, since a new law is not enough safeguard against abuses, elected leaders play a key role to make real changes in intelligence practices and culture. Thus, their roles in political control and in internal oversight were included. However, there are many difficulties regarding the relationship between intelligence "consumers and producers", being politicization one of the

most important. In the matrix, the proportion of military heads and other indicators of militarization were also included. The reason for this is that although Latin American countries foster democratization reforms, there is a tendency to post a civilian official in charge of intelligence services, but only as a testimonial figure.

The following two dimensions, Recruitment and Training, have to do with problems identified previously such as politicization of intelligence bureaucracies, lack of independence, weak ethical commitment, corruption and limited analytical skills. Since the enactment of a new democratic law is not enough to change intelligence practices and culture, a new approach regarding intelligence professionals is required. One of the first measures taken in many democratization reforms is to remove agents not adapted to the new democratic regime, but also to openly recruit profiles from different sectors of society in order to reflect its diversity and train them according to the mandate, rules and principles included in the new democratic law. The purpose of such measures is to promote "self-accountability" through commitment to professional standards and ethics (Andregg, 2012; Gómez de la Torre, 2013). For the case of El Salvador, Morales (2016) identified several "strategic factors" to examine the degree of the intelligence service professionalization: modern legal framework; inter-agencies relationships; multilevel governance of intelligence units; applied research programs; specialized training; design of strategic profiles; strategic partnerships (with the private sector, universities, think tanks, etc.); specialized publications and journals; intelligence and security technology, and international relations and multinational cooperation.

The sixth dimension to analyze includes all the procedures regarding collection of information. As noted previously, since in many cases intelligence practices imply secrecy and intrusive measures, it has to be clear for intelligence professionals when and how to perform them in order to respect human rights. For example, in some cases they may require previous authorization to conduct some operations. As mentioned before, in general terms, from an ethical and democratic perspective, there is a debate on the scope of secrecy since it "can be abused and may lead to inefficiency, unauthorized actions, or the misuse or politicization of intelligence agencies" (Born & Jensen, 2007: 257). Thus, some items of this dimension deals with secrecy and control of sensitive information.

The next dimension (external oversight)has already been developed in detail. Apart from financial and economic oversight (second dimension), and public oversight (eight dimension), the matrix includes in this dimension legislative oversight regarding its resources and access to information, but also its composition and special powers; and judicial oversight, that focus on propriety of intelligence activities (Caparini, 2007; Gómez de la Torre, 2013: 26). The last dimension deals with public oversight including both the civil society and the media's role in overseeing intelligence activities. Although many activities are secret, intelligence services must facilitate access to non -classified information in order to be accountable. This is particularly the case for the information produced in previous authoritarian regimes, since it can contribute to commissions of truth and criminal investigations on human rights abuses.

TABLE 1
Matrix of Intelligence Accountability

1. LEGISLATION	1.1. Is there a public law of Intelligence service?
	1.2. When and how many times was it reformed?
	1.3. Does the law define a precise mandate?
	1.4. Does the law define threats and interests of national security?
	1.5. Does the law define limits to secret intelligence special powers?
	1.6. Does the law or regulations define rules for the acquisition, processing, protection and use of personal data? Is authorization required for special procedures?
	1.7. Does the law define control and oversight mechanisms? Which ones?
	1.8. Does the law prioritize and guarantee respect for human rights and civil liberties?
	1.9. Does the law make any reference to intelligence employees status and professionalization?
	1.10. Does the law state the procedures to use public funds?
2. ECONOMIC-FINANCIAL OVERSIGHT	2.1. Is the intelligence budget reported in the general budget?
	2.2. Is the agency required by norms and procedures to account for its regular and secret expenditures?
	2.3. What is the proportion between secret and public expenditures?
	2.4. Is there any reported abuse of secret expenditures?
3. POLITICAL CONTROL	3.1. Does it have civilian leadership democratically elected or appointed by democratically elected authority?
	3.2. Do the political authorities establish national security policies?
	3.3. Do the political authorities appoint agency heads?
	3.4. Do the political authorities determine the budget of the agencies with legislative agreement?
	3.5. Does the agency have civil officers, besides agency heads?
	3.6. What is the proportion of military and civilian professionals?
4. RECRUITMENT	4.1. Are recruitment and training rules and requirements included in the new legal framework of intelligence service?
	4.2. Is the recruitment of intelligence officials meritocratic, public and open?
	4.3. Is the recruitment of intelligence officials not discriminatory?
	4.4. Is the recruitment of professionals based on profiles designed for the current intelligence requirements?
5. TRAINING	5.1. Is the training program authorized and supervised by civilian political authorities?
	5.2. Does the training emphasize updated technical skills?
	5.3. Does the training emphasize compliance with the guarantees of respect for freedoms of expression, association, movement?
	5.4. Does the training emphasize respect for diversity of all kinds (sexual, ideological, political, religious, ethnic, etc.)?
	5.5. Does the training focus on the threats and national interests identified in the new democratic law?
	5.6. What issues, by whom, how long and where the agents are trained?
	5.7. Does the training include specialized and updated courses for intelligence authorities, even including master degrees?
	5.8. Does the training institution have strategic partners such as private companies, universities, think tanks, and others?
	5.9. Does the training institution have fluid relationships of cooperation with prestige institutions of the field at national, regional and international levels?
	5.10. Does the training institution count with updated intelligence technology, bibliography and applied research programs?

6. INFORMATION COLLECTION	6.1. Does the law establish procedures for authorization by people outside of agencies for use of covert information gathering and covert action?
	6.2. What are the criteria followed for classification of information?
	6.3. What is the time period for declassifying secret information?
	6.4. Is there any evidence of changes in culture and in information collection practices according to the new democratic law?
	6.5. Is there consistency between intelligence policies established by the new law and the specific activities carried out?
7. EXTERNAL OVERSIGHT	7.1. Is there any combination of legislative, judicial and/or expert bodies that monitor the effectiveness and propriety of agencies?
	7.2. Is there a Parliamentary Oversight Commission?
	7.3. Is this Commission plural-partisan? How is it composed?
	7.4. How many times does it meet per year?
	7.5. How many reports does it produce per year?
	7.6. Does it have access to secret information?
	7.7. Does it have access to information regarding secret expenses?
	7.8. Does it have the power to require hearings?
	7.9. Does it have the power to sanction or apply sanctions?
	7.10. According to experts, is the Parliamentary Commission effective in overseeing intelligence?
8. PUBLIC OVERSIGHT	8.1. Does an active civil society make use of the limited transparency to support public debate on intelligence issues?
	8.2. Do the media have access to information, albeit limited, to generate public debate on intelligence issues?
	8.3. Are the files of past military dictatorships or authoritarian governments available for the public and the media?

Source: mainly based on Gill (2016), but also on Andregg (2012); Born and Jensen (2007); Caparini (2007); Gómez de la Torre (2013), Morales (2016), Schreier (2007), among others.

CONCLUSIONS

Scandals, lack of productivity, rivalry, old and new challenges lead to possible doctrinaire and organic reforms of intelligence both at international and regional levels. In Latin America, these problems are more pressing because the intelligence sector is in many cases an "authoritarian enclave" that resists democratization process. Indeed, in many cases they still operate with an opaque logic, conducting political intelligence for the ruling party or by selling their services to the highest bidder. In addition, its opacity, lack of real control, but high budgets and access to sensitive information, places them in a position of power in the shadows with ability to influence and blackmail political, judicial and economic actors, among others.

Given this scenario, it is reasonable to wonder about the need of intelligence in Latin America. Therefore, it was examined the difficulties still present in the intelligence sector in Latin America due to its lack of real democratization. In most countries, the laws were updated, but this has not always led to changes in intelligence culture and practices. To do this, it was pointed out the strategic role of political authorities to implement reforms, conduct professional intelligence bureaucracy, and manage secret expenditures and sensitive technology. Above all, they must

have an ethical and democratic commitment to avoid the politicization of intelligence for their own benefit and redirect to the general welfare of citizens through a public mandate by law.

In this regard, the need for academic studies of intelligence democratic governance is imperative, even in countries with established democracies. For doing so, a qualitative approach, and particularly a comparative method, should be used in order to study similar functions that are present in all agencies, but undertaken differently due to culture and human action. Thus, in order to facilitate comparative studies of Latin American intelligence sector, a matrix was developed with different dimensions of analysis that incorporates previous studies, especially the one of Peter Gill (2016). In sum, this paper intended to show the remaining challenges of democratization of intelligence in Latin America and in order to assess the degree of progress and setbacks of the democratic governance of intelligence in Latin American countries, a methodological tool was generated for comparative purposes.

NOTAS

1. Una versión previa de este trabajo fue presentado como "Intelligence challenges in Latin America and prospects for reform: A comparative matrix on democratic governance" en ISA Annual Convention, 2016, Atlanta, Georgia, 16-19 de Marzo, 2016.

* Investigadora Asistente, CONICET/IIGG-UBA. Doctora en Ciencias Sociales de la Universidad de Buenos Aires y de l'École des Hautes Études en Sciences Sociales (EHESS). otamendialejandra@gmail.com

** Consultor; integra el Portal de Seguridad (www.portalseguridad.org) eduardo_e_estevez@yahoo.com.ar

REFERENCES

ADC (2015), *El (des)control democrático de los organismos de inteligencia en Argentina*. Asociación por los Derechos Civiles, Buenos Aires.

Andregg, Michael (2012), "Do intelligence bureaucracies fear ethics, and if so, why?" *International Journal of Intelligence Ethics*, Vol. 3, No. 2, pp. 100-120.

Andregg, Michael M. & Peter Gill (2014), Comparing the Democratization of Intelligence, *Intelligence and National Security*, 29:4, 487-497.

Arslanian, León Carlos (2008), *Un cambio posible. Delito, inseguridad y reforma policial en la Provincia de Buenos Aires*, Argentina, Editorial Edhasa.

Barreiro, Katalina & Fredy Rivera Vélez (2011), "Rendición de cuentas, Democracia e Inteligencia". En: Rivera Vélez, Fredy (Coordinador). *Inteligencia estratégica y Prospectiva* . Quito: FLACSO ECUADOR – SENAIN – AECID.

Basombrío, Carlos &Rospigliosi, Fernando (2006), *La seguridad y sus instituciones en el Perú a inicios del Siglo XXI. Reformas democráticas y neomilitarismo*, Perú, Instituto de Estudios Peruanos.

Born, Hans and Fairlie Jensen (2007), "Intelligence Services: Strengthening Democratic Accountability", Chapter 15, pp. 257-269 in Born, Hans &Caparini, Marina (eds.) *Democratic control of intelligence services: containing rogue elephants*, England, Hampshire, Ashgate Publishing Limited.

Brandão, Priscila Carlos (2010), *Serviços secretos e democracia no Cone Sul: Premissas para uma convivência legítima, eficiente e profissional*, Brasil, Editora Impetus.

Brandão, Priscila Carlos, &Cepik, Marco (orgs.) (2013), *Inteligencia de segurança pública: Teoría e prática no control da criminalidade,* Brazil, Editora Impetus.

Bruneau, Thomas C. &Boraz, Steven C. (eds.) (2007), *Reforming intelligence: Obstacles to democratic control and effectiveness*, University of Texas Press.

Caparini, Marina (2007), "Controlling and Overseeing Intelligence Services in Democratic States", in Born, Hans &Caparini, Marina (eds.) *Democratic control of intelligence services: containing rogue elephants*, England, Hampshire, Ashgate Publishing Limited.

Cepik, Marco & Ambros, Christiano (2012), "Explicando falhas de inteligência governamental: Fatores histórico -institucionais, cognitivos e políticos", *Varia Historia*, Vol. 28, No. 47, pp. 79-99, Belo Horizonte.

CIDH (2009), *Informe sobre seguridad ciudadana y derechos humanos*, Comisión Interamericana de Derechos Humanos, OEA/Ser.L/V/II. Doc. 57, 31 de diciembre.

Coates, Brice (2013), "What is past is prologue: Historical and organizational factors in establishing a director of the United States Intelligence Community", Thesis, Faculty of Graduate Studies, University of Calgary, 200 pp. http://theses.ucalgary.ca/bitstream/11023/912/2/ucalgary_2013_coates_brice.pdf

Coyne, John W. &Bell, Peter (2011), "Strategic intelligence in law enforcement: a review", *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 6, No.1, pp. 23-39.

Coyne, John; Neal, Stuart; &Bell, Peter (2014), "Reframing intelligence: Challenging the Cold War intelligence doctrine in the information age", *International Journal of Business & Commerce*, Vol. 3, No. 5, pp. 53-68.

Crosston, Matthew (2016), "Bringing Non-Western Cultures and Conditions into Comparative Intelligence Perspectives: India, Russia, and China", *International Journal of Intelligence and CounterIntelligence*, 29: 110–131.

Davies, Philip H. J. & Kristian C. Gustafson (eds.) (2013), *Intelligence elsewhere: spies and espionage outside the Anglosphere*, Georgetown University Press, Washington, DC.

Diccionario LID Inteligencia y Seguridad (2013), España, LID Editorial.

Eissa, Sergio (2014), "Estado, sociedad y teorías de las políticas públicas", en Eissa, Sergio (coord.), *Políticas públicas y seguridad ciudadana*, Argentina, Editorial EUDEBA.

Eskens, Sarah, Ot van Daalen& Nico van Eijk (2015), *Ten standards for oversight and transparency of national intelligence services*, Institute for Information Law, Amsterdam, University of Amsterdam.

Estévez, Eduardo E. (2014a), "Comparing intelligence democratization in Latin America: Argentina, Peru, and Ecuador cases", *Intelligence and National Security*. Vol. 29, No. 4, pp. 552-580.

Estévez, Eduardo E. (2014b), "Inteligencia criminal: Una nueva disciplina para una antigua profesión", en Eissa, Sergio (coord.), *Políticas públicas y seguridad ciudadana*, Argentina, Editorial EUDEBA.

Estévez, Eduardo E. (2015), "La inteligencia en el banquillo / Intelligence in the hot seat", Argentina, mímeo.

Fernández, Jesús (2009), "Inteligencia criminal", *Inteligencia y Seguridad: Revista de análisis y prospectiva*, Nº 6, pp. 87-98.

Gill, Peter (2007), "Democratic and Parliamentary Accountability of Intelligence Services After 9/11", pp.195-216, in Born, Hans &Caparini, Marina (eds.) *Democratic control of intelligence services: containing rogue elephants*, England, Hampshire, Ashgate Publishing Limited.

Gill, Peter (2012), "Alguns aspectos da reforma da inteligência na América Latina", *Varia Historia*, Vol. 28, No. 47, pp. 101-120, Belo Horizonte.

GILL, Peter (2016), *Intelligence Governance and Democratisation.A comparative analysis of the limits of reform*. Londres, Routledge.

Gómez de la Torre, Andrés (2013), "Política y Legislación de Inteligencia en el Perú e Iberoamérica: Tendencias y Perspectivas", *Documento 1*, Instituto de Estudios Internacionales (IDEI), Pontificia Universidad Católica del Perú, Lima.

Gomez de la Torre Rotta, Andrés & Arturo Medrano Carmona (2015),"Intelligence Laws in Peru and Latin Americ a—Historical, Legal, and Institutional Evolution", in: Swenson, R. and Sancho, C. (ed.). *Intelligence Management in the Americas*. Washington D.C.: NI Press, june, pp. 29-47.

Jervis, Robert (2007), "Intelligence, civil-intelligence relations and democracy," en Bruneau, Thomas C. y Boraz, Steven C. (eds.), *Reforming intelligence: Obstacles to democratic control and effectiveness*, EE.UU, University of Texas Press.vii

Maldonado, Carlos (2009), "Dilemas antiguos y modernos en la inteligencia estratégica en Sudamérica", *Security and Defense Studies Review*, Vol. 9, Nros. 1 & 2, pp. 49-66.

Margaría, Paulo and Schnyder, Celeste (2014), "Cuando el poder político necesita información": Notas sobre el vínculo política y policía en la Argentina reciente, ESTUDIOS - N° 32 -ISSN 0328-185X (Julio-Diciembre 2014) 243-263

Markowitz, Lawrence P. (2011), "Unlootable resources and state security institutions in Tajikistan and Uzbekistan", *Comparative Political Studies*, Vol. 44, No. 2, pp. 156-183.

Marques Kuele, Giovanna, Gustavo Moller, Mariana Falcão Chaise& Pedro Romero Marques (2015), "Análise de Redes: possibilidades analíticas para o estudo comparado em Inteligência Governamental", *VIII Congreso Latinoamericano de Ciencia Política*, Universidade Federal do Rio Grande do Sul, Lima, 21- 24 june 2015.

Matei, Florina Cristiana &Bruneau, Thomas C. (2011a), "Intelligence reform in new democracies: Factors supporting or arresting progress", *Democratization*. Vol. 18, pp. 602–630.

Matei, Florina Cristiana &Bruneau, Thomas C. (2011b), "Policymakers and intelligence reform in the new democracies", *International Journal of Intelligence and CounterIntelligence,* Vol. 24, pp. 656-691.

Matei, Florina Cristiana (2014), "The media's role in intelligence democratization", *International Journal of Intelligence and CounterIntelligence*, Vol. 27, No. 1, pp. 73-108.

Morales Peña, Juan Carlos (2016), "Hacia una revisión estratégica del sector de inteligencia en El Salvador", *Revista Policía Y Seguridad Pública*, 5:2, 209-284, Centro de Investigación Científica.

Otamendi, Alejandra y Estévez, Eduardo (forthcoming), "Inteligencia en América Latina: desafíos de democratización y oportunidades para la seguridad ciudadana", in Fernández Rodríguez, J.J. y Sansó-Rubert Pascual, D. *Avances en Inteligencia*, Madrid, Plaza y Valdés Editores.

Otamendi, María Alejandra &Fleitas, Diego (2015), "Las mediciones de seguridad ciudadana, crimen organizado y monitoreo y evaluación de las fuerzas de seguridad en una sociedad democrática. Desafíos respecto a la construcción de indicadores y a sus fuentes de información en la Argentina", en Pontón Cevallos, Daniel (comp.), *Seguridad y Delincuencia Organizada: Nuevos indicadores y políticas públicas,* Ecuador, FLACSO Sede Ecuador.

Padilla, Tanals, &Walker, Louise E. (2013), "In the archives: History and politics", *Journal of Iberian and Latin American Research*, Vol. 19, pp. 1-10.

Piedra Cobo, Lorena Yáel (2012), *Coyunturas críticas en los sistemas de inteligencia*, Ecuador, FLACSO Sede Ecuador, 100 p.

PNUD (2013), *Informe regional de desarrollo humano 2013-2014 - Seguridad ciudadana con rostro humano: Diagnóstico y propuestas para América Latina*, Nueva York, Programa de las Naciones Unidas para el Desarrollo (PNUD), 265 p.

Ravndal, Jakob Aasland (2009), "Developing intelligence capabilities in support of UN peace operations: An institutional approach", Master's Thesis in Peace and Conflict Studies, Department of Political Science, Noruega, University of Oslo.

Sain, Marcelo (2008), "El Leviatán Azul. Policía y política en la Argentina", Argentina, Siglo XXI.

Sansó-Rubert Pascual, Daniel (2011), "Inteligencia criminal: una elección estratégica en clave de seguridad frente a la iniciativa de la delincuencia organizada", en Rivera Vélez, Fredy (ed.), *Inteligencia estratégica y prospectiva*, Ecuador, FLACSO-Ecuador y Secretaría Nacional de Inteligencia del Ecuador, pp. 215-238.

Schreier, Fred (2007),"The Need for Efficient and Legitimate Intelligence", pp. 25-44, in Born, Hans &Caparini, Marina (eds.) *Democratic control of intelligence services: containing rogue elephants*, England, Hampshire, Ashgate Publishing Limited.

Sheptycki, James (2008), "Policing, intelligence theory and the new human security paradigm: Some lessons from the field", en Gill, Peter; Marrin, Stephen; y Phythian, Mark (eds.), *Intelligence theory: Key questions and debates*, UK, Routledge.

Shiraz, Zakia (2015), "Writing in a time of war: Journalism, oversight and Colombia's intelligence community", paper prepared for the International Studies Association 2015 Annual Convention, EE.UU., New Orleans, LA, 18 – 21 February.

Spencer, Herbert (2005), "Management of National Intelligence", in Johnston, Rob, *Analytic Culture in the US Intelligence Community: An Ethnographic Study*, Central Intelligence Agency, The Center for the Study of Intelligence, Washington, DC.

Swenson, Russell G. (2015),"Management of National Intelligence, Introduction", in Swenson, Russell G. &Sancho, Carolina (eds.) (2015*) Intelligence Management in the Americas*, Washington, DC: Hirane Editors.

Ugarte, José Manuel (2014), "Panorama de la inteligencia criminal latinoamericana. Desarrollo, dilemas y dificultades", 41-54, *URVIO. Revista Latinoamericana de Estudios de Seguridad*, No. 17, Quito, diciembre 2015, FLACSO Sede Ecuador.

United Nations Human Rights Council (2010), "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/14/46, Geneve, United Nations, in: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

Zegart, Amy (1999), *Flawed by design: The evolution of the CIA, JCS and NSC*, EE.UU., Stanford University Press.

GUARDA OBRIGATÓRIA DE REGISTROS DE TELECOMUNICAÇÕES NO BRASIL: SOBRE AS ORIGENS DA RETENÇÃO DE DADOS E AS PERSPECTIVAS PARA DIREITOS FUNDAMENTAIS

Resumo: O ordenamento jurídico brasileiro obriga empresas do setor de telecomunicações a guardarem metadados preventivamente por um determinado período de tempo. A partir da análise do arcabouço regulatório brasileiro a nível legal e infralegal, este artigo traça as origens, identifica a abrangência e desvenda a motivação das obrigações de guarda de dados de telecomunicações no país. São discutidos dispositivos da Lei n. 12.850 de 2013 ("Lei das Organizações Criminosas"), da Lei n. 12.965 de 2014 ("Marco Civil da Internet") e das Resoluções nº 426 de 2005, 477 de 2007 e 614 de 2013 da Agência Nacional de Telecomunicações (ANATEL), aplicáveis às prestadoras de telefonia e de Internet, e feitas breves observações comparativas com o direito europeu. Investigar as origens das obrigações de retenção de dados e, em especial, as razões e justificativas dadas ao estabelecimento delas é exercício inédito e essencial para a discussão da constitucionalidade de tais obrigações no país.

Palavras-chave: Retenção de dados, Registros, Privacidade, Segurança pública, ANATEL.

Retención de datos de telecomunicaciones en Brasil: orígenes y perspectivas

Resumem: El ordenamiento jurídico brasileño exige que las empresas del sector de las telecomunicaciones mantengan metadatos preventivamente por un período determinado de tiempo. A partir del análisis del marco regulatorio brasileño a nivel legal e infra-legal, este artículo traza los orígenes, identifica el alcance y destapa la motivación de las obligaciones de guardia de datos de telecomunicaciones en el país. Se discuten dispositivos de la Ley n. 12.850 de 2013 ("Ley de las organizaciones criminales"), de la Ley n. 12 965 de 2014 ("Marco Civil de Internet") y de las Resoluciones n. 426 de 2005, 477 de 2007 y 614 de 2013 de la Agencia Nacional de Telecomunicaciones (ANATEL), aplicables a los proveedores de teléfono e Internet, y son hechas breves observaciones comparadas a la luz del derecho europeo. Investigar los orígenes de estas obligaciones y, en particular, las razones y justificaciones dadas para el establecimiento de las cuales es un ejercicio sin precedentes de fundamental importancia para la discusión acerca de la constitucionalidad de dichas obligaciones en el país.

Palabras clave: Retención de datos, Registros, Privacidad, Seguridad pública, ANATEL.

Telecommunications Data Retention in Brazil: origins and perspectives

Abstract: The Brazilian legal system requires companies of the telecommunications sector to retain metadata for a given period of time. Through the analysis of the Brazilian framework at the statutory and administrative levels, this paper traces the origins, identifies the scope and uncovers the motivation of the data retention mandates in the country. Provisions of Federal Law no. 12.850 of 2013 ("Law of Criminal Organizations"), Federal Law no. 12 965 of 2014 ("Civil Rights Framework for the Internet"), and Resolutions no. 426 of 2005, 477 of 2007, and 614 of 2013 of the National Telecommunications Agency (ANATEL), applicable to telephone carriers and Internet service providers, are examined and their significance is briefly discussed through a comparative lens. The reconstruction of the origins of these obligations and, in particular, the rationalebehind their establishment is a novel and essential studyfor an informed discussion on the constitutionality of such obligations in the country.

Keywords: Data retention, Logs, Privacy, Law enforcement, ANATEL.

JACQUELINE DE SOUZA ABREU*

INTRODUÇÃO

Na utilização de serviços de telecomunicações são gerados dados que são capazes de informar quem, quando, com quem e a partir de onde se comunicou. Eles são os chamados *metadados*. No uso da telefonia fixa, dizem respeito aos registros de ligação (os números entre os quais se estabeleceu uma ligação), data e hora da chamada e sua duração. No uso da Internet, referem-se ao endereço de IP, data, hora e duração da conexão à Internet ou do acesso a uma aplicação. No uso de aparelhos de telefonia móvel, com os quais tanto se faz ligações quanto se utiliza a Internet, somam-se aos citados os registros acerca da Estação Rádio Base (ERB) com a qual o aparelho se comunicou para que a conexão – seja a ligação ou o uso da Internet – pudesse ser feita.

A análise desses dados é bastante reveladora. Registros telefônicos são capazes de informar contatos e intensidade desses contatos; registros de uso da Internet revelam informações sobre a navegação do usuário e, assim, seus hábitos e interesses; registros de localização, decorrentes dos dados sobre a torre de rádio, informam, como já se supõe pelo nome, por onde a pessoa esteve. É por isso que eles, por um lado, (i) são sensíveis a questões sobre privacidade e sigilo das comunicações e, por outro, (ii) são bastante úteis como instrumentos de investigação e meios de prova (Abreu, 2015: 25).

A disponibilidade desses metadados, que garantiria a possibilidade de utilização deles em investigações e processos, é assegurada pelo Estado por meio da introdução de obrigações às prestadoras ou aos provedores de serviços de *guardá-los* ou *retê-los* por certo período de tempo. Do contrário, a disponibilidade estaria suscetível às políticas adotadas por cada empresa quanto à destruição ou apagamento de dados. A imposição de deveres de retenção por parte do Estado também se sobrepõe ao consentimento do titular dos dados sobre a guarda e aos termos acordados entre o usuário e a empresa de telefonia e internet; dados *devem ser* retidos, por prescrição legal. E não para aí: os dados de *todos* devem ser retidos, de onde se fala na criação de um aparato de vigilância em massa.

Tendo isso em vista, o objetivo do presente texto é apresentar (i) resultados de pesquisa sobre as origens, abrangência e *ratio legis* das obrigações de retenção de dados no Brasil e (ii) breves reflexões sobre a matéria à luz do direito comparado. Esse tipo de estudo basilar pode tanto auxiliar a elaboração de estratégias de reforma que pretendam desafiar a constitucionalidade de tais obrigações no país como antecipar as limitações jurídicas de uma tal iniciativa. É essa a contribuição que o presente artigo pretende fazer.

ORIGENS: O QUADRO JURÍDICO DE RETENÇÃO DE DADOS NO BRASIL

Obrigações de guarda a nível legal

O Congresso Nacional brasileiro recentemente aprovou duas leis que contêm obrigações de guarda de registros para provedores de telefonia, conexão à Internet e aplicações de Internet.

Aprimeira é a Lei das Organizações Criminosas (Lei nº 12.850, de 2 de agosto de 2013), queobrigaempresas provedoras de telefonia a guardar registros de chamada por 5 anos (art. 17):

> Art. 17. As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no art. 15 [o delegado de polícia e o Ministério Público], registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais.

Tal dispositivonão constava na origem da lei, o Projeto de Lei do Senado nº 150, de 24 de maio de 2006, proposto pela senadora Serys Slhessarenko (PT/MT). Ele foi somente incluído em substitutivo adotado em 3 de dezembro de 2009, após meses de reexame da matéria.[1] Apesar da ausência de justificativa expressa, a finalidade evidente do dispositivo é incrementar a eficiência na segurança pública, tendo em vista o teor do projeto de lei em que foi incluído.

Deste processo, cabe destacar que, apesar de a imposição do dever de guarda não servir apenas ao combate de organizações criminosas, mas sim a todo e qualquer procedimento administrativo, cível ou criminal que envolva coleta de provas, não se pretendeu reservar a inclusão de um tal dispositivo no ordenamento jurídico brasileiro a uma lei de caráter geral.

Esse raciocínio, contudo, limitou outras pretensões também incluídas no substitutivo, o qual previa:

> Art. 19. Os provedores da rede mundial de computadores – Internet – manterão, pelo prazo mínimo de 6 (seis) meses, à disposição das autoridades mencionadas no art. 17, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio da rede de equipamentos informáticos ou telemáticos. [...]

Tal artigo foi excluído após voto do relator da Comissão de Constituição e Justiça e de Cidadania Deputado Vieira da Cunha (PDT-RS), em 14 de dezembro de 2012, quando já havia se tornado partedo Projeto de Lei 6.578, de 09 de dezembro de 2009. A razão dada foi justamente a de que tal disposição deveria ser discutida em "legislação específica de caráter transversal que não esteja limitada à repressão das organizações criminosas" (Vieira da Cunha, 2012).

Com isso se chega ao segundo material normativo relevante. O Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) trouxe os seguintes dispositivos:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Contribuindo para clareza dos destinatários das obrigações de reter dados e dos limites delas, a lei inclui as definições dos termos-chave dos artigos: desde quem são "administradores de sistemas autônomos"[2] ao que se engloba nos termos"registros de conexão"[3] e "registros de acesso a aplicação". [4]

Relevante aqui é o fato de que estudos sobre os bastidores legislativos do Marco Civil da Internet apontam que a pressão de órgãos com atribuições investigativas operoudiretamente tanto na inclusão como na aprovação desses dispositivos na lei (Papp, 2014: 62, 108-10; Brito Cruz, 2015: 109-10).

Diante disso, pode-se concluir que a racionalidade dos dispositivos *legais* de retenção de dados de telecomunicações no Brasil se baseia fundamentalmente, com o perdão de reforçar o óbvio, na garantia de eficácia de processos que venham a depender ou possam se aproveitar dessas informações. Apesar de os dados também permanecerem disponíveis para eventuais procedimentos cíveis ou administrativos, a pressão pela criação desses dispositivos adveio especialmente de autoridades de investigação criminal, interessados na sua utilização para fins de segurança pública.

Obrigações de guarda a nível infralegal

Em 1997, com a privatização das telecomunicações no Brasil, foi criada a Agência Nacional de Telecomunicações (ANATEL) (Sundfeld, 2006). Por sua competência para expedição de normas infralegais (art. 19 da Lei nº 9.472, de 16 de julho de 1997), as *resoluções,* e no exercício de sua função de regulação das telecomunicações, tal agência organiza a prestação de serviços e concretiza direitos de usuários no Brasil.

Dessa regulação decorre a criação, mesmo que a princípio não intencional, de enormes bancos de dados (Abreu & Antonialli, 2015: 17): originam-se de regulamentos da ANATEL as obrigações de retenção de dados que primeiro transformaram provedores de telefonia e de Internet em "parceiros" do Estado na garantia da efetividade de processos e eficiência na segurança pública no Brasil; isto é, antes mesmo das duas leis vistas acima.

A Resolução nº 426, de 9 de dezembro de 2005 – Regulamento do Serviço Telefônico Fixo Comutado (STFC) prevê, no art. 22, que "Art. 22. A prestadora deve manter todos os dados relativos à prestação do serviço, inclusive os de bilhetagem, por um prazo mínimo de 5 (cinco) anos.".

Na prática, isso significa que não só registros de chamada, mas sim quaisquer outros dados gerados na prestação do serviço de telefonia fixa, devem ser obrigatoriamente guardados pelas empresas prestadoras de serviço de telefonia fixa.

Em comparação com a Resolução nº 85, de 30 de dezembro de 1998, que primeiro se aplicou aos serviços de telefonia fixa após a criação da ANATEL, essa obrigação foi uma inovação da nova resolução; isto é, não existia previamente. Na verdade, a análise dos anais da consulta pública que antecedeu a aprovação do novo regulamento (Consulta Pública nº 641, de 09 de setembro de 2005) permite verificar que o tal artigo também não constava na redação original da proposta de novo texto (ANATEL, 2005) e foi incluído somente após sugestão de Rubens Donati Jorge (Contribuição nº 754), em 02 de outubro de 2005, com os seguintes termos:

> Art. Novo. As prestadoras devem manter os registros decorrentes da bilhetagem de chamadas locais e de longa distância nacional e internacional armazenados, obrigatóriamente,[*sic*] por pelo menos 5 (cinco) anos a partir do registro dos dados.

Na justificativa, afirmou que a "necessidade de manter os registros decorre de eventuais contestações de débitos, investigações policiais, processos judiciais, etc.. O prazo de 5 anos é coerente com o utilizado na legislação tributária" (Jorge, 2008). Pouco tempo depois, em 10 de outubro de 2005, a ouvidoria da ANATEL fez exatamente a mesma proposta de novo artigo, com idêntica justificativa (Santos, 2005). O Instituto de Defesa do Consumidor, em sua contribuição à Consulta, acolheu a sugestão da ouvidoria e expressamente concordoucom a adição do mesmo artigo (IDEC, 2005).[5]

Como se vê da redação final do art. 22, a obrigação de guarda sugerida foi ampliada: *todos* os dados gerados na prestação do serviço, para *além* dos de bilhetagem, devem ser guardados. Além de não especificar quais dados são esses, a resolução também não informa por quem e a que fins tais dados retidos poderão ser usados (Abreu & Antonialli, 2015: 17).

Na telefonia móvel, a situação é em parte semelhante, em parte diferente. A Resolução nº 477, de 7 de agosto de 2007 – Regulamento sobre Serviço Móvel Pessoal (SMP) determina o seguinte, no art. 10, XXII:

> Art. 10. Além das outras obrigações decorrentes da regulamentação editada pela Anatel e aplicáveis a serviços de telecomunicações e, especialmente, ao SMP, constituem deveres da prestadora:
>
> XXII - manter, à disposição da Anatel e demais interessados, os documentos de natureza fiscal, os quais englobam ofs[*sic*] dados das ligações efetuadas e recebidas, data, horário de duração e valor da chamada, bem como os dados cadastrais do assinante, por um prazo mínimo de 5 (cinco) anos, em conformidade com o que prescreve o art. 11 da Lei nº 8.218/1991, de 29/08/1991, c/c art. 19 da Resolução nº 247, de 14/12/2000.

Os regulamentos aplicáveis a este serviço que antecederam essa normativa (Resoluções nº 245, de 8 de dezembro de 2000, e nº 477, de 27 de setembro de 2002) não continham tal obrigação de guarda.Nos autos da Consulta Pública nº 642, de 17 de novembro de 2005, que discutiu alterações ao regulamento prévio, também não há nenhuma sugestão de inclusão do tal artigo com tal redação. O mais provável é que a ANATEL tenha "adequado" o novo regulamento aplicável à telefonia móvel à luz dos deveres dos prestadores de telefonia fixa – o dever de reter dados por 5 anos, entre eles.

O interessante, no caso da telefonia móvel, é que a redação do dispositivo sugere qual a lógica por traz do estabelecimento de tal obrigação pela ANATEL: o atendimento ao que prescreve o art. 11 da Lei nº 8.218, de 29 de agosto de 1991, combinado com o art. 19 da Resolução nº 247, de 14 de dezembro de 2000. São eles:

> Art. 11. [Lei nº 8.218/1991] As pessoas jurídicas que utilizarem sistemas de processamento eletrônico de dados para registrar negócios e atividades econômicas ou financeiras, escriturar livros ou elaborar documentos de natureza contábil ou fiscal, ficam obrigadas a manter, à disposição da Secretaria da Receita Federal, os respectivos arquivos digitais e sistemas, pelo prazo decadencial previsto na legislação tributária.
>
> Art. 19. [Resolução nº 247/00] Os contribuintes do FUST [Fundo de Universalização dos Serviços de Telecomunicações] deverão manter à disposição Anatel todas as informações necessárias ao exercício da gestão do recolhimento da contribuição para o FUST, pelo prazo mínimo de 5 anos. [...]

Em outras palavras, existe uma regra geral prevista em lei de 1991 de que pessoas jurídicas mantenham documentos fiscais à disposição da Receita Federal pelo prazo decadencial previsto na legislação tributária, que é de 5 anos. Tal obrigação, então, foi transportada também para o regulamento da ANATEL. Ao mesmo tempo, pelo que se nota da referência ao art. 19 da Resolução nº 247, a preservação de registros por determinado período de tempo também serve à efetividade de procedimentos da ANATEL para apuração de descumprimento de obrigações por parte das prestadoras.

Nota-se, entretanto, um descompasso no atendimento desses objetivos pela ANATEL. Ao passo que, no regulamento de telefonia *móvel*, a redação do artigo expressou as intenções de atender a tal lei e regulamento, dentro de sua finalidade, no regulamento de telefonia *fixa*, a redação não fez a mesma referência e ainda extrapolou as razões dessa lógica, porque não limitou o dever de guarda aos documentos fiscais. Não coincidentemente, em novas consultas públicas que pretendem alterar o regulamento de telefonia *fixa* em vigor, algumas contribuições sugerem a delimitação dos termos do dispositivo aos fins buscados – com identificação de que os dados a serem guardados são os de natureza fiscal e com referência ao art. 11 da Lei 8.218/91 (Telefónica /Vivo, Contribuições nº 194 e 198, 2011).

Apesar de a justificativa da guarda de dados se voltar aos fins fiscais e fiscalizatórios da ANATEL, ambas as normas que estabelecem esses deveres na telefonia fixa e móvel sustentaram por longo período(ao menos 8 anos) também a conveniência da disposição desses dados para fins investigatórios e processuais (Abreu & Antonialli, 2015: 18). A Lei das Organizações Criminosas, que obrigou empresas de telefonia a guardarem dados expressamente a estes fins, é apenas de 2013.

Além disso, cabe ressaltar que, em razão dos termos dos regulamentos, os deveres de guarda de registros persistem mesmo quando se descolam de sua motivação: se o serviço de telefonia contratado é associado a tarifas fixas (*flat rates*), por exemplo, a duração de uma chamada ou o número a que se ligou não afetam a cobrança final do usuário que será tributada; mesmo assim, esses dados precisarão ser retidos pelas companhias. Portanto, os largos termos dos regulamentos fazem a ANATEL extrapolar sua competência de regulação das telecomunicações, atendendo, mesmo que indiretamente, a interesses de autoridades do Estado na garantia de eficácia dos processos e, especialmente, de órgãos de segurança pública do Estado nas atividades de prevenção e repressão criminal.

No processo que resultou na aprovação da Resolução nº 614, de 28 de maio de 2013 – Regulamento do Serviço de Comunicação Multimídia, a sensibilidade da ANATEL a razões e pressões externas ao órgão ficou evidente. O texto original da proposta de regulamento continha os seguintes termos (ANATEL, 2011):

> Art. 65. A Prestadora deve manter os dados cadastrais e os registros de conexão de seus Assinantes pelo prazo mínimo de três anos.
>
> Parágrafo único. A Prestadora de Pequeno Porte deve manter as informações mencionadas no caput pelo prazo mínimo de dois anos.

Quando o texto foi colocado em debate, pela Consulta Pública nº 45, de 8 de agosto de 2011,46 contribuições foram feitas quanto a este dispositivo. A maioria diretamente contestou tal previsão no âmbito da regulação das telecomunicações, uma vez que a ANATEL estaria atuando para a "preservação da segurança pública" e estaria se sobrepondo à discussão sendo conduzida pelo Ministério da Justiça, dentro do contexto das discussões sobre o Marco Civil da Internet, então ainda projeto de lei (Oi, 2011; Telefónica/Vivo, Contribuição nº 846, 2011; Grupo FOLHA/UOL, 2011; Oldenburg, 2011).

Ao cabo, os termos finais do regulamento foram os seguintes: "Art. 53. A Prestadora deve manter os dados cadastrais e os Registros de Conexão de seus Assinantes pelo prazo mínimo de um ano.".

O dever de guarda foi, portanto, reduzido a um ano e a diferenciação dos prestadores foi retirada. Por outro lado, foi incluída a definição de registros de conexão ("conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados, entre outras que permitam identificar o terminal de acesso utilizado"), inexistente na proposta original, ao art. 4º, XVII do regulamento, que é mais abrangente do que previa (e hoje prevê) o texto do Marco Civil da Internet.[6] As "outras" informações que permitem identificar o terminal de acesso não fazem parte da definição de registros de conexão do Marco Civil da Internet; o regulamento da ANATEL, portanto, o ultrapassa.

O prazo menor do regulamento da ANATEL para guarda de metadados relacionados ao tráfego na Internet a (relativa maior) clareza na definição do que deve ser guardado,quando comparado às obrigações referentes à telefonia, podem ser diretamente relacionados ao fato de a resolução ter sido elaborada no contexto de amplo debate público sobre o Marco Civil da Internet. Foi nessa época também que tribunais europeus emitiram decisões contrárias apráticas de retenção de dados, as quais receberam especial atenção da comunidade acadêmica e da sociedade civil no Brasil.[7] Essa conjuntura, portanto, acabou por constranger a ANATEL em sua regulação.

PERSPECTIVAS: OS DESAFIOS JURÍDICOS

As previsões legais e infralegais de retenção de dados geram controvérsias. No âmbito do discurso político, as preocupações giram em torno da expansão da vigilância em massa do Estado sobre todos os cidadãos; a crítica invoca o cenário orwelliano do *Big Brother*. No âmbito jurídico, questões são levantadas sobre a constitucionalidade dessas medidas. Isso porque a análise de metadados, ressalte-se outra vez, é capaz de oferecer retratos sobre personalidade, hábitos, interesses, círculo social e localização do usuário, que estão diretamente relacionados a sua privacidade e afetam o sigilo das comunicações, isto é, direitos fundamentais. Soma-se a isso o fato de que a guarda de registros ocorre *preventivamente*, sem estar conectada a um perigo concreto ou a uma suspeita individualizada de envolvimento em crime (Albrecht, 2015: 12-3), o que estaria em tensão com o princípio da presunção de inocência (Abreu, 2015: 25).

A questão jurídica relevante é, portanto, se a Constituição Federal autoriza o Congresso Nacional e/ou a ANATEL a instituir tais obrigações de guarda. E, se sim, *como, quando* e *em que termos*. A apresentação de uma resposta completa extrapola os objetivos desse texto e merece estudo próprio; no entanto, apresentam-se aqui breves observações à luz do direito comparado.

Em abril de 2014, a Diretiva europeia 2006/24/EG, que impunha aos países-membros da União Europeia o dever de sancionar a guarda obrigatória de metadados de telecomunicações para fins de prevenção e repressão penal, foi considerada inválida pelo Tribunal de Justiça da União Europeia (TJUE), por limitar os direitos à vida privada e à proteção de dados pessoais de modo "desproporcional" (Digital Rights Ireland, 2014).Em diversas cortes constitucionais de países europeus, as versões nacionais dessas leis também já vinham sendo desafiadas e derrubadas (Vedaschi & Lubello, 2015: 22-5). Em dezembro de 2016, o TJUE voltou a se manifestar contra retenção de dados: declarou que legislações nacionais que "estabeleça[m], com a finalidade de lutar contra a criminalidade, a conservação generalizada e indiferenciada de todos os dados de tráfego e localização de todos os assinantes e usuários [...]" também estariam em desacordo com a Carta de Direitos Humanos da União Europeia e a Diretiva 2002/58/CE sobre privacidade e comunicações eletrônicas (Tele2 Sverige AB, 2016).

O impacto da jurisprudência européia no Brasil já foi notado em críticas tecidas aos arts. 13 e 15 do Marco Civil da Internet, no âmbito do debate sobre a regulamentação da lei lei (Brito Cruz, Marchezan, & Santos, 2015: 25-35). Entretanto, a reflexão que essas decisões provocam para Brasil não deve parar por aí, uma vez que podem indicar que a sustentação de deveres de guarda de metadados no âmbito da prestação de serviços de telefonia e internet coloca o país na "contramão do mundo" (Lemos, 2015: 9).

A discussão precisará ser cuidadosa. Apesar da força retórica e do peso de autoridade, o raciocínio das decisões europeias mencionadas não é imediatamente importável ao Brasil. Lá, a doutrina e a jurisprudência partem de uma concepção abrangente do direito à autodeterminação informacional, que protege o controle do indivíduo sobre o tratamento (coleta, guarda, divulgação, utilização, etc) de seus dados pessoais, e da privacidade, que protege a vida privada, familiar, o lar e a correspondência das pessoas. Qualquer ação do Estado que interfira nesse controle ou nessa esfera privada – como a instituição do dever de guarda – é tida por *intervenção* no direito fundamental, que precisa ser necessariamente amparada em *lei* e *justificada* nos termos do princípio da proporcionalidade (Vedaschi & Lubello, 2015: 26-7).

No Brasil, além da ausência de um regime robusto e específico de proteção de dados, não é possível afirmar que a doutrina e a jurisprudência partem ou partirão de semelhante definição abrangente do âmbito de proteção dos direitos constitucionais à privacidade e ao sigilo das comunicações. Pelo contrário, comentadores apontam que as interpretações tradicionais do âmbito de proteção de tais direitos no Brasil são mais limitadas em seu escopo (Mendes, 2014: 161-5; Abreu & Antonialli, 2015:: 15-7; Azeredo, 2015), de forma que a própria questão da existência de uma "intervenção" em ou restrição a algum direito fundamental,em razão da

criação de um dever de guarda, ainda precisa ser enfrentada. O endereçamento da retenção de dados no Brasil, portanto, deverá superar esses percalços conceituais.

Paralelamente, vale destacar que a decisão do TJUE de 2014 não descartou a constitucionalidade da retenção de dados *em princípio*, como inconstitucional *per se*, mas sim a forma como foi concretizada na diretiva (Vedaschi & Lubello, 2015:: 24). Mesmo a decisão do TJUE de 2016 ainda deixou espaço para a criação de modelos de retenção de dados que ainda seriam compatíveis com o direito europeu, se não forem "generalizados e indiferenciados" (Woods A. K., 2016; Woods L., 2016). Diante disso, é preciso estar preparado para discutir como a retenção de dados hoje existente no ordenamento brasileiro poderia ser reconciliada com a Constituição brasileira, se equilibradamente redesenhada e acompanhada de um regime jurídico robusto de garantias processuais e substantivas dos cidadãos titulares de dados.

Na Alemanha, por exemplo, o tribunal federal constitucional admitiu que a delimitação das hipóteses e requisitos de acesso aos registros guardados, como pela restrição apenas a fins de persecução penal de crimes graves, na existência de indícios concretos de autoria e participação, e estabelecimento de regras de segurança na guarda dos dados e de transparência sobre a utilização pudessem tornar as obrigações de retenção de dados *proporcionais* (Vorratsdatenspeicherung, 2010).[8] Para o Brasil, isso provocaria a reflexão sobre a necessidade de reforçar os esforços de elaboração e aprovação de salvaguardas jurídicas que protejam cidadãos contra abusos de autoridades do Estado no que se refere ao manejo de dados pessoais e minimizassem os riscos advindos de um esquema de retenção de dados.

CONCLUSÃO

O artigo mostrou que a Lei das Organizações Criminosas, de 2013, e o Marco Civil da Internet, de 2014, primeiro instituíram o dever *legal* de retenção de registros de telecomunicações para fins de segurança pública no Brasil. Essa obrigação é mais antiga no Brasil a nível *infralegal*: no âmbito da regulamentação de serviços de telecomunicações, as Resoluções nº 426 de 2005, 477 de 2007 e 614 de 2013 da ANATEL asseguram a disponibilidade de metadados já há mais tempo. A existência de tais obrigações insere o Brasil em um debate global acerca da constitucionalidade de tais disposições dentro de um Estado democrático de Direito que assegura o direito à privacidade e a presunção de inocência.

NOTAS

* Líder do Projeto "Vigilância e Privacidade" no InternetLab (Brasil). Doutoranda em Direito na Universidade de São Paulo (Brasil). Mestra em Direito pela Ludwig-Maximilians-Universität München (Alemanha) e pela University of California, Berkeley (EUA). Contato: jacqueline@internetlab.org.br.

1. O pedido de reexame da matéria junto à Comissão de Constituição, Justiça e Cidadania do Senado Federal ocorreu em 31 de março de 2009, pelo requerimento nº 334 de 2009, feito pelo senador Romeu Tuma (PTB

-SP). O projeto recebeu propostas de emendas e foi objeto de duas audiências públicas neste período. Esse processo deu origem ao substitutivo citado, relatado pelo senador Aloizio Mercadante (PT-SP). Em audiência de 09 de junho de 2009, o presidente do Conselho Nacional dos Procuradores-Gerais do Ministério Público dos Estados e da União, Leonardo Azeredo Bandarra, chegou a defender que a preservação pelo período de 5 anos pode se revelar insuficiente e que deveria ser igual ao tempo de prescrição do crime.

2. Segundo o art. 5, IV do Marco Civil da Internet, é administrador de sistema autônomo "a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País". No Brasil, essa inscrição como sistema autônomo ocorre pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), braço operativo do Comitê Gestor da Internet, e só é feita mediante o preenchimento de certos requisitos (Abreu & Antonialli, 2015: 22, nota de rodapé). Para fins deste trabalho, isso é relevante porque nem todo provedor de conexão à Internet preenche a definição do Marco Civil da Internet que institui a obrigação da guarda de registros de conexão.

3. Art. 4, VI do Marco Civil da Internet: "conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados".

4. Art. 4, VIII Marco Civil da Internet: "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

5. O endosso não é de todo surpreendente, uma vez que a disponibilidade de tais informações também serve a consumidores que se sintam de alguma forma lesados pelas prestadoras, como no caso da verificação de uma cobrança indevida, por exemplo.

6. Ver nota 3 *supra*.

7. Paradigmaticamente, a decisão conjunta dos casos C-293/12 e C-594/12 pelo Tribunal de Justiça da União Europeia, de 08.04.2014, que invalidou a diretiva européia sobre retenção de dados, sob a fundamentação de que restringiria desproporcionalmente os direitos ao respeito à vida privada e à proteção de dados pessoais (Digital Rights Ireland, 2014).

8. Logo após a invalidação da lei alemã, e posteriormente, da própria Diretiva europeia, uma nova lei de retenção de dados foi aprovada, inspirada nos termos da decisão do tribunal alemão. Uma crítica que persiste mesmo aos novos termos é a da verificação empírica da necessidade de existência de obrigações de retenção de dados e seu efetivo impacto em termos de eficiência na segurança pública (Albrecht, 2015:: 26-30). Ver também Abreu & Antonialli (2015: 41-2).

REFERÊNCIAS

Abreu, J. d. S. (2015). Comentário. In F. C. Brito Cruz, J. C. Marchezan, & M. W. Santos, *O que está em jogo na regulamentação do Marco Civil da Internet? Relatório Final sobre o debate público promovido pelo Ministério da Justiça para a regulamentação da Lei 12.965/14* (p. 25). São Paulo: InternetLab.

Abreu, J. d. S., & Antonialli, D. (2015). *Vigilância das Comunicações pelo Estado Brasileiro e a Proteção a Direitos Fundamentais.* São Paulo: InternetLab.

Albrecht, H.-J. (2015). Direito à Privacidade e a Guarda Obrigatória de Dados para Investigações. (F. Brito Cruz, & B. Kira, Entrevistadores) São Paulo: InternetLab.

ANATEL. (2005). *Proposta de Alteração do Regulamento do Serviço Telefônico Fixo Comutado, aprovado pela Resolução nº 85, de 30 de dezembro de 1998.* Retirado de Anexo à Abertura da Consulta Pública nº 641, de 09 de setembro de 2005: http://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C735&Tipo=1&Opcao=finalizadas

ANATEL. (2011). *Proposta de Regulamento do Serviço de Comunicação Multimídia.* Retirado em 01 11, 2016, do Anexo à Consulta Pública nº 45, de 8 de agosto de 2011: http://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1514&Tipo=1&Opcao=finalizadas

Azeredo, J. (2015). Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet. In N. De Lucca, A. Simão Filho, & C. Lima (Eds.), *Direito & Internet III - Marco Civil da Internet* (Vol. Tomo II). São Paulo: Quartier Latin.

Brito Cruz, F. (2015). Direito, Democracia e Cultura Digital: A experiência de elaboração legislativa do Marco Civil da Internet. *Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de São Paulo*. São Paulo, Brasil.

Brito Cruz, F., Marchezan, J., & Santos, M. (2015). *O que está em jogo na regulamentação do Marco Civil da Internet? Relatório Final sobre o debate público promovido pelo Ministério da Justiça para a regulamentação da Lei 12.965/14.* São Paulo: InternetLab.

Digital Rights Ireland, C-293/12 e C-594/12 (Tribunal de Justiça da União Europeia 0804, 2014).

Grupo FOLHA/UOL. (2011, 09 16). *Contribuição nº 857.* Retirado em 01 11, 2016, da Consulta Pública nº 45, de 8 de agosto de 2011, da ANATEL: http://sistemas.anatel.gov.br/SACP/Relatorios/RelatorioDadosBd.asp?pCodProcesso=C1514&pCodTipoProcesso=1&pTipoRelatorio=1

IDEC. (2005, 10 10). *Contribuição nº E-24.* Retirado de Consulta Pública nº 641, de 09 de setembro de 2005, da ANATEL: http://sistemas.anatel.gov.br/sacp/Parametros/ArquivosAnexos/E-24%20-%20E-mail.PDF

Jorge, R. D. (2008, 10 02). *Contribuição nº 754.* Retirado em 01 11, 2016, from Consulta Pública nº 641, de 09 de setembro de 2005, da ANATEL: http://sistemas.anatel.gov.br/SACP/Relatorios/RelatorioDadosBd.asp?pCodProcesso=C735&pCodTipoProcesso=1&pTipoRelatorio=1

Lemos, R. (2015, 10 05). *Audiência Pública na CPI de Crimes Cibernéticos.* Retirado de Câmara dos Deputados: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt061015-crc-sem-revisao

Mendes, L. (2014). *Privacidade, proteção de dados e defesa do consumidor.* São Paulo: Saraiva.

Oi. (2011, 09 16). *Contribuição nº 827.* Retirado em 01 11, 2016, de Consulta Pública nº 45, de 8 de agosto de 2011, da ANATEL: http://sistemas.anatel.gov.br/SACP/Relatorios/RelatorioDadosBd.asp?pCodProcesso=C1514&pCodTipoProcesso=1&pTipoRelatorio=1

Oldenburg, S. (2011, 09 07). *Contribuição nº 825.* Retirado em 01 11, 2016, de Consulta Pública nº 45, de 8 de agosto de 2011, da ANATEL: http://sistemas.anatel.gov.br/SACP/Relatorios/RelatorioDadosBd.asp?pCodProcesso=C1514&pCodTipoProcesso=1&pTipoRelatorio=1

Papp, A. (2014). Em nome da internet: os bastidores da construção coletiva do Marco Civil. *Trabalho de Conclusão de Curso de Graduação em Jornalismo na Escola de Comunicações e Artes da Universidade de São Paulo*. São Paulo, Brasil.

Santos, A. d. (2005, 10 10). *Contribuição nº E-23.* Retirado em 01 11, 2016, de Consulta Pública nº 641, de 09 de setembro de 2005, da ANATEL: http://sistemas.anatel.gov.br/sacp/Parametros/Arquivos Anexos/E-23%20-%20E-mail.PDF

Senado Federal. (n.d.). *Projeto de Lei do Senado nº 150, de 2006.* Retirado de: http://legis.senado.leg.br /mateweb/arquivos/mate-pdf/8236.pdf

Sundfeld, C. A. (2006). A Regulação das Telecomunicações: papel atual e tendências futuras. *Revista Eletrônica de Direito Administrativo, 8*.

Tele2 Sverige AB, C-203/15 e C-698/15 (Tribunal de Justiça da União Europeia 2112, 2016).

Telefónica/Vivo. (2011, 09 16). *Contribuição nº 846.* Retirado em 01 11, 2016, de Consulta Pública nº 45, de 8 de agosto de 2011, da ANATEL: http://sistemas.anatel.gov.br/SACP/Relatorios/Relatorio DadosBd.asp?pCodProcesso=C1514&pCodTipoProcesso=1&pTipoRelatorio=1

Telefónica/Vivo. (2011, 03 21). *Contribuições nº 194 e 198.* Retirado em 01 11, 2016, de Consulta Pública nº 51, de 9 de dezembro de 2010, da ANATEL: http://sistemas.anatel.gov.br/SACP/Relatorios/ RelatorioDadosBd.asp?pCodProcesso=C1455&pCodTipoProcesso=1&pTipoRelatorio=1

Vedaschi, A., & Lubello, V. (2015). Data Retention and its Implications for the Fundamental Right to Privacy. *Tilburg Law Review, 20*, 14-34.

Vieira da Cunha, C. (2012, 06 14). *Parecer do Relator, Dep. Vieira da Cunha (PDT-RS), pela constitucionalidade, juridicidade e técnica legislativa e, no mérito, pela aprovação, com substitutivo ao Projeto de Lei nº 6.578, de 09 de dezembro de 2009.* Retirado em 02 11, 2016, de Câmara dos Deputados: http://www.camara.gov.br/ proposicoesWeb/prop_mostrarintegra?codteor=1002151&filename=Tramitacao-PL +6578/2009

Vorratsdatenspeicherung, Urteil des Ersten Senats vom 02. März 2010 (Bundesverfassungsgericht 0203, 2010).

Woods, A. K. (2016, 12 22). *Implications of the EU's Data Retention Ruling*. Retirado de Lawfare: https:// www.lawfareblog.com/implications-eus-data-retention-ruling

Woods, L. (2016, 12 21). *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*. Retirado de EU Law Analysis: http://eulawanalysis.blogspot.com.br /2016/12/data-retention-and-national-law-ecj.html

UMA ANÁLISE DE NAVEGAÇÃO NO MODO PRIVATIVO DO GOOGLE CHROME MOBILE

Resumo: Com as revelações sobre a invasão de privacidade ocorridas em 2013, houve um considerável aumento da busca por maior segurança na sociedade, fato que afetou a indústria de desenvolvimento tecnológico. Um exemplo seria o do navegador Firefox, que, na sua versão 43, adicionou ao modo de navegação privada o bloqueio de rastreadores de terceiros baseado na lista do Disconnect, uma empresa que atua no contexto de segurança e privacidade online.

A primeira ocorrência da implementação da funcionalidade de Modo Privativo (Privacy Mode) foi registrada em 2005, a qual tem como objetivo principal impedir o armazenamento local de dados de navegação que poderiam ser acessados posteriormente.

Na atualidade, a fração de usuários que acessam a web via navegador móvel aponta crescimento significativo – que acompanha, proporcionalmente, preocupações com relação à segurança e privacidade dos dados envolvidos em sua navegação. A maior porção desses usuários utilizam o navegador Google Chrome Mobile (número que cresce devido ao Google gradativamente tornar o Chrome o navegador padrão do Android a partir da versão 4.0) e entendem, de maneira geral, o Modo Privativo como uma ferramenta de incremento de segurança.

O presente trabalho apresenta uma análise do comportamento do navegador Google Chrome Mobile utilizando o Modo Privativo (Incognito Mode) por meio de duas abordagens:

1) Análise de consistência entre o propósito original da criação do Modo Privativo, veiculado via marketing, e sua utilização prática.

2) Análise de segurança e privacidade da navegação.

Palavras-chave: Privacidade, Segurança, Mobile, Browser, Google chrome.

THIAGO NOBAYASHI*
LEONARDO KAZUHIKO KAWAZOE**

Un análisis de la navegación en Modo Privativo de Google Chrome Mobile

Resumen: Con las revelaciones sobre la invasión de privacidad ocurridas en 2013, ocurrió un considerable aumento de la busca por mas seguridad en la sociedad, hecho que afectó la industria de desarrollo tecnológico. Un ejemplo sería el de navegador firefox, en que, en su versión 43, adicionó al modo de navegación privada el bloqueo de rastreadores de terceros basado en la lista del Disconnect, una empresa que actúa en el contexto de seguridad y privacidad online. La primera ocurrencia de implementación da funcionalidad del Modo Privativo (Privacy Mode) fue registrada en 2005, la cual tiene como objetivo principal impedir el almacenamiento local de datos de navegación a los que podría accederse posteriormente.

En la actualidad, la fracción de usuarios que accede a la web a través de navegador móvil señala un crecimiento significativo - que acompaña, proporcionalmente, preocupaciones con la relación a la seguridad y privacidad de los datos involucrados en su navegación. La mayor parte de estos usuarios utilizan el navegador Google Chrome Mobile (número que crece debido a que el Google gradualmente torna el Chrome, el navegador padrón del Android a partir de la versión 4.0) y entienden, de manera general, el Modo Privativo como una herramienta de aumento de seguridad.

El Presente trabajo presenta un análisis del comportamiento del navegador Google Chrome Mobile utilizando el Modo Privativo (Incognito Mode) por medio de dos enfoques:

1) Análisis de la consistencia entre el propósito original de la creación del Modo Privativo, vinculado vía marketing, y su utilización práctica.

2) Análisis de seguridad y privacidad de navegación.

Palabras clave: Privacidad, Seguridad, Móvil, Navegador, Google chrome.

A navigation analysis in Google Chrome Mobile Private Mode

Abstract: In consequence of the last revelations about the invasion of privacy in 2013 there was a considerable increase of the search for more security in society, which has been affecting the industry of technology development. An example is the Firefox web navigator, which in the version 43 added to its private navigation mode the block of third-party trackers based in the Disconnect list (Company engaged in the context of security and privacy).

The first occurrence of the implementation of the Private mode functionality was recorded in 2005, which aims to prevent the local storage of navigation data that could be accessed posteriorly.

Currently, the fraction of users who access the web via mobile browser points had significant growth accompanying proportionally concerns regarding the security and privacy of data involved in navigation. The major portion of these users use Google Chrome Mobile browser (number growing due to Google gradually make Chrome the default browser of Android from the version 4.0) and understand, in general, the Private Mode as a safety increment tool.

This work presents a Google Chrome Mobile browser behavior analysis using the Private Mode (Incognito Mode) through two approaches:

1) Consistency analysis between the original purpose of creation of the Private Mode, broadcasted via marketing, and its practical use.

2) Safety analysis and privacy of navigation.

Keywords: Privacy, Security, Mobile, Browser, Google chrome.

INTRODUÇÃO

Como colocado por Wood e Wright (2015) 11 de setembro de 2001 se torna um gatilho para a vigilância, e uma boa oportunidade para as agências de vigilância se fortaleçam em cima de uma nova via massiva de dados, muito mais que os dados “freely given” fornecidos pelos usuários de redes sociais. Presenciamos vários estados atacando as características que fazem a internet um espaço criativo e livre, em nome de vários os tipos de riscos (terrorismo, crime de identidade, crime de propriedade intelectual, pedofilia), e restringir a internet se torna uma maneira para que as diversas agências de inteligência como a Agência Nacional de Segurança dos EUA (NSA) a monitorem de maneira mais fácil.

Nesse contexto em 2013 Edward Snowden, um administrador de sistemas, trabalhando para a NSA, revela para o mundo documentos disponibilizados através dos jornais the *Guardian*, the *New York Times*, *Der Spiegel* e *Washington Post*, e com isso nasce um novo entendimento de várias dimensões do ciberespaço, Bajaj (2014). Revelando sobre a vigilância global feita pela NSA, Snowden muda toda a conjuntura mundial em volta do controle de informações e da privacidade de governos, empresas privadas e da sociedade civil, criando um debate mundial em torno da garantia dos direitos civis, privacidade e liberdade na rede.

Edward Snowden também revela informações sobre como as grandes empresas de tecnologia norte americanas sabiam sobre o esquema de vigilância e participavam de maneira ativa, umas destas empresas sendo o *Google*. No artigo "Google is not what it not what it seems" publicado no *WeakiLeaks* por Assange (2014), este compilando várias denúncias em relação a atuação do *Google* junto ao governo dos EUA. Sabendo que a privacidade das bilhões de pessoas que acessam a internet já estava comprometida por um acordo entre vários estados ao redor do mundo agora temos a maior companhia do mundo (Hern, 2016) atuando também no esquema global de vigilância.

Além das problemáticas de se usar produtos *Google*, e da vigilância realizada por órgãos de vigilância e de estados, alguns dos interesses pelos quais a sociedade civil opta usar o modo privativo dos navegadores como solução para problemas de privacidade acabam por não condizer com as funcionalidades divulgadas pelas empresas responsáveis pelos navegadores, muito menos condiz com a conjuntura global de vigilância do ciberespaço.

Nesse artigo vamos analisar especificamente o modo privativo do navegador Google Chrome por ser navegador mais utilizado no mundo atualmente, inclusive no ambiente mobile, que vem crescendo cada vez mais tanto em número absoluto de usuários, como também em porcentagem de usuários que acessa a internet exclusivamente via mobile segundo dados e análises da plataforma (http://www.internetlivestats.com/).

A Empresa lança sua navegação anônima (Incognito Mode) em 2008, vem com o objetivo de cobrir uma gama de usuários que buscam por alguns tipos de privacidade em níveis diferentes. Combinado com o aumento dos acessos à internet exclusivamente via mobile, temos alguns pontos para analisar:

- O modo privativo do Google Chrome Mobile cumpre as funcionalidades divulgadas pelo empresa?
- Seguindo os motivos citados por Aggarwal, Bursztein, Jackson & Boneh (2010) para qual motivos as pessoas usam o modo privativo, o navegador contempla essas funcionalidades?

ANÁLISE DE SEGURANÇA

Contexto

A primeira ocorrência da implementação da funcionalidade de modo privativo (privacy mode) foi registrada em 2005, no navegador Safari, segundo Satvat, Forshaw, Hao & Toreini (2014).

Quando ativa, impede que rastros de navegação, tais como histórico, cookies e arquivos temporários sejam armazenados no dispositivo local, diferentemente da mecânica usual. Esta – até então recente – mudança foi propagada para os demais, e, hoje, todos os principais navegadores possuem alguma função semelhante (Google Chrome, Mozilla Firefox, Internet Explorer).

O modo privativo no Google Chrome (para ambas as versões desktop e mobile) é implementado pela funcionalidade de modo incógnito (incognito mode). De acordo com suas especificações, os históricos de visitas a websites e de download não são armazenados nos dispositivos dos usuários (informações básicas como endereço de URL, páginas em cache ou endereços de websites visitados), qualquer cookie criado durante uma sessão privativa é deletado quando todas as sessões privativas são encerradas, permissões concedidas durante uma sessão anônima não são salvas ("Explore the Chrome Browser," n.d.), e traços de cache nem de armazenamento local são deixados ("Google Chrome," n.d.). Estes comportamentos são reiterados em seu documento de políticas de privacidade ("Google Chrome Privacy Notice," 2016).

Porém, é importante notar algumas ressalvas:

- Apesar do modo incógnito prevenir com que as atividades de visita não sejam armazenadas, o tráfego da rede pode ser monitorada por diversos agentes, tais como o administrador da rede ou o provedor do serviço de Internet;
- O navegador possui acesso às informações do perfil de usuário (senhas, sugestões baseadas em histórico de navegação), e estas são carregadas, mesmo durante uma sessão privativa;
- Páginas marcadas no modo incógnito serão salvas;
- A lista de downloads também não será salva, mas os arquivos descarregados serão salvos no diretório destinado a downloads da máquina do usuário.

Os pontos citados acima não são responsabilidades delegadas à segurança e privacidade dos navegadores – por não fazer parte de seu escopo de controle –, mas são características que proporcionam indiretamente brechas acidentais à integridade do usuário. O forte discurso de venda pode ser um fator agravante neste contexto, considerando que este tipo de tecnologia é universalmente difundido (não limitando seu acesso a especialistas) e a interpretação dos termos segurança e privacidade – enunciados pelo modo privativo – são subjetivos ao público de incidência.

Pode-se entender por privacidade neste contexto a definição colocada por Vianna (2009), em que se coloca a privacidade como um direito composto por três outros direitos, sendo eles:

- Direito de não ser monitorado, entendido como direito de não ser visto, ouvido, etc.;
- Direito de não ser registrado, entendido como direito de não ter imagens gravadas, conversas gravadas, etc.;
- Direito de não ser reconhecido, entendido como direito de não ter imagens e conversas anteriormente gravadas publicadas na Internet em outros meios de comunicação.

A análise será feita fundamentada pelos parâmetros definidos pela navegação privativa: o modo incógnito, enquanto sistema computacional, deve ser avaliado em termos de segurança de acordo com os objetivos assumidos pela ferramenta e como estes são cumpridos. A falha de execução de algum destes objetivos servirá de critério para definir este evento como uma violação do sistema e, portanto, da segurança.

Sendo assim, o tema do texto será discutido baseado nestas noções de segurança e privacidade.

Premissas

De acordo com um estudo conduzido e publicado pelo grupo de Criptografia Aplicada da Universidade de Stanford (Aggarwal, Bursztein, Jackson & Boneh, 2010), a implementação do modo privativo nos navegadores possui fundamentalmente dois propósitos:

1. Impedir que rastros de navegação sejam deixados nos dispositivos dos usuários (em outras palavras, proteger contra ataques locais). Em linhas diretas, impedir o acesso ao conteúdo de navegação, posteriormente ao término da sessão de um usuário. Não salvar o histórico de *websites* visitados e de *downloads* são medidas que contribuem para o anonimato desejado atingir por este objetivo;

2. Permitir que a identidade do usuário seja preservada enquanto navega e acessa o conteúdo da rede (proteger os usuários contra ataques na *web*). Portanto:

2.1. Impedir com que seja possível criar conexão entre o mesmo usuário ao utilizar perfis públicos e privativos;

2.2. Impedir com que seja possível criar conexão entre o mesmo usuário em diferentes sessões de perfis privativos;

2.3. E é desejável que não seja possível identificar quando um usuário está no modo privativo.

Deletar os *cookies* após todas as sessões anônimas serem encerradas, e não deixar *cookies* obtidos em navegação padrão disponíveis à navegação privativa podem ser encarados como uma tentativa de prevenção a este objetivo. Porém, não é suficiente.

Segundo Mayer (2009), uma série de características podem ser extraídas de um navegador utilizando apenas objetos JavaScript padrões, tais como nível de *zoom*, geolocalização, fontes instaladas, dados da rede, *plugins* instalados e resolução. Estas informações servem para corroborar a demonstração, feita pela Electronic Frontier Foundation (Eckersley, 2010), de que é possível utilizar as diversas características extraíveis do navegador para se gerar *fingerprints*, e, portanto, eliminar as chances de atingir os objetivos 2.1 e 2.2.

De acordo com Boneh *et al,* é possível classificar mudanças de estados persistentes em quatro categorias:

I. Mudanças iniciadas por *websites*, que não requerem interação com o usuário, tal como adicionar dados ao cache do navegador;

II. Mudanças iniciadas por *websites*, que requerem interação com o usuário, tal como adicionar uma senha à base de dados de senhas;

III. Mudanças iniciadas por usuários, tais como adicionar um *website* aos favoritos ou o *download* de um arquivo;

IV. Mudanças não específicas do usuário, tal como a instalação de *patches*.

ANÁLISE

Os navegadores tentam apagar as mudanças de estado do tipo I ao finalizar todas as sessões privativas. Caso isso não seja possível, pode-se considerar que há uma violação da navegação privativa.

Como os objetivos em 2 podem ser considerados como inalcançáveis, o que resta é tentar tratar de forma eficaz os objetivos em 1, que também não são triviais. Outro aspecto descrito por Aggarwal, Bursztein, Jackson & Boneh (2010) é de que ataques locais possuem inúmeras fontes, e um conjunto específico deles está relacionado ao sistema operacional (SO). Um destes problemas é o de que o navegador realiza a resolução de DNS ao acessar um dado *website*, e o SO frequentemente faz o cache desta resolução, deixando rastros da lista de acessos feitos. Uma solução para isto seria a limpeza do cache de DNS após o término das sessões privativas – o que aparentemente não é feito. Outro problema está relacionado ao *swap* de memória do SO, que pode acessar partições de memória e deixar rastros de atividades do usuário, enquanto navega.

Outro fato interessante é de que quando o Google Chrome utiliza a memória cache da GPU, esta não é deletada após o término de uma sessão (seja ela privativa ou não). Sendo assim, existem brechas que podem ser exploradas para que seja possível recuperar imagens renderizadas durante uma sessão anônima, utilizando o cache da GPU. Aparentemente este *bug* foi reportado, mas ignorado por não fazer parte do design do navegador.

Por fim, um simples experimento foi executado, utilizando a metodologia a seguir:

- Uma cópia da aplicação Google Chrome Mobile versão 54.0.2840.68 foi baixada e instalada num dispositivo móvel, rodando o Android sob a versão 4.1.2;
- A aplicação foi executada e ativado o modo incógnito;
- Foi verificado o *timestamp* dos diretórios pertencidos pela aplicação, em */data/data/* ;
- Foi executado um pedido HTTPS para um *website* ;
- O *timestamp* dos diretórios pertencidos pela aplicação, em */data/data/*, foi verificado novamente.

Pôde-se notar, sem grandes análises, que o *timestamp* de alguns diretórios foram alterados – talvez pelos dados de navegação terem sido deletados –, ou seja, é possível determinar quando um usuário utiliza a aplicação, em modo incógnito ou não.

MARKETING

A funcionalidade de modo incógnito é ofertada para ocasiões em que não se é desejado registrar os *websites* visitados e *downloads* feitos. De acordo com o estudo conduzido pela Universidade de Stanford (Aggarwal, Bursztein, Jackson & Boneh, 2010), é sugerido que o uso primário do modo privativo esteja relacionado ao acesso de conteúdo adulto – que pode ser resumido a atividades de caráter íntimo. Sendo assim, pode-se identificar que há compatibilidade entre o modo em que se é vendida a funcionalidade e como esta é utilizada de modo prático, majoritariamente.

CONSIDERAÇÕES FINAIS

O caso analisado é singular no sentido de que nem sempre a coerência entre como se é vendido e utilizado na prática, o produto, é positiva. A finalidade descrita por ambos empresa e usuários acabam por ser semelhantes, mas seus objetivos claramente vão em direções opostas, fato que potencialmente se estende a uma problemática interdisciplinar: o crescente número de usuários de navegadores móveis, em busca de privacidade acabam por cair em sua total contradição, em relação ao comportamento real do sistema enquanto máquina computacional, por exemplo.

A falsa sensação de privacidade e anonimato no ambiente virtual pode acabar por gerar consequências irreversíveis para usuários e para pessoas que, de alguma maneira, se relacionam com eles. Este artigo tenta expor que a análise dessas informações continuamente registradas e monitoradas em larga escala ou em nível pessoal geram impacto e controle sem precedentes na sociedade e em nossas vidas, sem ao menos que tenhamos noção, na maioria das vezes, de como isso nos afeta a nível pessoal e como indivíduo e em relação a conjuntura política internacional em torno da vigilância.

Percebe-se essa contradição tanto na falta de conhecimento ou abstração do quão problemática vigilância é nos âmbitos pessoais, sociais e políticos quanto no conhecimento técnico de como essas ferramentas funcionam. Isso acaba por gerar nesse grande espectro de usuários a falsa sensação de anonimato e privacidade quando estão no ambiente virtual, em relação a casos de uso diários como simples compras, pesquisas e acesso a conteúdo

NOTAS

* Estudante de Graduação no Bacharelado em Sistemas de Informação na Escola de Artes Ciências e Humanidades da Universidade de São Paulo (EACH - USP). thiago.nobayashi@usp.br

** Estudante de Graduação no Bacharelado em Sistemas de Informação na Escola de Artes Ciências e Humanidades da Universidade de São Paulo (EACH - USP). leonardo.kawazoe@usp.br

REFERÊNCIAS

Vianna, T. L. (2007). *Transparência pública, opacidade privada* (Doctoral dissertation, Universidade Federal do Paraná Curitiba).

Mayer, J. R. (2009). Any person... a pamphleteer": Internet Anonymity in the Age of Web 2.0. *Undergraduate Senior Thesis, Princeton University*.

Eckersley, P. (2010). A primer on information theory and privacy. *Electronic Frontier Foundation*.

Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010, August). An Analysis of Private Browsing Modes in Modern Browsers. In *USENIX Security Symposium* (pp. 79-94).

Bajaj, K. (2014). Cyberspace: Post-Snowden. *Strategic Analysis*, *38* (4), 582-587.

Google Is Not What It Seems. (2014). Recuperado de: https://wikileaks.org/google-is-not-what-it-seems/

Satvat, K., Forshaw, M., Hao, F., & Toreini, E. (2014). On the privacy of private browsing–a forensic approach. In *Data Privacy Management and Autonomous Spontaneous Security* (pp. 380-389). Springer Berlin Heidelberg.

Wood, D. M., & Wright, S. (2015). Before and After Snowden. *Surveillance and Society*, *13* (2), 132-138.

Browse in private with Incognito mode. (n.d.). Recuperado de: https://support.google.com/chrome/answer/95464?hl=en&p=cpn_incognito

Hern, A. (2016, 2 de fevereiro). How alphabet became the biggest company in the world. *The Guardian*. Recuperado de: https://www.theguardian.com/technology/2016/feb/01/how-alphabet-made-google-biggest-company-in-the-world

Explore the Chrome Browser. (n.d.). Recuperado de: https://www.google.com.br/chrome/browser/features.html

Google Chrome Privacy Notice. (2016, August 30). Recuperado de: https://www.google.com/chrome/browser/privacy/

Google Chrome. (n.d.). Recuperado de: https://www.google.com.br/mobile/chrome/

EJE 6

VIGILANCIA CORPORATIVA

WEARABLE TRACKERS E O RISCO OCULTO DO CONHECIMENTO DE SI ATRAVÉS DO DADO. UMA ANÁLISE DOS DOCUMENTOS ENDEREÇADOS AOS USUÁRIOS E INVESTIDORES DA FITBIT

Resumo: O artigo problematiza o significado atribuído ao "dado" nos documentos destinados aos usuários e investidores da Fitbit, maior empresa do mercado global de vestíveis da atualidade. Foram analisadas as duas últimas versões dos contratos de uso e privacidade e o relatório do mercado aberto (IPO) mais recente enviado aos investidores da marca. Os documentos foram explorados no software Atlas.Ti, levantando-se os conteúdos relacionados às políticas de uso, os argumentos associados à coleta dos dados biométricos e aos significados atribuídos ao dado. Os achados foram analisados à luz da Teoria Ator-Rede. As análises realizadas buscam contribuir para o debate acerca dos modelos ocultos de governança e gestão remota da saúde – mHealth – promovidos pelos wearables e que têm na captura e análise agregada de dados biométricos a base para tomadas de decisão nas esferas políticas e econômicas. Os achados indicam que, embora os discursos endereçados ao cliente valorizem o conhecimento através dos números e coloquem o dado como um benefício para o usuário, as narrativas dirigidas aos investidores destacam a garantia de segurança e privacidade dos usuários, os interesses governamentais no acesso aos dados e as políticas de regulação como os principais riscos para o negócio. A partir dos resultados, o texto defende o argumento de que as narrativas que comunicam e regulamentam as práticas de dado da empresa utilizam o termo como um truque retórico que oculta a rede político-econômica e as ameaças presentes nos hábitos de monitoramento e dataficação corporal através dos wearables.

Palavras-chave: Biometria, Fitbit, Privacidade, Teoria ator-rede.

ELIAS CUNHA BITENCOURT*

Monitores de vestir y el riesgo oculto del conocimiento de si a través del dato. Un análisis de los documentos dirigidos a los usuarios e inversionistas de la Fitbit.

Resumen: El artículo problematiza el significado atribuido al "dato" en los documentos destinados a los usuarios e inversionistas de la Fitbit, la mayor empresa del mercado global de dispositivos de vestir de la actualidad. Fueron analizadas las últimas versiones de los contratos de uso y privacidad y el informe del mercado abierto (IPO) más reciente enviado a los inversionistas de la marca. Los documentos fueron investigados en el software Atlas.Ti, haciendo un levantamiento de los contenidos relacionados a las políticas de uso, a las justificativas empleadas para la colecta de los datos biométricos y a los significados atribuidos al dato. Los hallazgos fueron analizados a la luz de la Teoría Actor-Red. Los análisis realizados buscan contribuir para el debate acerca de los modelos ocultos de gobernabilidad y de la gerencia remota de salud – mHealth – promovidos pelos wearables y que tienen en la captura y análisis agregado de datos biométricos la base para la tomada de decisiones en las esferas políticas e económicas. Los hallazgos indican que a pesar de que los discursos dirigidos al cliente valoricen el conocimiento a través de los números y coloquen el dato como un beneficio para el usuario, las narrativas dirigidas a los inversionistas destacan la seguridad de los datos, la garantía de la privacidad, los intereses gubernamentales en la accesibilidad de datos y las políticas de regulación como los principales riesgos del negocio. A partir de los resultados, el texto propone que las narrativas que regulan las prácticas de colecta de los datos de Fitbit utilizan el término como un truco retórico que oculta la red política y económica y las amenazas de los hábitos de monitoreo cuerpo a través de las tecnologías de vestir.

Palabras-clave: Biometría, Fitbit, Privacidad, Teoría actor-red.

Wearable Trackers and the hidden risks of knowing thyself trough data. An Analysis of documents addressed to Fitbit users and investors.

Abstract: This article discusses the different meanings of the term data that was used on official media discourse addressed to two of the most important audiences of Fitbit: users and investors. Fitbit was elected as the main object of interest since it is the largest corporation in the global wearable market. They were analyzed three different types of documents: the policy privacy terms, the legal term of use and the last IPO financial report of the company. The documents were examined under the Atlas.Ti software in order to identify the most common arguments and uses of "data" terminology in narratives that present Fitbit's services. These findings were debated from Actor-Network Theory (ANT) perspectives. The proposals aim to contribute for a critical reflection about unseen remote health management policies –mHealth –, and hidden governance models that underlies the political and economic decisions guided by personal data capture practices. Lastly, this investigation recognizes that despite the fact of media discourse addressed to users emphasize the benefits of sharing body personal data through Fitbit system, the message sent to investor is that the personal data security assurance, governmental interests in data accessibility and regulatory policies are the major risks to the company's business. The results allow us to argue that the narratives that regulate Fitbit's data collection practices use the term "data" as a rhetorical trick that disguises the political-economic network and the real threats of digital body monitoring habits trough wearable technologies.

Keywords: Biometry, Fitbit, Privacy, Actor-network theory.

INTRODUÇÃO

Em fevereiro de 2016 a Oral Roberts University – uma universidade americana localizada em Tusla, estado de Oklahoma–, anunciou que passará exigir que todos os seus 900 calouros utilizem um dispositivo vestível (*wearable*) para o monitoramento de atividades físicas da Fitbit, como requisito à aprovação semestral nas disciplinas de educação física da instituição (El Clarín, 2016; Frankel, 2016). Cada estudante deverá compartilhar, semanalmente, os dados de qualidade de sono, o número de passos e os batimentos cardíacos com o sistema da universidade. As exigências estabelecidas prevêem o mínimo de 10 mil passos diários e 150 minutos semanais de atividades

em ritmo cardíaco intenso – parâmetros definidos pelas zonas de frequência cardíaca *Peak* e *Fat Burn*[1] do sistema Fitbit.

Ações similares à da Oral Roberts University não são isoladas. Elas compõem um quadro mais amplo do recente fenômeno promovido pela difusão das tecnologias vestíveis e tornam-se cada vez mais populares em programas corporativos para redução de custos com seguros de saúde (Kau, 2015; Nield, 2014; Olson & Tilley, 2014) e em políticas de gestão remota da saúde (Biggs, Garrity, LaSalle, & Polomska, 2016; Campbell, 2014; George, 2016; Gould, 2016).

Diferentemente das já conhecidas ferramentas sociais de monitoramento e captura de dados difundidas pela web 2.0, os *wearables* são parte integrante da rede de objetos com computação embarcada (IoT) e representam uma modalidade bem mais complexa de extrair e produzir informação. Projetados para o uso permanente no corpo, eles são capazes de coletar e compartilhar dados sobre variadas esferas da atividade humana – o número de passos dados, a qualidade de sono, o ritmo cardíaco, a geolocalização, o humor (Feel Band), os ritmos gástricos (DFree), as posturas corporais (Upright), os fluxos menstruais (Looncup), e os padrões sexuais (Lovely)[2] são apenas alguns dos exemplos já disponíveis.

Os vestíveis não apenas reagem ao corpo dos usuários. Eles são dotados do que Lemos (2016) denominou "sensibilidade performativa" – a capacidade que todos os objetos da IoT possuem de captar sensações através de sensores e atuadores, produzir ações imediatas, futuras e sistêmicas em função de uma inteligência que deriva da coleta e do processamento computacional de dados. Os *wearables,* portanto, convocam o corpo a ocupar um novo lugar de centralidade na política econômica atual, manifestando-se como mediadores importantes nas experiências de gestão individual e coletiva da saúde, das ações e das práticas corporais contemporâneas.

A literatura específica tem levantado questionamentos acerca dos reflexos que os usos dessas tecnologias promovem em diversas esferas sociais. Dentre as publicações mais recentes sobre o tema, destacam-se os trabalhos que problematizam sobre os novos padrões de engajamento e percepção da saúde (Jutel & Lupton, 2015; Nascimento, 2014; Vesnic-Alujevic, Breitegger, & Guimarães Pereira, 2016); as investigações sobre a construção de práticas corporais orientadas ao dado (Karapanos, Gouveia, Hassenzahl, & Forlizzi, 2016; Lupton, 2015b; Smith & Vonthethoff, 2016); os debates acerca das políticas de gestão remota e de promoção de saúde (Chung, Skinner, Hasty, & Perrin, 2016; Lupton, 2015a); as pesquisas que discutem o cuidado de si e a tradução das subjetividades em função de procedimentos digitais de quantificação do eu (Crawford, Lingel, & Karppi, 2015; Lemos & Bitencourt, 2016; Lupton, 2016; Pantzar & Ruckenstein, 2015) e os textos que refletem a respeito dos modelos de governabilidade, ética e vigilância que emergem das tecnologias de dataficação do cotidiano (Cheney-Lippold, 2011; Fotopoulou & O'Riordan, 2016; Jethani & Raydan, 2015; Nafus & Sherman, 2014; Till, 2014; Whitson, 2015).

Embora os trabalhos destacados ponham em evidência os riscos que a captura e o compartilhamento dos dados corporais podem trazer para o campo da autonomia, da privacidade e da segurança,

os slogans que caracterizam as principais marcas no segmento de *wearables* frequentemente enfatizam a performance corporal voltada à quantificação e à produção de dado como uma via para o autoconhecimento e para a otimização de si – "*make every beat counts!*" (Fitbit Charge 2); "*Every move counts, so count every move.*" (Apple Watch 2); "*Understand your every move.*" (Xiaomi MiBand).

Na perspectiva dos usuários, entretanto, nem sempre o dado aparece como elemento central dos relatos de experiência. Embora os comportamentos de monitoramento sejam valorizados entre os pares, em uma recente investigação realizada no fórum da comunidade Fitbit, Lemos e Bitencourt (2016) identificaram que os membros não associam os "*steps*" registrados a um "dado" pessoal. Para os "Fitbitters", os "*steps*" são unidades materiais do comportamento que precisam ser acumuladas e recompensas numéricas a serem alcançadas.

Diante dessas questões, o artigo buscou investigar como as empresas ramo de *wearables* apresentam o "dado" para as suas principais audiências: usuários e investidores. Como objeto empírico elegeu-se a Fitbit, maior marca no segmento global de vestíveis. Para compor o *corpus* de análise, foram selecionadas as últimas versões da política de privacidade (completa e resumida), o termo de serviço e o último relatório financeiro anual direcionado ao mercado de capital aberto (IPO). O *corpus* foi explorado no *software* Atlas.ti através da análise quantitativa da frequência e densidade de palavras[3] e do procedimento de codificação focada.

Os achados indicam que, embora os discursos endereçados ao cliente valorizem o conhecimento através dos números e coloquem o dado como um benefício para o usuário, as narrativas dirigidas aos investidores destacam a garantia da privacidade e segurança, o interesse governamental no acesso ao dado e as políticas de regulação como principais riscos para o negócio da Fitbit. A partir dos resultados, o texto defende o argumento de que as narrativas que comunicam e regulamentam as práticas de dado da empresa utilizam o termo como um truque retórico. Um artifício de dissimulação da rede político-econômica e das ameaças presentes nos hábitos de monitoramento e dataficação corporal através dos *wearables*.

METODOLOGIA E DELINEAMENTO DO CORPUS

Criada em 2007, a Fitbit permanece na liderança do mercado de dispositivos vestíveis até 2016 – 24.5% de *marketing share* global[4] e cerca de 9.5 milhões de usuários ativos até 2015[5]. A empresa também é a única do setor que possui um portfólio de produtos voltado apenas ao segmento de monitores de atividades físicas, o capital aberto no mercado financeiro (IPO) e ocupa a posição de líder também no mercado corporativo. Segundo informações da própria marca, o programa de promoção de saúde (Fitbit Corporate Wellness) tem setenta das quinhentas corporações mais ricas da lista Forbes como clientes e agregou, só em 2015, mil usuários novos de empresas como Barclays, Godaddy.com e Target (FITBIT INC, 2016a) Diante dessas razões, elegeu-se a Fitbit como objeto empírico da presente investigação.

Foram selecionados os termos e políticas oficiais disponibilizados no site da empresa. Entre os documentos voltados aos usuários, priorizou-se aqueles cujas narrativas estão dedicadas à apresentação das práticas de coleta, compartilhamento, venda e proteção dos dados. Obedecendo esses critérios, compuseram o *corpus* : o documento de privacidade resumido (FITBIT INC, 2016a), a política de privacidade completa (FITBIT INC, 2016b), o termo de uso dos serviços (FITBIT INC, 2015b) e o ultimo relatório IPO (FITBIT INC, 2015a).

Com o objetivo de investigar os principais significados atribuídos ao termo "dado" e os contextos mais frequentes de sua aplicação, foram empregadas ferramentas quantitativas de análise de densidade de palavras e procedimentos de codificação focada no software Atlas.ti. Proposta pela teoria fundamentada no dado (Strauss & Corbin, 2008), a codificação focada tem por intuito priorizar uma primeira abordagem às questões de interesse[6] (Latour, 2012) que brotam do corpus selecionado segundo a ótica dos atores envolvidos, evitando o enquadramento precoce dos dados nas categorias teóricas familiares ao pesquisador.

Primeiros achados

De acordo com esses procedimentos, verificou-se que o termo "*data*" possui 240 ocorrências totais e ocupa o nono lugar em volume de uso no corpus. Analisando os documentos individualmente, "*data*" é empregado 129 vezes no relatório financeiro, 76 vezes na política de privacidade, 29 vezes na versão resumida do documento de privacidade e 6 vezes nos termos de serviço. Embora em números absolutos o relatório financeiro acumule a maior quantidade de citações, a versão resumida da política de privacidade é o documento onde "*data*" alcança a maior frequência e a maior densidade (5.2% de densidade), seguido pela versão completa da mesma política, onde a palavra ocupa o segundo lugar em frequência e atinge 4.6% de densidade. No termo de serviço e no relatório financeiro, "*data*" ocupa, respectivamente, o 38º e o 39º em frequência e registra apenas 0.30% e 0.35% de densidade.

Os contextos de uso foram analisados segundo duas categorias gerais de código: "significados atribuídos" e "argumentos associados" no emprego do termo. Na primeira categoria, "significados", destaca-se que a palavra "*data*" foi usada 95 vezes no sentido técnico[7] (39.5%) e 91 vezes como referência aos dados pessoais dos usuários[8] (37.9%). Avaliando os documentos separadamente, "*data*" é mais empregado como referência ao "dado do usuário" na política de privacidade resumida – 48% dos registros no documento –, e no relatório financeiro da empresa – 31% das ocorrências no documento. Na política de privacidade completa e no termo de serviço, a palavra "*data*" é mais aplicada com o sentido técnico – foram registradas 39 citações na política de privacidade (51%) e 5 empregos nos termos de uso da empresa (83%).

No segundo grupo, "argumentos associados", identificou-se três empregos recorrentes da palavra "*data*": risco (contextos que tratam dado como uma ameaça aos usuários ou ao negócio da marca), vantagem (enunciados que associam o dado a um benefício) ou descrição (uso em enunciados informativos sem juízos de valor). Na segunda etapa de codificação focada – análise

detalhada dos argumentos –, foram excluídas as categorias "significado financeiro", "significado estatístico". Nesse novo recorte foram considerados 211 dos 240 registros da palavra. Nele, "data" ocorre 68 vezes (32.2%) em contextos de descrição e detalhamento de processos, 69 vezes (32.7%) como fragilidade para o negócio da empresa ou ameaça à segurança e privacidade do usuário e 74 (35%) vezes associada a um benefício para o usuário, uma vantagem competitiva ou um diferencial dos serviços oferecidos pela marca.

Analisando-se a coocorrência entre as categorias "significados" e "argumentos", verifica-se que o "dado do usuário" é empregado 41% das vezes como uma vantagem e 36% como um risco. Entretanto, quando aplicado com o sentido técnico, "*data*" é mais usado para denotar risco (58% dos registros) ou descrever processos (42% das citações). Nos usos do termo para designar os serviços da Fitbit, "*data*" também é preponderantemente associado a uma vantagem (77.7% das citações). Apenas 13% do "dado como serviço" recebeu conotação de risco.

Entre os usos que ligam "*data*" a vantagem, sobressaem as narrativas que apresentam o dado como uma forma de proteger usuários e serviços da marca (mencionado 32 vezes), como um benefício para a experiência do usuário (23 ocorrências), como uma vantagem competitiva da marca (17 citações) ou ferramenta para a melhoria dos serviços da Fitbit (10 menções). Nas aplicações onde "*data*" sugere risco, destacam-se: os processos legais em função de patentes e vazamentos de dados (38 citações), a regulação dos dados e os interesses governamentais como um problema para o negócio da marca ou uma ameaça aos usuários (32 ocorrências) e problemas técnicos que atentem contra o serviço e à privacidade dos usuários – como invasões hackers, fragilidade de servidores e falhas de processamento (23 ocorrências).

O DADO COMO UM TRUQUE RETÓRICO

Os achados apontam que, embora os contextos de risco e de benefício tenham frequências absolutas muito próximas – 69 e 74 citações, respectivamente –, há uma variação no sentido e no argumento associado ao "dado" em função da audiência. Nos documentos que regulam a segurança e a privacidade dos usuários, o termo é empregado apenas como um benefício ou uma qualidade técnica, sem qualquer ligação a riscos – 59% dos registros ligando "*data*" a uma vantagem estão nos documentos direcionados aos usuários. As ameaças, quando comunicadas, também oscilam em função do público e ocorrem nos espaços onde "*data*" é usado com a menor densidade – 64 das 69 (92%) citações que relacionam dado a risco estão presentes exclusivamente no relatório para investidores onde o termo possui apenas 0.35% de densidade.

Adicionalmente, nos termos de serviço, único documento direcionado ao cliente onde "*data*" é vinculado a risco, o termo é empregado preponderantemente como um termo técnico (4 das 5 citações). Dos seis registros que o documento acumula, só há uma ocasião onde a palavra "data" refere-se à informação do usuário associada a risco: a eventual falta de precisão ou incompletude dos dados apresentados pelo sistema. Diferentemente, o relatório financeiro indica como principais ameaças ao negócio: as sansões legais que decorrem de vazamento de dado, perdas

de patentes e dados imprecisos (37% das ocorrências); as exigências governamentais para acesso aos dados e burocracias envolvendo regulação dos sistemas, dispositivos e transferências de dados entre países (31.6% dos registros); as fragilidades técnicas em garantir a segurança dos dados em função de quebras de contrato com terceiros ou invasão de servidores (21.7% das citações).

De outra forma, é possível verificar indícios de mecanismos retóricos que enfatizam os benefícios que o uso do dado traz à autonomia e ao empoderamento dos corpos, e minimizam os riscos que envolvem as práticas de coleta, extração, comercialização e compartilhamento de informação promovidas pelo serviço. Ao usar "*data*" como um termo técnico ou como uma qualidade digital da informação do usuário – 45% e 43% das ocorrências no *corpus*, respectivamente –, a palavra exerce uma função retórica de encantamento, dissimulando riscos, delegando responsabilidades, atenuando efeitos colaterais e valorizando os resultados positivos. Nas análises realizadas, "*data"* é aplicado com função muito próxima da que Gillespie (2015) rotulou de "talismã" – uma entidade com poder de legitimar e proteger produtos, serviços e organizações. Ao atribuir uma qualidade digital à informação do usuário ou reforçar o caráter computacional de um procedimento técnico, o dado evoca ideias de confiabilidade e neutralidade matemática, assumindo uma "autoridade cultural"(Gillespie, 2015) em relação à falibilidade das ações baseadas em julgamento humano (Wolf, 2010).

Neste sentido, optar pela acepção "técnica" de "*data*" para descrever os riscos das práticas de dataficação corporal promovidas pelos serviços Fitbit – 58% das citações que ligam dado a risco usam a palavra no sentido técnico –, é também uma forma diplomática de minimizar a responsabilidade da empresa e o papel dos outros atores da rede no que tocam às medidas de segurança ou às ações que atentam contra a privacidade e a autonomia dos usuários. De uma forma ou de outra, a função "talismã"(Gillespie, 2015) não só legitima os serviços e protege a imagem da instituição. Ela também contribui para a construção de um imaginário coletivo entre os usuários da marca. Repertório em que o "dado" é um ator cuja confiabilidade numérica instrumentaliza o gerenciamento do corpo, otimiza o conhecimento de si, mobiliza o compartilhamento de informação pessoal e formata novas identidades de grupo (Lupton, 2015b; C. Nascimento e Bruno, 2013).

Assim, o emprego do termo "*data*" nos enunciados analisados opera como um truque retórico. Um artifício que endossa as práticas de extração dados da Fitbit e obscurece os riscos que o uso dos *wearables* da marca oferecem à autonomia, liberdade, privacidade e segurança dos usuários. O dado é apresentado como uma caixa-preta (Latour, 2012), um enunciado cujo significado foi estabilizado e dificulta a identificação dos valores políticos e ideológicos envolvidos nos serviços de análise de dado, nos modos como as informações pessoais circulam na rede da plataforma ou, ainda, com quais objetivos elas são compartilhadas e utilizadas por empresas parceiras e governos.

Neste sentido, embora hajam rastros que evidenciem a agência de outros atores políticos, comerciais e tecnológicos, a descrição do ator-rede Fitbit ou a composição da rede corpo-wearable é inicialmente imperceptível. Aspectos como a presença do Senador democrata Edward Schumers

(principal apoiador da PIPA[9]) validando a política de privacidade no site, a criação do Fitbit Group Health – grupo corporativo dedicado a otimizar as articulações entre gestores, empresas de seguro saúde e pesquisadores da área clínica (FITBIT INC, 2016c) –, ou os relatórios indicando o uso dos *wearables* da Fitbit como ferramentas de redução nos custos de saúde de empresas (Springbuk, 2016) nem sempre são ligados ao "dado do usuário" ou a um risco que comprometa a autonomia dos sujeitos monitorados.

Em outras palavras, usado como "talismã" (Gillespie, 2015) nas narrativas oficiais que firmam os compromissos de privacidade e segurança, "*data*" figura como um truque retórico para ocultar a rede político-econômica da plataforma Fitbit. Somado às estratégias motivacionais presentes nas interfaces dos usuários e nos programas de ação implícitos nos sistemas, o dispositivo do truque contribui para obscurecer os usos e as mediações desviantes que o dado possui na rede que se organiza a partir da associação entre os corpos e os *wearables* da empresa investigada.

CONSIDERAÇÕES FINAIS

O artigo analisou o significado e os contextos de uso do termo "*data"* nas versões mais recentes dos documentos que regulamentam e comunicam a política de uso dos dados pessoais nos serviços da Fitbit, maior empresa no mercado global de *wearables.* Os resultados apontam que há uma variação no modo como o dado é empregado nos enunciados oficiais da marca, priorizando-se as acepções positivas e minimizando-se as associações negativas do termo naquelas narrativas que são orientadas aos usuários. Adicionalmente, verificou-se que a comunicação explícita do risco ofertado pelo uso dos dados privilegia o significado "técnico" da palavra e o emprego em enunciados destinadas aos investidores, onde o termo também possui uma baixa densidade. Nestes, a garantia de segurança e privacidade dos usuários, os interesses governamentais e as políticas de regulação figuram enquanto os principais riscos que o dado oferece para o negócio da marca, contrastando com o caráter vantajoso e inofensivo com que "data" é apresentado ao cliente.

Os achados permitiram levantar o argumento de que o tratamento do termo "*data*" nos discursos oficiais da marca compõe um dispositivo retórico. Um mecanismo de convencimento e dissuasão que recorre ao dado como um truque, um artifício que contribui para dissimular a rede político-econômica da plataforma, legitimar os serviços oferecidos pela marca e ocultar os riscos para a autonomia, segurança e privacidade dos usuários.

Secundariamente, as análises também permitiram identificar alguns dos principais mediadores que compõem a rede estruturada ao redor dos serviços oferecidos pela Fitbit, bem como alguns dos dispositivos de controle que operam de maneira opaca através das funções desviantes reguladas pelas políticas de privacidade e termos de uso da marca, objeto de outro texto. Por fim, embora ainda preliminares, os resultados apresentados podem contribuir para o desvelamento de atores e traduções que ainda permanecem ocultas na rede. Programas de ação que encontram em dispositivos retóricos, similares aos que aqui foram expostos, uma estratégia de estabilização

da percepção do "dado" enquanto um aliado necessário à instrumentalização de práticas corporais que obedecem à modelos governabilidade, interesses econômicos e valores éticos nem sempre acessíveis aos usuários, mesmo nos canais dedicados a esse fim.

NOTAS

* Mestre e Doutorando Programa de Pós-Graduação em culturas contemporâneas – POSCOM/UFBA; Professor Auxiliar Universidade do Estado da Bahia – UNEB, eliasbitencourt@gmail.com.

1. Mais detalhes do cálculo aqui: https://help.fitbit.com/articles/en_US/Help_article/1565

2. A pulseira inteligente Feel monitora os padrões emocionais e sugere insights para administrá-las (http://www.myfeel.co). O Dfree identifica os padrões gástricos e informa antecipadamente o horário da evacuação (http://dfree.biz). O Upright acompanha os padrões posturais e sinaliza quando eles são inadequados (http://wearable-technologies.com). O Looncup informa o volume do fluxo menstrual e o horário de esvaziar o recipiente. O lovely monitora as atividades sexuais masculinas, o desempenho da ereção e sugere posições mais adequadas para economia ou gasto de energia corporal (http://www.digitaltrends.com/wearables/lovely-wearable-sex-toy/).

3. A densidade de palavras é um procedimento quantitativo que divide o número total de ocorrências do termo pelo total de palavras no documento investigado. A densidade é um fator importante para avaliar a frequência relativa da temática em um dado contexto e para estabelecer análises comparativas entre documentos com diferentes extensões.

4. Fonte: relatório IDC http://www.idc.com/getdoc.jsp?containerId=prUS41284516

5. Fonte: http://expandedramblings.com/index.php/fitbit-statistics/

6. Para Latour (2012) as questões de interesse são aquelas que estabelecem entre os atores e não enquanto pressupostos empíricos do pesquisador.

7. Por sentido técnico compreende-se toda ocorrência onde "data" é usado como um rótulo de um procedimento técnico – ex. *data mining* –, uma qualidade computacional ou digital da informação – ex. "*data collected by devices, heart data"*.

8. Foram classificados como "dado do usuário" todas as citações onde termo está associado diretamente ao usuário ou em contextos onde há uma clara referência às informações digitais do cliente – ex: "*you consent that we may process the data that we collect from you*".

9. *Project IP ACT* (PIPA) defendia o controle governamental dados de acesso aos portais com conteúdo de propriedade intelectual

REFERÊNCIAS

Biggs, P., Garrity, J., LaSalle, C., & Polomska, A. (2016, outubro 22). Harnessing the Internet of Things for Global Development. *The Huffingtonpost*, p. 61. Recuperado de: http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

Campbell, D. (2014, outubro 6). Reward healthy people with tax rebates to save the NHS , urges thinktank Source. *The Guardian*, p. 13–14. Recuperado de: http://www.2020health.org/2020health/Press/Press-2014/May/Guardian-1-5-14.html

Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, *28* (6), 164–181. https://doi.org/10.1177/0263276411424420

Chung, A. E., Skinner, A. C., Hasty, S. E., & Perrin, E. M. (2016). Tweeting to Health: A Novel mHealth Intervention Using Fitbits and Twitter to Foster Healthy Lifestyles. *Clinical Pediatrics*. JOUR. https://doi.org/10.1177/0009922816653385

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies*, *18* (4–5), 479–496. https://doi.org/10.1177/1367549415584857

El Clarín. (3 de febrero de 2016). Para cuidarles la salud, exigen a estudiantes que usen pulsera inteligente. *El Clarín*. Recuperado de http://next.clarin.com/gadgets/cuidarles-exigen-estudiantes-pulsera-inteligente_0_1516048615.html

FITBIT INC. (2015a). *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the fiscal year ended December 31, 2015* (Vol. 15). Whahington D.C. Recuperado de: https://www.sec.gov/Archives/edgar/data/1447599/000144759916000018/fitbit123120151 0k.htm

FITBIT INC. (2015b). FITBIT Terms of Service. Recuperado 10 de outubro de 2016, de: https://www.fitbit.com/legal/terms-of-service

FITBIT INC. (2016a). Fitbit Privacy Policy [Short Privacy Policy]. Recuperado 10 de outubro de 2016, de Disponivel em: https://www.fitbit.com/legal/privacy Acesso

FITBIT INC. (2016b). Full Fitbit Privacy Policy. San Francisco, CA. Recuperado de: https://www.fitbit.com/legal/privacy-policy

FITBIT INC. (2016c, outubro 10). Fitbit Introduces " Fitbit Group Health " for Corporate Wellness, Weight Management Programs, Insurers and Clinical Research. *Business Wire*, p. 1–4. Recuperado de: http://www.businesswire.com/news/home/20160607005759/en/

FITBIT INC. (2016d, outubro 10). Two Fitbit Group Health Customers Demonstrate Cost Savings From Corporate Wellness Programs. *Business Wire*, p. 1–4. San Francisco, CA. Recuperado de: http://www.businesswire.com/news/home/20161004006269/en/

Fotopoulou, A., & O'Riordan, K. (2016). Training to self-care: fitness tracking, biopedagogy and the healthy consumer. *Health Sociology Review*, 1–15. JOUR. https://doi.org/10.1080/14461242.2016.1184582

Frankel, T. C. (7 de outubro de 2016). Fitbits now mandatory for students at this Oklahoma university. *The Whahington Post*. Recuperado de: https://www.washingtonpost.com/news/the-switch/wp/2016/02/02/fitbits-now-mandatory-for-students-at-this-oklahoma-university/

George, S. (2016, outubro 28). Better data means better health for the world ' s disease-troubled areas. *The Guardian*, p. 16–18. Recuperado de: https://www.theguardian.com/health-revolution/2016/mar/22/data-health-world-disease-information-smartphones-development

Gillespie, T. (2015). Algorithm. In B. Peters (Org.), *Digital Keywords. A Vocabulary of Information Society and Culture* (p. 297). Nova Jers: Princeton University Press Princeton and Oxford. Recuperado de: https://www.academia.edu/12401314/Algorithm_Keyword_

Gould, H. (2016, outubro 10). From app doctors to big data: five ways tech will shape healthcare. *The Guardian*, p. 17–19. Recuperado de: https://www.theguardian.com/sustainable-business/2016/may/17/from-app-doctors-to-big-data-five-ways-tech-will-shape-healthcare

Jethani, S., & Raydan, N. (2015). Forming Persona through Metrics: Can we Think Freely in the Shadow of our Data? *Persona Studies*, *1* (1), 76–93.

Jutel, A., & Lupton, D. (2015). Digitizing diagnosis: a review of mobile applications in the diagnostic process. *Diagnosis*, *2* (2), 89–96. https://doi.org/10.1515/dx-2014-0068

Karapanos, E., Gouveia, R., Hassenzahl, M., & Forlizzi, J. (2016). Wellbeing in the making: Peoples' experiences with wearable activity trackers. *Psychology of Well-Being: Theory, Research and Practice*, *2013*. https://doi.org/10.1186/s13612-016-0042-6

Kau, A. (2015). *Bring Your Own Wearable and Its Enterprise Implications*. Recuperado de: https://www.tractica.com/wearable-devices/bring-your-own-wearable-and-its-enterprise-implications/

Latour, B. (2012). *Reagregando o social: uma introdução à teoria do ator-rede*. Book, Salvador: Edufba.

Lemos, A. (2016). Sensibilités Performatives. Les nouvelles sensibilités des objets dans les métropoles contemporaines. *In Revue Sociétés*, *in press* (in press). Journal Article.

Lemos, A., & Bitencourt, E. (2016). *" I feel my wrist buzz ". SmartBody and Performative Sensibility in FitBit Devices*. Salvador, in press.

Lupton, D. (2015a). Health promotion in the digital era: A critical commentary. *Health Promotion International*, *30* (1), 174–183. https://doi.org/10.1093/heapro/dau091

Lupton, D. (2015b). Personal data practices in the age of lively data. *Available at SSRN 2636709*. Journal Article.

Lupton, D. (2016). *The Quantified Self*. Malden: Polity Press.

Nafus, D., & Sherman, J. (2014). Big data, big questions| this one does not go up to 11: the quantified self movement as an alternative big data practice. *International journal of communication*, *8*, 11. Journal Article.

Nascimento, C., e Bruno, F. (2013). QUANTIFIED SELVES: contar, monitorar e conhecer a si mesmo através dos números. In *Anais da 22 COMPÓS* (p. 1–19). Salvador.

Nascimento, L. da C. (2014). *O auto-conhecimento através dos números: as práticas de auto- monitoramento dos quantified selves* (Tese). Universidade Federal do Rio de Janeiro, Escola de Comunicação, Rio de Janeiro.

Nield, D. (2014). *Employee wellness programs now one of Fitbit's fastest growing areas*. Recuperado de: http://www.digitaltrends.com/mobile/employee-wellness-programs-now-one-fitbits-fastest-growing-areas/

Olson, P., & Tilley, A. (2014). *The quantified other: Nest and Fitbit chase a lucrative side business*. Recuperado de: http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/#1024a8905403

Pantzar, M., & Ruckenstein, M. (2015). The heart of everyday analytics: emotional, material and practical extensions in self-tracking market. *Consumption Markets & Culture*, *18* (1), 92–109. Journal Article.

Smith, G. J. D., & Vonthethoff, B. (2016). Health by numbers? Exploring the practice and experience of datafied health. *Health Sociology Review*, (July), 1–16. https://doi.org/10.1080/14461242.2016.1196600

Springbuk. (2016). *Wearable Technology : Unlocking ROI of Workplace Wellness Contents. An Employer Case Study in Health Care Cost Management*. Indianapolis. Recuperado de: https://www.springbuk.com/wearable-study/

Strauss, A., & Corbin, J. (2008). *Pesquisa Qualitativa: Técnicas e Procedimentos para o Desenvolvimento de Teoria Fundamentada*. (L. de O. Rocha, Trad.) (2º ed). Porto Alegre: Artmed.

Till, C. (2014). Exercise as Labour: Quantified Self and the Transformation of Exercise into Labour. *Societies*, *4* (SEPTEMBER 2014), 446–462. https://doi.org/10.3390/soc4030446

Vesnic-Alujevic, L., Breitegger, M., & Guimarães Pereira, Â. (2016). Do-It-Yourself? Healthcare? Quality of Health and Healthcare Through Wearable Sensors. *Science and Engineering Ethics*, 1–18. https://doi.org/10.1007/s11948-016-9771-4

Whitson, J. R. (2015). Foucault's Fitbit: Governance and Gamification. In P. Walz, Steffen & S. Deterding (Orgs.), *The Gameful World. Approaches, Issues, Applications* (p. 339–358). London: MIT Press.

Wolf, G. (2010, abril 26). The data-driven life. *The New York Times*. New York. https://doi.org/10.1353/wsq.2012.0006

EMPRESAS TRANSNACIONALES DE SEGURIDAD Y VIGILANCIA EN LA ARGENTINA

Resumen: La expansión de las prácticas de vigilancia está estrechamente relacionada con la globalización de empresas transnacionales de seguridad, como ADT, Prosegur, Securitas, entre otras. Estas empresas proveen de tecnologías a los organismos estatales, comercios, y ciudadanos de distintos países. A pesar de su importancia en los procesos actuales de vigilancia, las actividades de las trasnacionales de seguridad han pasado desapercibidas en el ámbito académico y/o periodístico de Latinoamérica en general, y de Argentina en particular.

A fin de iniciar una mayor percepción sobre esta problemática, en esta presentación mostraré resultados preliminares de un proyecto de investigación en curso sobre transnacionales de seguridad en Argentina. Esto incluirá, en primer lugar, una comparación del discurso global de seguridad de las transnacionales en sus reportes anuales, con el discurso que utilizan a nivel local. En segundo lugar, basado en datos primarios y secundarios presentaré un mapa de las principales empresas de seguridad y TICs que venden equipos de vigilancia en la Argentina, y describiré las formas en la que las transnacionales han logrado volverse parte de la "cultura" local. Finalmente, contrastaré el discurso de estas empresas con casos controvertidos difundidos en los medios de comunicación y otras organizaciones, que revelan serios interrogantes sobre la forma de operar de estas transnacionales. A la vez, esto me permitirá listar un conjunto de áreas de vacancia para estimular futuras investigaciones y discusiones para enfrentar el desafío causado por estas transnacionales.

Palabras clave: Empresas transnacionales de seguridad, Vigilancia, Argentina, Adaptación.

MAXIMILIANO VILA SEOANE*

Corporações transnacionais de segurança e vigilância na Argentina

Resumo: A expansão das práticas de vigilância está intimamente ligada à globalização das empresas de segurança transnacionais como ADT, Prosegur, Securitas, entre outras. Estas empresas fornecem tecnologias para as agências governamentais, empresas e cidadãos de diferentes países. Apesar da sua importância no atual processo de monitoramento das atividades de segurança transnacional, elas passaram despercebidos em o contexto académico e jornalística da América Latina em geral, e da Argentina em particular.

Para iniciar uma maior consciência sobre esta questão, nesta apresentação mostrarei os resultados preliminares de um projeto de investigação em curso sobre corporações transnacionais de segurança na Argentina. Isto incluirá, em primeiro lugar, uma comparação do discurso de segurança das corporações transnacionais nos seus relatórios anuais com o discurso usado localmente. Em segundo lugar, com base em dados primários e secundários, vou apresentar um mapa das principais empresas de segurança que vendem equipamentos de vigilância na Argentina, e descreverei as maneiras em que as empresas transnacionais têm conseguido se tornar parte da "cultura" local. Finalmente, contrastarei o discurso dessas empresas com casos controversos divulgados nos meios de comunicação e outras organizações que revelam sérias questões sobre como operar essas transnacionais. Por sua vez, isso vai permitir-me listar um conjunto de áreas de vacância para estimular futuras pesquisas e discussões para o desafio causado por estas empresas.

Palavras-chave: Corporações transnacionais de segurança, Vigilância, Argentina, Adaptação.

Transnational security companies and surveillance in Argentina

Abstract: The expansion of surveillance practices is closely linked to the globalization of transnational electronic security companies, like ADT, Prosegur, Securitas, among others, who provide the needed technologies to states, businesses and citizens of diverse countries. In spite of their importance in contributing to the growth of surveillance, the activities of these transnationals have been scarcely researched in academia and the press of Latin America in general, and of Argentina in particular.

In order to contribute to greater public discussions on this issue, in this presentation I shall show preliminary results on an ongoing research Project on transnational security companies in Argentina. This will include, first, a comparison between the global features of the discourse of these transnationals in their annual reports, with the one that they use locally. Second, based on primary and secondary data I will map the main security firms in the country, and list some of the strategies that they are employing to become local. Finally, I shall contrast the claims of the discourse of these firms with controversial cases from the press and other organizations, which raise serious questions on the operation of these transnational corporations. These will suggest a number of gaps to deepen in future research projects and in the general public debate on the impacts of surveillance in society.

Keywords: Transnational security companies, Surveillance, Argentina, Localization.

INTRODUCCIÓN

En la literatura académica de los últimos años, crecen los estudios sobre el rol de empresas privadas en la guerra, e incipientemente el rol de empresas en la implementación de la seguridad privada (Avant, 2005). Según los críticos, la privatización de la seguridad debilita la capacidad del Estado de garantizarla como un bien público (Zedner, 2006). Por el contrario, otros analistas más optimistas sostienen que lo que se observa es un una transición de la provisión centralizada por parte del Estado de los servicios de seguridad pública, a una red de múltiples actores donde nuevos actores privados participante activamente, pero donde el Estado aún retiene la preponderancia (White, 2011). Estas tendencias son importantes para estudiar la vigilancia en nuestras sociedades contemporáneas, ya que muchas de las empresas de seguridad privada son

las que proveen la tecnología y los servicios que las hacen posibles. Siguiendo a Gill (2008), entiendo a la expansión de las prácticas de vigilancia masivas como un producto del nuevo orden mundial timoneado por los Estados Unidos, que difunde la hegemonía de una globalización neoliberal. En este contexto, las prácticas de vigilancia son centrales, no sólo por cuestiones geopolíticas, sino también para reducir los riesgos en la acumulación de capital, y en generar identidades de acorde a sus intereses.

Este crecimiento de las prácticas de vigilancia, se está expandiendo por todo el planeta gracias a empresas transnacionales de seguridad, ya sea estadounidenses u otras que copian sus prácticas, ya que sus estrategias de negocio se están focalizando cada vez más en el desarrollo de soluciones de seguridad tradicional en convergencia con soluciones de seguridad electrónica. Debido a la creciente importancia de estas organizaciones, ya hay incipientes trabajos sobre las mismas en la literatura Anglófona, pero escaso o nulos que analicen su accionar en el contexto de América Latina. En tal sentido, este artículo esboza resultados preliminares sobre un proyecto en curso sobre trasnacionales de seguridad y vigilancia que aporten al conocimiento de estas organizaciones en la región, tomando como fuentes primarias de observación al caso de Argentina. En el texto se adopta una perspectiva de economía política, que entiende que las empresas transnacionales de seguridad son actores económicos y políticos, que emergen en un contexto de hegemonía de políticas neoliberales, y que a la vez emplean un conjunto de estrategias de legitimación para operar a la par de las fuerzas de seguridad nacionales (White, 2011).

En particular, empleo la estrategia posestructuralista de los estudios de seguridad, que entiende que la 'seguridad' no es algo que puede ser definido de forma objetiva, que tiene una esencia, al contrario, se tiene que entender como un proceso de nombrar algo, que al hacerlo, tiene efectos en lo que se entiende como un problema de seguridad, y cómo se actuará ante el (Waever, 1995). Esta forma de entender la seguridad ha sido útil para comprender como los Estados han expandido la definición de seguridad, más allá de las amenazas militares, por ejemplo, seguridad ambiental, económica, ciberseguridad, etc. Y en este artículo extiendo esta idea para el estudio de cómo las empresas trasnacionales definen ¿qué es un problema de seguridad? Al fin y al cabo, si las mismas ofrecen productos y servicios para resolver el problema de la "inseguridad", implícitamente tienen una definición de la misma, que si nos guiamos por esta teoría, también es construida socialmente.

En cuanto a la organización del artículo, primero muestro estadísticas sobre las empresas dedicadas a la seguridad electrónica en el país. Segundo, esbozo las principales características de sus discursos globales, haciendo foco en qué tipo de problemas de seguridad identifican. Tercero, listo sus formas de adaptación y legitimación para operar en el contexto de Argentina. Finalmente, comparo los argumentos de estas empresas con información periodística, de organizaciones sindicales y otras no gubernamentales, que revelan las contradicciones del discurso y el accionar de las empresas de seguridad transnacional, y que plantean serios interrogantes generados por sus actividades.

MÉTODOS

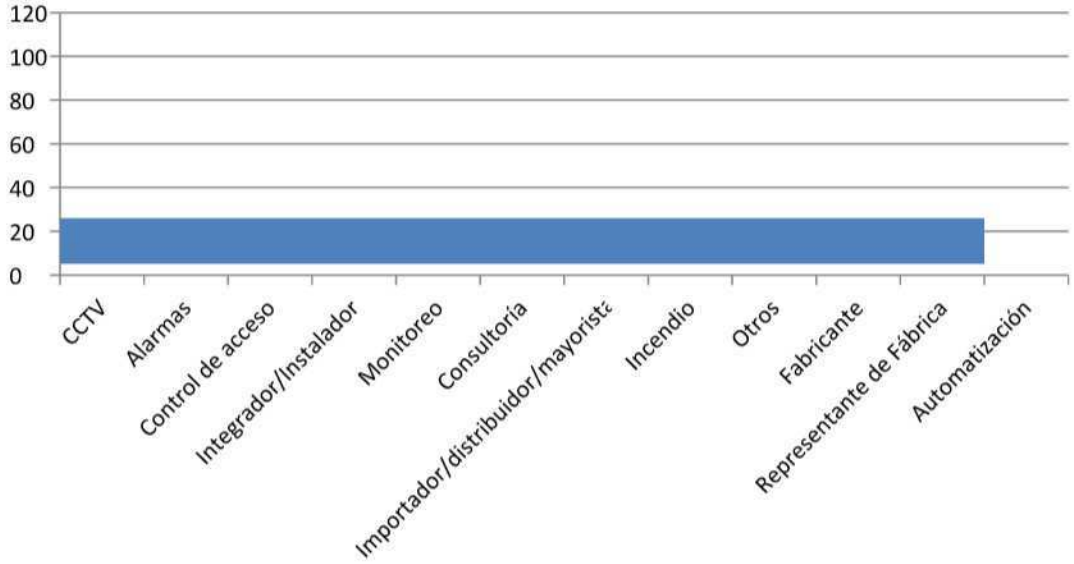
Se utilizaron cuatro tipos de fuente de información: a) los reportes anuales de las empresas, donde se justifica su modelo de negocio, su perspectiva sobre la industria actual y a futuro, y una explicación de sus productos y servicios; b) se obtuvo información detallada de sus productos y servicios, tanto en sus páginas internacionales (generalmente en Inglés), y su respectiva versión Española para el mercado de Argentina; c) se recolectó información sobre la operación de estas empresas en la ciudad de Buenos Aires, y observaciones del autor en un evento del sector; d) artículos en internet en periódicos, foros y organizaciones relacionadas al sector de la seguridad (cámaras empresarias y sindicatos) y la vigilancia, donde se relatan situaciones problemáticas de estas para resolver los problemas que supuestamente resuelven.

EMPRESAS TRANSNACIONALES DE SEGURIDAD EN ARGENTINA

Estadísticas

En Argentina hay una diversidad de empresas de seguridad electrónica, que son las que suministran diversos productos y servicios para las crecientes prácticas de vigilancia en comercios, hogares, espacios públicos, entre otros. Desde la Cámara Argentina de Seguridad Electrónica, que nuclea a las principales firmas tanto nacionales como extranjeras en el país, tienen registradas a 146 organizaciones relacionadas con la seguridad electrónica en el país, que operan en diferentes áreas, tal como se observa en el siguiente Figura 1.

FIGURA 1: CANTIDAD DE ORGANIZACIONES REGISTRADAS EN CASEL POR ÁREA.



Fuente: CASEL.

Casos de transnacionales

Los datos de la Figura 1 sugieren una dinámica industria de la seguridad en Argentina. No obstante, esto oculta que tal como está ocurriendo en otros países, las empresas transnacionales son las que mayor peso tienen en términos económicos y tecnológicos. De hecho, al juntar las categorías de monitoreo y de CCTV, que son las áreas más directamente asociadas a la vigilancia electrónica, se detectan 9 empresas que operan en más de 1 país, que prevalecen en la oferta de servicios de vigilancia. Por lo tanto, en esta sección me focalizo en algunas características del discurso global de las principales empresas transnacionales de seguridad electrónica. Entre ellas, consideré a: ADT (USA), G4S (Reino Unido), Prosegur (España) y SECURITAS (Suecia). Cabe resaltar que ADT ofrece mayoritariamente soluciones de seguridad electrónica, mientras que las otras empresas tienen a la seguridad electrónica como un complemento cada vez más importante de un portfolio más amplio de productos y servicios de seguridad. Por ejemplo, vigilancia presencial, móvil, consultoría en seguridad, etc. A pesar de sus diferencias, estas empresas comparten algunas características en común en su discurso global que detallo en las siguientes sub-secciones: la forma arbitraria en definir qué es un problema de seguridad; la financialización de sus operaciones; y la propuesta de una solución tecnológica.

Las empresas transnacionales se nos presentan como actores centrales para alcanzar sociedades más seguras. Por ejemplo, la presidente de Prosegur dice que "La seguridad es un pilar básico para el normal desarrollo de la sociedad y nosotros jugamos un papel relevante en la consecución de un entorno más seguro y, por tanto, de más libertad" (Prosegur, 2015: 7).

Pero estas declaraciones no tendrían mucho sentido sin una explicitación de qué entienden estas empresas por 'seguridad'. Sin embargo, en sus reportes no encontramos una definición precisa, sino que un conjunto de "motores" de crecimiento de la industria o riesgos a enfrentar. Por ejemplo, G4S (2015: 14) identifica al terrorismo, las migraciones masivas, la instabilidad económica, pandemias, el cambio climático y la ciberseguridad. Del mismo modo, SECURITAS (2015: 2) consideran al terrorismo y a los refugiados, como fuentes de inseguridad. Esto indica que la seguridad es un concepto abierto en estas transnacionales, es decir que no tiene una esencia estable, y que se construye a partir de las declaraciones discursivas de los miembros de estas empresas y de sus textos corporativos. Por lo tanto, también se pueden detectar los procesos que Waever denominó de securitización y desecuritización en las empresas transnacionales de seguridad, que muestran la definición dinámica y variable de seguridad que emplean.

Además de esta arbitrariedad en la definición, la selección de prioridades se corresponde con temáticas 'globales', es decir, aquellas que son prioritarias en las regiones de mayor peso económico y político del mundo. Por ejemplo, el tema de los refugiados es central para Europa y EEUU, como lo es la amenaza del terrorismo y la ciberseguridad. Si bien esto no es malo en sí, pues las soluciones que funcionan en un dado lugar pueden llegar a transmitirse y aplicarse en otro, el énfasis en los problemas causados por inestabilidad económica, tal vez la mayor causa de casos de inseguridad en América Latina, no tiene la prioridad que uno esperaría. Por lo tanto,

las prioridades de estas empresas parecieran reflejar las prioridades de las economías más ricas del planeta, de donde estas empresas obtienen una parte importante de sus ingresos.

Hay otro aspecto central en la operación de las multinacionales que tiene que ser destacado de forma general, y en particular para el caso de aquellas dedicadas a la seguridad. En las últimas dos décadas estamos viviendo un proceso de 'financialización' de la economía global, que básicamente refleja el creciente poder del sector financiero en la economía, y la expansión de sus prácticas a nivel nacional, empresarial e individual (French, Leyshon, y Wainwright, 2011). Entre los varios cambios que este proceso está produciendo, en este trabajo es importante destacar la creciente presión que los administradores de las empresas transnacionales tienen para mostrar un continuo crecimiento del valor de sus acciones en las diferentes bolsas donde cotizan. Esta presión para devolver mayor valor a sus accionistas es algo evidente en todos los sitios de las empresas estudiadas, donde tenemos acceso a información detallada de sus acciones, por ejemplo, a la curva histórica de cotización, y sus cambios recientes. No obstante, esta dependencia con los mercados financieros somete a las empresas a una intensa presión para reducir sus costos, para volverse más eficientes y mostrarles a sus accionistas las ganancias financieras que obtienen con la empresa. Este es uno de los motivos por los cuáles tienen que buscar ofrecer nuevas soluciones tecnológicas que las distingan de sus competidores (G4S, 2015: 13).

Si bien las empresas analizadas no convergen en sus definiciones de los problemas de seguridad, sí lo hacen al momento de creer en la capacidad de la tecnología de ofrecer problemas a los problemas de inseguridad que las sociedades contemporáneas enfrentan. De hecho, las principales empresas transnacionales se encuentran en una intensa competencia en ver quién desarrollará las mejores tecnologías para enfrentar los problemas de 'seguridad' que identifican. A continuación delineo algunas tendencias en esta área:

- Idealmente, las empresas buscan vender 'soluciones integrales' de seguridad (G4S, 2015: 41), es decir, no solamente los equipos, pero también diseños adaptados a las necesidades de los clientes, incluyendo personal de seguridad. Las empresas multinacionales aseguran que su experiencia global las posiciona de forma única para ofrecer tales servicios.

- Bajo esta tendencia, la tecnología juega un rol central, pues permite vender toda una gama de productos y servicios para mantener la seguridad a distancia, presentados por Prosegur como formas de 'disuasión creativa', o por ADT como una forma de "no dejarlos entrar".

- Entre las tecnologías más difundidas en el mercado encontramos la vigilancia móvil y la video vigilancia. La última contempla los circuitos de CCTV que permiten tener una observación las 24h y a tiempo real de zonas de interés. Por ejemplo, en Buenos Aires se destaca el servicio de vigilancia remota de Prosegur denominado El Ojo del Halcón, que consiste en un tótem, con una pantalla, cámara y parlantes, que le permite a un guardia de Prosegur controlar a la distancia varios hogares que lo tengan instalado.

FIGURA 2

El Ojo del Halcón.

Fuente: Prosegur.

- En cambio, la vigilancia móvil le agrega a la videovigilancia la capacidad de realizar el control de personas (georeferenciamiento) y de cámaras, pero a la distancia desde smartphones u otro tipo de dispositivos con acceso a internet. Por ejemplo, la herramienta FIND U de ADT es el típico ejemplo de sousveillance, que nos permite saber en tiempo real la ubicación geográfica de otras personas, que incluso pueden enviar señales de pánico con sus celulares en caso de emergencias. Estas propuestas de control son generalmente de menor costo que las de vigilancia realizada en persona. En suma, estas tecnologías prometen un control a la distancia de lo que valoramos en nuestras sociedades de riesgos, creando complejas redes humano-máquina. Las soluciones de seguridad electrónica contribuyen a que esta fantasía del control absoluto, a tiempo real y a distancia se vuelva realidad.

- Sumado a estas tendencias, las empresas transnacionales de seguridad están invirtiendo en el área de 'ciberseguridad', y estratégicamente en el largo plazo en soluciones de robótica (SECURITAS, 2015: 4). El desarrollo de drones por parte de Prosegur en conjunto con start-ups Españolas es un ejemplo de esto (Prosegur, 2015: 23).

FIGURA 3
Drón de Prosegur.

Fuente: Prosegur.

- Por último, es importante señalar que estos productos y servicios de vigilancia generan un flujo continuo de información que las empresas multinacionales recolectan en sus 'centros de datos' (data centers), donde se registran y analizan las diferentes señales de los instrumentos de observación empleados por y para sus clientes.

En síntesis, lo que vemos es que la tecnología se está volviendo uno de los factores centrales en los modelos de negocio y competitividad de las empresas transnacionales de seguridad.

Adaptación de las multinacionales a la Argentina

Antes de analizar el accionar de las empresas transnacionales de seguridad en Argentina, es importante tener en cuenta algunas características de la seguridad en el país. Según Saín (2013), tras la democratización se arrastran serios problemas institucionales, principalmente el desgobierno político que llevó a un sistema de auto-gobierno policial, y una criminalización selectiva que padecen los sectores más pobres de la sociedad, pero no otros. Además, en los últimos años creció la percepción de inseguridad por parte de la población. Estas tendencias llevan a que la población desconfíe del accionar de la policía. También varias figuras políticas promueven el uso de tecnologías para paliar las consecuencias de los hechos de inseguridad, como el uso de botones anti-pánico, o el uso de CCTV. Esto describe un escenario propicio para la expansión de empresas de seguridad privada (nacionales y transnacionales) que ofrezcan 'soluciones' a las empresas y ciudadanos para

los problemas que el Estado deja vacante. De hecho, la industria de la seguridad privada comenzó a expandirse con mayor velocidad en el país en los 80s y 90s (SECURITAS, 2014: 13), que coinciden con la intensificación de la globalización, y con la desmilitarización del país, que propició la contratación de ex miembros de las fuerzas armadas y de seguridad por estas empresas. Gracias a la fundación de CASEL en 2001, junto con la llegada de ADT y Prosegur, se propició el crecimiento del mercado de oferta de productos de seguridad electrónica (SECURITAS, 2014: 37). Y hoy en día hay una pujante demanda por sus productos y servicios. Según el informe de SECURITAS (2014: 27) sobre la industria de seguridad privada, los organismos que más tienden a adquirir los productos y servicios de estas empresas de seguridad son los bancos, seguidos por supermercados, autoservicios y shoppings. Le siguen otro tipo de industrias y grandes empresas, entre ellas, las basadas en la extracción de recursos naturales (petróleo, gas, minería, etc.), y de transporte. Las PYMES y comercios son otros de los clientes principales. Es decir que todas estas categorías coinciden con la importancia de proteger las ganancias del sector corporativo, que es coherente con la concepción de Gill (2008) sobre la creciente vigilancia mundial con el fin de reducir los riesgos en los procesos de acumulación de capital. Finalmente, las empresas incluyen a los clientes individuales, que en las páginas en español suelen estar abiertas con distinto nivel de detalle según la empresa. Por ejemplo, Prosegur menciona a 'jóvenes y parejas', 'familias con hijos', 'adultos mayores', y 'el nuevo emprendedor'.

Pero la expansión y aculturación de las empresas transnacionales de seguridad electrónica en Argentina no fue ni es homogénea. Al contrario, se detectan estrategias más sofisticadas de localización en algunas empresas que en otras, que les permite pasar casi como locales. Por un lado, las empresas occidentales emplearon mayoritariamente la estrategia de adquisición de empresas locales de seguridad privada, como el caso de SECURITAS que llegó en la crisis del 2001, adquirió una empresa local, y en los años siguientes unas nueve más, de forma tal de trasladar su metodología de trabajo a diferentes regiones del país (SECURITAS, 2014: 19). Por el otro lado, actualmente hay un proceso de expansión de empresas Chinas en el país, como Dahua y Sinovision, cuyo modelo no analizo en este artículo, pero que pareciera estar enfrentando más dificultades para adaptarse a la región.

En el caso de las transnacionales occidentales, estas empresas emplean múltiples estrategias para adaptar y legitimar sus actividades al contexto de los países donde operan (White, 2011), que resumo a continuación en base a mis observaciones en el contexto Argentino:

- Argumentan que ser 'global' es algo 'bueno', pues implica que son capaces de operar de forma 'seria' y 'continua' en diversos países, adaptándose a las distintas condiciones, y transfiriendo prácticas de una zona a otra. De hecho, las transnacionales de seguridad si bien tienen una dependencia fuerte de sus casas matrices, suelen operar con modelos de gestión y operación localizados, pues contratan muchas veces a personal del país en donde operan.

- La simbología ocupa un rol importante en la legitimación de estas empresas. Vemos como utilizan sus mismos logos alrededor del mundo, en los uniformes de sus empleados, en sus

transportes, o en zonas vigiladas por cámaras en hogares y edificios, de forma tal de anunciar su operación en tales espacios, y de disuadir potenciales actividades criminales. Esto les sirve para simular cierta similitud con las fuerzas de seguridad nacional, y así generar cierta confianza en la población y sus clientes.

- Otra estrategia usual es mostrar su pertenencia a otros organismos internacionales de seguridad, de forma de probar su seriedad en la oferta de productos y servicios según los estándares transnacionales. Por ejemplo, muchas de las empresas alegan ser parte del pacto global de Naciones Unidas, que las compromete a respetar los derechos humanos.
- La mayoría de las transnacionales tienen un área dedicada a la Responsabilidad Social Empresaria (RSE), donde argumentan por intermedio de reportes anuales y de 'casos' las contribuciones que hacen al desarrollo social de las comunidades en donde operan. Esta es una forma de contrarrestar la crítica de que sólo se interesan por las ganancias económicas, y a la vez, contrarrestar las críticas de organizaciones externas sobre sus violaciones a los derechos humanos.
- Las empresas legitiman sus intervenciones en base a previos 'casos de éxito', en los cuáles lograron ofrecer sus productos y servicios, como en shoppings, estadios u organismos estatales.
- A su vez, se suelen remarcar los premios que ganan en competencias de nuevos desarrollos de seguridad.
- Finalmente, algunas transnacionales como Prosegur y SECURITAS han creado sus propios centros de entrenamiento en el país, dedicados a capacitar y especializar a sus empleados. Esto legitima el conocimiento en seguridad de estas empresas.

En fin, las empresas transnacionales de seguridad adaptan la oferta de sus productos y servicios a las regiones en donde operan en base a un mix de diferentes estrategias.

Casos conflictivos – La inseguridad de la seguridad

Si bien las empresas transnacionales de seguridad se presentan como genios que resolverán los principales problemas que sus potenciales clientes enfrentan, esta forma ideal de 'venderse' soslaya varios de los inconvenientes que estas empresas enfrentan en la práctica, y que detallo en esta sección.

Dependencia tecnológica

La competencia entre las transnacionales para ofrecer las mejores tecnologías que resuelvan los problemas de inseguridad, impulsa a las mismas a utilizar estrategias de protección de su propiedad intelectual, por ejemplo mediante patentes. Esto les permite demandar a sus competidores, y hacerles pagar un elevado costo si quieren entrar en su nicho tecnológico, lo cual es un riesgo ya que 'legaliza' el proceso de innovación tecnológica (ADT, 2016: 95), y lleva a una concentración de conocimiento en estas empresas. Esto es problemático en el área de la

seguridad, ya que muchas de las actuales y futuras tecnologías de vigilancia quedaran bajo el monopolio temporal de estas transnacionales, reduciendo las capacidades de los Estados de incidir en las decisiones sobre el diseño de las tecnologías de seguridad. A su vez, esto les limitará el accionar de las empresas locales, que van a ver, al menos por el período que dure la patente, limitada su capacidad de innovación. Asimismo, las empresas transnacionales están generando sus propios centros de entrenamiento en el uso de sus tecnologías y métodos de trabajo, que no es difícil de imaginar que se convertirán en sistemas paralelos y cerrados de entrenamiento para las fuerzas de seguridad, desafiando al sistema público.

No obstante, estas observaciones no impiden que las transnacionales puedan desarrollar tecnologías adaptadas a las necesidades locales. De hecho, ya lo están haciendo. Por ejemplo, la sede Argentina de Prosegur elaboró localmente El Ojo del Halcón, y presentó la solicitud de la patente para esta invención. Es decir, es un desarrollo local, ajustado a las necesidades de bajar el costo, y a la vez, de disuadir a posibles criminales, que se puede expandir a toda la transnacional. Y en tal caso, el problema que se detecta para otras tecnologías generadas en el exterior, lo tendrán que padecer otras jurisdicciones. Sin embargo, esto no niega, sino que confirma la existencia de un proceso de redistribución del poder entre los actores dedicados a la seguridad, donde las transnacionales ganan, gracias a sus ventajas en términos de desarrollo tecnológico.

Falsas soluciones tecnológicas para complejos problemas sociales

El proceso de financialización de la industria de la seguridad es evidente en el concepto de "crecimiento sostenible y redituable" que se utiliza en el informe anual de G4S (2015: 13), y que figura similarmente en las otras transnacionales. En todos los casos, la presión por conseguir mejores resultados financieros empujan estas empresas por senderos de desarrollo tecnológico que les permite ofrecer soluciones diferenciadas con respecto a sus competidores. Ahora bien, una crítica que se puede hacer es que esta presión financiera necesita que el problema de la inseguridad continúe, pues sino la industria se volvería insustentable e innecesaria. Esto explicaría por qué la industria se inclina por soluciones tecnológicas simples, que son totalmente inadecuadas para resolver definitivamente los problemas de inseguridad. La Argentina, como muchos otros países de América Latina, tiene un preocupante problema de inseguridad ciudadana, que es un fenómeno de múltiples causas, aunque una de las principales en la región es la alta desigualdad de ingresos y oportunidades entre la población. Sin embargo, la 'desigualdad' como causa de la inseguridad está prácticamente ausente de los reportes de estas empresas. Por lo tanto, contar con avanzados sistemas de video-vigilancia, vigilancia móvil, drones, etc., puede ser útil para algunos sectores de la población, pero altamente insuficientes para resolver el problema de la inseguridad en la región. Desde mi punto de vista, estamos ante 'falsas soluciones tecnológicas', ofrecidas por culpa de la competencia financiera entre estas transnacionales, que soslayan las complejas causas de los problemas de inseguridad, muchas veces retroalimentándose con los discursos más conservadores de mano dura y castigo de 'criminales´, en vez de intervenir para reducir los determinantes sociales de tales actos.

Fallas tecnológicas

Si bien las empresas de seguridad prometen que sus soluciones son eficaces para resolver la inseguridad de sus clientes, en la práctica estas promesas no siempre se cumplen por culpa de distinto tipos de fallas que todo sistema socio-técnico puede llegar a sufrir. Entre las que afectan a la vigilancia, se pueden detectar las siguientes:

- Las imágenes grabadas por las cámaras de vigilancia no siempre son fidedignas para identificar a los sospechosos, que puede terminar con condenas equivocadas.
- Si bien la cantidad de dispositivos de vigilancia está en aumento, no hay evidencia contundente sobre su capacidad de disuadir actividades criminales. De hecho, su existencia no quita que los perpetradores no puedan encontrar formas de sobrepasar estas medidas, como cubrir sus rostros, o atacar las cámaras.
- Las alarmas pueden fallar, de hecho, ADT considera estos fallos un riesgo para su negocio, ya que en EEUU y Canadá se les cobra si la empresa le envía falsas señales a los servicios de seguridad.
- El incremento de dispositivos electrónicos de vigilancia, que registran en muchos casos información confidencial sobre los clientes de las empresas transnacionales, son susceptibles de ciberataques, que curiosamente limitan la capacidad de estas empresas de ofrecer la seguridad total que nos prometen (ADT, 2016: 90).

Desigualdad en la protección

Si las multinacionales de seguridad se vuelven un actor cada vez más central en la oferta de productos y servicios para la población, ¿cómo afectará su lógica de obtención mayores beneficios a partir de complejas soluciones tecnológicas el acceso a la seguridad? No es arriesgado afirmar que la lógica de operación de estas empresas apunta a los pequeños segmentos capaces de pagar por sus servicios (Monahan, 2008). De hecho, si uno analiza las imágenes de segmentación de mercado que utilizan, en muchos casos se menciona 'familias', pero al mirar detalladamente al tipo de familias que hacen alusión, no se trata de cualquier tipo de familia, sino de aquellas con integrantes de tez blanca, posiblemente de clase media o alta del país, con el suficiente dinero para acceder a sus servicios. Es decir que los productos y servicios de estas empresas, al operar en un contexto nacional con alta desigualdad, mayoritariamente favorecerán a los sectores de mayores ingresos, soslayando a los que no puedan ocupar el rol de 'clientes' de estas empresas, profundizando las asimetrías en el acceso a los servicios de seguridad, que de por sí ya son bastante desiguales en Argentina.

CONCLUSIÓN

En este artículo describí el creciente rol de las empresas transnacionales de seguridad en la provisión de soluciones de seguridad electrónica. Entiendo que esto es parte de un proceso de

globalización de estas empresas, que en el marco de una globalización neoliberal impulsada por EEUU, son presionadas por la lógica financiera de obtener la mayor cantidad de ganancias, y esto las lleva a competir para ofrecer las soluciones tecnológicas más avanzadas. Esto les permitió expandirse por múltiples continentes donde proveen productos y servicios de vigilancia, adquiriendo un poder económico y político no imaginado unas décadas atrás. No obstante, el surgimiento de este nuevo actor económico y político trae aparejado varios desafíos para la provisión de la seguridad.

En primer lugar, si bien en el contexto de países centrales se habla de 'gobernanza nodal', donde se redistribuye el poder entre actores públicos y privados, estas imágenes subestiman que tales procesos son más pronunciados en los países periféricos, donde hay una menor capacidad Estatal de regulación de las actividades de estas empresas. No es novedad afirmar que el poder corporativo saca ventajas en países con gran desigualdad social, donde las instituciones no funcionan como deberían, y donde faltan mecanismos de rendición de cuentas. En estos contextos las empresas pueden fácilmente utilizar sus recursos económicos para influenciar a los decisores de política pública con el fin de alcanzar sus objetivos. Esto es problemático, porque les permite fácilmente definir que es un problema de seguridad, y cómo resolverlos, con escasa o nula participación de actores estatales o de la sociedad civil.

En segundo lugar, la solución de los problemas de inseguridad por medio de tecnología puede llevar a nuevas dependencias. De hecho, la especialización y concentración de soluciones tecnológicas en pocas empresas transnacionales posiblemente aumentará la subordinación tecnológica de las fuerzas de seguridad con estas transnacionales, que están sistemáticamente protegiendo sus desarrollos por propiedad intelectual. Además, el diseño de tales sistemas es algo que no está abierto a la sociedad civil, que es un nuevo déficit democrático, donde lo que está en disputa es la relación entre seguridad y el bien común. La tendencia actual que se observa es de empresas que se concentran en soluciones tecnológicos para los sectores de la sociedad que las puedan pagar, perjudicando a los de menores recursos. Esto en muchos casos va en contra de políticas más progresistas de seguridad, que buscan resolver las causas, y prevenir los delitos, donde sin duda la desigualdad es uno de las principales causas en los países de la región. No obstante, esto está ausente en los discursos y en las soluciones tecnológicas que ofrecen estas empresas transnacionales, peligrosamente retroalimentando los discursos más conservadores de mano dura.

En síntesis, estamos ante el crecimiento de nuevas y sofisticadas estructuras de observación de la población, que ya no se encuentran directamente bajo el control del Estado, sino que de empresas transnacionales. El problema central con esta tendencia es que se reduce el espacio de decisión ciudadana sobre cómo deberían funcionar los sistemas de seguridad y de vigilancia, que cada vez más quedarán sujetos a los diseños y propuestas del poder transnacional. Por tal motivo, estoy de acuerdo con los representantes de estas transnacionales que demandan mayores regulaciones para el sector. Sin embargo, pienso que estas no tienen que ser a medida de los intereses corporativos, sino que precisan incluir las indispensables perspectivas de representantes

de la sociedad civil, junto con adecuados mecanismos de control de las actividades empresariales a fin de implementar políticas progresistas en el área de seguridad ciudadana, que distribuyan los nuevos instrumentos de vigilancia de una forma democrática y equitativa entre los sectores de la sociedad.

NOTAS

* Investigador Junior, Center for Development Research (ZEF), maxi@vilaseoane.com

REFERENCIAS

ADT. (2016). *The ADT corporation 2015 annual report* (p. 183). Florida, USA.

Avant, D. D. (2005). *The market for force. The consequences of privatizing security*. Cambridge, UK: Cambridge University Press.

French, S., Leyshon, A., y Wainwright, T. (2011). Financializing space, spacing financialization. *Progress in Human Geography*, *35* (6), 1–22.

G4S. (2015). *Securing your world. Integrated report and accounts* (p. 204). London, UK.

Gill, S. (2008). *Power and resistance in the new world order* (2nd ed.). New York, USA: Palgrave Macmillan.

Monahan, T. (2008). Editorial: surveillance and inequality. *Surveillance & Society*, *5* (3), 217–226.

Prosegur. (2015). *Informe Anual* (p. 391). Madrid, España.

Saín, M. F. (2013). La oscilación. Los vaienes de la reforma del sector seguridad en la Argentina reciente. In *¿A dónde vamos? Análisis de políticas públicas de seguridad ciudadana en América Latina* (pp. 263–297). Washington, DC, USA: Woodrow Wilson International Center for Scholars.

SECURITAS. (2014). *Los desafíos de la seguridad privada en Argentina. Presente y futuro de una profesión* (p. 69). Buenos Aires, Argentina.

SECURITAS. (2015). *Annual Report* (p. 128). Stockholm, Sweden.

Waever, O. (1995). Securitization and Desecuritization. In *On Security* (pp. 46–86). New York, USA: Columbia University Press.

White, A. (2011). The new political economy of private security. *Theoretical Criminology*, *16* (1), 85–101.

Zedner, L. (2006). Liquid security: managing the market for crime control. *Criminology & Criminal Justice*, *6* (3), 267–288.

EJE 7

DIMENSIONES CULTURALES DE LA VIGILANCIA

GUERRA DE IMAGENS: A POLÍCIA MILITAR DE SÃO PAULO SOB VIGILÂNCIA

Resumo: Fazendo uso das Tecnologias de Informação e Comunicação (TIC), cidadãos hoje produzem imagens em qualquer situação que desejarem. Dentre as possibilidades que se conectam a esse panorama, há um fenômeno de produção de vídeos e fotografias que são divulgados como verdade, denúncia e prova. É o caso dos registros que expõem policiais cometendo algum ato violento, como abordagens truculentas, agressões e execuções. Nesse contexto, o presente trabalho, a partir de estudos bibliográficos sobre policiamento e vigilância, e da análise da repercussão pública de dois casos específicos, pretende discutir quão efetivas são as táticas de contra-vigilância no combate à violência policial. Os eventos escolhidos são ambos protagonizados pela Polícia Militar do Estado de São Paulo: as agressões na Favela Naval, na Grande São Paulo, em 1997, que culminaram na morte de um morador da região; e uma execução dupla ocorrida no bairro do Butantã, zona oeste da capital, em 2015. As considerações ao final apresentadas evidenciam que, embora separadas por um intervalo de quase duas décadas, os dois exemplos guardam semelhanças no que diz respeito à nova visibilidade do poder público, e diferenças sobre as plataformas usadas para trabalharem nesse sentido, além de um aumento exponencial observado pela apropriação das novas tecnologias. Em ambos observam-se tensões entre Estado e sociedade que podem motivar mudanças na percepção pública e o policiamento, ainda incipientes, no entanto.

Palavras-chave: Contra-vigilância, Violência policial, Imagens, São Paulo.

GABRIEL CUNHA VITURI*

Guerra de imágenes: la policía militar de são paulo bajo vigilancia

Resumen: Haciendo uso de las Tecnologías de la Información y Comunicación (TICs), ciudadanos producen hoy en día imágenes en cualquier situación que deseen. Dentre las posibilidades que se conectan a ese panorama, se presenta un fenómeno de producción de vídeos e fotografías que se divulgan cómo verdad, denuncia y prueba. Es el caso de los registros que exponen policiales cometiendo algún acto violento, caso de abordajes truculentas, agresiones y ejecuciones. En ese contexto, el presente trabajo, a partir de estudios bibliográficos sobre policiamento y vigilancia, y del analisis de la repercusión pública de dos casos específicos, se propone a discutir cuán efectivas son las tácticas de contra-vigilancia en el combate a la violencia policial. Ambos los eventos escogidos son protagonizados por la Policia Militar el Estado de São Paulo: las agresiones en la Favela Naval, en la Gran São Paulo, en 1997, que han culminado en la muerte de un habitante de la región; y una execución doble ocurrida en el barrio Butantã, zona oeste de la capital, en 2015. Las consideraciones presentadas al final evidencian que, aunque separadas por un intervalo de casi dos decadas, en los dos ejemplos hay similitudes en lo que se refiere a la nueva visibilidad del poder publico, y diferencias sobre las plataformas usadas para trabajar en ese sentido, además de un aumento exponencial observado por la apropiacion de las nuevas tecnologías. En los dos se observan tensiones entre Estado y sociedad que pueden motivar cámbios en la percepcion publica y la vigilancia, aunque todavia sigan incipientes.

Palabras clave: Contra-vigilancia, Violencia policial, Imágenes, São Paulo.

Image wars: São Paulo's Police under surveillance

Abstract: Making use of Information and Communication Technologies (ICTs), citizens today are able to produce imagery at will. Among the possibilities put forward by this background we are able to witness the emergence of a phenomenon of citizens capturing footage of police officers resorting to unnecessary force, such as abusive approaches, uncalled for aggressions and outright executions. Given this context, this work intends to hunch over policing and surveillance bibliography, as well as the analysis of public repercussion of two specific cases of police abuse, to assess the effectiveness of counter-surveillance tactics employed by citizens against police brutality. The two events at the center of this study were both perpetrated by São Paulo State's Military Police: the assaults on Favela Naval, which took place in greater São Paulo's in 1997 and culminated with the death of a local resident; and a double execution in the Butantã neighborhood in the city's west side in 2015. Although separated by almost two decades, these events share traits that allows us to observe the rise of a new layer of visibility over the State, while also stressing the difference in the means used to achieve it, and making evident the exponential rate of adoption of new technologies for this end. In short, both are exemplary cases of state-society tensions with potential to drive changes the public perception and police action – both of which have been, thus far, incipient.

Keywords: Counter-surveillance, Police brutality, Footage, São Paulo.

Cada vez mais recorrentes e mais abrangentes em suas causas, as manifestações populares têm ganhado fôlego em grandes metrópoles brasileiras. Com isso, sobretudo em são paulo, berço do levante que tomou as ruas em junho de 2013 (peruzzo, 2013), os confrontos entre policiais e manifestantes se tornaram, nos últimos três anos, uma cena corriqueira. Nesses casos, durante e após as ações, uma quantidade imensurável de fotografias e vídeos é produzida e compartilhada nas redes sociais em tom vigilante, geralmente apontando policiais e agentes do Estado cometendo algum tipo de abuso, como agressões aparentemente injustificadas e movimentos autoritários e repressivos de toda espécie.

Esse processo foi potencializado pelo crescimento e pela popularização das Tecnologias de Informação e Comunicação (TIC), que permitiu não só um aumento significativo na produção dos registros, como também possibilitou o compartilhamento desse conteúdo de forma espontânea e autônoma. Gregory R. Brown (2015) atribui a recente intensificação da exposição pública de performances e abusos de autoridade a três mudanças, caracterizadas por ele como tecnosociais:

a onipresença de equipamentos móveis com dispositivos que permitem captação de imagens; a proliferação de novas mídias e interações em ambiências digitais, que permite uma visão múltipla e heterogênea de pontos de vista narrativos; e a capacidade de engajamento do cidadão e a sensação de que pessoas comuns também podem documentar eventos que venham a ter repercussão pública. Logo, e principalmente a partir de plataformas como o Facebook e o YouTube, a sociedade passou a produzir de forma generalizada um discurso que se volta à fiscalização sobre instituições do Estado, levando esse material –e seus consequentes efeitos– a outros ambientes que extrapolam o espaço de suas ferramentas, tais como grandes grupos de comunicação e jornalismo, além de órgãos estatais e diferentes instâncias da Justiça.

Como aponta Bart Cammaerts (2013: 27), a internet serve hoje "como infra-estrutura de informação e comunicação que produziu um ímpeto em termos de facilitar a organização e a mobilização para protestos", além de possibilitar que o usuário se informe e se conecte diretamente com os interessados em sua causa. Mesmo partindo da compreensão de que há ampla desigualdade no que diz respeito ao acesso às TIC, parece pertinente destacar que, em 2013, um estudo da ONU, cujo objetivo principal era fazer um alerta para a extensa falta de saneamento básico nas regiões mais pobres do mundo, revelou que mais pessoas têm acesso a celulares do que a banheiros (Wang, 2013) – foram contabilizados àquela época 6 bilhões de aparelhos. No cenário atual, em que um número crescente de pessoas é capaz de produzir, comentar, compartilhar imagens, e inclusive questionar ou desacreditar notícias, é pertinente suscitar questões que (re)conectem cidadão, novas tecnologias de informação e comunicação e Estado, sem isolá-los, e sim fazendo um recorte transversal que permita mapear práticas e tendências nessas três esferas que estão de fato interconectadas e influenciando-se mutuamente.

Ano após ano, fica mais evidente que se trata de um fenômeno global, do qual participam personagens de diferentes frentes: cidadãos, ativistas, jornalistas, policiais, autoridades em geral e até as próprias vítimas dos abusos e de eventuais crimes participam de forma direta ou indireta dessa construção de narrativas. Essas imagens são produzidas e compartilhadas partindo de uma perspectiva que coloca a pessoa que as fez como uma testemunha inquestionável (Polydoro, 2016). Ou seja, tal conteúdo produzido tem um caráter de prova, de verdade, e serve ali como uma denúncia mediada apenas pelas ferramentas de tecnologia e comunicação usadas por quem a faz, numa tentativa de materializar a cena exatamente da forma como ela foi testemunhada.

Dentre as múltiplas possibilidades que se conectam a esse panorama de denúncia a partir de narrativas construídas com imagens, este trabalho pretende explorar dois casos de violência ocorridos no estado de São Paulo, ambos protagonizados pela Polícia Militar, cujas ações levaram três pessoas à morte. Diferentemente do quadro geral que vem se constituindo desde que as manifestações de massa se tornaram mais frequentes, quando agentes do Estado se organizam para reprimir protestos e ocupações de forma supostamente ordenada e articulada em diferentes frentes,[1] as duas ocorrências que pretendo explorar aqui são resultado de um patrulhamento rotineiro, que faz parte do cotidiano de policiais militares, e foram captadas por cidadãos comuns que habitavam os arredores de onde aconteceram os fatos, além de uma câmera estática de segurança em uma rua onde um dos crimes foi cometido.

O primeiro caso ocorreu em 1997, quando Francisco Romeu Vanni, também chamado à época de Pica-Pau, captou abusos policiais em uma favela em Diadema, na Grande São Paulo; filmados em três dias diferentes, os oficiais foram flagrados agredindo e torturando moradores locais em falsas blitzes. Em uma das imagens, que se tornou a mais notória, um PM conhecido como Rambo dispara duas vezes na direção de um automóvel que havia sido liberado da abordagem, atingindo pelas costas o conferente Mário José Josino, morador da região, que acabou morrendo pouco mais tarde em um hospital do bairro. Na época, o vídeo foi revelado durante edição do Jornal Nacional,[2] da Rede Globo, no dia 31 de março daquele ano, e reproduzido pelos noticiários de outras emissoras. O material exibido chocava pela violência explícita, já que, além das cenas suficientemente nítidas para que não houvesse interpretações equivocadas, a captação de áudio também denotava a desproporcionalidade da ação policial, em que tapas e agressões se faziam audíveis.

Sobre a divulgação da reportagem sobre a Favela Naval, como o caso ficou conhecido, Theophilos Rifiotis (1999: 33) escreveu:

> Dos aparelhos de televisão, como num filme, vimos e ouvimos cenas e sons da maior nitidez, em que policiais militares de São Paulo torturavam e maltratavam cidadãos que não pareciam esboçar a menor reação (...) A força daquelas imagens era tamanha que embora os dias e as horas em que foram gravadas estivessem registrados no vídeo, apontando para os primeiros dias de março, elas pareciam fora de tempo e de lugar, ganhavam uma estonteante atualidade. Este aparente deslocamento entre passado e presente fazia com que as imagens se confundissem com os "fantasmas" que povoam a nossa percepção do abuso de poder a da ação dos agentes de segurança do no Brasil.

O outro caso aconteceu quase duas décadas depois, mas suas imagens são tão expressivas quanto as do primeiro. Após uma perseguição no feriado de 7 de setembro de 2015, policiais executaram dois suspeitos de roubo no Butantã, bairro da na zona oeste da capital paulista. A primeira versão divulgada, a oficial, é a de que eles teriam reagido e haviam sido mortos durante uma perseguição pelas ruas do bairro. Como veremos mais adiante, o boletim de ocorrência inicial trazia essa narrativa em detalhes. Quatro dias depois, no entanto, surgiram imagens que confrontavam os fatos registrados pelos policiais na delegacia. O primeiro material que veio à tona era o registro de uma câmera de segurança posicionada em uma das ruas onde se deu a ocorrência,[3] e mostrava Paulo Henrique Porto de Oliveira, um dos suspeitos, até então escondido dentro de uma lixeira, saindo e se rendendo. No vídeo, é possível ver que ele se livra da jaqueta e deita de bruços no chão. Algemado pelos PMs que estão no local, ele é levado para perto de um muro, desalgemado e baleado. Logo em seguida, um oficial vai até a viatura e pega um objeto que posteriormente é colocado na cena do crime.

O vídeo da câmera de segurança havia sido obtido pelo departamento de homicídios e proteção à pessoa (dhpp) e foi enviado ao ministério público estadual (mpe), que pediu a prisão dos envolvidos naquela ocorrência (Ribeiro, 2015). À reportagem do portal de notícias da rede globo, o g1, o promotor rogério leão zagallo afirmou (Araújo, 2015):

> Me parece claro que houve uma execução. Pelas imagens que a gente tem aqui, as cenas mostram a pessoa [Oliveira] sendo detida, revistada, algemada. O rapaz tira a camisa como forma de mostrar que não está armado. Os policiais tiram a algema dele e o levam para um local próximo. Na sequência, ele fica sentado e recebe dois tiros. Me parece uma cena clara de uma conduta covarde de execução.

Com a prisão dos envolvidos na morte dessa vítima já decretada, ainda restava esclarecer o que havia acontecido com a outra, que também tinha sido morta a poucas quadras dali, quase que simultaneamente, em uma suposta troca de tiros com a polícia. No sábado, dia 12 de setembro, contudo, um vídeo de celular revelado em um jornal local da TV Globo,[4] o SPTV, mostrava o segundo suspeito, Fernando Henrique da Silva, rendido em um telhado, quando o PM que o dominava o empurra para fora do quadro. Alguns segundos depois, são ouvidos quatro tiros, que atingiram abdômen, lombar, virilha e mão esquerda, o que pode indicar tentativa de defesa (Caramante, 2015). Já na segunda-feira a prisão dos outros envolvidos na ocorrência também foi decretada, totalizando onze policiais militares inicialmente detidos para que as circunstâncias das duas execuções fossem investigadas.

POLICIAMENTO OSTENSIVO

Antes de retomar cada um dos casos com mais detalhes, explicitando suas semelhanças e diferenças, é necessário fazer uma contextualização breve sobre a atuação da Polícia Militar brasileira, dando alguma ênfase para o estado de São Paulo. Como aponta teresa caldeira (2002), a tarefa de transformar uma instituição de policiamento em uma instituição democrática, onde o respeito aos direitos individuais do cidadão prevaleça, é bastante árdua, sobretudo em democracias mais recentes, como é o caso do brasil, que vem de um longo histórico de autoritarismo e de desrespeito às fronteiras da legalidade (Caldeira, 2002).

Divulgada em julho de 2015, uma pesquisa realizada pelo Datafolha (Turollo Jr., 2015), encomendada pelo Fórum Brasileiro de Segurança Pública (FBSP), revelou que 62% dos moradores de cidades brasileiras com mais de 100 mil habitantes têm medo de sofrer agressões perpetradas por policiais militares – dentre os que responderam que temem a instituição, 71% são negros, um dado que vai ao encontro da atuação evidentemente mais repressiva da PM a esses jovens, a maioria deles habitando áreas periféricas. Segundo o Atlas da Violência 2016,[5] também organizado pelo FBSP e pelo Instituto de Pesquisa Econômica Aplicada (Ipea), em 2014 foram 3.009 mortes decorrentes de intervenção policial no país, com uma taxa de 37,5 para cada 100 mil habitantes entre negros, contra 15,6 de não-negros. É importante destacar que as análises do Atlas da Violência 2016 se basearam no Sistema de Informação sobre Mortalidade (SIM), do Ministério da Saúde, e em informações policiais publicadas no 9º Anuário de Segurança Pública, do FBSP, parte delas coletada através da Lei de Acesso à Informação. Assim, o que salta aos olhos é que os dados do Ministério diferem muito dos dados sistematizados pelo Atlas: são mais de três mil óbitos contra "apenas" 681, segundo dados oficiais, o que pressupõe uma subnotificação em níveis elevados por parte da Polícia Militar. Segundo o estudo,

"o que está em discussão é o padrão operacional das polícias e para tal a necessidade de transparência e confiabilidade dos dados que permitam orientar esse debate".[6]

É consenso entre organizações que lutam pelo acesso à informação no Brasil, como a Artigo 19,[7] no entanto, que existe, sobretudo em São Paulo, um cenário extremamente desfavorável no que diz respeito à transparência do Estado sobre assuntos de segurança. Um dos exemplos emblemáticos mais recentes é do dia 5 de fevereiro de 2016, quando o Diário Oficial trouxe a público uma resolução da Secretaria de Segurança Pública (SSP) em que o Gabinete da SSP, a Polícia Militar, a Polícia Civil e a Superintendência da Polícia Técnico Científica teriam seus dados e informações resguardadas e protegidas de acordo com parâmetros estabelecidos pela Secretaria. A norma estabelecia duas categorias de documentos – 'Pessoais', a fim de proteger a intimidade e a vida privada de envolvidos, e 'Sigilosos', sob pretexto de garantir a segurança do Estado – e os classificava como 'Reservados', 'Secretos' e 'Ultra-Secretos', determinando um período de sigilo para consulta do material que variava entre cinco e cinquenta anos.

A resolução como um todo estabelecia algumas ressalvas sobre o sigilo: o artigo 1º, por exemplo, decretava que os procedimentos tinham finalidade de "garantir a efetividade do direito fundamental de acesso à informação dos órgãos públicos, ressalvadas as informações pessoais e sigilosas".[8] Em outras palavras, qualquer documento que a Secretaria desejasse ocultar poderia se encaixar nessas ressalvas, de acordo com seus interesses internos. O artigo 3º trazia uma exceção:

> Os documentos, dados e informações que versem sobre condutas que impliquem violações dos direitos humanos praticadas por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso[9].

De lá pra cá, devido à repercussão negativa que os decretos sobre sigilo gerou (houve também restrições de acesso a documentos sobre transporte público, que ajudaram a engrossar as críticas ao governador Geraldo Alckmin), o governo recuou. No dia 19 de fevereiro, com o decreto nº 61.836, o Governo decretava que "o acesso aos documentos, informações e dados observará os princípios da publicidade e transparência com preceito geral e do sigilo como exceção".[10]

A digressão sobre acesso e transparência serve para reforçar o isolamento existente hoje em dia entre sociedade civil e a Polícia Militar brasileira. Embora tenha sido formada no século XIX, ainda na época do Império, a PM ganhou força durante a ditadura militar (1964-1985), principalmente a partir do início da década de 1970, quando foi colocada sob a coordenação do Exército. A ideia era que policiais militares fossem uma força de reserva, que passou a agir sobretudo nos espaços urbanos a fim de reprimir os opositores do regime ditatorial. Mesmo após o processo de redemocratização, todavia, a corporação continuou organizada militarmente, conforme prevê a Constituição de 1988, no artigo 144, destinando aos policiais militares o patrulhamento ostensivo e mantendo a subordinação às Forças Armadas como exército de reserva. Em resumo, sob coordenação dos governos estaduais, a PM continuou atuando no mesmo *modus operandi* dos tempos mais repressivos da história recente do país.

Por conta desse histórico essencialmente autoritário, não por acaso, há uma série de projetos de desmilitarização da instituição em discussão, sendo o mais recente (e mais atual) deles a PEC 51/2013,[11] apresentada pelo senador Lindbergh Farias (PT-RJ), cuja votação não tinha previsão de acontecer até o fechamento deste texto. Entre outras medidas, a proposta estabelece o Ciclo Completo das polícias, em que as três fases do policiamento – ostensivo, investigativo e preventivo – seriam executadas por uma polícia unificada, extinguindo a divisão entre polícias Civil e Militar. Por fim, é importante destacar que policiais militares vivem um cenário de precariedade, com baixos salários, treinamento ruim, falta de equipamentos, e trabalham sob a rigidez hierárquica presente nas instâncias superiores do Exército. A pesquisa *Opinião dos Policiais Brasileiros sobre Reformas e Modernização da Segurança Pública,*[12] também elaborada pelo FBSP, por exemplo, revelou que cerca de 76% dos PMs são a favor da desmilitarização, um dado que endossa a necessidade de uma reforma urgente na estrutura da Polícia Militar.

QUEM NÃO DEVE NÃO TEME

Como consequência dessa desconfiança sobre as instituições policiais, conforme já foi tratado aqui anteriormente, há uma série de grupos que tem usado tecnologias de vigilância para monitorar agentes do Estado a fim de tornar transparentes casos de violência policial (Serisier, Wilson, 2010). A prática de contra-vigiar a polícia, como definem Linnemann e Wall (2014: 142), "subverte e se apropria de dois slogans policiais familiares, e os joga de volta aos agentes do Estado: 'Se você vir algo, diga algo!', e 'Se você não fez nada errado, não há o que temer!'".[13]

Um dos exemplos pioneiros sobre a capacidade de contra-vigiar agentes de segurança pública foi o caso de Rodney King Jr., brutalmente espancado em uma abordagem policial na cidade de Los Angeles, em 1991.[14] A ocorrência se tornou um símbolo contra a violência policial e um estopim para a discussão sobre o assunto. Com a divulgação do vídeo, captado por um cinegrafista amador, ficou evidente que o Estado havia perdido sua posição de patrulhar os fatos que aconteciam nas ruas (Brown, 2015). Tal noção pode ser também enquadrada na ideia de "Nova Visibilidade" defendida por John Thompson (2008), sobre transformar o real, porém invisível, em algo visível e acessível. Em outras palavras, "trata-se de uma estratégia explícita por parte daqueles que bem sabem ser a visibilidade mediada uma arma possível no enfrentamento das lutas diárias" (Thompson, 2008: 16), sendo essa mediação proporcionada pelo uso de algum tipo de tecnologia.

Ainda que os casos da Favela Naval e do Butantã estejam separados por um longo intervalo cronológico, e portanto apresentem uma série de diferenças sobre suas narrativas, há uma semelhança essencial entre ambos: a capacidade de provocar mudanças e reações a partir de imagens explícitas, expondo as forças policiais do Estado e gerando a necessidade de uma resposta oficial rápida.

Estruturalmente, o que difere as duas ocorrências pode ser observado nos seguintes elementos: o crime na Favela Naval aconteceu em 1997, quando o acesso a tecnologias móveis ainda era

precário. Assim, a ação do cinegrafista, que captou as imagens com uma câmera de VHS sobre um tripé (Pastore, 1997), foi planejada após ele constatar que os abusos de autoridade vinham ocorrendo com frequência no local. Com o material em mãos, o autor dos vídeos procurou grandes emissoras de televisão, como a Globo e a Bandeirantes, para vender as fitas, que acabaram sendo veiculadas pela primeira, em circunstâncias não esclarecidas sobre a aquisição do material. Nesse caso, a versão sobre o fato surgiu como uma narrativa única, pois não havia antes relatos sobre as operações da Polícia Militar naquela favela em Diadema. Já no Butantã, em 2015, havia primeiramente uma versão oficial: no Boletim de Ocorrência obtido pela Ponte Jornalismo (Caramante, 2015), sobre o primeiro homicídio consta que "os militares visualisaram (sic) um indivíduo saindo de dentro de uma lixeira, após troca de tiros, o militar conseguiu atingir o indivíduo. Foi acionado socorro médico (...)". Sobre o segundo, o boletim narra que "(...) indivíduo não identificado, vindo da casa vizinha pulou no quintal da casa onde os policiais militares estavam. O indivíduo disparou em direção do policial Lapiana. Os policiais foram obrigados a disparar (...)". As imagens, captadas pelos vídeos de uma câmera de segurança recolhida pelo DHPP e por um celular de um morador da região, surgiram como uma forma de desmentir a versão oficial contada pelos PMs e, apesar de terem sido divulgadas em canais de televisão e em sites de notícias, foram replicadas no Facebook e no YouTube por diferentes usuários.

Nos dois casos, houve repercussão na imprensa e na esfera judicial, sendo que o caso mais recente, de 2015, ainda não foi concluído. Os policiais envolvidos na Favela Naval tiveram penas diferentes e foram demitidos ou expulsos da corporação, e Otávio Lourenço Gambra, o responsável pelo tiro que tirou a vida de Mário Josino, teve a pena mais significativa: cumpriu oito anos de reclusão no regime fechado antes de progredir para o semiaberto, em um processo que envolveu duas vezes o Tribunal de Júri[15] e duas apelações ao Tribunal de Justiça; as imagens divulgadas inicialmente pela Rede Globo foram levadas ao noticiário de outras emissoras na época, e continuam hospedadas em canais de compartilhamento de vídeos. Segundo a TV Record,[16] mais de mil pessoas cercaram a delegacia onde estavam os policiais acusados na intenção de agredi-los, e o próprio policial que efetuou o disparo que matou o morador da Favela Naval, o Rambo, disse na mesma reportagem da emissora, em 2014, que dificilmente teria sido preso caso as imagens não tivessem vindo à tona.

Em texto publicado dois anos depois do crime em Diadema, o professor Theophilos Rifiotis (1999: 29), da Universidade Federal de Santa Catarina (UFSC), lista uma série de ações que foram tomadas depois da denúncia amadora publicada na TV Globo, entre outras:

> Embora não tenha sido responsável direto por eventos que o sucederam no tempo, o caso da Favela Naval guarda sobre eles um valor emblemático. Nos dias que sucederam imediatamente sua divulgação, importantes propostas em andamento foram concretizadas. No dia 3 de abril, o Senado aprovou em regime de urgência um projeto que tramitava desde agosto de 1994, tipificando o crime de tortura. No dia seguinte, a Comissão de Constituição e Justiça da Câmara aprovou a emenda constitucional que federaliza os crimes contra os direitos humanos. O Presidente da República sancionou a lei que tipifica o crime de tortura e o torna inafiançável no dia 6 de abril. A criação da Secretaria Nacional de Direitos Humanos, anunciada desde março e prevista para 13 de maio, foi antecipada também para o mesmo dia.

No caso do Butantã, a juíza da 5ª Vara do Júri do Fórum Criminal Central, Giovanna Christina Colares, determinou que seis policiais envolvidos na execução dupla serão submetidos ao júri popular. Os oficiais foram acusados de homicídio triplamente qualificado (motivo torpe, meio cruel e recurso que dificultou a defesa da vítima) e não poderão ficar em liberdade até a data do julgamento. Na sentença,[17] a magistrada faz diferentes menções às imagens, que constam no processo que corre sob segredo de justiça.

O guia *Vídeo como prova jurídica* (Artigo 19, Witness, 2015), uma parceria da Witness[18] com a Artigo 19, explora pontos de conexão entre imagens com denúncias de violações e efeitos punitivos na esfera jurídica. O material afirma que há inúmeros casos em que os vídeos não determinam ou auxiliam na condenação dos acusados, mas lista quatro pontos importantes que caminham nessa direção (Artigo 19, Witness, 2015: 12-13):

> **(i)** Quando ocorre algum tipo de responsabilização em casos de violações de direitos humanos, em geral há algum vídeo da violação. **(ii)** Em casos de violência policial em particular, a existência de algum vídeo se destaca como ferramenta importantíssima para fortalecer e acelerar os processos por justiça, desafiando a impunidade crônica que costuma resultar em inquéritos arquivados sem a devida investigação. **(iii)** Há ainda uma dificuldade em analisar e avaliar o potencial do vídeo como prova, pois juízes dizem muito pouco (ou nada) a respeito da influência de vídeos em suas decisões. **(iv)** Trata-se de fenômeno relativamente novo e um caminho importante a ser trilhado por defensores, advogados, comunicadores, videoativistas e qualquer cidadão que possa vir a testemunhar e filmar uma violação de direitos humanos.

PANORAMA

Os dois casos aqui explorados, todavia, não são capazes de confirmar que as táticas de contra-vigilância a partir da captação de imagens são suficientemente eficazes no combate à violência policial, e mais especificamente sobre a Polícia Militar de São Paulo. Mesmo antes da Favela Naval, houve uma série de casos que também foram veiculados em emissoras de televisão e não surtiram efeitos de magnitude semelhante (Rifiotis, 1999) e, no caso do Butantã, embora tenha sido determinado que os policiais irão a julgamento por júri popular, não há garantias de que isso constituirá uma mudança no *modus operandi* da PM do estado. Nas duas ocorrências aqui descritas, é possível perceber que em duas décadas, a despeito da repercussão que a primeira gerou, não houve uma mudança substancial na forma de atuação da corporação.

Por outro lado, há estudos que sugerem no horizonte uma mudança de comportamento dentro de instituições do Estado. Ex-policial, Gregory R. Brown é um pesquisador canadense que fez um trabalho empírico com policiais sobre as transformações pelas quais a corporação vem passando no país a partir do uso das TIC. Ele entrevistou 231 oficiais, e chegou à conclusão que 94% deles sabiam que estavam sendo filmados durante suas abordagens; desses, 74% declararam ter mudado sua maneira de se comportar nas ruas por conta da capacidade dos cidadãos de registarem suas ações (Brown, 2015). Essa diferença de abordagem, no entanto, precisa ser problematizada, pois reflete o que Ajay Sandhu (2016) chama de "camera-friendly policing", uma espécie de poder disciplinador que confunde o "ser bom" com o "parecer bom" de um

policial. Em outras palavras, a atuação sob o rigor da legalidade frente às câmeras não significa necessariamente uma nova forma de policiamento, e sim uma forma de se proteger da nova visibilidade (Thompson, 2008).

Nos últimos anos, tem se discutido com frequência as abordagens violentas contra cidadãos que registram ações policiais em vídeo (Serisier, Wilson, 2010), bem como a institucionalização do uso de câmeras acopladas aos uniformes dos oficiais (Timan, 2016), caracterizando uma guerra não mais física somente, de corpo a corpo, mas sim imagética. É fundamental destacar que a divulgação de abusos policiais explícitos e suas respectivas consequências fazem parte de uma discussão que integra um epicentro global de instabilidade social e política, e mobiliza todas as frentes envolvidas no processo. Justamente por isso, precisa ser pensada transversalmente, como um processo em constante mudança, configurando uma Guerra de Imagens que deixou de ser metafórica para se integrar à realidade das forças policiais e da sociedade como um todo.

NOTAS

* Aluno do programa de mestrado em Divulgação Científica e Cultural na Universidade Estadual de Campinas (Unicamp) (gabriel.vituri@gmail.com)

1. Em grandes eventos políticos, sobretudo nas capitais, é comum que o policiamento seja feito com viaturas e motocicletas de diferentes batalhões, incluindo muitas vezes o apoio de um helicóptero e de unidades especiais, como a Tropa de Choque, por exemplo.
2. Disponível em: http://memoriaglobo.globo.com/programas/jornalismo/coberturas/favela-naval.htm.
3. Disponível em: https://www.youtube.com/watch?v=1IcXNL6-9Jk
4. Disponível em: http://g1.globo.com/sao-paulo/noticia/2015/09/novas-imagens-mostram-acao-da-pm-que-terminou-em-morte-no-butanta.html
5. Disponível em: http://infogbucket.s3.amazonaws.com/arquivos/2016/03/22/atlas_da_violencia_2016.pdf.
6. Idem (p.16).
7. Fundada em Londres na década de 1980, a Artigo 19 luta pelo acesso à informação e pela liberdade de expressão, direitos previstos no artigo 19 da Declaração Universal dos Direitos Humanos. No brasil, a organização atua desde 2008.
8. Diário Oficial do Estado de São Paulo, 5 de fevereiro de 2016.
9. Idem.
10. Diário Oficial do Estado de São Paulo, 19 de fevereiro de 2016.
11. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/114516

12. Disponível em: http://www.forumseguranca.org.br/storage/download/ApresentacaoFinal.pdf

13. (...) subverts and appropriates two familiar police slogans and spits them back at state agents: "If you see something, say something!" and "If you've done nothing wrong, then you have nothing to fear!". *Tradução minha.*

14. Disponível em: https://www.youtube.com/watch?v=sb1WywIpUtY.

15. Em 1996, durante o mandato do presidente Fernando Henrique Cardoso, a lei 9299 determinou que os homicídios cometidos por militares fossem julgados na Justiça Comum, e não mais na Justiça Militar, onde os processos costumam ser mais lentos e menos rigorosos com seus pares.

16. Disponível em: http://noticias.r7.com/cidade-alerta/videos/ele-me-abracou-e-riu-relembra-marcelo-sobre-entrevista-com-rambo-17102015

17. Disponível em: http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=36444

18. A Witness foi fundada nos Estados Unidos, em 1992, como uma resposta às cenas de espancamento contra Rodney King Jr., um ano antes. Desde o seu surgimento, a organização ajuda ativistas a usarem vídeos como ferramentas de denúncia a violações de direitos humanos.

REFERÊNCIAS

Artigo 19, WITNESS. Vídeo como prova jurídica. 2015. Disponível em: http://artigo19.org/blog/2015/12/10/o-video-como-prova-juridica-para-defesa-dos-direitos-humanos-no-brasil/

Araújo, G. (2015). PMs são presos após vídeo mostrar execução em SP, diz promotor. En *G1*. 11 setembro 2015. Disponível em: http://g1.globo.com/sao-paulo/noticia/2015/09/pms-sao-presos-apos-video-mostrar-execucao-em-sp-diz-promotor.html

Brown, G. (2016). The blue line on thin ice: police use of force modifications in the era of cameraphones and YouTube. En *British Journal of Crimonology. Vol.* 56. 293-312.

Caldeira, T. (2002). The paradox of police violence in democratic Brazil. En *Ethnography.* Vol. 3 (3). 235-263.

Cammaerts, B. (2013). Lógicas de protesto e a estrutura de oportunidade de mediação. En *MATRIZes*. Vol. 7. No. 2. Disponível em: http://www.matrizes.usp.br/index.php/matrizes/article/view/477/pdf.

Caramante, A. (2015). Mais 6 PMs de SP são presos por armar farsa para encobrir execuções de 2 jovens. En *Ponte Jornalismo.* 14 setembro 2015. Disponível em: http://ponte.org/mais-6-pms-de-sp-sao-presos-por-armar-farsa-para-encobrir-execucoes-de-2-jovens/

Caramante, A. (2015). Veja os documentos que mostram como PMs de SP mentiram para encobrir as execuções de 2 jovens. En *Ponte Jornalismo.* 14 de setembro de 2015. Dispoível em: http://ponte.org/veja-os-documentos-que-mostram-como-pms-de-sp-mentiram-para-encobrir-as-execucoes-de-2-jovens/

Linneman, T., Wall, T. (2014). Staring down the State: police power, visual economies, and the "war on cameras". En *Crime Media Cultura.* Vol. 10 (2). 133-149.

Pastore, K. (1997). Olhar escondido. En *Veja.* Vol. 1490. p. 32.

Peruzzo, C., Krohling, M. (2013). Movimentos sociais, redes virtuais e mídia alternativa no junho em que "o gigante acordou". En *MATRIZes.* Vol. 7. No. 2. 2013. Disponível em: http://www.matrizes.usp.br/index.php/matrizes/article/view/487/pdf.

Polydoro, F. (2016). Realismo, verdade e política em vídeos amadores de acontecimentos. Apresentado em: *XXV Encontro Anual da Compós*, Universidade Federal de Goiás, 2016. Disponível em: http://www.compos.org.br/biblioteca/artigocompo_s2016final_3333.pdf.

Ribeiro, B. (2015). Vídeo de execução faz Justiça decretar prisão de 5 policiais. En *O Estado de S. Paulo.* 11 setembro 2015. Disponível em: http://sao-paulo.estadao.com.br/noticias/geral,video-de-execucao-faz-justica-decretar-prisao-de-5-policiais-,1760805.

Rifiotis, T. (1999). Violência policial e imprensa: o caso da Favela Naval. En *São Paulo Perspec*. São Paulo. Vol. 13. No. 4. 28-41.

Sandhu, A. (2016). Camera-friendly Policing: How the Police Respond to Cameras and Photographers. En *Surveillance & Society.* Vol. 14 (1). 78-89. 2016. Disponível em: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/camera-friendly/friendly.

Serisier, T., Wilson, D. (2010). Video activism and the ambiguities of Counter-Surveillance. En *Surveillance & Society.* Vol. 8 (2). 166-180. 2010. Disponível em: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3484.

Thompson, J. (2008). A nova visibilidade. En *MATRIZes.* Vol. 2. 15-38. 2008. Disponível em: http://www.revistas.univerciencia.org/index.php/MATRIZes/article/view/5230/5253.

Timan, T. (2016). The Body-worn Camera as a Transitional Technology. En *Surveillance & Society.* Vol. 14 (1). 145-149. 2016. Disponível em: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/cdebate6.

Turollo Jr., R. (2015). Maioria da população diz ter medo da Polícia Militar, aponta Datafolha. En *Folha de S. Paulo*. 31 julho 2015. Disponível em: http://www1.folha.uol.com.br/cotidiano/2015/07/1662655-maioria-da-populacao-diz-ter-medo-da-policia-militar-aponta-datafolha.shtml.

Wang, Y. (2013). More people have cell phones than toilets, U.N. study shows. En *TIME.* 25 março 2013. Disponível em: http://newsfeed.time.com/2013/03/25/more-people-have-cell-phones-than-toilets-u-n-study-shows/.

UNA LECTURA EN PERSPECTIVA DE 'VIGILANCIA' DE LA HIPÓTESIS CIBERNÉTICA DE TIQQUN

Resumen: “La hipótesis cibernética” es una reflexión teórico-militante de vanguardia a propósito de un salto epistémico y de las consecuencias teóricas y políticas en términos del gobierno y de la producción de subjetividades en nuestros tiempos. Más allá de reponer el argumento de este libro que nos llega desde la penumbra y el anonimato que implica la escritura colectiva, me propongo recorrer un par de lecturas que se han hecho sobre esta reflexión militante con un interés específico en lo que tiene que ver con el tema de la vigilancia. Como en el libro, las lecturas a las que acudiré entienden la vigilancia en términos amplios y no sólo como un fenómeno referido a las políticas de videovigilancia o de control biométrico. Se trata de un fenómeno que tiene que ver con los procesos de subjetivación contemporáneos, con lo que se presenta como una encrucijada ética y política para la acción 'revolucionaria' o 'subversiva' en nuestros tiempos. Así, simplemente a modo de hipótesis de lectura, este texto propone simplemente un acercamiento crítico a propósito de las nuevas gramáticas que no sólo la vigilancia aumentada implica, sino de las que estaríamos llamados a producir para poder si acaso imaginar una forma de hacerle frente.

Palabras clave: Hipótesis cibernética, Vigilancia, Subjetivación, Tiqqun.

Uma leitura em perspectiva de "Vigilância" da Hipótese Cibernética de Tiqqun

Resumo: "A hipótese cibernética" é uma reflexão teórico-militante de vanguarda que diz respeito a um salto epistemológico e às consequências teóricas e políticas em termos de governo e da produção de subjetividades em nossos tempos. Além de resgatar o argumento deste livro que chega a nós desde a penumbra e o anonimato que resulta da construção coletiva, proponho uma passagem por algumas leituras que foram feitas sobre esta reflexão militante com um interesse específico com respeito ao tema da vigilância. Como no livro, as leituras as quais vou me referir entendem a vigilância em termos abrangentes e não só como um fenômeno que se refere às políticas de vigilância com câmeras ou de controle biométrico. Trata-se de um fenômeno que tem a ver com os processos de subjetivação contemporâneos, com o que se apresenta como uma encruzilhada ética e política para a ação 'revolucionária' ou 'subversiva' nos nossos tempos. Dessa forma, simplesmente como modo de hipótese de leitura, esse texto propõe simplesmente uma aproximação crítica com respeito às novas gramáticas que não só o aumento da vigilância implica, senão também daquelas que seríamos chamados a produzir para poder, de repente, imaginar uma forma de confrontá-las.

Palavras chave: Hipótese cibernética, Vigilância, Subjetivação, Tiqqun.

Tiqqun's Cybernetic hypothesis: A reading from a 'surveillance' perspective

Abstract: "The cybernetic hypothesis" is an avant-garde theoretical-militant reflection on the epistemic leap and its theoretical and political consequences in terms of government and the production of subjectivities in our times. Beyond telling the argument of this book that comes from the darkness and anonymity that involves collective writing, I propose to go through a couple of readings that have been made on this militant reflection with a specific interest in what it has to do regarding surveillance. As in the book, the readings I will use understand surveillance in broad terms and not just as a phenomenon related to video surveillance or biometric control policies. It is a phenomenon that has to do with the processes of contemporary subjectivation, with what is presented as an ethical and political crossroads for the 'revolutionary' or 'subversive' action nowadays. Thus, simply as a reading hypothesis, this text just proposes a critical approach to the new grammars that not only increased surveillance implies, but also those we would be called upon to produce in order to be able even to imagine a way to deal with it.

Keywords: Cybernetic Hypothesis, Surveillance, Subjectivation, Tiqqun.

CAMILO RIOS*

PRESENTACIÓN

Desde la penumbra, como suele ser recurrente, nos llega un texto urgente. Más bien podríamos hablar de dos textos urgentes. Aunque sean nominalmente (y tal vez algo más que nominalmente) diferentes, tanto Tiqqun como el Comité Invisible comparten resonancias teóricas, políticas y epistémicas suficientes para que, al menos a los fines de lo que quisiera proponer acá, los consideremos parte de un universo común. Dos textos urgentes, entonces: por un lado, la (Carta) a nuestros amigos (Comité Invisible, 2015), que actualiza un diagnóstico sociopolítico de época y llama a la reorganización de los afectos en pos de una lucha política a la altura de un adversario complejo. Por otro, La hipótesis cibernética (Tiqqun, 2015), que se desliza filosóficamente por una de las líneas que consideran más importantes para describir la racionalidad de gobierno contemporánea. Ambos textos, ambos llamados, ambos panfletos (en el mejor de los sentidos), comparten importantes elementos teóricos. Ninguno pierde de vista el papel preponderante de la tecnología y de la técnica en la configuración de procesos de subjetivación de nuestros tiempos, y esto me interesa particularmente, en función de lo que acá intentaré esbozar.

Tiqqun, que ya venía trabajando tangencialmente sobre la importancia política que reviste la relación que establecemos con los artefactos que nos rodean (2013) sobre todo en lo concerniente a las nuevas formas de la alienación, la configuración de una ideología objetualista y las transformaciones en el mundo del trabajo, radicaliza su apuesta acercándose mucho más a las fuentes teóricas que constituyen el dispositivo de gobierno actual. De alguna forma, este nuevo texto hace converger la línea de análisis de textos como el del 2013, con los intereses de corte más anárquico y subversivos del grupo, más claramente esbozados en un texto como Llamamiento (2010) (que si bien algunos sostienen que hace parte de la producción del Comité Invisible, se encuentra editado y ampliamente difundido bajo el sello de los Tiqqun; he ahí una de las razones de la indiferenciación que proponemos más arriba, puesto que nos parece poco fértil avanzar en la disputa autoral de dos grupos clandestinos).

No me propongo reponer acá el argumento de la hipótesis cibernética (además porque es un texto liberado en la web en múltiples idiomas), ni tampoco evaluar la calidad o la precisión de la lectura que hacen de los fundadores de la cibernética (cosa que estaría por demás en manos de especialistas en la materia); más bien, me remitiré, a fines de poder sobrevolar y analizar críticamente algunas de las consecuencias políticas y éticas de su propuesta, a los argumentos que otros especialistas han hecho de la hipótesis.

No significa lo anterior que desconozca ni el contenido ni las fuentes de Tiqqun en este texto, sino que me concentraré en un fenómeno que se puede llamar de 'recepción' analítica de sus propuestas, para poder desde ahí proponer una serie de comentarios, desde el punto de vista de la vigilancia, al respecto de la paradoja que encierra lo que se presenta como una suerte de sinsalida teórico-política. Si se quiere, es posible sostener que no pretendo un análisis exegético de la hipótesis, sino aportar algunos elementos en torno a lo que ella puede decir de nuestros contextos.

Por eso, los comentarios a los que me referiré son propios de investigadores y activistas relativamente locales. Por un lado, la nota que hizo Amador Fernandez-Savater (2015) respecto de la recién publicada hipótesis. Por otro, tres intervenciones de Pablo Estéban Rodríguez al respecto, un texto que aparece como el Extrálogo del libro de los Tiqqun (Rodríguez, 2015b), y dos entrevistas a propósito de la hipótesis (2016) y de las sociedades de control (2015a). Finalmente, me referiré también a la entrevista que recientemente dio Peter Pál Pelbart (2016) a propósito de lo que considera algunas alternativas posibles a esta racionalidad de gobierno imperante.

LA HIPÓTESIS CIBERNÉTICA COMO DISTOPÍA

En su nota, Amador Fernandez-Savater (2015) propone irónicamente leer la hipótesis como una distopía, pues le resulta aterrador pensarla como una descripción de la realidad actual. Tras caracterizar este escenario distópico como uno de totalmente transparente, interconectado y autoorganizado y fluido, reconoce en los Tiqqun la línea central de su argumento: un desplazamiento en la racionalidad de gobierno, que va del liberalismo, caracterizado por la razón y el interés, a la cibernética, que establece una relación generalizada entre orden y caos en función de la entropía. "Gobernar el comportamiento de personas o máquinas exige mecanismos de control que aseguren el orden, contrarrestando la tendencia a la desorganización." (Fernandez-Savater, 2015).

En este escenario, la clave del gobierno es la información, y en ese sentido la vigilancia empieza a perfilarse como una actividad transversal. Una vigilancia que se entiende como gobierno de la probabilidad en función de la predictibilidad; la fórmula foucaultiana de 'conducción de la conducta' ha llegado a un nuevo nivel de complejidad. Como también sostendrá Rodríguez (2016), se trata de un sistema descentralizado, una red de sistemas que se autoorganizan a partir de la dispersión de mecanismos de retroalimentación que nos hacen partícipes de las prácticas de gobierno que operan sobre nosotros mismos. Una suerte de capitalismo cibernético emerge como la traducción, o al menos la traductibilidad, de toda actividad a información, a masas de datos que son procesadas por algoritmos que relanzan el mecanismo garantizando el feedback que constituye su eficacia.

Se trata de una nueva lógica, una lógica algorítmica que emplaza una nueva gramática que ya no entiende la realidad en términos de estado, sujeto o producto, sino de flujos, velocidades y aceleraciones. Esta racionalidad trae consigo una forma de poder que implica un gobierno que produce a los gobernados como participantes activos del proceso de gobierno mismo. Lejos de rechazar el caos o el desorden, lo que busca es un equilibrio en el desorden mismo, cosa que sólo es posible haciendo uso de dispositivos flexibles de recolección y seguimiento de datos. He acá la forma de vigilancia que la hipótesis cibernética plantea.

Siguiendo a Fernandez-Savater, el escenario así presentado es uno en el que la transparencia se dice como reducción a 'perfil' del individuo, cosa que en su opinión recorta la realidad, dejando por fuera precisamente la potencia de la resistencia. Se trata además de una pulsión aceleracionista

que pone “la vida entre paréntesis” para demandar producción de rastros (metadata), lo que reduce al mismo tiempo la creación a la inmediatez y la superficialidad. Por último, se trata de una reducción de la relación a la interconexión, que, en su opinión deja por fuera todo lo que tenemos de 'humanos': el deseo, el sentido. Al respecto, debo decir que no comparto esta visión 'humanista' que contrapone Fernandez-Savater a la hipótesis, ya que pierde de vista elementos que retomaré en la lectura de los argumentos de Rodríguez (2016).

Con esa lectura irónicamente distópica, la resistencia se porpondría como una reivindicación humanista que exige la recomposición de lo humano de ese recorte informacional que implica la cibernética. Se trataría de 'devenir irrepresentables', lo que implicaría ser “opacos a su ojo de cíclope, ilegibles para sus máquinas binarias de sentido, impredecibles para sus técnicas de control.”; se trataría de poder crear una forma de comunicación que no “embrutezca”, que no “atonte”, que dejen espacio y libertad al lector; se trataría de una lentitud que se diga como desaceleración y desconexión, interrupción y fuga a modo de sabotaje de modo que se habilite de nuevo “la posibilidad del proceso y el encuentro. Permite darse tiempo. Para mirar hacia los lados y no sólo hacia adelante. Para ver, sentir o pensar las situaciones que habitamos. Para que lo nuevo pueda acontecer.”; se trataría de encontrar un nuevo “ritmo” que no desatienda la “cojera” que le es propia a lo humano: “Nunca el ritmo automático y unilateral de la máquina (que descarta lo pesado, lo lento, las asperezas, etc.). Tampoco el ritmo musical, armónico, que sigue paso a paso la partitura (el programa). En todo caso, el ritmo del free jazz (<https://www.youtube.com/watch?v=xbZIiom9rDA>) plural, disonante, abierto a la improvisación. Un ritmo que asume e incorpora los silencios, las mareas bajas, los fallos, los accidentes, etc.”; se trataría, finalmente, de producir la niebla: “La niebla sería la estrategia que confunde las exigencias de transparencia, de univocidad, de identificación.” (Fernandez-Savater, 2015)

Lo que se hace evidente en estas propuestas poéticas es precisamente su carácter inasible. ¿En qué consisten realmente? La pregunta es doblemente tramposa. Por un lado, realmente no es claro establecer lo que estar propuestas proponen en un sentido práctico, pragmático, programático. Pero por otro, preguntárselo es precisamente retrotraer nuestro sentido dentro de la lógica cibernética misma (pidiendo estabilidad, equilibrio, certeza), en vez de abandonarnos precisamente a las gramáticas emergentes. Todo esto lleva a una reflexión imposible de desarrollar acá respecto de el campo de lo político y de la política, que en todo caso necesitaría ser re-definido.

VIGILANCIA, CIBERNÉTICA Y SOCIEDADES DE CONTROL

No cabe duda que la hipótesis cibernética guarda una estrecha relación con lo que a partir del opúsculo de Deleuze (2005) se llaman sociedades de control. Y uno de los vínculos más claros y evidentes es la vigilancia. En un primer momento concebida como videovigilancia, la noción abarca hoy en día los sistemas de control biométrico y otros sistemas de monitoreo que trascienden el reino de la imagen. Una de las cosas que Deleuze no ve en su breve pero incisivo diagnóstico del momento bisagra que olfateaba empezando 1990 es precisamente lo que la hipótesis cibernética

presenta en términos de extensibilidad de la vigilancia. Apoyados en los teóricos de la cibernética de primera generación, los Tiqqun presentan nuestros tiempos como una escena de ciencia ficción hiperrealista, que aun necesitan ser pensados, analizados, descifrados para dar cuenta de la complejidad que implican.

En el extrálogo del libro, Pablo Esteban Rodríguez (2015b) tensiona la hipótesis cibernética misma, haciéndola superficie espejada para mirarnos a nosotros mismos. En ese sentido, es posible pensar que más que una estructura de poder vertical y centralizada que nos engaña técnicamente, asistimos a un escenario en el que la 'servidumbre voluntaria' ha encontrado su máximo nivel de complejidad. Alimentamos voluntaria y gozosamente las bases de datos de las que reprochamos por vigilarnos. Sin duda, las bases de datos constituyen los sistemas de vigilancia contemporáneos, pero estas no pre-existen autónomamente, sino muy por el contrario, su eficacia depende en altísima medida de la participación activa del 'usuario' en la interconexión. La vigilancia comporta entonces una paradoja: no nos importa realmente ser vigilados (pues alimentamos plácida y constantemente las bases de datos que constituyen el sistema de vigilancia por excelencia), y a los que por cualquier razón les importa no alimentan las bases de datos, cosa que implica algunos asuntos que repondré más adelante.

Allí mismo, Rodríguez (2015b) resume en una serie de deslizamientos la propuesta que, en términos políticos pareciera esbozar el libro. Ante la información (clave del gobierno), habría que contraponer una 'energética anticibernética'; ante la circulación de mensajes, ejercicios de 'interferencia', o también, tomando la fórmula de Deleuze (1996: 275), 'valuolas de no-comunicación'; ante el par paranoia/visibilidad, mayor 'opacidad' e 'intensidad'; y ante la ganancia de tiempo, la creación de “espesores de tiempos del lado de lo invisible”. Y de nuevo estamos frente a la política poética de los Tiqqun: ¿qué es exactamente una 'energética anticibernética?, ¿de qué tipo de interferencia se trata?, ¿cómo opera una 'vacuola de no-comunicación'?, ¿opacidad e intensidad de qué, en función de qué, respecto de qué?, ¿qué es un 'espesor de tiempo'? Y de nuevo la reflexión sería la misma, no tanto avanzar aceleradamente hacia la formulación de respuestas a estas preguntas, sino renunciar a la tentación de formularlas. Rodriguez da una pista: “por eso no hay que confundirse: el esoterismo no equivale a la clandestinidad” (2015b: 19), una pista que nos (des)orienta estratégicamente, haciendo dirigir nuestra atención hacia una política-poética-esotérica.

En el contexto en el que nos encontramos el primer paso que adeudamos es uno de cangrejo, hacia atrás. En una entrevista reciente, Rodríguez (2016) nos ofrece algunas ideas que me permito sobreescribir, parafrasear y reensamblar en función de lo que pretendo exponer (así, lo que sigue es una composición de sus reflexiones con mis interpretaciones).

Habrá que desandar el lenguaje de lo político para poder ver que 'el sistema' no existe más, sino que a partir de la hipótesis cibernética todo hace parte del sistema, que en todo caso es una red de sistemas. Tal es el postulado de gobierno de la cibernética en el fondo: si todo es parte del sistema, la autorregulación del mecanismo garantiza los objetivos que éste se proponga. Estamos

ante la radicalización de la 'mano invisible' del liberalismo, una radicalización fundamentalmente técnica y tecnológica que se alza sobre el ethos neoliberal para hacer que todos seamos partícipes de el mecanismo de autorregulación propuesto. El uso técnico es el éxito del nomos cibernético en un contexto éticamente neoliberal. La técnica y la tecnología son aspectos centrales que enlazan la hipótesis cibernética con las sociedades de control, y que por algoritmización de la vida, la traducen en ejercicio de vigilancia expandida. Del empresario de sí al algoritmo de sí: Facebook como caso paradigmático.

La vida entonces no es sino vigilancia sobre vigilancia, todo es parte del funcionamiento de un algoritmo que "traza los movimientos de las conexiones, y el usuario tiene la sensación de que le están dando lo que está buscando, pero no, te están acomodando en una estadística" (Rodríguez, 2015a). Un panorama que sería mejor leer como distopía tal y como propone Fernández-Savater. La siguiente tentación que nos rodea es entonces reemplazar 'el sistema' por 'el algoritmo', lo que al mismo tiempo generaría una exterioridad absoluta y una imposibilidad política de intervenir o de pensar una estrategia. Los algoritmos son el nuevo ecosistema, y en ese sentido habría que pensar si hay una forma de habitar el algoritmo sin reproducir inmediatamente el nomos cibernético y el ethos neoliberal. La respuesta no está dada, pero el advenimiento del algoritmo lo que hace es mostrar que asistimos a un nuevo modo de dominación ideológica (para hablar en gramáticas ya muy viejas) y que es allí donde se abren nuevos terrenos de disputa (por lo que no pueden ser inmediatamente exteriorizados).

Segundo paso importante: actualizar los valores que están en juego. Un ejemplo que tomo de la entrevista a Rodríguez (2016); ante la pulsión de comunicación y de emisión constante, ¿cómo evitar la exhibición de la intimidad? De hecho, ¡no hay tal! Cuando Debord habla de espectáculo (2010), se refiere a una actitud pasiva de sobreexposición y sobreestimulación sensorial, y hoy asistimos a una altísima estimulación que nos hace partícipes, todo lo contrario a una actitud pasiva. La intimidad, por otro lado, es por definición lo no exhibible, así que si se exhibe deja de serlo. Es entonces lo que entendemos por intimidad lo que ha cambiado. Lo que se exhibe es 'vuelto público', publicidad, y por tanto no puede ser íntimo. En el fondo, una crisis de la noción de individuo.[1] Lo público es lo político, y entonces lo que era íntimo ha entrado en definitiva en esa esfera. El algoritmo ha logrado que perdamos de vista al menos la mitad del movimiento de subjetivación que trae aparejado: el 'perfil' (metadata, dividual) no sólo es lo que yo gestiono de mí mismo, sino que él mismo gestiona lo que soy en la medida que yo alimento (gestionándolo) lo que él necesita para modular y orientar mi conducta. Si llevamos esta hipótesis a sus últimas consecuencias, encontraremos que somos nosotros mismos, sin saberlo del todo y seguramente sin proponérnoslo, los que nos vigilamos a nosotros mismos.

¿Se trata entonces de proponer un retiro masivo de la red? Esto sería desconocer la materialidad de la realidad contemporánea, un giro humanista como el que propone Fernández-Savater. Ser anacoreta en nuestros tiempos es incluso un lujo que el mercado ofrece bajo condiciones controladas, para asegurar el bienestar del participante. Más bien, nos sugiere Rodríguez (2016), se trataría de una apropiación que implique un uso diferente, pero no al contrario, es decir, no

un uso que se diga como apropiación (en el último apartado del texto retomaré esta idea). En un mundo recientemente dividual, todavía hace falta trabajo para asumir que ya no somos sólo cuerpo (y alma, si se quiere).

> Lo que pasa con los cuerpos es algo muy interesante porque en teoría si nosotros aplicamos el criterio 'restringido' de materialidad, parecería como si hubiera una especie de erosión o un eludible de los cuerpos, y la verdad es que los cuerpos están presentes de una manera muy diferente a la manera en la que lo estaban en el pasado (...) La cibernética que lo que hacen es una especie de deconstrucción y reconstrucción del cuerpo a otro nivel: el cuerpo como comunicación. De hecho, como decía Paul Vaslavick, no se puede no comunicar. Y eso significa que cualquier cosa que uno haga es, en un sentido, comunicación. (...) Hay toda una codificación del cuerpo, y esa codificación es la sociedad de control, porque no son las disciplinarias, no se intenta construir el cuerpo máquina como el mecanismo newtoniano; es una máquina de información. Entonces todos los gestos que ustedes están haciendo yo los estoy procesando: el sí, el no, la duda, todo eso puede ser explotado y es explotado hoy. (Rodríguez, 2015a)

La actualización de las gramáticas no se reduce a una operación semántica o puramente terminológica, pues incluso la vigilancia es algo que ha cambiado epistémicamente: "...la vigilancia uno la siente como intromisión respecto de algo; y efectivamente lo que ocurre hoy es casi lo contrario." (Rodríguez, 2015a), las fugas del 'no tengo nada que ocultar' se han vuelto sentido común que reproducen la brecha entre el mundo que habitamos y la posibilidad de programar uno nuevo; "...uno de los elementos de la vigilancia es que alguien te esté vigilando y todos estamos manifiestamente dejando datos, y no nos importa, entonces la idea misma de vigilancia se va un poco..." (2015a). De hecho, en esa transvaloración cibernética de los valores "es un mal menor el hecho de estar vigilado ante el hecho de qué pasa si no estoy comunicado" (2015a).

La vigilancia entonces es un vector de reorganización de los procesos de subjetivación contemporáneos, un vector cibernético que se camufla muy bien en la estrategia de la autorregulación y, en ese mismo sentido, de la pulsión altamente efectiva de participación activa de los sujetos en la reproducción y el fortalecimiento de los mecanismos que los gobiernan. De manera paralela, se trata de un gesto ético-político que reorganiza el valor de los valores y pone a circular nuevos valores jerarquizados bajo la rúbrica del neoliberalismo. Por eso no es impensable una máquina teórica que ensamble como gran dispositivo a la hipótesis cibernética con el neoliberalismo y las sociedades de control, elementos conceptuales que operarían como caras de un prisma de visibilidad del mundo contemporáneo.

SILENCIO Y SOLEDAD

Siguiendo la línea deleuziana, esbocé en el Simposio anterior (Rios, 2015) algunas ideas en torno a la lectura de la posdata de Deleuze y a algunos textos de Guattari en clave de vigilancia. Desconociendo en ese momento la hipótesis cibernética, intenté un vínculo entre la preeminencia de la técnica y la tecnología y la vigilancia como ejercicio primordial de subjetivación en las sociedades de control. Más tarde habría de recordar los aportes de Peter Pál Pelbart alrededor

de esta cuestión. Su pluma se me ofrece como el gong que marca el intenso pero suave ritmo de alguna meditación. Siempre paciente para señalar la paradoja dentro de lo que se ofrece como nuevo sentido común, renuncia a hacer un diagnóstico riguroso para aventurarse a jugar con lo que las fuerzas que nos configuran ofrecen. Por ejemplo, ante la idea de que esta sociedad cibernética es una sociedad productora de soledades, Pál Pelbart contrapone la reflexión puramente deleuziana que sostiene que "el problema no es que nos dejan solos, es que no nos dejan lo suficientemente solos." (Pál Pelbart, 2009: 43) Ante la figura de la vacuola deleuziana, sostendrá que no se trata de una operación de silenciamiento, sino de la creación de un tiempoespacio que genere las condiciones de posibilidad para poder tener algo qué decir, realmente.

Comprende que 'desconectar' es prácticamente imposible, pues "cada vez que alguien se desconecta, permanece en silencio, no responde a la expectativa, se genera un malestar, una sensación de incomodidad, de desasosiego, una molestia" (Pál Pelbart, 2016) que será sancionada sin duda, sea vía ostracismo (imposibilidad de acceso a consumo, trabajo, comunicación), sea vía sobreexposición (el desconectado es altamente sospechoso para el sistema de vigilancia cibernética). Su apuesta en todo caso tiene que ver con un cierto silencio, con la producción de un silencio en el que por fin se encuentre algo para decir, de una soledad poblada de nuevos ritmos afectivos; una apuesta que presenta como respuesta al nivel de insoportabilidad que la sociedad de control ha generado. Muy al contrario de lo que parece, la hipótesis cibernética no opera produciendo insularidad sino sobreexplotando la juntura:

> La voluntad de estar juntos todo el tiempo, con todos a la vez, no permite oír nada en absoluto. La soledad no refiere a la idea romántica que tenemos de oír nuestra voz interna; más bien se trata de una soledad poblada. La soledad puede ser atravesada por muchas voces. (…) no es una oda a la soledad misma como una especie de insularidad. No se trata de eso. Es precisamente lo opuesto: es necesario tener cierta soledad para poder establecer otras conexiones que el gregarismo no permite. (…) La idea no es volver nostálgicamente al sujeto autónomo que fuimos por no sé cuánto tiempo, a nuestro ideal humanista, sino tomar algo de este caos contemporáneo y hacer algo con eso, como producir desvíos. Una opción es establecer una relación profundamente arraigada con el presente: "Todo es terrorífico, así que me cerraré sobre mí mismo en una resistencia radial y permaneceré en las periferias". Esta sería la vieja forma de pensar la resistencia propia. Pero se pueden producir otros tipos de redes en medio de todo estos influjos, producir otros tipos de movimientos, a la vez individuales y colectivos. A pesar de partir de la idea de soledad poblada, no deberíamos necesariamente tomar esto como algo literal: es posible vivir en grupos, en colectivos en los que otros modos de 'espaciotiempos', otros ritmos y maneras –incluyendo intercambios en los que nadie hablase o en lo que no se espere respuesta inmediata– sean inventadas. (Pál Pelbart, 2016)

Una nueva ventana se abre, al menos parcialmente; sin un retorno humanista a lo que sería 'constitutivo' del hombre, sino más bien renegando de eso, esto es, siendo absolutamente consciente de las gramáticas que traman la realidad contemporánea, Pál Pelbart propone una estrategia que entiendo como la radicalización de las condiciones de subjetivación contemporáneas: habitar los términos hasta hacerlos provocar cortocircuitos entre sí. Habitar la paradoja sin proponerse superarla. El elemento clave de su propuesta, a mi entender, es el de la experimentación, que sin duda trae de la propuesta deleuziana. Experimentación que trae consigo la necesidad

de hacerle frente a sinnúmero de riesgos (imprevisibles por definición). Por eso, cuando le preguntan por lo que consideraría el reto más grande de nuestros tiempos, responde certero:

> Crear nuevos medios de interrupción. La imagen del freno de emergencia de un tren viene a mi mente. Sin embargo, con una interrupción así de abrupta, definitivamente son posibles los descarrilamientos. Y éstos son y serán, en muchos casos, necesarios. (Pál Pelbart, 2016)

HABITAR LA PARADOJA: NO SONRÍA, LO ESTAMOS FILMANDO

Pareciera que nos encontramos atrapados en la paradoja de no poder no formular la cuestión de la resistencia –porque en definitiva la vigilancia es un tema de primera línea en términos políticos– y verificar que cada respuesta posible es menos y menos eficaz ante un diagnóstico más o menos cuidadoso.

No se trata, en definitiva, en declarar un rechazo tajante a la vigilancia, pues es innegable que se trata de un elemento constitutivo de nuestra realidad actual. La tecnofobia es una reacción más o menos 'normal' ante el hecho de darnos cuenta, como en la película, que 'no hay cuchara' (o en este caso, que la cuchara es todo lo que hay). Pero tampoco se trata de declarar la vigilancia (o a algunos de sus usos, es decir, también a la 'contravigilancia') como la vía de liberación del sistema –"destruyéndolo desde dentro". La tecnofilia también hace agua en términos del grado de su alcance y de lo que podemos llamar 'feedback' funcional al sistema, su mecanismo de autorregulación.

Sin embargo, tampoco se trata de huir del binarismo argumentando que la vigilancia es neutral y que sólo el uso que se le da carga con el peso moral y/o político. La hipótesis de neutralidad tecnológica es demasiado próxima –casi una excusa retórica para acercarse– a la postura tecnofílica (pero también tecnofóbica, o incluso a ambas al tiempo). Lo que nos queda en el menú es un grupo de estrategias demasiado poco claras, tal vez afortunadamente. 'opacidad', 'interrupción', 'silencio' (vacuola de no-comunicación), y otras por el estilo.

La cuestión del uso de las tecnologías (ahora todas de vigilancia aumentada) permite proponer brevemente una discusión de orden ético-político que repondré a partir del hilo argumental de Rodríguez (2016). Si aceptamos que la idea de individuo es(tá) puesta en crisis por la lógica algorítmica de subjetivación, entonces es claro que todo 'uso' es neoliberal de entrada. No podría plantearse la cuestión política a partir del uso porque esto implicaría dos cosas: por un lado, proponer en simultánea que la tecnología constituye una exterioridad absoluta respecto del sujeto, lo que implica una visión puramente instrumental de la técnica, y que aún como exterioridad puede erigirse como medio para un fin que es su propia superación. Estamos es más bien ante una brecha epistémica que es la que precisamente hace que consideremos a la técnica, a la tecnología, al algoritmo como algo ajeno a toda actividad humana.

Esta brecha es un efecto deseado por la cibernética, que ha logrado naturalizar el uso por encima de cualquier otra actividad, y ahí radica la oportunidad: no se trata de proponer un cambio en la relación con la técnica que se diga sólo en términos de uso, pues esto simplemente

significaría una ampliación del territorio de gobierno contemporáneo, sino primero y ante todo en términos de conocimiento. La fórmula puede plantearse de la siguiente forma: a menor entendimiento técnico, mayor gobierno algorítmico. Simondon (2007, 2015) no hizo sino alertarnos al respecto mucho antes de que existiera algo así como la World Wide Web al señalar que no es suficiente saber conducir, sino que es preciso conocer el funcionamiento interno de los motores que hacen que nuestros automóviles hagan lo que hacen. Un buen indicador de esta brecha lo constituye el corredor de doble vía que nos lleva del uso a la relación tecnofílica /tecnofóbica y de vuelta; se trata de un pasadizo que obtura y anula la pregunta por el funcionamiento de los aparatos. De la vigilancia a la contravigilancia, a la contra-contravigialncia y al infinito; pero rara vez al estudio del funcionamiento técnico de las cámaras, los cableados, la transmisión de imágenes por satélites, la sintetización digial de imágenes, etc. Y es que si la vida hoy pasa por (y es traducida a, dividuada) sistemas técnicos, entonces se hace necesario saber de sistemas técnicos.

En su interesante intervención en el IV Simposio Lavits, Fernanda Bruno apuntaba muy acertadamente en este sentido que el algoritmo no es una representación de la dinámica social contemporánea, sino un agente performativo dentro de ella. La implicación que tiene este giro es que debemos encarar una nueva ontología, una nueva epistemología que nos permita disponer una grilla de inteligibilidad para aprehender que el objeto de la vigilancia ampliada es un efecto de la visión algorítmica y no un hecho que la preexiste; esto es, que la vigilancia crea, hace emerger aquello que vigila, lo que implica un desplazamiento teórico-metodológico que de cuenta ya no de la causa ni del responsable por las estrategias de vigilancia, sino de los efectos de sus operaciones. Estamos ante el reto de pensar la política de una normatividad sin norma, o en todo caso, una normatividad que se dice como comportamiento que genera sus propias normas, a posteriori. Así como el algoritmo de Facebook ubica al usuario en una franja estadística de comportamiento, haciéndole creer que realmente encuentra lo que busca, la vigilancia ampliada se propone prever el futuro para modificarlo, cuando lo que realmente hace es producir ese futuro que quiere evitar. En ambos casos opera la misma lógica. La pregunta, en este caso, por la resistencia ante un escenario en el que lo que es 'falso' sucede efectivamente, se dice como la pregunta por procesos de subjetivación de desactiven la paranoia sin desconocer el funcionamiento de la dinámica.[2]

Nos queda aun sobre la mesa la “estrategia Snowden”: reclamar que el secreto no sea la regla, que la menor cantidad de cosas posibles sean secreto. Sin embargo, la paradoja de esta estrategia es que esta demanda es altamente compatible y computable con la transparencia que la hipótesis cibernética impulsa. La estrategia Snowden pierde de vista el sesgo moral que la constituye: se trata de una estrategia válida, siempre y cuando no sea puesta en práctica por el gobierno (o por las instituciones de turno).

Finalmente, y simplemente a modo de incitación, pensar por un momento en el primer capítulo de la tercera temporada de Black Mirror, titulado “Nosedive”, en el que se presenta una socialidad absolutamente dependiente de la interacción digital. Una gran red social que sobredetermina

las posibilidades afectivas, sociales, laborales, de consumo y de gasto habita, como en la película Her, los dispositivos cotidianos de aquella sociedad. Además de la obviedad que implica señalar la muy corta distancia de aquella 'distopía' respecto de nuestra realidad contemporánea, me preguntaría si acaso no es ese escenario (allí en la pantalla, pero al mismo tiempo en nuestras pantallas de la vida diaria) una prueba de que la hipótesis cibernética y su vector vigilante se hicieron ya con la estrategia de las vacuolas de no-comunicación deleuzianas. Es decir, si ya esta 'estrategia' no ha sido cooptada por el algoritmo contemporáneo y en ese sentido tendríamos que abandonar esta empresa, o si por el contrario, sólo se trata, como podría argüir Pál Perbart, de un uso poco sofisticado, de un sofisma, de un espejismo que precisamente pretende generar como efecto la imposibilidad de disputar ese terreno y que por lo mismo oculta que no son esos los silencios, las soledades a las que refiere la figura de las vacuolas deleuzianas, y que es precisamente en ese espejismo donde está el territorio de disputa por las condiciones de posibilidad de hacer-nos nuestro propio desierto, de poblar-nos las solitudes, de poder encontrar por fin algo qué decir-nos.

Así, considero que estamos en un momento de seguir adelantando juiciosa y detalladamente estudios, análisis y experimentaciones que nos permitan precisamente darnos cuenta que estamos de nuevo ante una "Ironía del dispositivo [...]: *(pues)* nos hace creer que en él reside nuestra liberación". (Foucault, 2013: 152; añadido mío.)

NOTAS

* Estudiante del Doctorado en Ciencias Sociales, UBA. Becario Doctoral, CONICET. E-mail: cerrsociologicus@gmail.com

1. Junto con Fernanda Bruno, Pablo Esteban Rodríguez ha venido trabajando la hipótesis de una nueva 'secuencia' subjetiva que puede ser entendida bajo el prisma de lo 'dividual'. No es este el momento, ni tengo la experticia, para poder desarrollar este interesante punto, que en todo caso puede entenderse como un prolegómeno a una nueva teoría del sujeto en tiempos cibernéticos (al respecto, la conferencia que pronunciaron en Lavits, 2016: https://www.youtube.com/watch?v=yLkuRkTETlE&t=22s)

2. Existe registro audiovisual de esta intervención, disponible en: https://www.youtube.com/watch?v=rDA5wTvFkvc&t=76s

REFERENCIAS

Comité Invisible. (2015). *Carta a nuestros amigos*. Buenos Aires: Hekht.

Debord, G. (2010). *La sociedad del espectáculo*. Valencia: Pre-textos.

Deleuze, G. (1996). Control y devenir. En *Conversaciones*. pp. 265-276. Valencia: Pre-Textos.

Deleuze, G. (2005). Posdata sobre las sociedades de control. En Ferrer, C. (Comp.). *El lenguaje libertario. Antología del pensamiento anarquista contemporáneo*. pp. 115-121. La Plata: Terramar.

Fernandez-Savater, A. (2015). La pesadilla de un mundo en red. Diponible en: http://www.eldiario.es/interferencias/pesadilla-mundo-red_6_412668752.html

Foucault. M. (2013). *Historia de la sexualidad. 1. La voluntad de saber*. Buenos Aires: Siglo Veintiuno.

Pál Pelbart, P. (2009). Como vivir solos. En *Filosofía de la deserción. Nihilismo, locura y comunidad*. pp. 43-50. Buenos Aires: Tinta Limón.

Pál Pelbart, P. (2016). Producir otro ritmo, otra respiración, otra empatía, otros silencios, de modo que algo pueda hacer sentido de nuevo. Entrevista con Peter Pál Pelbart. Disponible en: http://anarquiacoronada.blogspot.com.ar/2016/11/producir-otro-ritmo-otra-respiracion.html

Rios, C. (2015). Vigilancia y monitoreo en el dispositivo de modulación: notas para una estética de la existencia en Deleuze y Guattari. En *Anais do III Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territorios*. Rio de Janeiro: Lavits/Medialab-UFRJ. Mayo. pp. 694-711. Disponible en: http://medialabufrj.net/download/lavits2015-anais/10/3.Resumo39.pdf

Rodríguez, P. (2015a). Clinämen: ¿Qué es la sociedad de control?. Conversación con Pablo Estéban Rodríguez. Disponible en: http://anarquiacoronada.blogspot.com.ar/2015/12/clinamen-que-es-la-sociedad-de-control.html

Rodríguez, P. (2015b). Extrálogo. En Tiqqun. *La hipótesis cibernética*. pp. 11-19. Buenos Aires: Hekht.

Rodríguez, P. (2016). ¿Qué es la hipótesis cibernética?. Conversación con Pablo Estéban Rodríguez. [Audio en dos partes]. Disponible en: http://ciudadclinamen.blogspot.com.ar/2016/11/que-es-la-hipotesis-cibernetica.html

Simondon, G. (2007). *El modo de existencia de los objetos técnicos*. Buenos Aires: Prometeo.

Simondon, G. (2015). *La individuación a la luz de las nociones de forma e información*. Buenos Aires: Cactus.

Tiqqun. (2010). *Llamamiento*. Buenos Aires: Folia.

Tiqqun. (2013). *Primeros materiales para una teoría de la jovencita. Hombres máquina: modo de empleo*. Buenos Aires: Hekht.

Tiqqun. (2015). *La hipótesis cibernética*. Buenos Aires: Hekht.

CUANDO ALGO “ME GUSTA” EN FACEBOOK: IDENTIFICACIÓN Y PRODUCCIÓN DE PERFILES A PARTIR DE SUS PREFERENCIAS

Resumen: En la red social *Facebook* se han diseñado distintos mecanismos de identificación que van desde la solicitud del nombre real de la persona, la identificación biométrica de las fotografías, la solicitud del número de celular, hasta el rastreo de los datos producidos por la IP, la navegación por fuera y dentro de la misma plataforma. Estas tecnologías, principalmente, están enfocadas en identificar el perfil desarrollado con el de la persona fuera de la red a partir del reconocimiento de datos sobre su vida y biométricos. No obstante, a partir del año 2010 comenzó a desarrollarse toda una tecnología en el rastreo y análisis, no ya de datos físicos, sino de las preferencias y gustos de los usuarios. Esto se dio a partir de la creación del botón “Me gusta” (Like button) y de su integración al Protocolo *Open Graph* . Si bien su invención pudo estar destinada a una relación mercantil y de expansión de la plataforma de Facebook a la Web, con posterioridad se volvió objeto de análisis por parte de neurocientíficos que encontraron allí la posibilidad de rastrear, identificar y analizar perfiles de usuarios. El caso más significativo es el estudio realizado en 2013 por Michal Kosinski (Et. Al.), quienes, a través de un aplicativo, pudieron desarrollar un método para identificar aspectos de los usuarios a partir del uso que le daban al botón “Me gusta”: algunos de los datos arrojados demostraron altas capacidades para identificar rasgos como la personalidad, la etnia, inclinaciones políticas y sexuales. El objetivo del presente trabajo está enfocado en analizar este tipo de tecnologías de identificación, resultantes del cruce entre ciencia, tecnología y sociedad.

Palabras Clave: Botón “Me gusta”, Identificación, Preferencias, Facebook.

JUAN CAMILO GÓMEZ BARRERA*

Quando dou "Curtir" no Facebook: identificação e produção de perfis com base em suas preferências

Resumo: Em Facebook criaram-se mecanismos de identificação diferentes que vão desde a aplicação do nome real da pessoa, fotografias de identificação biométrica, ate a aplicação de número de telefone celular para os dados de controle produzidos pela IP, o navegação fora e dentro da mesma plataforma. Estas tecnologias, principalmente, estão focadas em identificar o perfil desenvolvido com a pessoa fora da rede a partir do reconhecimento dos fatos sobre sua vida e biometria. No entanto, a partir de 2010, começou a desenvolver uma tecnologia no acompanhamento e análise, os dados não físicas, dos gostos e preferências dos utilizadores. Isso ocorreu após a criação do botão "Curtir" (Like button) e integração Open Graph Protocol. Embora sua invenção poderia ser destinado a uma relação comercial e expansão da plataforma Facebook para a web, depois de ser analisada virou por neurocientistas descobriram a capacidade de rastrear, identificar e analisar os perfis de usuário. O caso mais significativo é o estudo realizado em 2013 por Michal Kosinski (Et. Al.) que, através de uma aplicação capaz de desenvolver um método para identificar aspectos de usuários a partir do uso que lhe deu o botão "Like" : alguns dos dados mostrou jogado altas capacidades para identificar traços tais como personalidade, etnia, política e orientação sexual. O objetivo deste trabalho está focado na análise deste tipo de tecnologias de identificação, resultantes do cruzamento entre ciência, tecnologia e sociedade.

Palavras chave: "Botão Curtir", Identificação, Gostos, Facebook.

When something I "Like" on Facebook: identification and production of profiles from the preferences

Abstract: In the Facebook it can be observed different identification mechanisms, wich go from the use of real names for signing in, biometric identification of the photographs, mobile numbers, until the tracking of both data produced by IPs and navigation outside and inside the platform. Primarily, these *technologies* were focused on *verify* the correspondence between virtual and real-life profils using data about his/her life and biometrics. However, starting from the year 2010 Facebook began to develop*technologies* of tracking and analysing of users not based on physical data but on their personal preferences and 'tastes'. The creation of the 'like' button and its integration into the Open Graph Protocol was the pillar of this recent 'taste' identification. Eventhough the latter invention is destined to commercial relationships and the expansion of the Facebook platform itself among the Internet, it has also become an important analysis subject for neuroscientists that found in the platform a possibility to track, identify and analyse users profiles. The most significant case of this sort of studies is the one developed by Michal Kosinski (*Et.*) in 2013, who created a method to identify different aspects of the users relied on 'Like' button functions. Some of the results showed high capabilities of identify personality, ethnic, political inclination and sexual orientation of Facebook users. The aim of this paper is analyze this type of *identificationtechnologies* as the result of science, technology and society insight exchanges.

Key words: Like button, Identification, Likes, Facebook.

A los trabajos que se suscriben bajo la hipótesis de que las redes sociales funcionan como mecanismos de poder se los puede asociar en, por lo menos, dos predominantes derivas: por un lado, se las piensa como entramados en donde se preponderan lógicas y dinámicas asociadas al *panoptismo*, como lo puede leerse en Constante (2013), o, por otro, vinculadas a sistemas diseñados con objetivos de vigilancia, como es el caso de Chaverry (2013). Con respecto a la primera forma de análisis, pareciera que la idea de un panóptico, entendido como un dispositivo disciplinario cuyos objetivos eran la producción de sujetos dóciles y útiles, no encajara completamente del todo en las estructuras y funcionamiento de las redes sociales, por cuanto no hay como tal un único centro desde donde se ve, sino construcción de múltiples miradas descentradas que determinan las redes como espacios atravesados por la presencia siempre constante de otros, como lo ha sabido mostrar Marinucci (2010); con respecto a la vigilancia, si bien igual-

mente es un mecanismo propio de la disciplina, de acuerdo a Lyon (1994), sería necesario pensar una actualización de la noción de vigilancia, más allá de la planteada por Foucault, en la era digital y en las redes sociales.

Entonces, pensar a *Facebook* como un mecanismo de poder implica más asociarlo a los dispositivos de la sociedad de control y no tanto a una disciplinaria, en la medida en que permite un acople más adecuado a los modos de funcionamiento de este tipo de dispositivos: así, por ejemplo, está más emparentado con la idea de una *circulación* y una *modulación*, que a una noción de *encierro* y de *moldeo*. El hecho de que a través de las redes sociales se apele constantemente a la libertad de contenido –así, por ejemplo, se lee en los principios de *Facebook*[1], que toda persona tiene la liberta de acceso a toda la información que cualquier contacto ponga a su disposición —o que se incite constantemente la exhibición, daría cuenta de una modalidad que escapa no sólo al modelo de vigilancia y de panóptico, sino que inscribe la red social dentro de un dispositivo más propio de la biopolítica, tal como lo ha sabido plantear Lasalle (2015).

Ahora bien, la extracción de información y datos utilizada como mecanismo de explotación capitalista, así como su utilización también por parte de Agencias de Seguridad, ha permitido pensar las redes sociales como mecanismos y focos de poder aprovechado por el mercado y los gobiernos. Sin embargo, para que dicho mecanismo se ponga en marcha es necesario que existan modos de hacerse "visible" y "enunciable" (Deleuze, 1987, pág. 75 y ss.) no sólo los espacios, sino, precisamente, dichos mecanismos de poder. Es decir, es necesario observar si las redes sociales producen saberes específicos que posibilitan pensarlas no simplemente como canales en donde se transita, transmite y almacenan datos que son utilizados por otros agentes externos y, que en ello, radicara su modo de operación como dispositivo de poder; de hecho, en este caso concreto, esta utilización de los datos por parte del mercado es pensada como si fuera de por sí ya una condición de producción de ejes de poder, como sostiene Lasalle (2015), sin preguntarse si dentro de esa misma dinámica se producen modos de *ver*, o de visibilizar, y de *hablar*, que complementaran e hicieran posible los dispositivos de poder.

En otras palabras, consideramos que a la postura que intenta analizar las redes sociales como mecanismos de poder es necesario reajustarla a través del estudio de las modalidades en las que, previamente, se determinan campos de saber; por ejemplo, si bien una de las cuestiones más interesantes resulta ser el suministro de datos de los usuarios a agencias de seguridad y a actores del mercado, cabe preguntarse si estos datos mismos son ofrecidos a dichos agentes externos de forma pura o directa, es decir, sin un trabajo previo, o si son permeados por formas de saber que ya elaboran un trabajo sobre los datos mismos al interior de la plataforma para después ponerlos a circular. Esto es, antes de pensar las redes sociales como focos puramente de poder, en donde se pueden procurar modalidades en las que se efectúan mecanismos de vigilancia y control, consideramos que es necesario pensarlas como focos, o núcleos, de saber.

Esta pregunta acerca de si las redes sociales son productoras de saberes, es decir, modos de ver y hablar, además de permitir generar formas de conocimiento más preciso sobre su funciona-

miento y las implicaciones en la sociedad que puedan tener –se trate del estudio de su funcionamiento como focos de poder o del modo en que despliegan identidades, como lo plantean Wandel y Beaver (2010)—, puede ayudarnos a desmontar, en algo, la imagen mítica del *robot* que reposa sobre los aparatos técnicos, la cual se centra en la atribución a esos objetos tecnológicos de un "alma y una existencia separada, autónoma, que le confiere el uso de sentimientos e intenciones contra el hombre" (Simondon, 2007, pág. 32), es decir, plantear que, como tal, no se trata del funcionamiento interno de la plataforma lo que viene a concentrarse como un foco de poder, sino los convenios, tratados, pactos, etc., que se realizan con los actores externos y, por otro lado, que las redes no realizan como tal procesos de subjetivación aisladamente, sino que sobre ellas operan y son usadas bajo modos de ver que se corresponden con otros focos de poder; a saber, dicho sea de paso, que se inscriben también dentro de una *episteme* propia que, tal como lo veremos, se corresponde con una racionalidad algorítmica.

Un caso muy específico que nos permite dar cuenta de todo ello resulta ser el laboratorio de investigaciones científicas de *Facebook*, *Research at Facebook*, que tiene como función principal el estudio de las modalidades en las que se relacionan los seres humanos para proveer no sólo hipótesis sobre ciertos campos específicos, sino análisis y procesos directos sobre ciertas tendencias que se pueden implementar a la hora de elegir, por ejemplo, marcas o en campañas electorales; a saber, bajo la impronta de "comprender el mundo"[2] en su totalidad, generan también saberes específicos a través de los datos almacenados. El caso concreto que queremos mostrar en la presente ponencia es una serie de investigaciones que se realizaron en torno al uso del botón "Me gusta" de *Facebook* ; en esta, específicamente, se puede observar no sólo cómo se da todo una modalidad de *visibilizar* objetos, en el caso concreto los gustos, sino modos de *hablar* o de trabajar con los mismos: en este campo, de igual manera, nos resulta bien interesante analizar cómo se inscriben dentro de una serie de rasgos de una racionalidad algorítmica.

DETRÁS DE LOS "ME GUSTA" DE *FACEBOOK*

Ya se trate del consumo del entretenimiento, las compras que se realizan, la forma de relacionarse con los demás, y en sí una gran cantidad de actividades humanas, todas estas pueden hoy día ser medidas, calculadas y analizadas gracias a los dispositivos digitales que permiten la recolección de grandes cantidades de datos al respecto: no sólo por transacciones bancarias que se realizan, sino por la interacción misma que se tiene a través de la navegación misma por la Web: tanto en páginas que se visitan, su frecuencia y permanencia, interacción con otros usuarios, etc. La medición de dichos comportamientos ha generado el desarrollo de distintas herramientas metodológicas como la computación social, que surge como mezcla entre la economía computacional y la cliodinámica; la medición a través de motores de búsqueda personalizados y diferentes sistemas que se despliegan a partir de la recomendación individualizada, utilizada por diversas plataformas y que se erige como una de las modalidades de comercio más usada en la Web; y la comercialización dirigida, que ha precisado de un estudio detallado e individualizado de los usuarios.

Bajo esa rúbrica, en el año 2013 se realizó un estudio por parte de una serie de científicos de la Universidad de Cambridge, encabezados por el neuropsicólogo M. Kosinski, con un número determinado de usuarios de *Facebook* a quienes se les aplicó un experimento piscométrico que tenía la función de analizar el registro de datos que tienen del uso del botón "Me gusta" de *Facebook* para estudiar el comportamiento de los mismos. Dicha investigación no resulta para nada novedosa. Por el contrario, se inscribe en una larga tradición de estudios que se han propuesto analizar y formular modelos de predicción de los comportamientos de los usuarios para ser usados en investigaciones concernientes tanto al campo de la economía, como la sociología, la política. Se pueden mencionar trabajos, entre otros más, que han intentado rastrear y extraer información que permita generar campos predictivos a través de los textos escritos biográficos en distintas plataformas, como blogs y demás tal como lo muestra Fast (2008); el uso de pruebas psicométricas directas y aplicadas por distintos medios, o el análisis de los modos en que se construyen espacios personales, como las habitaciones, oficinas, etc., tal como lo muestra Gosling (2002).

La constante y en gran escala utilización de medios digitales, en distintas plataformas y modalidades –como celulares y diferentes dispositivos digitales—también ha impulsado la aparición de estudios que procuran el análisis de las predicciones de los comportamientos a través de distintas acciones que tienen los usuarios. Una de las más analizada, justamente, tiene que ver con el estudio de los sitios de navegación (Hu, Zeng, Li, Niu y Chen, 2007), el contenido de sitios personalizados (Marcus, Machilek y Schütz, 2006) o en sitios específicos como las redes sociales, ya sea a partir de la cantidad de amistades que se tienen, tal como lo han mostrado los estudios de Quercia, Lambiotte, Kosinski, Stillwell y Crowcroft (2012), o el de Bachrach, Kohli, Graepel, Stillwell, Kosinski (2012); la construcción misma de los perfiles, como en el caso de Quercia, Kosinski, Stillwell, Crowcroft (2011) o su interacción con el entorno mismo de las plataformas y otros usuarios, tal como lo plantean Golbeck, Robles, Edmondson y Turner (2011).

Teniendo como base, pues, el hecho de que existen registros digitales que son capaces de suministrar no sólo herramientas, sino posibilidades metodológicas para estimar con precisión una gran cantidad de atributos y comportamientos personales que son considerados dentro del ámbito de lo privado –sin que ello deje de ser problemático desde un punto de vista ético-legal, tal como lo indican Narayanan y Shmatikov (2008) — el estudio que se realizó sobre los "Me gusta" de *Facebook* apunta poder extraer perfiles procesados sobre comportamientos individualizados y colectivos a partir de la manifestación de las preferencias de contenidos que están presentes en la plataforma y en la Web –debido a que el protocolo *Open Graph* permitió la expansión del botón "Me gusta" a distintas plataformas, como ya lo señaló Roosendal (2011).

Dicho uso, determinado a partir de una herramienta que, básicamente, consiste en la recopilación de datos que manifiestan los usuarios de *Facebook* sobre preferencias de contenidos que van desde amigos, fotos, páginas externas, productos, música, comida, etc., permite el registro digital de una serie de actividades y manifestaciones, cuya capacidad de predecir eventos futuros –ya se trate de la compra de un producto o cierto nivel de riesgo para una agencia de segu-

ridad—es mucho mayor con respecto a otras formas de predicción en entornos específicos de la red social. Utilizando distintos métodos de análisis, entre los que cabe mencionar el *Five Factor Model* para los modelos de personalidad, las Matrices de Raven Progresivo Estándar (SPM) para medir los modelos de inteligencia, o las LOC (*Lines of Code*) para medir las escalas de SWL (Lenguaje corto de la Web), la base de datos de los gustos permitió a Kosinski (2013) plantear un modelo de identificación a partir de los datos expresados por los usuarios, que se consideran especialmente intrusivos, de predicciones de distintos factores como la orientación sexual, el origen étnico, las opiniones políticas, la religión, niveles de inteligencia, aspectos de la personalidad como la satisfacción con la vida, el consumo de sustancias –como alcohol, drogas, cigarrillo—, años que permaneció con los padres, así como aspectos demográficos más globales como edad, género, modos de relación con otros usuarios, etc.

El estudio, por ende, se basó en una muestra de 58.466 voluntarios y usuarios de *Facebook*, mayoritariamente provenientes de Estados Unidos, que, al tener un promedio de 170 gustos manifestados aproximadamente en el mes inmediatamente anterior al estudio, cedieron el registro de sus preferencias y realizaron a la par una prueba psicométrica que permitió contrastar la información extraída producto del análisis de los "Me gusta".[3]

El estudio produjo un aplicativo que permitía analizar las variantes dicotómicas medidas y luego arrojaba una matriz de resultados, teniendo como base general una división entre hombres y mujeres. Dichos resultados lograron, pues, medir variables que posibilitan la identificación de distintos rasgos de la personalidad de perfiles de usuarios, que al contrastarse con la prueba psicométrica que se les realizó, pudo determinar un alto grado de asertividad. Así, por ejemplo, se identificaron en un 95% de los casos el género del usuario; su creencia religiosa, medida sobre cristianos y musulmanes, tuvo un acierto del 82%; las tendencias políticas, con variables como demócratas o republicanas, obtuvieron un 85%; la orientación sexual en varones fue de un 88% y en mujeres de un 75%. Otros factores demográficos como el estado civil y el consumo de sustancias fue acertada en un 65% y un 73% respectivamente y la permanencia con los padres, cuya medida estándar fue de 21 años, en un 60%; estos elementos, que no gozaron de tanta asertividad, dependen de una variabilidad o de un estudio que determine un periodo de tiempo más prolongado.

En relación a factores específicos de la personalidad, como la inteligencia o el grado de felicidad, fueron determinados a partir de distintos matices predictivas debido a las variaciones en los cambios de humor, y el registro de los "Me gusta" fue tomado a nivel estándar y por lo tanto permitía medir a nivel general sus niveles de felicidad, por ejemplo, y no tanto en el momento del estudio; es decir, no se tuvo en cuenta la posibilidad de variaciones constantes en los gustos, sino que se lo pensó como algo fijo y estándar dentro de periodos de tiempos prolongados.

Los vectores estudiados que determinan los rasgos de la personalidad usados en el estudio varían de acuerdo a los métodos utilizados; de esta manera, por ejemplo, para el nivel de inteligencia se tuvieron en cuenta gustos de la "lluvia" o relacionados a las ciencias para niveles

superiores, o relacionados a ser "mamá" o gustos por la motocicletas con niveles más bajos; para la identificación de rasgos en términos de inclinaciones sexuales se tuvieron en cuenta, en el caso de los varones, gustos asociados a cosméticos y ciertas músicas –como el rap, hip-hop para la heterosexualidad—o el gusto manifiesto por N0 H8, o campañas asociadas al matrimonio Gay o músicas como Britney Spears. Para determinar otros rasgos específicos de la personalidad, se tuvieron en cuenta gustos relacionados a marcas como Hello Kitty, asociadas a un alto nivel de agradabilidad, pero a una baja estabilidad emocional. En relación a temas políticos, el agrado a Obama fue asociado a una tendencia democrática, aunque también cristiana, de descendencia afroamericana y personas homosexuales.

En definitiva, se tomaron una serie de vectores que se analizaron y asociaron a unos rasgos de personalidad y a una *predictividad* de posibles acciones y comportamientos también a futuro. El estudio de estos patrones y vectores que se usan para determinar los rasgos en personalidad puede permitir una comprensión más detallada de valores asignados a productos culturales de acuerdo a dinámicas, muchas veces, diferenciadoras de acuerdo a su modo de uso y a criterios sociales, tal como ha sido planteado por Bourdieu (1998); sin embargo, se trata de algo que dejaremos de soslayo.

En cierta medida, en el estudio se reconoce el hecho de que si bien es necesario otro tipo de análisis y pruebas para determinar con más precisión factores de la personalidad de los usuarios, se revela cómo el análisis de los datos asignados por el uso del botón "Me gusta" de *Facebook* puede tener el potencial de identificar rasgos y atributos del comportamiento de los perfiles de la red social. Entre los posibles usos que puede tener este tipo de estudio y de aplicativo se destaca el mercado, ya que permite sobre todo una mejor precisión en lo que respecta a la adquisición de servicios y productos. También puede ser utilizada, indican, para rediseñar nuevos modelos de medición de patrones psicológicos, aunque, todo ello centrado en la posibilidad de mejorar técnicamente la función del botón "Me gusta" y precisarlo aún más –algo que ha venido sucediendo con la posibilidad de manifestar más reacciones a los contenidos. También dentro del estudio se menciona la posibilidad de de convertirse en una herramienta útil para las agencias de seguridad nacional, por cuanto puede predecir con alta fidelidad riesgos potenciales en los individuos que se derivan de sus comportamientos: se menciona, por ejemplo, la posibilidad de identificar a alguien neurótico y de poder suministrarle la atención requerida. Se sugiere, de igual manera, la posibilidad de rastrear tendencias no sólo a nivel individual, sino de población; esto es, un análisis de metadatos y de minería de datos a partir de este procesamiento.

El estudio no niega, por su parte, posibles consecuencias en el uso del aplicativo. Ya se trata de empresas, instituciones estatales, o personas pueden acceder a información sensible y convertir esta función en una amenaza para las libertades individuales (Kosinski, 2013). Sin embargo, hace la salvedad el estudio de cómo cada vez es más difícil para los usuarios controlar la información que se suministra a terceros; no quiere decir que sea una situación que no se pueda remediar y que incluso pueda poner en riesgo el uso mismo de la tecnología, sino que se debe

generar cada vez más confianza en el uso de las tecnologías con el objetivo de mejorar y superar los riesgos digitales, aún cuando el estudio y aplicativo que presentan ya es en sí un riesgo.

Lo interesante para nosotros, adicional a esta advertencia que se realiza sobre los riesgos de vigilancia que presente el aplicativo y el estudio, es observar cómo se configura como una herramienta que plantea una manera de procesar y analizar una serie de datos para ponerlos a circular; más aún, adicional a poner en evidencia una serie de datos almacenados, de procesarlos y convertirlos en fórmulas y análisis biométricos, se puede observar cómo se sustentan en factores deterministas como el hecho de que por darle preferencia a temas relacionados con ser mamá se considera a un usuario de menor inteligencia. Es bajo esta operación que consideramos que dicha tecnología se constituye como un campo de visibilidad de aspectos de los individuos que procuran una subjetivación. Esta operación, como lo vimos, se realiza mediante el uso de una serie de operaciones conceptuales previas al estudio mismo que van más allá de los métodos y herramientas utilizadas de la psicometría y demás. Se trata, en especial, de la noción que se tiene sobre el gusto no ya sólo como una cuestión puramente determinante y diferenciadora de un sector social, sino entendido como un dato posible de ser matematizado y que refiere a una potencia del individuo; ambas, queremos plantear, devienen de un *gobierno algorítmico* cuyos rasgos más importantes apuntan a establecer procesos racionales matemáticos como ejes de verdad indiscutibles.

EL GOBIERNO ALGORÍTMICO Y EL GUSTO COMO DATO

Una de las hipótesis que se puede interpretar de todo este proceso de producción de campos de saber-poder a través de un trabajo de identificación, rastreo, almacenamiento, producción sobre los datos es la de un *gobierno algorítmico*. Es Rouvroy (2008) quien acuñó el concepto de "gubernamentalidad algorítmica" a partir de trabajo sobre los modos de ejercicio de poder en la biopolítica, desarrollado por Foucault en los cursos en el Collège de France entre 1976-1980. Con este concepto quiere dar a entender la existencia de un gobierno estadístico que es capaz de rastrear, de manera readaptable, a toda la población. Este rastreo se lleva a cabo a través de saberes que están por fuera del individuo mismo y que se enfocan en elementos pre-individuales de los sujetos, como lo puede ser el caso de los gustos e intereses. De esa manera, lo define como "cierto tipo de racionalidad (a) normativa o (a) política que reposa sobre una recolección, agregación y análisis automatizada de datos en cantidades masivas de modo que se pueda modelizar, anticipar y afectar, por anticipación, los comportamientos posibles" (Rouvroy y Berns, 2015: p. 41). Es decir, es una forma de ejercer el gobierno a partir de los datos y no tanto de los sujetos directamente –algo que era mucho más característico de las sociedades disciplinarias que planteó Foucault en *Vigilar y castigar*.

Si bien desde el siglo XIX se inició un gobierno que tenía como base la estadística, la característica fundamental del modo de operación de la gubernamentalidad actual es la centralidad que tienen los algoritmos. Tal como lo plantea Desrosières (2004), la razón estadística es una

forma de comprensión de los modos de ver que tienen las sociedades y la generación de representaciones a partir de conceptos, índices, tablas, gráficos que se inició a partir del siglo XVIII con la noción de probabilidad. Sin embargo, la operación actual estaría descentrada de la mirada humana, para ser administrada por máquinas informáticas, cuya capacidad de análisis de datos es inmensamente superior.

Así, pues, esta extracción automatizada de datos "pertinentes" de usuarios cuya finalidad, como lo hemos señalado, incluye actores políticos y mercantiles, tiene para Ruvroy y Berns (2015) por lo menos tres consecuencias inmediatas; o si se quiere, tres efectos sobre la sociedad. La primera de ellas consiste en la creación de una dupla de lo real. Este procedimiento consiste en una serie de operaciones que se inician con una recolección de datos cuyo ejemplo se ve en la existencia de los *data warehouses*, elementos constitutivos de la denominada *Big data*. Estos datos son utilizados como elementos que han sido vaciados de su contexto y con ello se ven reducidos a su "naturaleza más bruta". De esta manera, estos datos son trabajados por las distintas entidades como una materia absolutamente objetiva sobre la realidad misma.

Todo el trabajo de extracción y almacenamiento sobre información de los usuarios, en las que claramente es un ejemplo el funcionamiento de los "Me gusta" de las distintas redes sociales y de la navegación de la Web en sí, es producto de programas que son capaces de reconocer esas mismas emociones y comportamientos y transformarlos en un plano estadístico que permita no sólo una finalidad comercial –como calcular las probabilidades de venta de un producto o su receptividad—, sino para realizar ejercicios de gubernamentalidad como muestras de intenciones de voto, tendencias ideológicas, etc. Lo interesante para Ruvroy y Berns (2015) es que este dato comporta por lo menos dos características fundamentales: por un lado, una supuesta *inofensividad* y una especie de *objetividad* que evita y borra cualquier rastro de subjetividad.

La principal consecuencia de la supresión de las huellas del sujeto es la desaparición de la figura del hombre –tal como se ha comprendido a partir del siglo XVIII, como bien lo ha explicado Foucault en sus *Palabras y las cosas*. Este procedimiento se lleva a cabo al centrar los "comportamientos", y en especial sus huellas, de un usuario y una colectividad como un aspecto de lo real. Puede entenderse como una "abstracción" del dato puro que tiene la pretensión de dar cuenta de la realidad misma. El desplazamiento de un poder sobre los individuos, propio de las sociedades disciplinarias, queda ahora centrada en los datos objetivos o huellas de los mismos, que no son otra cosa que sus comportamientos convertidos en datos estadísticos y probabilísticos, tal como sucede en el momento de extracción de los intereses de usuarios a partir de los "Me gusta" de las redes sociales y de la web.

Además de la operación de recolección de datos, cuyas consecuencias son poner como eje central datos objetivos que vienen a dar cuenta de la realidad, Ruvroy y Berns (2015) indican que hay una operación de procesamiento y análisis de dichos datos, denominada *data mining*, o minería de datos, cuyo objetivo más relevante es hacer que surjan relaciones entre los datos mismos. La búsqueda de conexiones, coincidencias, rupturas, en fin, todo la operación de correlación

de los datos almacenados a partir de su procesamiento tiene la función de "producir un saber" estadístico que se elabora a partir de las correlaciones de informaciones heterogéneas. Lo fundamental de esta operación es que esta producción de saber, que podía encontrarse antes en ciencias como la medicina, ciencias judiciales, pedagógicas, es ahora automatizado por medio de algoritmos; es decir, es un saber producido con una intervención mínima de la mirada humana y, como lo indicamos anteriormente, evitando cualquier forma de subjetividad.

Al contar con una gran cantidad de datos almacenados sobre comportamientos, en el caso concreto sobre los intereses develados en los "Me gusta" de las redes sociales y de las páginas web, no sólo se puede observar que hay un almacenamiento y procesamiento de dicha información. En un tercer momento de la existencia de las bases de datos Ruvroy y Berns (2015) señalan ciertas acciones sobre estos comportamientos, como lo puede ser la creación de perfiles sobre las huellas mismas encontradas, así como la elaboración de contenidos y tendencias producidas por el trabajo sobre las intenciones mismas en una constante retroalimentación. Se percibe, entonces, una constante acción sobre los comportamientos: se intensifican las necesidades, se suprimen los elementos no deseados, se persiguen los comportamientos considerados como peligrosos, etc.

Tenemos entonces, en un primer nivel de análisis de Ruvroy y Berns (2015), el manejo de los datos que se realizan en la gubernamentalidad algorítmica, en donde encontramos una extracción y almacenamiento, procesamiento y producción de saber y una actuar sobre estos datos extraídos, que no son otra cosa que las huellas de los usuarios, sus comportamientos puestos en datos y estadísticas. Sin embargo, los efectos de este trabajo sobre los datos con operaciones automatizadas van mucho más allá de este primer nivel.

Una segunda consecuencia que señalan Ruvroy y Berns (2015) tiene que ver con el hecho de que al plantearse una extracción de datos como central para dar cuenta de lo real y, al mismo tiempo, ser un algoritmo el que realiza las operaciones de análisis y de acción, tenemos que hay una especie de "gobierno sin sujeto". El trabajo sobre los datos lo que hace es contornar y evitar a los humanos; al alimentarse de datos "infraindividuales" que aisladamente son insignificantes, crea perfiles de comportamientos que son "supraindividuales", que van más allá de los individuos concretos, y bajo esa operación evita el contacto o interpelación directa a cualquier sujeto: "pero sin jamás convocarlo o darse cuenta por sí mismo de aquello que es, ni aquello en lo que podría convertirse" (Rouvroy y Berns, 2015: p. 40).

No quiere decir esto que exista una supresión de los sujetos, como entidades concretas individuales. Por el contrario, lo que señala Ruvroy (2008) es que hay un surgimiento de "hipersujetos" en donde adquieren forma únicamente como potencia; es decir, como producción de sujetos que están centrados no tanto en lo que son, o en el *presente* que los atraviesa, algo que es mucho más característico en las sociedades disciplinarias, tal como lo planteó Foucault en su curso de 1978, sino en lo que *van* a hacer, en su *futuro* : es decir, el gobierno algorítmico se enfoca en las potencias de los sujetos, en sus acciones a largo plazo, en lo que pueden comprar, en lo

que pueden hacer, pues es justamente esta la finalidad que se encuentra en el saber en torno a qué tipo de producto le gusta a un usuario específico o qué tipo de ideología comporta cierta población en el mundo.

Los efectos de este centramiento en las potencias de los usuarios, en sus propensiones y no tanto en sus acciones, genera que la gubernamentalidad algorítmica produzca una realidad "aumentada", una "memoria del futuro" que debe comprenderse como un "acaso" sistematizado. Las normas se anticipan, lo real se convierte como en aquello que es posible, elementos sobre el que comienzan a deslizarse los sujetos mismos. Todo ello se da, indican Ruvroy y Berns (2015), debido a que nunca antes había surgido una tecnología que registrara, clasificara y evaluara los "sueños", los intereses y los gustos, aquello que se proyecta hacia el futuro.

En síntesis, la supresión de los sujetos como objeto de acción directa de la gubernamentalidad implica un trabajo directo sobre las relaciones que se ponen en juego tras la extracción de información. Los datos los entienden Ruvroy y Berns (2015) como puras relaciones, o mejor dicho, cruces de informaciones; los saberes que se producen son "relaciones" de las "relaciones", y las acciones normativas se aplicarían al producto de los saberes que arrojan los entrecruces de datos. De esa manera, la gubernamentalidad algorítmica se centra en un trabajo en el que los seres humanos se tornan invisibles, pues solo se registran sus datos, y a la vez, aparece la potencia hacia el futuro, las probabilidades de acción, como el elemento central sobre el que se debe actuar. Las consecuencias más inmediatas es que los sujetos se tornan inoperantes en este nuevo tipo de ejercicio del poder, así como sus acciones y su tiempo presente se diluye en las acciones que probablemente haga en un futuro, cuyo ejemplo más determinante es la centralidad que tiene hoy día las compañías de seguros, determinantes de lo que se debe considerar como la vida. Ahora bien, este tipo de poder, que a diferencia de las sociedades disciplinarias no está centrado en el *presente* de los cuerpos, recae sobre los sujetos y deja unas marcas sobre sus identidades y modos de ser.

A MANERA DE CONCLUSIÓN

El surgimiento de la estadística determinó no sólo mecanismos y herramientas para la constitución de los estados, sino que también instauró lógicas y modos de pensar que fueron volviéndose imperantes. La cientificidad pasa por allí y la construcción de subjetividades no está pensada de otro modo: el cálculo de lo que puede ser probable no sólo se ha vuelto una necesidad estatal, sino una lógica que carece de duda y escepticismo. Al haber eliminado la huella humana, el algoritmo se erige en razón suficiente y muestra indiscutible de verdad. Así, por ejemplo, el rastreo de los "Me gusta" de los usuarios, su procesamiento y análisis es capaz de *hablar* con más eficacia sobre los individuos que pruebas psicométricas o que, incluso, lo que él mismo puede decir sobre sí. No obstante, al hacer un rastreo breve sobre el modo de construcción del algoritmo mismo, se puede observar que responde a lógicas para nada supra-humanas: por el contrario, hacen hincapié, y refuerzan, patrones y estereotipos socialmente dominantes. Es decir, la

programación finalmente es hecha por un *hombre*, cuyos algoritmos no dejan de reflejar aquello que considera normal, mejor, peor, feo o bonito. Así, la supuesta racionalidad algorítmica, erigida como una luz de verdad, al tocarse los entramados de su interior, no puede ocultar su teatralización.

Por otro lado, consideramos que es justamente en la posibilidad de hacer ver zonas antes oscuras y en hablar sobre ellas, como es el caso específico del gusto, en donde se estructuran las redes sociales como focos de poder; a saber, como productoras también de modos de ver y de hablar sobre los individuos: tomados ahora como datos potenciales. Esto, por su parte, se determina al estudiar el fenómeno más allá del riesgo inmanente de la propiedad privada que supone la circulación de los datos a agentes externos; se hace, como vimos, al estudiar el modo de funcionamiento interno de la plataforma y los núcleos de saber que dentro de la misma se realizan: la consideración, entonces, de que son dispositivos de control, creemos, pasa por allí.

NOTAS

* Estudiante de la Maestría en Comunicación y cultura de la Facultad de ciencias sociales de la Universidad de Buenos Aires. Correo: jcgomezba@gmail.com

1. La información detallada se puede encontrar en: https://www.facebook.com/principles.php

2. Muchos de estos informes y análisis realizados se pueden encontrar en: `https://research.facebook.com/datascience` (fecha de consulta, agosto, 2015).

3. Toda la información detallada, tanto del estudio, como de los resultados puede consultarse en: `http://www.mypersonality.org/wiki`, fecha de consulta, octubre 2015.

REFERENCIAS

Berns, T., y Rouvroy, A. (2015). Gubernamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação e la relação. *Revista Eco Pós: Tecnopolíticas e vigilância*, 18(2), 36-56.

Bachrach, Y., Kohli, P., Graepel, T., Stillwell, DJ., y Kosinski, M. (2012) Personality and patterns of Facebook usage. *ACM Web Science Conference.* Proceedings of the ACM Web Science Conference, 36–44. Recuperado de: `http://www.websci12.org/paper-sessions`

Bourdieu, P. (1998). *La distinción*. Madrid: Taurus.

Chaverry, R. (2013). "Redes sociales. Hacia una nueva subjetividad de la vigilancia". En Constante, A. (coor.) *Las redes sociales: una manera de pensar el mundo* (pp. 37-50) Universidad Autónoma de México. México: Ediciones sin nombre.

Chen, Y., Pavlov, D., y Canny, J., (2009). Large-scale behavioral targeting. *International Conference on Knowledge Discovery and Data Mining*, 209–218. Recuperado de: `http://www.kdd.org/kdd-cup`

Constante, A. (2013). "¿Qué son las redes sociales?", En: Constante, A. (coor.), *Las redes sociales: una manera de pensar el mundo*. (pp. 13-33). Universidad Autónoma de México. México: Ediciones sin nombre.

Deleuze, G. (1987). *Foucault*. Barcelona: Paidós.

Desrosières, A. (2004). La política de los grandes números: historia de la razón estadística. Barcelona: Melusina.

Fast, L., y Funder, D. (2008). Personality as manifest in word use: Correlations with self-report, acquaintance report, and behavior. *J Pers Soc Psychol* 94(2), 334–346.

Golbeck, J., Robles, C., Edmondson, M., y Turner, K. (2011) Predicting personality from Twitter. *IEEE International Conference on Social Computing*, pp 149–156. Recuperado de: http://www2016.ca/organization/past-www-conferences.html

Gosling, S., Ko, S., Mannarelli, T., y Morris, M. (2002). A room with a cue: Personality judgments based on offices and bedrooms. *J Pers Soc Psychol*, 82(3), 379–398.

Hu, J., Zeng, H., Li, H., Niu, C., y Chen, Z. (2007) Demographic prediction based on user's browsing behavior. *International World Wide Web Conference*, 151–160. Recuperado de: http://www2016.ca/organization/past-www-conferences.html

Kosinski, M., Kohli, P., Stillwell, D., Bachrach, Y., y Graepel, T. (2012). Personality and website choice. *ACM Web Science Conference*, pp 251–254. Recuperado de: http://www.websci16.org/paper-sessions

Lasalle, M. (2015). "Facebook como dispositivo de seguridad: una aproximación al estudio de las actuales sociedades de control". En: *Hipertextos*, 4(2). Recuperado de: http://revistahipertextos.org/wp-content/uploads/2015/12/Facebook-como-dispositivo-de-seguridad-Martina-Lassalle.pdf

Lyon, D. (1994). *The Electronic Eye*. Minneapolis: University of Minnesota Press.

Marcus, B., Machilek, F., y Schütz, A. (2006) Personality in cyberspace: Personal Web sites as media for personality expressions and impressions. *J Pers Soc Psychol* 90(6), 1014–1031.

Marinucci, M. (2010). "You can´t front on Facebook", En: Wittkower, D., (ed.) *Facebook and Philosophy: What´s on your mind?* Chicago: Open Court

Narayanan, A., y Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *IEEE Symposium on Security and Privacy*, 111–125. Recuperado de: http://www.ieee-security.org/TC/SP2008/oakland08.html

Quercia, D., Kosinski, M., Stillwell, D., y Crowcroft, J. (2011). Our Twitter profiles, our selves: Predicting personality with Twitter. IEEE International Conference on Social Computing. Proceedings of the 2011. *IEEE International Conference on Social Computing*, 180–185. Recuperado de: http://www.ieee-security.org/TC/SP2011/

Quercia, D., Lambiotte, R., Kosinski, M., Stillwell, D., y Crowcroft, J. (2012). The Personality of popular Facebook users. ACM Conference on Computer Supported Cooperative Work. Proceedings of the ACM 2012. *Conferenceon Computer Supported Cooperative Work*, pp 955–964. Recuperado de: http://cscw2012.org/program/papersnotes.php

Roosendal, A. (2011). Facebook tracks and Traces Everyone: Like This. En: *Tilburg Law School Legal Studies Resarch Paper Series*, 3 Tilburg University. Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563

Rouvroy, A. (2008). *Human Genes and Neoliberal Governance: A Foucauldian Critique*. Routledge-Cavendish: New York.

Wandel, T. y Beavers, A. (2010). "Playing Around with Identity". En: Wittkower (ed.) *Facebook and Philosophy: What´s on your mind?* Chicago: Open Court.

Zukerfeld, M. (2010). *Capitalismo y conocimiento: materialismo cognitivo, propiedad intelectual y capitalismo informacional* (Tesis doctoral), FLACSO, Argentina.

REACCIONES PÚBLICAS ANTE LAS REVELACIONES DE SNOWDEN: LOS MEMES DE INTERNET COMO INDICIO

Resumen: El objetivo de este trabajo es analizar los memes de internet como modo de reconocimiento y comentario de noticias periodísticas de alto impacto mundial. Específicamente, estudiaremos memes de tipo "imagen estática + texto" sobre las revelaciones de Edward Snowden acerca de los programas de vigilancia masiva de la *National Security Agency* (NSA), de Estados Unidos. Entre las conclusiones del estudio se destaca que, lejos de representar una forma de resistencia a la violación de derechos humanos denunciada por Snowden, algunos memes constituyeron solo una excusa para hacer juegos de lenguaje o consolidar la pertenencia a ciertas subculturas. Y que aunque lo denunciado por Snowden afectara a todo el globo, la reacción discursiva en forma de memes tematizó primariamente sus implicancias solo para Estados Unidos.

Palabras clave: Memes de internet, Snowden, Vigilancia, Privacidad, Espionaje.

Public reactions to Snowden's revelations: Internet memes as a clue

Abstract: The purpose of this study is to analyze internet memes as a way of reckoning and commenting worldwide high-impact journalistic news. Specifically, we study memes structured as "static image + text" about Edward Snowden's revelations of United States' National Security Agency (NSA) mass-surveillance programs. Among our conclusions, we can mention that far from representing a way of resisting against the human rights violation reported by Snowden, some memes are only an excuse to produce language games, as well as to reinforce belonging to certain subcultures. Besides, even though what Snowden denounced affected the entire world, some meme-shaped discursive reactions thematised its implications for the United States only.

Keywords: Internet-memes, Snowden, Surveillance, Privacy, Espionage.

As reacções públicas para as revelações de Snowden: memes da Internet como indicaçãos

Resumo: O objetivo deste estudo é analisar os memes da internet como forma de avaliar e comentar notícias jornalísticas de alto impacto em todo o mundo. Especificamente, estudamos memes estruturados como "imagem estática + texto" sobre as revelações de Edward Snowden dos programas de vigilância em massa da Agência de Segurança Nacional (NSA) dos Estados Unidos. Entre as nossas conclusões, podemos mencionar que, longe de representar uma maneira de resistir contra a violação dos direitos humanos relatada por Snowden, alguns memes são apenas uma desculpa para produzir jogos de linguagem, bem como para reforçar a pertença a determinadas subculturas. Além disso, embora o que Snowden denunciou afetasse o mundo inteiro, algumas reações discursivas em forma de meme criticavam suas implicações apenas para os Estados Unidos.

Palavras chave: Internet-memes, Snowden, Vigilância, Privacidade, Espionagem.

LAURA SIRI*

El objetivo de este trabajo es analizar sociosemióticamente ejemplos de memes de tipo "imagen estática + texto" que tratan sobre el escándalo de las revelaciones de Edward Snowden. Como se recordará, en 2013, este ex técnico de la CIA y del contratista de la *National Security Agency* (NSA) Booz Allen Hamilton contactó a los periodistas Glenn Greenwald y Laura Poitras y les entregó documentos sobre ciertos programas mundiales de vigilancia masiva por parte de los servicios secretos de Estados Unidos, Reino Unido, Nueva Zelanda, Australia y Canadá. Desde el punto de vista comunicacional, el asunto de Snowden es interesante porque es improbable que hubiera tenido la misma repercusión de no haberse publicado en grandes medios tradicionales. Sin embargo, el tema de la noticia se vinculaba con los peligros para la privacidad asociados al uso de nuevos medios. Asimismo, dicha repercusión se dio, en gran medida, a través de los mismos nuevos medios que estaban siendo cuestionados. En Facebook, por ejemplo, la primera nota en *The Guardian* fue compartida más de 103.000 veces antes de las 2PM, hora del este, del día de su publicación, junto con comentarios y memes que expresaban enojo, confusión y sorna (Kim, 2014). En Twitter, ese reportaje fue compartido más de 10.200 veces antes de las 10AM, hora del este, de dicha jornada. El hashtag #NSA alcanzó el primer lugar como *trending topic* del día y alcanzó 250 mil menciones en 24 horas. También fueron destacables las reacciones ante un tuit del actor Jason Biggs burlándose del eslogan publicitario "*Can you hear me now?*", de Verizon, que recibió 330 retuits y 130 favoritos en las primeras 24 horas. Similar repercusión se vivió en otras plataformas, como Reddit y Tumblr. También se destacó el blog de Tumblr *Obama is Checking Your Email*, lanzado el 8 de junio de 2013 para burlarse del presidente de Estados Unidos y de su participación en el escándalo. A lo largo de los meses se fueron revelando más documentos y programas secretos originados en Snowden y también se multiplicaron las controversias y reacciones sobre la evidencia de la vigilancia masiva por parte de corporaciones y gobiernos. De todas esas reacciones por parte del público, en este trabajo nos concentraremos en un tipo de discurso a menudo considerado marginal: los memes de internet, o imemes que, como dice Limor Shifman, son textos que, en muchos casos, proponen "cómo debería ser el mundo y cuál es el mejor modo de llegar allí" (Shifman, 2014: 120). Las características genéricas de este tipo de producciones en lo que hace a dispositivos, rasgos discursivos y prácticas sociales vinculadas ya han sido muy bien estudiadas por autores como Shifman (2013 y 2014), Knobel y Lankshear (2005 y 2008) y Marino (op. cit.), entre muchos otros.

Qué son los memes de internet

Según Gabriele Marino (2015: 50), los memes de internet: (i) son textos; (ii) pueden tener diferentes *sustancias expresivas*, usualmente sincréticas; (iii) que se derivan de un proceso de *intervención* sobre textos pre existentes (iv) de acuerdo con reglas de *pertinencia* y buena formación (v) caracterizadas por una *eficacia* colectivamente asignada y reconocida, así como (vi) por tener un espíritu juguetón, (vii) por la *anonimidad* del creador y (viii) por sus modalidades de difusión repetitivas, adaptativas, apropiativas y, en general, *participativas*. Los memes de internet, según Knobel y Lankshear (2008), se hacen con varios propósitos, principalmente expresar solidaridad o afinidad, hacer planteos políticos o, simplemente, para divertirse.

Conviene subrayar también que, para que algo sea un imeme, no precisa ser viral ni haber logrado propagarse. Lo que sí tienen en común es que siempre exhiben un *punctum* (cf. Barthes, 1989: 59), definible como algún tipo de incongruencia o error que llama la atención. Pueden ser errores gramaticales, como suelen tener los LOLcats, o ambigüedades, imágenes imposibles, exageraciones, inadecuaciones. Todos estos son, sin duda, mecanismos clásicos de otros productos culturales, como la comedia, pero no son necesariamente propios de cualquier producto de internet. En cuanto a formato, pueden ser en video, texto, imagen plana o combinaciones de estos elementos. Los subgéneros de imemes pueden definirse según cuán específicos sean sus temas y formatos. Con la aclaración de que no se trata de una clasificación exhaustiva ni un producto terminado, así es como la autora los distingue:

1) Subgéneros basados en la documentación de momentos de la "vida real" concreta y fuera de lo digital

   a) *Photo fads*: son fotos pose donde la gente imita posiciones o acciones específicas en diferentes situaciones.

   b) *Flash mobs*: cuando un grupo de extraños se reúne en un espacio público, realiza al mismo tiempo un acto particular y rápidamente se marcha. La reunión se coordina mediante mensajes de internet o celular, se registra y se manda a la Red el video o la foto.

2) Subgéneros basados en manipulación explícita de contenido visual o audiovisual proveniente de los medios masivos. Usualmente se apropian de noticias y otros productos de la cultura popular.

   a) *Lipdubs*: clips donde una persona o un grupo imita los movimientos labiales de cantar una canción popular.

   b) *Traducciones fonéticas*: videos con traducciones falsas y humorísticas de sonidos hablados o escritos, sin importar el significado real. También puede ser el subtitulado a otro idioma de un original cuya lengua se presume poco conocida, como el famoso "Hitler se entera de…".

   c) *Tráilers reeditados*: se trata de tráilers falsos de películas, basados en la reedición o remezcla de secuencias fílmicas. A veces se crean nuevas películas en base a otras dos.

   d) *Photoshops reactivos*: imágenes que usan Photoshop u otros programas de edición para resignificar fotos emblemáticas (como la "sala de situación" que muestra a la plana mayor de la Casa Blanca la noche de la muerte de Osama bin Laden).

3) Subgéneros nacidos del nuevo universo del contenido digital memético. Involucran una compleja grilla de signos que solo pueden descifrar los que están versados en cierta subcultura. En general, se originan en sitios específicos como 4chan, Tumblr y Reddit.

   a) *LOLCats*: imágenes de gatos acompañados de textos con errores gramaticales y ortográficos (un habla conocida en la jerga memética como *LOLSpeak*).

b) *Rage Comics*: dibujos estereotipados y de aspecto amateur que representan rostros expresivos, cada uno asociado con un comportamiento típico. Por ejemplo, Cara de Troll es un personaje enojado o amenazante. Se usan para calificar a los ganadores y perdedores de la vida real, en opinión del autor del meme.

c) *Personajes o iconos arquetípicos reutilizables* (*stock character macros*): se basan en imágenes reutilizables que representan personajes estereotípicos asociados con conductas determinadas, acompañadas de subtítulos relativos a cualquier temática, pero conservando el atributo o formato sintáctico asociado por convención. También se los llama "*Advice animals*" (animales consejeros), aunque no siempre incluyen consejos y los animales en cuestión pueden ser humanos.

Memes de la forma "imagen + texto"

Para este trabajo resultaron especialmente relevantes los imemes de los subgéneros 2d (Photoshops reactivos) y 3c (personajes arquetípicos). En general, ambos tipos asumen el formato de una imagen con un texto superpuesto (también pueden no incluir texto, pero es lo menos habitual).

La clave de la popularidad de los memes basados en imágenes estáticas es, según Tay (2012), que pueden comunicar significados e ideas en forma fácil y rápida, todo con un solo cuadro.

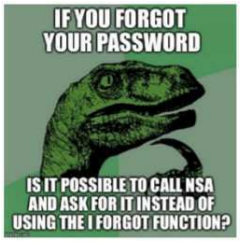
Lo que hicimos

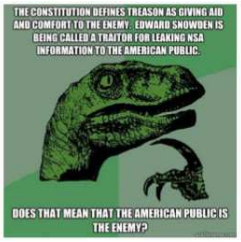
Para rastrear memes relacionados con las revelaciones de Snowden, primero se realizó una observación preliminar sobre cómo se los acostumbraba etiquetar en sitios como *memepedia, knowyourmeme, memecenter, memebase* o Reddit. En general, las etiquetas "NSA" y "Snowden" aparecieron como prevalentes. Dada la capacidad del buscador de imágenes de Google para reconocer este tipo de metadatos, así como su habilidad de recuperar archivos ubicados en una enorme cantidad de sitios diferentes, se buscaron allí las expresiones "NSA + meme" y "Snowden + meme". La búsqueda se realizó el 7 de febrero de 2016.

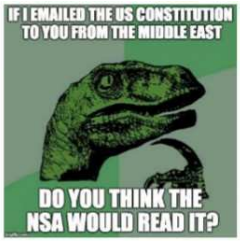
Aparecieron 518 resultados, de los cuales 150 se descartaron por 1) ser historietas firmadas por profesionales o autores de webcomics, no memes anónimos, 2) no estar realmente relacionados con el escándalo de la NSA, sino ser falsos positivos del buscador. De este modo, quedaron 368. Con excepción de muy pocos en castellano, alemán y ruso, todos los memes hallados estaban en inglés. Shifman justamente resalta que, aunque existen en todos los idiomas, predomina el inglés como *lingua franca*.

De los subgéneros que enumera la autora, no apareció ninguno del tipo 1 (situaciones de la "vida real"). La inmensa mayoría se basaban en Photoshops reactivos y personajes arquetípicos

reutilizables (subgéneros 2c y 3c). Por ejemplo, todos los de abajo se basan en el personaje arquetípico *Philosoraptor*.







Como queda claro, al ser los memes fenómenos instrínsecamente efímeros, hay que asumir que no necesariamente todos los algune vez producidos tendrían que aparecer en nuestra búsqueda, aunque más no fuese debido al tiempo transcurrido desde el escándalo noticioso que les diera origen. Y también se debe advertir de la posibilidad que la cantidad exacta de resultados hubiese podido variar de realizarse antes o después, como sucede con cualquier búsqueda online.

Se analizaron las siguientes cosas:

Nivel del dispositivo (En base a Fernández, 2008)
Textos escritos - imágenes - Espacio gráfico - Tratamiento de la imagen - Relación imagen/texto

Formato retórico (En base a Bremond, 1970 y Hamon, 1994: 45-60)

Argumentativo					Descriptivo	Narrativo
Tono del orador	Vía	Móvil				
Franco	Convencer	Pragmático	Ético	Hedónico		
Objetivo						
Cómplice	Conmover					
Otro						

Función predominante (En base a Jakobson, 1981)

Referencial	Emotiva	Conativa	Metalingüística	Poética	Fática

Operaciones de figuración (En base a Fernández y Tobi, 2009)

Construcción	**Referenciación**		**Inserción**	
Sustracción	Comparación	Contigüidad	Paradigmática	Sintagmática
Adjunción	Abstracción	Concreción	Expresión	Contenido
Conmutación	Condensación	Desplazamiento	Cápsula	Secuencia
Permutación	Ampliación	Atenuación		
Transmutación	Anclaje	Relevo		

Operaciones de tematización (En base a Segre, 1985 y Metz, 1978)
Tema [más allá de lo relativo a NSA y Snowden] – Estereotipos – Verosímiles – Motivos

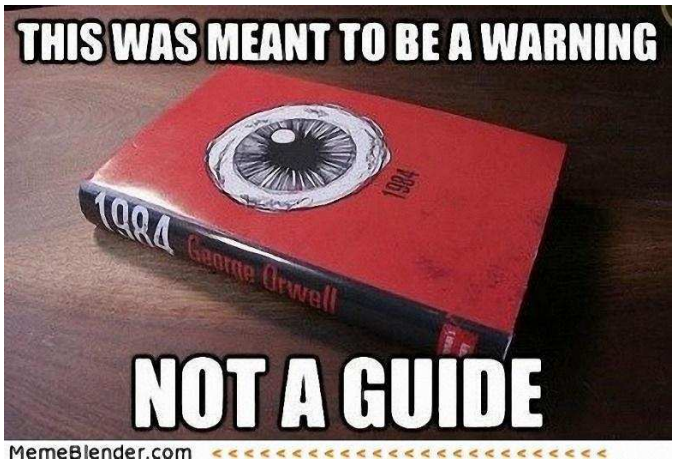
Operaciones de enunciación (En base a Fernández, 1994 y a Verón, 1985)

Simetría	Complementariedad
Sujeción	Independencia
Jerarquía	Igualación
Exclusión	Inclusión
Presuposición cultural	Presup. de segmento o tipo discursivo

A continuación, mostramos el análisis detallado de algunos ejemplos, dado que la extensión de este trabajo no nos permite tratarlos todos.

Detalle de cada ejemplo analizado

FIGURA 1
"Se suponía que esto fuera una advertencia, NO UNA GUÍA"



La Figura 1 muestra un ejemplar de *1984*, la novela distópica donde George Orwell mostraba un futuro caracterizado por la hipervigilancia. No es una imagen reutilizable, sino una foto sin manipulación digital, seleccionada específicamente para comentar el escándalo de Snowden. Como figura retórica, puede considerarse una inserción paradigmática que, para su interpretación, requiere conocer lo que connota. Para reforzar este esfuerzo por parte del enunciatario, la le-

yenda usa el deíctico *This*, en vez de decir "La novela 1984". El efecto de conjunto es argumentativo, con móvil ético. La tipografía es mayor en la segunda línea y, al subrayar que el libro no debía ser tomado como una guía, se dirige a un enunciatario que estaría haciendo exactamente eso. Un enunciatario que, si reconoce la inserción, es que sabe exactamente lo que hizo y que, por lo tanto, queda definido por sus acciones. No hay, en cambio, marcas del enunciador, que aparece como una genérica voz acusadora. Este imeme, por lo tanto, es una crítica pública al Estado y, aunque levemente irónica, es más un reproche que una broma. Es interesante también por lo que no dice: no tematiza exactamente cómo se habría tomado como guía para la realidad aquello que era una obra ficcional destinada a ser una advertencia. Se supone conocido tanto para el enunciador como para el enunciatario, así como para el paradestinatario que presenciaría este supuesto diálogo. En síntesis, indica que un verosímil construido para la ficción resultó serlo también en la realidad.

FIGURA 2

"La NSA está escuchando: quizá deberíamos usar el cono del silencio"

La imagen de la Figura 2 está tomada de la conocida serie de los '60 *El superagente 86*. Allí, cuando debían hablar de algo secreto acudían a un inútil y aparatoso dispositivo: el cono del silencio. Por lo tanto, no es una plantilla reutilizable, sino un reciclamiento de una pieza de cultura mediática televisiva, en una relación de puro anclaje con el texto, ya que no hace más que fijar su sentido sin añadir nada demasiado nuevo. Aunque el formato es argumentativo, el saber compartido acerca de la inutilidad que tenía en la serie el consabido cono permite interpretar que lo que podamos intentar para evitar que la NSA nos escuche es eso: inútil.

La tipografía es mayor en la primera línea, que establece el problema, que en la segunda, donde se propone la solución absurda, marcando una diferencia de importancia entre ambas. Lo que se tematiza es, por lo tanto, la omnipresencia de los oídos de la agencia. También se percibe el motivo del espionaje propio de la NSA y de Snowden, parodiado con la presencia de los conocidos personajes del "recontraespionaje" Maxwell Smart y el Jefe. La situación enunciativa presupone el conocimiento de la serie y simula un enunciador que aconseja y un enunciatario aconsejado. También, claro está, se presupone que el enunciatario está al tanto del escándalo de Snowden. Pero la misma ambigüedad creada por el motivo "espionaje" también permite entender que *we* no se refiere solamente al enunciador y el enunciatario genéricos, sino específicamente a los personajes bajo el cono. Este tipo de efecto polisémico es muy frecuente en los imemes. Como dice Shifman, por ejemplo, un imeme con Obama vestido de Jedi luchando con un sable lumínico puede ser una burla a su persona, pero también puede dar a entender que está del lado "bueno" de la Fuerza. La polisemia es parte del efecto gracioso.

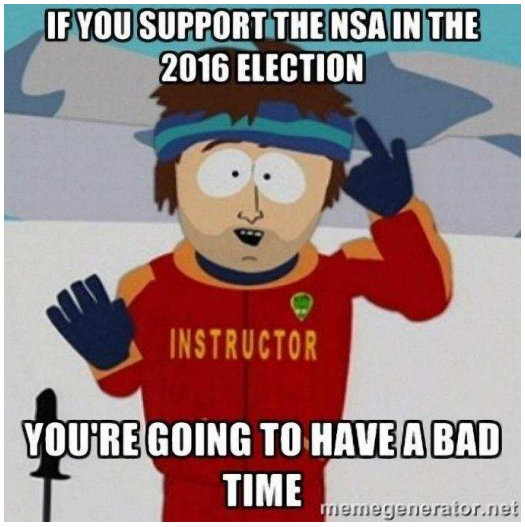
FIGURA 3
"No me asusta la NSA: uso el modo incógnito"

El imeme de la Figura 3 se basa en un personaje arquetípico reutilizable llamado *Idiota chica nerd*. En este esquema, la primera línea de texto usualmente contiene referencias a la *cultura geek* y, la segunda, demuestra falta de conocimiento real sobre el tema. En este caso, para entender la broma, hay que saber que el modo incógnito de los navegadores en realidad no protege en absoluto contra la vigilancia. Así, este imeme en particular no busca abogar contra el

espionaje hacia civiles comunes, ni promueve una acción colectiva, ni se expresa para cuestionar a nadie. Lo que en realidad hace es aprovechar el *trending topic* de las revelaciones de Snowden para reírse de las personas demasiado ignorantes sobre el funcionamiento de la Red. Con lo cual, está claro que hay complicidad entre enunciador y enunciatario. Pero el enunciador no coincide con quien dice *yo*. Por la escasez de contenido informativo de la pieza se puede decir que predomina la función fática.

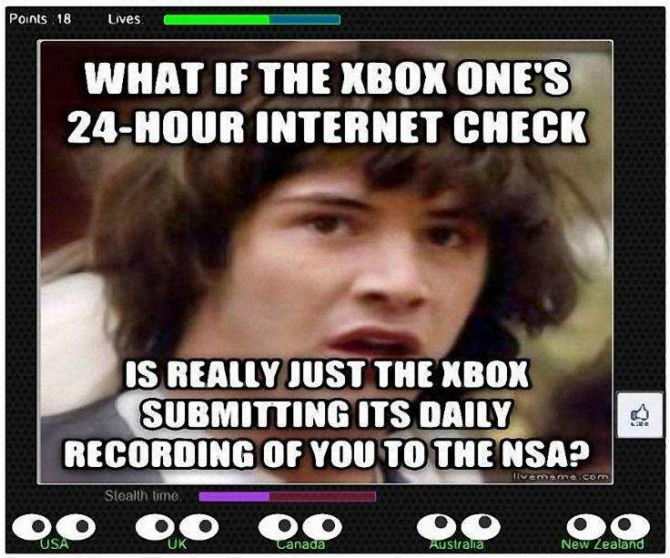
FIGURA 4

"Si apoyas a la NSA en la elección de 2016, la vas a pasar mal"



El meme de la Figura 4 está basado en la imagen reutilizable *Super cool ski instructor*, un *Advice Animal* (recordemos que esa categoría no excluye a los humanos) que parodia al instructor de esquí del episodio *Asspen* de la serie animada South Park, emitido por primera vez el 20 de marzo de 2002. La estructura de los textos acompañantes argumentativa: "si haces tal cosa desaconsejable, la vas a pasar mal". En el caso del ejemplo, lo que traería malas consecuencias sería "apoyar a la NSA en la elección [presidencial, EEUU] de 2016". El efecto cómico se realiza mediante una figura de supresión, por la cual el lector debe reponer algo que no se dice: que la NSA sería de algún modo "candidata" en esos comicios y que, si gana, sería muy malo. Esa reposición resulta cómica, asimismo, porque plantea la incongruencia de que el candidato no sea una persona física, sino una dependencia gubernamental ya existente cuya función es espiar. También juega con la ambigüedad ya que, si no se explicita a quién exactamente representaría a la NSA en los comicios, quiere decir que cualquiera de ellos es igual. Hay, por lo tanto, complicidad entre enunciador y enunciatario.

FIGURA 5
Keanu conspirativo



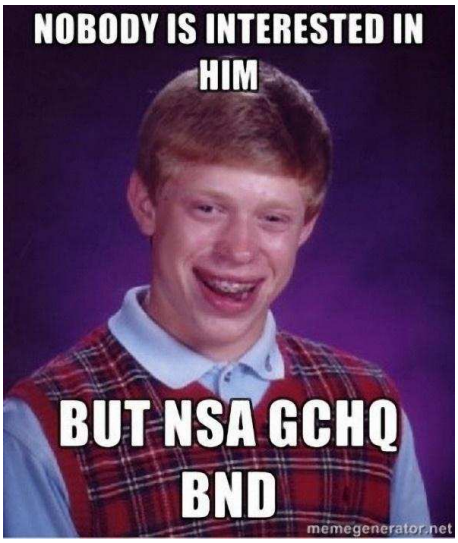
La base del imeme de la Figura 5 es el personaje arquetípico reutilizable *Conspiracy Keanu*, donde siempre aparece el actor Keanu Reeves con expresión de preocupación, acompañado de un texto con preguntas conspirativas. En el caso del ejemplo, la foto aparece con un marco negro donde se incluye el símbolo del *me gusta*, de Facebook y alusiones a los llamados *Cinco Ojos*: los países que formarían parte de la hipervigilancia global de los servicios secretos hacia personas comunes, según Snowden (Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda). En la parte superior de dicho marco se muestran alusiones a *puntos* y *vidas*. Abajo se indica un *stealth time*. El modo *stealth*, en los juegos, permite a un jugador mantenerse oculto ante los adversarios. De hecho, hay muchas alusiones a juegos de consola. A su vez, esto alude a uno de los documentos de Snowden, donde precisamente decía que las Xbox formaban parte del conjunto de dispositivos espiados por los servicios secretos. Todas estas alusiones dentro de alusiones hacen que solo quien esté al tanto de cierta estrecha intersección de referencias extratextuales pueda entender el conjunto. Básicamente, el efecto de sentido es que lo que parece un simple juego puede no serlo, o que mantenerse en modo *stealth* quizá proteja de la mirada de otros jugadores, pero no de los servicios de inteligencia. En cuanto a la situación enunciativa, aparece un enunciador que supuestamente duda y pregunta para que el enunciatario responda. Pero la pregunta presupone una respuesta afirmativa.

FIGURA 6
El paralelo entre Manning y Snowden

En el ejemplo de la Figura 6 predomina una figura de comparación: la antítesis, marcada por la oposición de elementos claros contra oscuros. El texto ancla lo expresado por la imagen, bajo la forma de paradoja. En efecto, la primera línea (letra negra sobre fondo blanco), dice "Si violas la privacidad del gobierno vas preso". Dicha línea se yuxtapone con una foto del soldado Manning, quien entregó a Wikileaks más de 800 mil documentos clasificados y que por ello fue condenado a 35 años de prisión. La segunda línea, en blanco sobre fondo negro, dice "si el gobierno viola la tuya, lo llama Ley Patriota" (que habilitó espiar a cualquiera). Se yuxtapone con el escudo de la NSA. Un epígrafe en letra chica deja ver el origen del imeme: la página en Facebook de *Mentally Emancipated*, un grupo libertario de derecha de Estados Unidos, afín al senador Ron Paul. Desde lo temático, prima la idea de la opresión del individuo por el estado, un verosímil ideológico frecuente en dicho movimiento. Entre los motivos se pueden mencionar la crítica a la violación de la privacidad individual y a la Ley Patriota. Como puede verse, hay una estructura argumentativa que expresa una paradoja, con un móvil pragmático, ya que resalta el resultado de acciones. En el caso de la primera línea, ese resultado es concreto: ir preso. En la segunda, es abstracto: reformular el sentido de la acción por medio de una operación de antífrasis. Dicha antífrasis funciona como una inserción sintagmática: hace sentido en el interior del texto. Pero la foto de Manning y el escudo de la NSA son inserciones paradigmáticas. Para entender la primera, es necesario conocer y recordar el escándalo de Wikileaks. Para entender la segunda, hay que estar al tanto del de Snowden y, además, poder hacer un parale-

lo entre ambos casos de fuga masiva de información. Asimismo, se observa una operación de condensación, en este caso una metáfora de personalización. En efecto, si uno puede violar la "privacidad" del gobierno, es que se asimila a éste con una persona. En cambio, la yuxtaposición del escudo de la NSA con la palabra *government* es una operación de desplazamiento, en este caso una sinécdoque, por la cual se identifica a todo un gobierno solo por una de sus dependencias: la agencia de espionaje. La situación enunciativa es tal que enunciador y enunciatario se suponen pertenecientes a un mismo grupo que tiene una subcultura compartida.

FIGURA 7
Mala suerte Brian



El imeme de la Figura 7 también está basado en una *image macro*: *Bad Luck Brian*. Representa a un adolescente rubio que usa frenos, con un chaleco con estampado escocés, probablemente un uniforme escolar. Normalmente se acompaña de un texto que describe alguna circunstancia desgraciada o vergonzosa. En el caso del ejemplo, una voz en *off* dice "Nadie se interesa por él, excepto la NSA, la GCHQ y la BND". El GCHQ o *Government Communications Headquarters* es el organismo de inteligencia del Reino Unido. BND es la sigla de *Bundesnachrichtendienst*, su análogo alemán. Está claro que no muchos conocen a estos organismos, así que para entender se requiere estar particularmente informado, de modo que enunciador y enunciatario se encuentran a un mismo nivel, ajeno a terceros. El efecto cómico se genera por la incongruencia de sostener que los servicios secretos, en lugar de perseguir terroristas, espían a chicos así. Y resulta

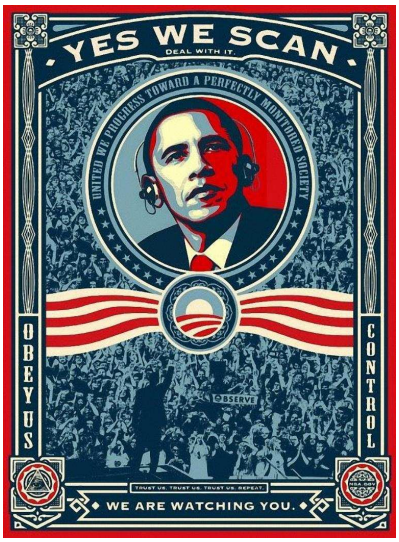
verosímil porque, según Snowden, dichas agencias recolectan comunicaciones de millones de personas comunes no sospechosas de ningún delito. De hecho, muchos imemes sobre la NSA sugieren que, en vez de espiar para prevenir grandes amenazas, lo haría para conocer banalidades sobre la intimidad de personas intrascendentes.

FIGURA 8
Corazón Valiente

El meme de la Figura 8 usa la plantilla llamada *William Wallace*, tomada de un cuadro de la película *Corazón Valiente*, en el momento en que el héroe escocés interpretado por Mel Gibson dice: "podrán tomar nuestras vidas pero nunca tomarán nuestra libertad". El formato del texto acompañante siempre es paródico y con la forma "podrán tomar nuestro X, pero nunca tomarán nuestro Y". Es decir, opera por conmutación. En el caso del ejemplo, dice "Podrán tomar nuestra privacidad, pero nunca tomarán nuestros memes". Es claro que esta plantilla favorece especialmente la función poética del lenguaje, porque lo que más destaca es la forma de lo dicho, no su contenido. Lo que hace es aprovechar un tema de actualidad muy comentado para decir una trivialidad sobre los memes en sí. En el ejemplo, parte de la broma es la hipérbole de asimilar la lucha medieval por la independencia de Escocia con el derecho a hacer memes. Incluso sugiere que, si hay que optar entre la privacidad (alusión a lo extratextual del escándalo de Snowden) y dicho derecho, es más importante este último. La situación enunciativa es de inclusión, ya que enunciador y enunciatario se presumen pertenecientes al mismo colectivo de

quienes pueden entender estos guiños. Es un buen ejemplo de que no siempre los imemes sobre noticias de gran trascendencia pública constituyen una forma de protesta social. A veces son simples humoradas, destinadas en última instancia a reforzar las reglas de conformación de los géneros meméticos online y de las redes intersubjetivas que los sustentan.

FIGURA 9
Obama



El meme de la Figura 9 y variantes circuló mucho cuando se difundieron las revelaciones de Snowden. Es una parodia del eslogan de la campaña de Obama *Yes, we can*, donde el texto más visible adjunta una "s" y dice *Yes, we scan* (subtitulado con un *Deal with it*). El motivo temático del "escaneado" o "escrutinio", como podría traducirse, se ve reforzado por varios elementos: los auriculares de Obama, la pancarta que dice *Observe* sostenida por alguien en la multitud, las leyendas verticales *Control* y *Obey us*, y la horizontal *We are watching you*, así como *Trust us, trust us, trust us, repeat*. También se observa en la esquina inferior izquierda el símbolo del ojo, presente asimismo en los dólares y, a la derecha, *NSA.gov*, la dirección web de la agencia de inteligencia. En el círculo que rodea la imagen del presidente, dice *United we progress toward a perfectly monitored society*. Los colores son los de la bandera de Estados Unidos. Es, en suma, un Photoshop reactivo muy elaborado. No es un imeme como los que cualquiera podría hacer con *memegenerator*, por ejemplo. La situación enunciativa es de sometimiento del enunciatario por el enunciador. Por ejemplo, mediante una tipografía minúscula que remeda la letra chica de un contrato, algo no escrito con la intención de facilitar la lectura. También es interesante cómo

la parodia desplaza el *nosotros* presuntamente inclusivo del original *Yes, we can* por otro que deja fuera al destinatario: *We are watching you*. Globalmente, se puede decir que se describe una situación dada por hecha. Pero también hay un efecto argumentativo al pretender convencer al enunciatario de conformarse con dicha situación.

FIGURA 10
Burlándose de Obama

Como muestra la figura 10, Barack Obama fue uno de los personajes más prevalentes en el universo de imemes considerado. En el caso del ejemplo de la Figura 11, no se trata de un único cuadro sino una especie de diálogo, como en una fotonovela, formado por dos tomas distintas. A la izquierda el presidente y la derecha la imagen del anuncio "¿Puedes oírnos?" de la compañía de telecomunicaciones Verizon (que, como hemos dicho, figura en documentos de Snowden donde se reproduce una orden secreta forzándola a entregar al FBI y la NSA datos de llamadas telefónicas de millones de estadounidenses). Tanto Obama como el personaje de Verizon tienen un celular y la yuxtaposición genera la impresión de que estuvieran hablando entre sí. El efecto cómico se produce porque lo que parecen ser una pregunta y una respuesta fáticas, en realidad en el contexto del escándalo y siendo eslóganes producen un efecto referencial. La resultante es literalmente verosímil: que el gobierno puede escuchar todo lo que hablan los ciudadanos. Y no son éstos quienes aparecen afirmándolo, ni Snowden, sino los mismos involucrados (Obama como metonimia del gobierno, el supuesto operario de Verizon tomado de la publicidad como metonimia de esa empresa).

FIGURA 11
"¿Puedes oírme?"

FIGURA 12
Picard enojado

Picard Enojado es una *image macro* que representa una captura de pantalla de la serie *Star Trek: The Next Generation*, donde el capitán Jean-Luc Picard tiene una expresión de exasperación. El texto acompañante siempre comienza con la pregunta retórica enfática y coloquial *How the fuck?,Why the fuck?* o *What the fuck?* En la Figura 12, mostramos el meme junto con su cotexto porque, para ser comprendido, requiere haber visto el paratexto *As a Canadian reading about Bradley Manning, Edward Snowden, and the NSA…*, que funciona como primera parte del enunciado *Why the fuck have Americans not revolted yet?* No importa si fue creado por un verdadero canadiense. Más bien, interesa el estereotipo vigente en Estados Unidos de que los ciudadanos del Canadá son tan flemáticos que no se enojan con nada. Es como decir "hasta un canadiense se rebelaría ante estos hechos". O sea, se trata de una figura de referenciación por comparación. Predomina la función conativa, ya que insta a la rebelión social y el formato general es argumentativo, orientado a convencer debido a un móvil ético.

Desde el punto de vista temático, resulta significativo que, aunque supuestamente toda la humanidad habría sido espiada y perjudicada por las acciones secretas del gobierno de Estados Unidos, incluidos los canadienses, quienes deberían rebelarse son los estadounidenses. ¿Por qué no habrían de rebelarse personas de todas las nacionalidades? De hecho, en Alemania y en Brasil las revelaciones de Snowden tuvieron mucho impacto y generaron incidentes diplomáticos. En Estados Unidos, en cambio, se cuestionó mucho más que ese país pudiera estar espiando a sus propios ciudadanos que si hacía lo mismo con millones de extranjeros. En cualquier caso, la situación enunciativa planteada en la Figura 11 es ambigua. Porque el enunciatario podría tanto ser otro canadiense o bien un estadounidense. En el primer caso, serían dos canadienses pertenecientes a un mismo escalafón jerárquico construido por el texto. En el segundo caso, en cambio, el canadiense estaría en posición de reclamarle una explicación a su presunto interlocutor. Es decir, se estaría poniendo en una posición de superioridad.

Complementariamente, queremos llamar la atención sobre el meme de la Figura 13, una transformación digital del anterior, donde se conmuta el rostro de Picard por el de Snowden. El propósito es el mismo: llamar a la acción contra el gobierno. En cuanto a la enunciación, a diferencia del anterior, no habla de un *ellos* sino que se dirige directamente a un *tú*.

FIGURA 13
Snowden fusionado con Picard

El rostro de Snowden ha sido uno de los *Advice Animals* más utilizados, junto con Obama, en la tematización del escándalo de la NSA. En la Figura 14 vemos algunos ejemplos más.

FIGURA 14
Snowden como Advice Animal

FIGURA 15
Confesiones de un oso

El ejemplo de la Figura 15 es una respuesta a imemes como el de la Figura 13. Se basa en *Confession Bear*, una *image macro* que representa un oso malayo apoyado en un tronco. Los textos suelen manifestar opiniones controversiales. En el caso del ejemplo, prima la función emotiva, ya que exterioriza un sentimiento de frustración y de desesperanza. No insta a hacer algo: asume que no vale la pena ni intentarlo. Incluso se da la paradoja de que un aparentemente tierno animal utilice un insulto. Desde el punto de vista temático, este imeme trata de la apatía social frente al abuso. Expresa un verosímil social acerca de la imposibilidad del cambio.

CONCLUSIONES

Una de las cosas que verificamos en este trabajo es que muchos tópicos usuales del comentario político también se usaron para reconocer el tema que nos ocupaba. Por ejemplo, los memes donde Obama o el presidente de cualquier país aparece diciendo cosas ridículas o donde se los parodia o deforma son un clásico y surgen ante cualquier noticia periodística que los involucre. Los formatos meméticos prevalentes –Photoshop reactivos y personajes estereotipados– también son comunes con muchos otros temas. De hecho, aunque varias de esas plantillas se originan en fotos inicialmente creadas en Estados Unidos (como *Conspiracy Keanu*), son reutilizadas en muchos otros países sin inconvenientes culturales. La producción memética usa, en gran me-

dida, un lenguaje global, aun cuando se orienta al comentario de fenómenos locales. Así, encontramos muchos memes hechos con imágenes reutilizables, útiles tanto para este tema como para cualquier otro. No obstante, hay algunas que se convirtieron en símbolos específicos de este escándalo en particular. Por ejemplo, la foto de Snowden, el escudo de la NSA y los anuncios de Verizon y AT&T.

Es interesante señalar que, en principio, también el alcance de las revelaciones de Snowden es global. Se supone que se trata de que Estados Unidos y sus aliados de los Cinco Ojos interceptan las comunicaciones de casi toda la población mundial. Sin embargo, apenas encontramos en el universo de memes sobre el tema alguno no referido a Estados Unidos y a su política interna. Hallamos muy pocos realizados en México, Brasil y Alemania. De hecho, en estos países el escándalo tuvo mayor alcance que en otros porque parte de lo informado fue que Estados Unidos espiaba los celulares de sus respectivos presidentes. Sin embargo, la inmensa mayoría de los memes sobre el escándalo de la NSA están en inglés y hasta requieren conocer bastante la cultura y la política estadounidenses para su comprensión. Dado cómo funciona internet, no se puede afirmar que no existan ni hayan existido en el momento de los hechos más memes sobre Snowden enfocados en motivos temáticos de otras geografías: solo podemos decir que no los encontramos. De todos modos, es una ausencia notoria.

Desde lo retórico, los recursos que prevalecen en son comunes a la generalidad de los memes de internet. En especial, los que tienden a construir ironías y parodias. Lo único distintivo que hemos hallado es que las inserciones sintagmáticas y paradigmáticas utilizadas requieren en general un dominio muy específico de ciertos asuntos. Es decir que quien no pertenezca a determinadas subculturas queda fuera. Desde ya, siempre quedan fuera de la comprensión de los memes quienes no estén familiarizados con las convenciones del género. Pero, en el caso de nuestros ejemplos, además es necesario estar al tanto de cosas tales como qué es el modo incógnito y por qué es inútil, de qué trataba la serie *El Superagente 86*, cómo funciona una consola Xbox, quién es Bradley (Chelsea) Manning y por qué puede compararse con Snowden o qué son el GCHQ y la BND.

También comprobamos que no siempre las funciones predominantes fueron las que uno a priori podría suponer más apropiadas para el comentario político. Y se notó una significativa presencia de memes donde predominaban las funciones poética y fática. Es decir que el escándalo de Snowden resultó, en algunos memes, una simple excusa para hacer juegos de lenguaje o consolidar la pertenencia a ciertas subculturas.

Además, si un meme es humorístico o irónico siempre define *insiders* y *outsiders*, qué es lo bueno y qué es lo malo, qué es parte de un "nosotros" y qué se atribuye a "ellos". Y, si como dice Mary Douglas (1975), una broma siempre es un ataque a alguna forma de control, cuánto más lo será en el caso de una colección de memes dedicados precisamente a cuestionar el vigilantismo estatal. Así, se construye enunciativamente mediante el humor o la ironía unos "ellos", culpables de haber convertido la sociedad real en lo que describía una ficción distópica (*1984*).

También unos "ellos" que nos estarían espiando y, para evitarlo, no es mucho lo que "nosotros" los ciudadanos podemos hacer (el cono del silencio). Hay unos "ellos" que creen estar a salvo de la vigilancia y no se da cuenta de que no saben nada del funcionamiento de la Red (la chica nerd). Hay unos "ellos" que si ganan la elección presidencial dará igual cómo se llamen, porque serán idénticos a la hora de controlarnos (el instructor de ski). Hay unos "ellos" que nos venden máquinas para divertirnos que, en realidad, nos vigilan a "nosotros", los consumidores (Keanu y la Xbox). Otros "ellos" nos venden celulares, supuestamente para que disfrutemos de comunicarnos y, en realidad, para que nos pueda vigilar el gobierno estadounidense (Verizon). Hay unos "ellos" con el poder de enviarnos arbitrariamente a la cárcel si revelamos secretos del poder (Manning y la NSA). Hay unos "ellos" que escudriñan cada detalle de unos insignificantes y poco interesantes "nosotros" (*Bad Luck Brian*). Hay unos "ellos" que nos vigilan, pero no importa, seguiremos desafiándolos con nuestras construcciones discursivas online (William Wallace). Hay un "él", Obama, que nos dijo "nosotros (juntos) podemos" y en realidad debería haber dicho "nosotros, el poder, te vigilamos a ti" (*Yes, we scan*). Hay unos "ellos" que merecerían que ya mismo nos rebeláramos (Picard Enojado). Pero hay unos "nosotros" que somos demasiado cobardes para hacerlo (*Confession Bear*).

Dicho todo esto, sinteticemos los principales motivos temáticos que encontramos:

- Estados Unidos se estaría convirtiendo en el Gran Hermano
- La inutilidad de la resistencia
- La ignorancia de los usuarios de las redes
- Los candidatos a presidente son todos iguales a la hora de espiar
- Las empresas, como Microsoft (con su Xbox) y Verizon son cómplices del poder
- Si uno cuenta lo que pasa irá preso
- Nadie se salva de la hipervigilancia
- Mejor olvidar todo y dedicarse a hacer memes
- Las campañas políticas expresan lo contrario de lo que piensan hacer
- La necesidad de la rebelión
- La desesperanza de que las cosas puedan cambiar

En cuanto a la autoría real, más allá del enunciador construido por el texto, ya hemos dicho que la producción de memes se realiza frecuentemente con sistemas y prácticas sociales que activamente previenen la atribución (Davidson, 2012). De hecho, podrían no ser en absoluto originados en "usuarios comunes", sea lo que sea que represente esa vaga categoría, porque de hecho a veces forman parte de deliberadas campañas publicitarias, en especial políticas, destinadas a

movilizar la opinión pública en medios sociales online. Así, como dice Vélez Herrera (2015), los memes de internet "pueden ser un indicador de la opinión pública, aunque sus variaciones también pueden ser una herramienta para dirigirla". Los ejemplos analizados no son la excepción, aunque se cuentan algunos casos (como el del ejemplo de Manning), donde sí hay marcas de un autor concreto, en ese caso un grupo libertario de derecha.

En cuanto a los subgéneros meméticos, es interesante que no se encontraron materiales en video o audio (de nuevo, eso no implica que no existan). Los subgéneros de elección resultaron ser los de manipulación de fotografías (*Photoshops reactivos*) y los nacidos del nuevo universo del contenido digital memético, en especial personajes o iconos arquetípicos reutilizables. Es decir que el verosímil social de la vigilancia gubernamental se construyó en los memes principalmente por medio del reciclaje, *remix* o bricolaje de elementos de origen discursivo más que de mediatizaciones más "cercanas" a su referente, como videos y audios.

Por otra parte, como se acostumbra en los géneros meméticos, verificamos que en los memes sobre Snowden las tematizaciones se concretan en general por medio del recurso a los estereotipos. Además, puede decirse que, más que escándalo por lo que las agencias de inteligencia de los países centrales le estarían haciendo a los ciudadanos comunes de todo el mundo, en los memes recolectados hay escándalo ante lo que le estarían haciendo específicamente a los estadounidenses. Lo que les preocuparía a los estadounidenses es que su propio gobierno los espíe sin ser sospechosos de nada, no tanto que haga lo mismo con otros. Lo que expresan en conjunto estos memes es entonces una sensación de traición a los "valores americanos" y a la democracia tal como la concibieron los Padres Fundadores. Así, un fenómeno que en sí es global, se trata como local.

NOTAS

* Universidad de Buenos Aires, Facultad de Ciencias Sociales, Fundación Vía Libre, laura.siri@gmail.com
Una versión previa de esta ponencia está pendiente de publicación en la revista *LIS: Letra, Imagen y Sonido*.

REFERENCIAS

Barthes, R. (1989). *La cámara lúcida: nota sobre la fotografía*. Barcelona, Paidós.

Bremond, Cl. (1970) "El rol de 'influenciador". VV. AA., Investigaciones retóricas II. Barcelona, Ediciones Buenos Aires.

Davidson, P. (2012). The Language of Internet Memes. En M. Mandiberg (Ed.) *The social media reader* (pp. 120–134). New York / London: New York University Press.

Douglas, M. (1975). Jokes. *Rethinking Popular Culture: Contemporary Perspectives in Cultural Studies*. Oxford: University of California Press, 291-310.

Fernández, J. L. (1994). La entrada enunciativa. *Los lenguajes de la radio*. Buenos Aires, Atuel.

(2008). La construcción de lo radiofónico: modos de producción de la novedad discursiva. Fernández, J.L. (Dir.) *La construcción de lo radiofónico,* Buenos Aires, La Crujía.

Fernández, J. L. y Tobi, X. (2009). Criminal y contexto: estrategias para su figuración. *L.I.S. Letra. Imagen. Sonido. Ciudad mediatizada*, 2(1). Buenos Aires.

Hamon, P. (1994). *Introducción al análisis de lo descriptivo*. Buenos Aires: Edicial.

Jakobson, R. (1981). Lingüística y poética. *Ensayos de lingüística general*. Barcelona: Seix Barral

Kim, B. (2014). 2013 NSA Surveillance Scandal. *Knowyourmeme.com*. Recuperado de http://knowyourmeme.com/memes/events/2013-nsa-surveillance-scandal

Knobel, M. y Lankshear, C. (2008). Remix: The Art and Craft of Endless Hybridization. *Journal of Adolescent & Adult Literacy*, *52* (1), 22–33.

(Noviembre, 2005). Memes and affinities: Cultural replication and literacy education. *Memes and affinities: Cultural replication and literacy education*,

Marino, G. (2015). Semiotics of spreadability: A systematic approach to Internet memes and virality. *Punctum. International Journal of Semiotics*, *1* (1), 43–66.

Metz, Ch. (1978 [1962]). El decir y lo dicho en el cine: ¿hacia la decadencia de un cierto verosímil?*Lo verosímil*. Buenos Aires: Editorial Tiempo Contemporáneo.

Shifman, L. (2013). *Memes in digital culture*. Mit Press.

(2014). The Cultural Logic of Photo-Based Meme Genres. *Journal of Visual Culture*, *13* (3), 340–358.

Segre, C. (1985). Tema / motivo. *Principios de análisis del texto literario*. Barcelona: Crítica.

Tay, G. (2012). *Embracing LOLitics: Popular Culture, Online Political Humor, and Play*. University of Canterbury, Reino Unido.

Vélez Herrera, J. (2015, marzo-abril). Influyendo en el ciberespacio con humor: imemes y otros fenómenos. *Versión. Estudios de Comunicación y Política*, (35), 130–146.

Verón, E. (1985). El análisis del contrato de lectura, un nuevo método para los estudios de posicionamiento de los soportes de los media. *Les medias: experiences, recherches actuelles, aplications*. Paris: IREP.

EJE 8

RESISTENCIAS Y CONTRAVIGILANCIA

MULHERES E A SEGURANÇA DA INFORMAÇÃO: A TRAJETÓRIA DE UM HACKERSPACE FEMINISTA NO BRASIL

Resumo: O objetivo deste trabalho é discutir como o anonimato e a segurança da informação têm sido mobilizados como recursos do ativismo político na Internet, tendo como foco os coletivos feministas. O artigo apresenta a experiência do MariaLab,*hackerspace* feminista criado no Brasil, cujo objetivo é reunir e promover projetos de tecnologia desenvolvidos por mulheres. O coletivo surgiu em 2013 e hoje reúne cerca de 200 mulheres em uma lista de discussão por e-mail e promove debates e oficinas de tecnologia. Alguns dos principais trabalhos desenvolvidos pelo MariaLab são as oficinas de segurança da informação e o projeto de uma servidora que vai oferecer serviços *on-line* para coletivos feministas, com o intuito de aumentar a segurança e autonomia das mulheres na Internet. Manifestações e grupos feministas têm ganhado cada vez mais repercussão na Internet e evidenciam a violência contra a mulher também no ambiente virtual, em casos como *cyberbullying* , assédios, ameaças e pornografia de vingança. Em alguns eventos de cultura digital e cultura *hacker* que acontecem no Brasil, a relação entre gênero e tecnologia tem sido um tema recorrente e muitos grupos vêm se articulando para discutir a visibilidade das mulheres no campo da ciência da computação e na Internet. Entre os debates, destacam-se a importância da criptografia e segurança da informação como proteção pessoal e resistência para coletivos feministas. Para esses grupos, a criptografia e as ferramentas de segurança são mais do que instrumentos de combate à vigilância massiva, mas também são formas de resistência à misoginia e ao machismo.

Palavras-chave: Gênero, Tecnologia, Hacktivismo, Segurança, Criptografia

DANIELA ARAÚJO*
LEDA GITAHY**

Mujeres y la seguridad de la información: la trayectoria del un hackerspace feminista en Brasil

Resumen: Este trabajo discute como el anonimato y la seguridad de la información están siendo movilizados como recursos del activismo político en Internet por colectivos feministas. El trabajo presenta la experiencia del MariaLab, primer *hackerspace* feminista creado en Brasil para promover proyectos de tecnología desarrollados por mujeres. Este colectivo fue creado en 2013 y hoy reúne cerca de 200 mujeres en una lista de discusión por email e organiza debates y oficinas de tecnología. Entre ellos se destacan las oficinas de seguridad de la información y el proyecto de una "servidora" que va a ofrecer servicios *on-line* para colectivos feministas para aumentar la seguridad y la autonomía de las mujeres en *internet* . En los últimos dos años grupos feministas evidenciaran los casos de violencia en contra de la mujer en el ambiente de *internet* en casos de *cyberbullying* , asedios, amenazas y *revenge porn.* En eventos de cultura digital y cultura *hacker* en Brasil, la relación entre género y tecnología ha sido un tema recurrente y diversos grupos están se articulando para discutir la visibilidad de las mujeres en el campo de la ciencia de computación y en *internet* . Entre esos debates se destaca la importancia de la criptografía y seguridad de la información como forma de protección personal y resistencia para colectivos feministas. Para esos grupos la criptografía y las herramientas de seguridad son más que instrumentos de combate a la vigilancia masiva , pero formas de resistencia a la misoginia y al machismo.

Palabras clave: Género, Tecnologia, Hacktivismo, Seguridad, Criptografia

Women and information security: the trajectory of a feminist hackerspace in Brazil

Abstract: The purpose of this paper is to discuss how the anonymity and information security have been mobilized as political activism resources on the Internet, focusing on feminist collectives. The paper presents the MariaLab experience, a feminist hackerspace created in Brazil to promote technology projects developed by women. The group emerged in 2013 and today gather together 200 women in a mailing list. The initiative also promotes debates and workshops. The main activities are information security workshops and the web server project, which hosts online services for feminists groups. In the last years, feminist groups and demonstrations have been a great reverberation on Internet and highlighted an usual online violence against women, in cases such as cyberbullying, harassment, threats and revenge porn. In some digital culture and hacker culture events that take place in Brazil, the relation between gender and technology has been repeated and many groups have been discussing the women visibility in the field of computer science and the Internet. Among the main themes are the importance of encryption and information security as strategies for personal protection and resistance for feminists groups. For these groups, the encryption and the security tools are the main ways to fight against the surveillance as also the forms of resist misogyny and sexism.

Key-words: Gender, Technology, Hacktivism, Security, Encryptation

INTRODUÇÃO

A proposta deste artigo[1] é localizar as mulheres dentro da discussão a respeito de privacidade. Tomando a perspectiva feminista como amparo, faz-se necessário reconhecer que o viés de gênero diferencia as experiências e vivências de homens e mulheres. O mesmo não seria diferente quando tratamos de Internet.

As duas primeiras sessões fazem uma breve descrição de alguns dos problemas relacionados à privacidade na Internet que têm sido temas de discussão em coletivos feministas e ONGs de defesa dos direitos humanos. Em seguida, apresentaremos como um coletivo feminista no Brasil, MariaLab *Hackerspace*, tem abordado tais questões e como tem se articulado para empoderar mulheres na tecnologia.

Os dados apresentados neste artigo fazem parte da pesquisa de doutorado da primeira autora. A tese discute as interações entre o movimento de mulheres e a cultura *hacker*, procurando

identificar os grupos feministas que têm se articulado dentro do movimento *hacker*, como eles se organizam e quais temas abordam. Ao mesmo tempo, discute como os valores da cultura *hacker* vêm sendo apropriados como forma de articulação política e como os temas relacionados a gênero e diversidade têm sido apropriados nos projetos de tecnologia da informação e comunicação (TICs) que esses grupos têm desenvolvido.

A pesquisa de doutorado que deu origem a este artigo tem sido realizada por meio de pesquisa etnográfica em eventos de cultura *hacker,* incluindo aqueles promovidos pela MariaLab. Outros dados foram colhidos através da lista de discussão por e-mail e redes sociais mantidas pelo grupo e por meio de entrevistas com as organizadoras.

ESTRATÉGIAS DE SILENCIAMENTO: CALANDO VOZES DISSONANTES

Novembro de 2015. A página "Feminismo sem Demagogia"[2] e "Jout Jout Prazer"[3] foram retiradas do ar pela moderação do Facebook. Ambas são canais famosos entre a militância feminista no Brasil e foram derrubadas depois de uma avalanche de denúncias que relatavam publicações com conteúdo pornográfico e discurso de ódio. Nenhum material com esse teor foi publicado, no entanto.

A derrubada foi provocada por uma tática que subverte os termos de uso de plataformas como Facebook (essa tática é usada também em outras plataformas). Ao enviar um grande número de denúncias sobre uma mesma página, os responsáveis por esses ataques sobrecarregam as equipes de funcionários que avaliam essas questões e, na ânsia por emitir uma resposta rápida, a remoção é feita com base no volume de reclamações.

Essas ações são articuladas por grupos que também se organizam via redes sociais e têm como objetivo propagar conteúdo ofensivo, na maioria das vezes homofóbico, racista e machista. Na linguagem da Internet eles podem ser chamados de *haters* ou *trolls*.

Outra estratégia usada como instrumento de censura é o assédio on-line por meio de mensagens públicas ou privadas com insultos ou ameaças. A tática é conhecida como *dog piling*, quando várias contas bombardeiam seu alvo com mensagens de ódio. O *dog pilling* ficou bastante conhecido durante o episódio do Gamergate, quando Zoë Quinn, desenvolvedora de jogos alternativos, e Anita Sarkeezian, feminista americana que grava vídeos falando sobre o sexismo em games, receberam inúmeras mensagens pelo twitter com todo tipo de ofensa de cunho sexista e até ameaças de estupro e morte.

O *doxing* é uma estratégia ainda mais perversa, que expõe dados pessoais dos alvos, como números de documentos, fotos, endereço e até informações de familiares. Anita Sarkeezian foi vítima desse ataque e precisou mudar de residência para garantir sua segurança. No Brasil, a publicação de dados pessoais e ameaças a familiares aconteceu com a feminista Lola Abronovich, autora do *blog* "Escreva Lola Escreva"[4].

A questão é muitas vezes negligenciada pela próprias plataformas de redes sociais e outros serviços on-line. Em levantamento feito pela *Association for Progressive Communication,* entre 22 companhias analisadas, nenhuma continha compromissos públicos com os direitos humanos nem proibia ameaças de violência física ou sexual em seus termos de serviços[5].

Os ataques públicos com ofensas e ameaças ou a derrubada de páginas e perfis feministas são estratégias de silenciamento, que acontecem por meio de censura, quando os canais de comunicação das ativistas fica impossibilitado de manter a comunicação, ou pela autocensura, que faz com que mulheres deixem de manifestar suas opiniões ou mesmo retirem seus perfis da Internet por medo de qualquer tipo de ataque pessoal. São táticas que atingem, dessa forma, o direito fundamental de liberdade de expressão.

REVENGE PORN: VIOLAÇÕES DE CORPOS CIBERNÉTICOS

A separação entre virtual e real, comum no início dos estudos sobre cibercultura, não se aplica a experiência contemporânea com as tecnologias digitais que estão imbricadas em quase todos os aspectos da nossa existência: dos dados de saúde ao tráfego pelas vias urbanas até os relacionamentos interpessoais.

Para falar sobre privacidade na Internet, especialmente das mulheres, é preciso mencionar a exposição de imagens íntimas sem consentimento, ou como vem sendo chamada, a pornografia de vingança (do inglês *revenge porn*). Não são raros e nem recentes os casos de imagens e vídeos vazados expondo mulheres em situações de intimidade. Em 2015, a SaferNet[6], entidade que é referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, recebeu cerca de 1800 chamadas com pedidos de atendimento. Entre esses atendimentos, 322 correspondiam a casos de exposição íntima, dos quais 240 foram relatados por mulheres. Em âmbito internacional, foram registrados 1126 casos de violência contra a mulher na Internet entre 2012 e 2014, segundo pesquisa realizada pela *Association for Progressive Communication (APC)*. Esses dados, no entanto, são parciais, pois há uma subnotificação dos crimes, como acontece com os diversos casos de violência contra a mulher.

O livro "O corpo é o código", lançado por pesquisadoras do InternetLab, Centro de pesquisa em Direito e tecnologia, baseado em São Paulo, aborda a pornografia de vingança sob o aspecto jurídico e demonstra que os casos levados à justiça ainda enfrentam dificuldades no judiciário. A lei Maria da Penha (Lei Nº11.340), que criminaliza a violência doméstica no Brasil, poderia ser usada em diversos casos, mas tem sido acionada com pouca frequência. Isso revela que ainda há certa dificuldade em entender a exposição de imagens íntimas sem consentimento como um tipo de violência. Além disso, as vítimas ainda precisam lidar com julgamentos que levam em conta aspectos morais que acabam por culpabilizar a vítima. Ultrapassar essas barreiras expõem as vítimas a situações de vergonha e humilhação, o que acaba por tornar os casos cada vez mais subnotificados.

Muitas vezes, os agressores são conhecidos das vítimas, principalmente companheiros ou ex-companheiros. Em alguns casos, mais do que humilhação pública, as imagens são usadas como chantagem, em geral coagindo a vítima a manter relações sexuais com o agressor, configurando crime de estupro.

As imagens são digitais, mas as consequências dessas exposições extrapolam a humilhação on-line. Em 2013, duas adolescentes brasileiras cometeram suicídio depois da divulgação de imagens íntimas nas redes sociais. Muitas outras mulheres têm sofrido com depressão, isolamento, abandonaram emprego ou estudos e são assediadas via telefone e nas ruas. Em países extremamente conservadores, como no Oriente Médio, Sul da Ásia e Norte da África, as consequências são ainda mais devastadoras, podendo resultar em pena de morte para as mulheres expostas e inúmeras sanções e humilhações para suas famílias. Nessas regiões, as imagens sequer precisam ter cenas de sexo explícito ou nudez, basta uma mulher ser exposta sem o *hijab* para que isso seja motivo de repúdio.

CONTRARESISTÊNCIA ORGANIZADA: O HACKERISMO ENTRE MULHERES

Se por um lado a Internet facilitou que conteúdos de caráter ofensivo se propagassem em volume cada vez maior, por outro, ela é um espaço importante para promover discussões que são negligenciadas na mídia *mainstream* e fundamental para a articulação de ativistas (Moawad, 2016). Dessa forma, além das pautas tradicionais do movimento feminista, o debate acerca da segurança on-line passou a figurar os assuntos de interesse de coletivos feministas.

Ao mesmo tempo, em eventos e grupos voltados para a discussão de segurança, privacidade na rede, governança da Internet e cultura *hacker,* o tema gênero e tecnologia tem aparecido com frequência em discussões e atividades, geralmente impulsionado por mulheres que já transitavam por essas comunidades. Exemplos são o Espaço Ada Lovelace criado na Cryptorave[7], evento sobre segurança, privacidade e liberdade na rede que acontece em São Paulo; as diversas palestras, oficinas e debates a respeito de gênero e tecnologia realizadas nas últimas edições do Fórum Internacional de Software Livre (FISL)[8] e na Campus Party[9]; e a mesa de debate "Mulheres na Computação" que aconteceu no VI Fórum da Internet no Brasil[10].

Dentro desse movimento, começam a surgir *hackerspaces* feministas, espaços criados por mulheres e para uso exclusivo do público feminino. *Hackerspaces*[11] são espaços físicos com livre acesso à Internet e com uma estrutura propícia para a discussão, desenvolvimento e experimentação com *softwares* e *hardwares* livres*,* criação de projetos colaborativos com TICs, além de promoverem a socialização entre seus membros associados e os visitantes que frequentam o local (Maxigas, 2012; Toupin, 2014). Os grupos reunidos nesses *hackerspaces* se propõem tanto ao desenvolvimento de *softwares*, experimentações com *hardware*, quanto à discussão de temas voltados para cidadania, participação social na política e governança da Internet.

Toupin (2014) ao analisar experiências de *hackerspaces* feministas nos Estados Unidos, afirma que alguns deles vão se afirmar como espaços interseccionais e, dessa forma, buscam evidenciar

a heterogeneidade presente na cultura *hacker*. Os *hackerspaces* feministas e de forma mais ampla, as mulheres inseridas na cultura *hacker*, questionam alguns valores éticos e normativos dessa cultura, especialmente a ideia de abertura e meritocracia (Toupin, 2014). Ao mesmo tempo, esses grupos trazem à tona a discussão em torno da invisibilidade das mulheres na área de TI e os motivos que levam a essa sub-representarão (Haché, Cruells e Bosch, 2013; Toupin, 2014).

Exemplos na literatura tendem a apontar que as mulheres estão menos interessadas no universo dos computadores e também se afastam da ideia de cultura *hacker* por associá-la a práticas criminosas no ciberespaço (Toupin, 2014). Um outro olhar sobre essa questão, demonstra que o problema está em considerar a ética e a cultura *hacker* como um todo homogêneo, no qual as mulheres não se encaixam. O argumento de Toupin (2014) é de que as mulheres estão ressignificando e expandindo o conceito de *hacker*. A partir de uma série de entrevistas, a autora constatou que elas se identificam com aqueles pontos que julgam "positivos", como a curiosidade e criatividade, a autonomia, a colaboração e o compartilhamento.

Iniciativas como os *hackerspaces* feministas e outros grupos de mulheres que vêm se articulando em torno do tema gênero e tecnologia têm sido importantes para combater a invisibilidade feminina nessa área e criam espaços de colaboração e apoio entre mulheres. Alguns exemplos dessas iniciativas são o *Mothership HackerMoms*[12], em Berkeley, Califórnia, que afirma ser o primeiro *hackerspace* criado por mulheres no mundo; e o Mz Baltazar Laboratory[13], em Viena, Austria, e se define como um *hackerspace* feminista.

O Brasil também já tem iniciativa parecida. A MariaLab *Hackerspace*[14] foi criada em 2013 e tem como proposta ser um espaço de articulação, debate e desenvolvimento de projetos feito por mulheres e para mulheres. Apesar de se denominarem como um *hackerspace*, a MariaLab ainda não tem um espaço físico próprio. As atividades do coletivo são realizadas em locais cedidos por outros grupos ou em espaços de uso público na cidade de São Paulo. Essa característica colabora para que as atividades do coletivo sejam itinerantes e assim consigam atingir grupos diferentes a cada evento produzido. Ainda assim, pode ser definido como um *hackerspace* porque valorizam e estimulam a colaboração, o compartilhamento de conhecimento e a experimentação com tecnologias entre os membros. Em 2016, algumas oficinas foram realizadas também no Rio de Janeiro, estreitando laços entre coletivos feministas das duas cidades. A proposta é criar um *hackerspace* aos moldes da MariaLab também na capital fluminense.

Algumas das fundadoras do coletivo já frequentavam outro *hackerspace,* no qual a presença feminina era minoria. As poucas garotas que apareciam no local se sentiam inibidas em questionar ou dar opiniões em um espaço majoritariamente masculino e onde há um forte discurso de autoridade associado ao domínio do conhecimento sobre tecnologia. Elas chegaram a propor reuniões só para mulheres, mas a ideia não foi bem aceita. Para os demais membros do grupo, criar atividades para um público exclusivo seria uma atitude segregadora.

O coletivo mantém uma lista de discussão que em junho de 2016 reunia cerca de 250 mulheres. A lista tem uma variedade de temas, desde a divulgação de vagas de emprego ou *freelancer* até

articulações para colaboração em projetos de TICs. Mas toda a organização do coletivo, como gerenciamento da lista de discussão e redes sociais, promoção de eventos e condução dos projetos ficam a cargo de nove mulheres, algumas delas presentes desde a criação da MariaLab.

Há muitas mulheres profissionais do setor de TI, mas há muitas outras que não atuam na área e não dominam assuntos de tecnologia. O grupo também é diverso com relação a etnia, orientação sexual e transgeneridade.

Como forma de incentivar e inspirar a participação das mulheres na tecnologia, a MariaLab realizou alguns encontros para trocas de experiências, nos quais participantes se voluntariavam para fazer curtas apresentações. Também foi organizado um grupo de estudos de programação para programadoras, no qual elas têm a oportunidade de explorar em conjunto novidades tecnológicas e compartilhar conhecimento.

Uma das principais preocupações do coletivo é a segurança da informação e privacidade na Internet. Esse é um tema muito discutido em todos os grupos envolvidos com a cultura *hacker,* mas para as mulheres esse é um assunto essencial. A maioria dos casos de assédio, difamação e pornografia de vingança tem mulheres e meninas como alvo. Algumas oficinas foram criadas pela MariaLab com o intuito de disseminar criptografia e ferramentas de segurança na rede, ensinando às mulheres como podem manter seus dados sigilosos e permanecer anônimas. As oficinas são direcionadas tanto para coletivos feministas como para a segurança individual. Conhecer melhor como funciona a comunicação em rede e os riscos aos quais estão expostas, faz com que as mulheres tenham mais consciência e controle sobre suas ações na rede.

As oficinas e rodas de conversa sobre segurança no compartilhamento de imagens íntimas colaboram para um tema mais amplo a respeito da decisão sobre o próprio corpo e a liberdade sexual das mulheres.

A segurança de coletivos feministas é outro ponto ao qual se dedicam. Em 2015, a MariaLab, junto com outras iniciativas na cidade de São Paulo, foi vencedora do Prêmio Mulheres Tech em Sampa[15]. A premiação é organizada pela Rede Mulher Empreendedora, *Google for Entrepreneurs* e Tech Sampa, órgão da Prefeitura de São Paulo de fomento à empresas de tecnologia. A primeira edição do prêmio aconteceu em 2014 e a cada ano escolhe cinco grupos de mulheres que atuam como incentivadoras da participação feminina na tecnologia. Cada uma das iniciativas premiadas recebeu 10 mil reais para serem revertidos em projetos de capacitação e empreendedorismo feminino. Esse prêmio está sendo usado pela MariaLab para a realização de oficinas voltadas ao público feminino e para o financiamento do projeto de uma "servidora feminista". Consiste em um servidor *web* que vai hospedar sites de coletivos feministas e ferramentas que possam auxiliar na organização e comunicação desses coletivos. O serviço será disponibilizado gratuitamente, mas cada caso será avaliado para estabelecer os padrões de segurança necessários. O projeto está sendo desenvolvido colaborativamente e pretende oferecer um suporte de segurança para páginas que têm sido frequentemente atacadas na Internet no intuito de silenciá-las.

PODE A INTERNET SER FEMINISTA?

O caso da MariaLab demonstra como coletivos feministas têm atuado para impulsionar a participação das mulheres na tecnologia, tanto no aspecto profissional como no engajamento político. A proposta de trabalhar com oficinas demonstra que há um foco na aprendizagem e no compartilhamento do conhecimento como estratégia de empoderamento.

Reafirmam também o protagonismo feminino na tecnologia, valorizando as experiências e conhecimentos que cada uma tem para compartilhar e criando uma rede de colaboração que tem se articulado, dentro e fora do coletivo, para o desenvolvimento de outros projetos que tenham como preocupação a autonomia e a segurança das mulheres na Internet.

Proteger a privacidade das mulheres na Internet significa reivindicar e defender o direito à autonomia e controle sobre seus próprios corpos. A internet é extensão do nosso corpo e da vida cotidiana. E também é uma forma de garantir a livre circulação e expressão de ideias.

As ferramentas de segurança são instrumentos de resistência e existência para as feministas na rede. Não são soluções para os problemas recorrentes e a violência de gênero, mas são essenciais para garantir que essas mulheres possam continuar a se articular e ir em busca de direitos.

Os Princípios para uma Internet Feminista[16] reivindicam preceitos de inclusão digital e social, liberdade e igualdade. Não se restringe, portanto, ao movimento de mulheres, e demanda uma internet livre e aberta para todos. Estabelece assim uma estreita conexão com as discussões que se têm feito sobre liberdade na rede no mundo todo. Não existe liberdade sem privacidade, e essa é também uma condição essencial para amplificar o discurso feminista.

NOTAS

* Universidade Estadual de Campinas (Unicamp), Departamento de Política Científica e Tecnológica (DPCT /IG), Brasil. E-mail: daniela.araujo@riseup.net.

** Universidade Estadual de Campinas (Unicamp), Departamento de Política Científica e Tecnológica (DPCT /IG), Brasil. E-mail: E-mail: leda@ige.unicamp.br.

1. A apresentação deste trabalho no IV Simpósio Lavits foi viabilizada pelo Fundo de Apoio ao Ensino, à Pesquisa e à Extensão da Pró-Reitoria de Pesquisa da Unicamp (FAEPEX/PRP).

2. https://www.facebook.com/FeminismoSemDemagogiaMarxista0riginal/

3. https://www.facebook.com/prazerjoutjout/

4. http://escrevalolaescreva.blogspot.com.br/

5. Link para a pesquisa: http://www.genderit.org/onlinevaw/

6. http://new.safernet.org.br/

7. https://cryptorave.org/

8. http://softwarelivre.org/fisl17

9. http://brasil.campus-party.org/

10. http://forumdainternet.cgi.br/

11. Além da denominação *hackerspaces*, alguns desses espaços de colaboração também vão ser denominados *hacklabs*, *fablabs*, *makerspaces* etc. Para saber mais sobre as diferenças dessas denominações ver: Maxigas (2012) e Fonseca (2014).

12. http://mothership.hackermoms.org/

13. http://www.mzbaltazarslaboratory.org/

14. http://marialab.org/

15. http://mulherestechemsampa.com.br/

16. http://www.feministinternet.org/

REFERÊNCIAS

Fonseca, F. S. (2014) *REDELABS: laboratórios experimentais em rede*. (Dissertação de mestrado). Instituto de Estudos da Linguagem, Universidade Estadual de Campinas, São Paulo, Brasil.

Haché, A., Cruells, E., e Bosch, N. V. (2013). Eu programo, tu programas, ela hackea: mulheres hackers e perspectivas tecnopolíticas. Em G. Natansohn (ed). *Internet em código feminino: teorias e práticas*. Ciudad Autónoma de Buenos Aires: La Crujía.

Maxigas. (2012) Hacklabs and hackerspaces: tracing two genealogies. *Journal of Peer Production,* 2. Recuperado de: http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/.

Moawad, N. (2016) One and the other: Fighting Online Misogyny, Fighting a Corporatised Internet. *Sexuality, Sexual and Reproductive Health and Rights, and the Internet,* 22(1), 6-8. Recuperado de: http://arrow.org.my/wp-content/uploads/2016/08/AFC22.1-2016.pdf

Toupin, S. (2014). Feminist hackerspaces: The Synthesis of Feminist and hacker Cultures. *Journal of Peer Production*, 5. Recuperado de: http://peerproduction.net/issues/issue-5-shared-machine-shops/peer-reviewed-articles/feminist-hackerspaces-the-synthesis-of-feminist-and-hacker-cultures/.

GOVERNANÇA DA INTERNET, INFRAESTRUTURA E RESISTÊNCIA

Resumo: Pode-se dizer que o recente campo da "governança da Internet" vêm sofrendo uma "virada para a infraestrutura" (*turn to infrastructure*). Cedo ou tarde ficou claro que os princípios políticos da Internet são desempenhados por sua arquitetura e modo de funcionamento, e que a maneira mais eficaz de fazer prevalecer tais ou quais princípios políticos e morais na rede passa por influenciar sua tomada de forma. A "infraestrutura" que dá suporte ao funcionamento da Internet é caracterizada como o conjunto de meios materiais e lógicos que atualizam a transmissão, o armazenamento e o processamento do montante de dados produzidos pela crescente digitalização da atividade humana e não humana. A inteligibilidade da importância política da técnica, no entanto, parece não surtir efeito, uma vez que o controle sobre as infraestruturas de comunicação e informação se exerce de modo cada vez mais concentrado e sob poder privado. Esse artigo pretende partir da sobreposição entre tecnologia e política e do contexto de concentração de poder sobre diferentes camadas da Internet, para discutir as possibilidades de escape e resistência à vigilância em massa e a falta de autonomia sobre os próprios meios (coletivos e individuais) de comunicação e informação. De modo específico, o artigo pretende apresentar as "redes comunitárias" como meio de resistência, sobretudo na medida em que exercem autonomia relativa sobre sua infraestrutura de conexão.

Palavras-chave: Cibercultura, Ativismo, Tecnopolítica, Informação, Redes digitais.

Gobernanza de Internet, Infraestructura y resistencia

Resumen: Se puede decir que el nuevo campo de la "gobernanza de Internet" sufrió un "giro a la infraestructura" (*turn to infrastructure*). Se hizo evidente que los principios políticos de Internet son realizados por su arquitectura y operación, y que la forma más eficaz para hacer cumplir tales y tales principios políticos y morales en la red pasa a través de la influencia de su información. La "infraestructura" que soporta el funcionamiento de Internet se caracteriza por la combinación de medios físicos y lógicos que actualizan la transmisión, almacenamiento y procesamiento de los datos producidos por la actividad humana y no humana. Sin embargo, la inteligibilidad de la importancia política de la técnica parece no tener efecto, puesto que el control de la infraestructura de comunicación y la información se ejerce cada vez más de manera concentrada y bajo poder privado. Esta propuesta tiene como objetivo abordar la superposición entre la tecnología y la política, así como el contexto de concentración de poder sobre las diferentes capas de Internet, para discutir las posibilidades de escape y la resistencia a la vigilancia masiva y a la falta de autonomía sobre nuestros propios medios de comunicación e información. En concreto, el documento tiene como objetivo presentar las "redes comunitarias" como una forma de resistencia, sobre todo en el ejercicio de relativa autonomía sobre la infraestructura de conexión.

Palabras clave: Cibercultura, Activismo, Tecnopolítica, Información, Redes digitales.

Internet Governance, Infrastructure and resistance.

Abstract: It is fair to state that the "Internet governance" research field has suffered a "turn to infrastructure". It became clear that the political principles of the Internet are made concrete by its architecture and mode of operation. In other words, the most proficuous way to enforce moral and political values online goes through the shaping of the Internet infrastructure and functioning. The "infrastructure" that support the Internet operation can be understood as the material and logical apparatus through which data can be transmitted from end to end. This paper proposal intends to depart from the intersection between technology and politics and briefly describe the current context of concentration of power over the Internet infrastructure to discuss possibilities of resistance to mass surveillance mechanisms. More specifically, this proposal intends to introduce the "community networks" initiatives as a way of resistance once they exert relative autonomy (collective and individual) over connectivity infrastructure, which is understood as *commons* . This is an exploratory proposal that aims to deal with the relation between community based initiatives, autonomy, and counter-surveillance practices.

Keywords: Cyberculture, Activism, Technopolitics, Information, Digital networks.

DIEGO VICENTIN*

INTRODUÇÃO

Recentemente me deparei com o livro "*The Turn to Infrastructure in Internet Governance* " (Musiani, F., Cogburn, D.L., Denardis, L. y Levinson, N.S., 2016) em que, a começar pelo título, se apresenta o argumento de que a governança da Internet sofreu uma "virada para a infraestrutura". Na introdução do livro fica claro que a perspectiva adotada se encaixa na tradição norte-americana dos estudos STS (*Science and Technology Studies*) que possui algum acúmulo de pesquisa sobre infraestruturas de informação. Nessa perspectiva, a infraestrutura é comumente definida de modo relacional na medida em que se coloca como base para uma série de práticas que supõem seu funcionamento. Assim, uma infraestrutura é algo que se toma como dado. Algo invisível, que passa despercebido a não ser quando uma falha lhe dá visibilidade ao interromper o fluxo das práticas para as quais serve de base. O intento do livro é, de algum modo, ele próprio dar visibilidade para ações de governança que são tomadas via infraestrutura. Trata-se de desvelar decisões políticas que estão sendo incorporadas no funcionamento da rede; um tipo de governança que é feita *by design*.

Cedo ou tarde ficou claro que os princípios políticos da Internet são desempenhados por sua arquitetura e modo de funcionamento, e que a maneira mais eficaz de fazer prevalecer tais ou quais princípios políticos e morais na rede passa por influenciar sua tomada de forma. A "infraestrutura" que dá suporte ao funcionamento da Internet é caracterizada como o conjunto de meios materiais e lógicos que atualizam a transmissão, o armazenamento e o processamento do montante de dados produzidos pela digitalização da atividade humana e não humana. No entanto, a inteligibilidade da importância política da técnica parece não surtir efeito, uma vez que o controle sobre as infraestruturas de comunicação e informação se exerce de modo cada vez mais concentrado e sob poder privado. Esse artigo pretende partir da sobreposição entre tecnologia e política e do contexto de concentração de poder sobre diferentes camadas da Internet, para discutir as possibilidades de escape e resistência à vigilância em massa e a falta de autonomia sobre os próprios meios (coletivos e individuais) de comunicação e informação. De modo específico, o artigo pretende apresentar as "redes comunitárias" como forma de resistência, sobretudo na medida em que exercem autonomia relativa sobre sua infraestrutura de conexão, que é compreendida na chave do *commons*. Trata-se de um artigo exploratório, que deve tratar da relação entre autonomia, iniciativas comunitárias de comunicação e práticas anti -vigilância.

CONCENTRAÇÃO DE PODER NA E SOBRE A REDE

Na passagem para o século XXI a Internet parecia ter chegado para concretizar um tipo de comunicação ativa, emancipadora, que produziria outra ordem social. De fato, é inegável que a Internet alterou o balanço de poder sobre os meios de informação e comunicação. Ela expandiu a possibilidade de encontro no ciberespaço[1] e serviu, no mínimo, como catalisador de mudanças

políticas, culturais e produtivas que alteraram a vida em suas mais variadas dimensões. Com a Internet faz sentido pensar que "qualquer jovem pode construir um novo protocolo, um novo aplicativo, um novo site, alterar a audiência e atrair a atenção de milhões" (Silveira, 2007:87).

A defesa desse potencial de liberdade e auto-concretização está na base das revelações feitas por Snowden (Greenwald, 2014), justamente porque o conteúdo das revelações aponta a efetivação da tendência contrária. Hoje, tornou-se impossível alegar desconhecimento das práticas de controle e vigilância que constituem a Internet. O próprio Tim Berners-Lee, criador da *web*[2] ** e figura proeminente no W3C[3], reconheceu que a *web* tomou rumos indesejáveis e que é preciso reinventá-la[4]. Em 2012, o *cyberpunk* Bruce Sterling declarou que já não faz mais sentido falar de Internet, porque, quase sempre, quando dizemos "Internet" estamos na verdade nos referindo ao que ele chama de "*five stacks* " o grupo formado por Facebook, Google, Microsoft, Apple e Amazon.[5] Cada *stack* (pilha, torre, armazém) é definido como um "império de mídia social verticalmente integrado" cuja principal função é tirar os usuários da Internet e trazê-los para dentro de sua própria "pilha" sem que esses últimos sequer percebam. A Internet é convertida numa infraestrutura ultrapassada ("*legacy network*")[6] que serve essencialmente como meio de trânsito entre *stacks*. Cada *stack* tem seu modelo de negócio específico, mas basicamente todas vivem de vender a privacidade de seus usuários, que se acumulam dentro das "pilhas" aos montes e de maneira parcialmente voluntária.

Trata-se de uma "mudança topológica"[7] que aponta na direção da concentração de poder na rede e sobre a rede. Cada *stack* concentra em si uma capacidade incalculável de armazenamento, processamento, análise e transmissão de dados. Kanashiro, M. M., Bruno, F., Evangelista, R. A., Firmino, R. J. (2013) fazem o esforço de decodificar os termos de uso e a política de privacidade do Google e, com isso, fazem ver a maquinaria que extrai valor daquilo que insistimos chamar de privacidade. As *stacks* concentram em si o controle sobre uma imensa quantidade de dados gerados por seus usuários e também por aqueles que estão em relação com esses usuários, mas não necessariamente utilizam os serviços da empresa. Serviços, aliás, que são interligados de tal modo que um mesmo "perfil" possa trafegar entre eles e não seja encorajado a sair da *stack* para nada; quando isso eventualmente acontece, o monitoramento das atividades do usuário final não para. A concentração na infraestrutura da rede em torno desses "gigantes" (Musiani, 2015), torna o trabalho da NSA[8] e de outras agências de vigilância e espionagem bem mais fácil de ser realizado (Abdo, 2015).

Para Shoshana Zuboff (2015) trata-se de uma nova etapa no sistema produtivo, o "capitalismo de vigilância", que se baseia numa lógica coerente de acumulação cujo fim último é extrair valor não apenas da capacidade de predizer o comportamento dos consumidores-usuários, mas, sobretudo, de influenciá-lo na direção desejada. O capitalismo de vigilância tem como base o modelo de negócios estabelecido pelo Google, em que a capacidade de predição e controle do comportamento do usuário-consumidor depende da coleta e tratamento massivo de dados provenientes de diversas plataformas, aplicativos e aparelhos. Daí o apetite voraz não só do

Google, como também das outras *stacks*, em adquirir novas empresas e adentrar em mercados "vizinhos", que servem de suporte a seu funcionamento e dos quais sua expansão depende em alguma medida. O exemplo mais claro é o mercado que provê serviços de conexão; já são bem conhecidas iniciativas como *Google Fiber*, *Google Loon* e *Aquila*[9]. As *stacks* dependem da existência e da qualidade da infraestrutura que conecta o usuário final à rede e, por isso, têm que lidar com o setor das telecomunicações, onde também se observa concentração de poder e mercado.

O termo "Tele" é utilizado comumente para se referir às empresas operadoras de rede, concessionárias do ramo das telecomunicações. No Brasil, assim como em boa parte do mundo, tais empresas foram originalmente provedoras monopolistas de telefonia fixa. Com a onda de privatizações que varreu o setor nas duas últimas décadas do século XX, e a série de fusões e aquisições que tomou conta do mercado internacional desde então, hoje essas empresas se configuram como enormes conglomerados transnacionais que concentram em si uma série de serviços, como: telefonia (fixa e móvel), Internet banda larga (fixa e móvel), TV a cabo, TV por satélite, e outros tantos.

A concentração de mercado não é privilégio da América Latina e do Caribe, onde os grupos *América Móvil* e *Telefônica* disputam o poder hegemônico[10]. Nos EUA, Tim Wu (2012) conta como a empresa AT&T reconstruiu seu império depois de ter sido desmembrada; hoje o mercado norte -americano também vive sob uma espécie de duopólio onde apenas AT&T e Verizon tem cobertura de alcance nacional de telefonia e de banda larga móvel. Na Europa, DeFilippi e Tréguer (2014) demonstram como o mercado inovador de pequenos provedores de Internet, que surgiu em meados dos anos 1990, foi engolido pelas grandes corporações do setor.

Um desdobramento recente desse processo de concentração pode ser visto na iniciativa das Teles de implementar o modelo "*data caps",* que impõe limites de franquia na "Internet fixa" (cabo /WiFi) a exemplo do que já acontece na "Internet móvel" (rede celular). Nesse modelo, quando o usuário atinge um limite determinado de dados trafegados sua conexão é interrompida. Redes "móveis" e "fixas" formavam dois mercados que até pouco tempo eram considerados distintos, mas que agora se conjugam em muitos aspectos, impulsionados pela economia de escala e pela padronização técnica. O mercado que emerge dessa fusão ainda está tomando forma, mas é de se esperar que as Teles defendam o modelo que lhes confere mais poder sobre a infraestrutura de rede, controlando e taxando o *fluxo* dos dados (seu volume) e não apenas o acesso à rede (a conexão*)*. Trata-se de implementar um novo regime de escassez que, se concretizado, terá efeitos negativos aumentando as barreiras de entrada na cultura digital e diminuindo a capacidade de protagonismo do usuário final.

Além disso, tal escassez atinge diretamente as empresas protagonistas do "capitalismo de vigilância", que terão de barganhar ainda mais junto às operadoras de rede, seja para ter acesso a "vias rápidas" dentro da rede, ou para "pagar a conta" do consumidor-usuário no melhor estilo *zero-rating*[11]. Assim, fazer valer o modelo por franquia é garantir que as operadoras de rede se apropriem de parte dos ganhos produzidos pelo capitalismo de vigilância. De um lado, esse

movimento faz sentido já que as próprias Teles reconhecem que o futuro está mesmo no modelo de negócios implementado pelo Google; não é de hoje que elas vêm demonstrando interesse em rentabilizar os dados produzidos por seus clientes. Isso já vem sendo feito, por exemplo, quando as operadoras monetizam os dados de geolocalização e de navegação (*browsing*) de seus usuários[12]; assunto que foi tema de recente regulação nos EUA.[13]

Com isso, quero chamar atenção para o processo de concentração de poder na rede e sobre seu modo de funcionamento. Esse processo é duplo e, como tentei most, atinge a Internet tanto em sua camada de conteúdo/aplicações, quanto na infraestrutura de conexão que opera a transmissão dos dados. A bibliografia que trata do desenvolvimento da Internet e das redes informacionais levanta fortes indícios, em diversas frentes, que apontam para essa alteração topológica, para a concentração de poder.[14] No limite, o que se vê é o surgimento de uma *megamáquina* (Mumford, 1970; 1979) contemporânea cujo funcionamento domina o usuário final capturando sua atenção, seu tempo e sua capacidade produtiva. O humano é tornado parte componente de um sistema que lhe transcende: "peças componentes intrínsecas, 'entradas' e 'saídas', *feed-back* ou recorrências, que pertencem à máquina e não mais à maneira de produzi-la ou de se servir dela" (Deleuze e Guattari, 1997:158).

No entanto, esse processo de *sobrecodificação* de fluxo não acontece sem provocar fluxos desviantes, rotas de fuga, que resistem à concentração de poder na e sobre a rede. Muitos deles tomam corpo nas camadas mais altas da Internet, especialmente a partir de aplicações de arquitetura P2P (*peer-to-peer*)[15] que favorecem o anonimato dos usuários bem como o compartilhamento de recursos computacionais. O compartilhamento de arquivos via *torrent* é um exemplo; a navegação anônima via redes *Tor*, é outro. A lista é longa, e passa por redes sociais (*diaspora*) e pelo armazenamento remoto (*Drizzle*). São aplicações que se colocam como alternativa às *stacks* e à centralização da rede que elas atualizam; aplicações baseadas em P2P favorecem o compartilhamento, a descentralização e a autonomia do usuário, abrindo espaço para o anonimato e o exercício da liberdade na Internet. Já nas camadas mais baixas da infraestrutura de rede, que inclui o meio físico de conexão, emergem as "redes comunitárias". Vejamos.

REDES COMUNITÁRIAS, DESVIO E RESISTÊNCIA

> [...] as comunicações por computador e telefonia celular estão literalmente se fundindo para formar enormes gigantes que irão ter o monopólio sobre múltiplos meios de comunicação. Nesse contexto, um contramovimento vibrante de empreendedores, programadores, pesquisadores e ativistas começou a organizar sistemas alternativos de comunicação, controlados pela comunidade. (Meinrath, 2005:236)

O encontro entre *comunidade* e *computação em rede* emerge a partir de um caldo político que tomou corpo justamente com a descentralização dos meios de comunicação promovida pela Internet em seus primeiros anos. Esse encontro é marcado por aspectos da contracultura e dos movimentos baseados na vida comunitária que se espalharam pela costa oeste dos EUA na década de 1960 (Turner, 2005)[16]. Não sem razão, uma das primeiras redes comunitárias surge em Seattle

(EUA, 1994) cidade que ficou conhecida também pelo movimento de mídia independente, ou *Indymedia,* no contexto dos protestos antiglobalização (Coleman, 2013). Antes da abertura da Internet comercial, as "redes comunitárias" se colocavam como único meio de conexão à Internet para aqueles que não tinham acesso na universidade ou no trabalho (Powell, 2006). Uma das primeiras publicações acadêmicas sobre o tema é o livro escrito por Schuler (1996)[17] um dos fundadores da rede comunitária de Seattle (*Seattle Community Network, SCN*)[18].

Redes comunitárias como essa, de Seattle, surgiram na América do Norte nos anos 1990 como resultado da ação conjunta de ativistas ligados à tecnologia e líderes comunitários, que trabalharam para desenvolver "serviços computacionais orientados pela e para a comunidade" (Schuler, 1996:00). Assim, as *redes comunitárias* apareceram ainda antes da mobilidade concretizada pelos *notebooks* e *smartphones*, empunhando a bandeira da democratização do acesso (material e cognitivo) à computação em rede como uma de suas principais demandas políticas. A rede é geralmente estabelecida a partir da parceria com instituições como universidades, bibliotecas e ONGs; sua infraestrutura computacional conta com terminais de acesso (computadores) instalados em espaços públicos como: bibliotecas, terminais de ônibus, centros comunitários, etc. Também faz parte da infraestrutura das redes comunitárias um ambiente de rede local em que o usuário pode se comunicar com os demais membros da comunidade, desenvolver ferramentas, acessar e disponibilizar informações de interesse público. A computação é vista como incentivo à vida comunitária e à resolução negociada de problemas locais e de interesse comum[19].

A introdução de aparelhos WiFi no mercado, em 1999, expandiu o potencial das redes comunitárias para o espectro radioelétrico. A tecnologia foi apropriada, experimentada e desenvolvida por amadores, entusiastas e ativistas ainda antes de ser adotada pelas grandes operadoras de rede. É possível encontrar o registro de *redes comunitárias sem fios* em publicações acadêmicas já na primeira metade dos anos 2000 (Sandvig, 2004; Meinrath, 2005). Desde então, já se acumula uma bibliografia considerável sobre o tema. DeFilippi e Tréguer (2014) indicam que as redes comunitárias incorporam

> "(...) o*ethos* e o modelo de governança da Internet original: uma rede de pares que se relacionam como iguais e que se comunicam livremente numa arquitetura fim-a-fim descentralizada, em que o controle sobre as ferramentas usadas para a comunicação é exercido de baixo para cima, particularmente através da utilização de *software* livre" (p. 04).

Ainda antes, Powell (2006) já havia apontado para ligações entre as redes comunitárias e alguns princípios do *hacking* e do *software* livre como, por exemplo, a defesa de que "produtos não-comerciais e desenvolvidos coletivamente têm qualidade superior aos produtos comerciais-proprietários" (p. 04) e ainda que "estruturas organizacionais autônomas e descentralizadas são superiores às centralizadas" (p. 04).

Parte considerável dessas redes surge impulsionada pela inabilidade das operadoras comerciais em expandir sua infraestrutura com boa qualidade de banda passante para locais em que há pouco ou nenhum interesse comercial; os altos preços cobrados pelas operadoras entram nessa

equação como agravante e como impeditivo, a depender do caso (Bode, 2015; Brodkin, 2015). Noutras palavras, parte da motivação para a implementação das redes comunitárias advém do desejo de conectividade que não é satisfeito pelo mercado. No mínimo, então, as redes comunitárias são legitimadas pela vontade de compartilhar com vizinhos e amigos um sinal de Internet rápida via interface de rádio[20].

Assim, as motivações para a implementação de uma *rede comunitária sem fios* podem variar muitíssimo, numa amplitude que vai desde o simples desejo por uma conexão à Internet que tenha qualidade satisfatória e preço acessível, até motivações tecnopolíticas mais refinadas, de grupos que pretendem exercer algum grau de autonomia sobre os meios através dos quais se comunicam, ou seja, querem exercer autonomia sobre seu próprio sistema de informação. Daí que as redes comunitárias se vinculam e se associam a outros movimentos que também atravessam e informam a dimensão tecnopolítica da realidade. Já nos referimos ao *hacking*, aos movimentos de *software* livre e de mídia alternativa (*Indymedia*) mas, além deles, podemos ainda citar os movimentos de rádios livres, de comunidades tradicionais e indígenas, quilombolas, e de proteção do anonimato e da privacidade na rede.

O *design* da rede está relacionado às pretensões de cada comunidade. As redes *Mesh*[21], por exemplo, em princípio favorecem uma arquitetura descentralizada, em que cada nodo pode se conectar diretamente aos demais participantes da rede. Numa rede *Mesh* cada nodo, cada "usuário", é também um ponto de roteamento do fluxo de dados que atravessa a rede. Ou seja: cada usuário da rede funciona como meio de transmissão para o tráfego gerado pelos demais usuários aos quais ele se conecta diretamente. Desse modo, o mapa da rede não é fixo e varia de acordo com o número de usuários, alterando as possíveis rotas do fluxo entre dois nodos. Isso torna as redes *Mesh* mais robustas e adaptáveis, além de favorecer a proteção da privacidade (DeFilippi, 2015:304). O modo de operação dessa infraestrutura técnica ressoa com a pretensão de um modelo comunitário em que a participação de todos é requerida igualmente; uma arquitetura em que cada participante é ativo (Sinnreich, Graham, & Trammel, 2011).

Esse papel ativo que o usuário potencialmente assume numa rede comunitária subverte a lógica pela qual estamos acostumados a enxergar a Internet comercial, como serviço oferecido no mercado. Echaniz (2015) defende uma mudança no olhar sobre a rede cujo foco deve partir do menor para o maior; sugere um olhar em que a "última milha" torna-se "primeira milha" porque as bordas da rede devem ser valorizadas. De certo modo essa valorização vem ocorrendo: as redes comunitárias começam a chamar atenção como alternativa real e viável à concentração de poder sobre os meios de comunicação; sobre as redes que trafegam nossos dados de um canto até outro do planeta. Como veremos mais adiante, instituições ligadas ao funcionamento e governança da Internet vêm demonstrando interesse crescente nas redes comunitárias. Ficou claro nos últimos anos que a disputa sobre o modo de funcionamento e a apropriação da infraestrutura de transmissão e processamento de dados é a própria (re)distribuição de potências do mundo contemporâneo; é onde acontece a luta política para definir o(s) modo(s) como nos conectamos a uma dimensão da realidade que cresce em importância: o ciberespaço (para não nos restringirmos à Internet).

Assim, as redes comunitárias desdobram o problema da relação entre tecnologia e política porque potencialmente concretizam uma resistência local, comunitária, frente aos grupos que controlam nossos meios de informação e comunicação em escala global. Trata-se da possibilidade de exercer poder local sobre a infraestrutura de rede que é usualmente caracterizada como "última milha" (convertida, assim, em "primeira"). Isso implica a potencial adoção de tecnologias livres, minoritárias em relação aos padrões utilizados pelo mercado e, portanto, que resultam em modos de operação (de funcionamento) que diferem das redes comerciais em vários aspectos.

REDES COMUNITÁRIAS E GOVERNANÇA DA INTERNET

O tema das redes comunitárias vem recebendo atenção crescente, inclusive de organizações que desempenham papéis importantes como mecanismos de tomada de decisão que modulam o funcionamento da Internet.[22] Parte dessa atenção vem acompanhada da expectativa de que as próprias comunidades desenvolvam a capacidade de fazer avançar a expansão da Internet para localidades que não despertam grande interesse de mercado. Desse modo, as redes comunitárias são colocadas numa chave específica que advoga pela "conectividade". Essa expectativa estimula a formalização da existência das redes comunitárias, abrindo espaço no debate regulatório e de políticas públicas.

Em 2015, houve o surgimento de uma "coalizão dinâmica" no bojo do IGF (*Internet Governance Forum*)[23] que se dedica à conectividade comunitária.[24] O DC3 (*Dynamic Coalition on Community Connectivity*)[25] é uma coalizão multissetorial que pretende definir um conjunto de "melhores práticas" para o funcionamento e a organização das redes comunitárias, bem como fazer recomendações de políticas que favoreçam o desenvolvimento dessas redes. O grupo reúne voluntários de vários países, em sua maioria membros da sociedade civil organizada e pesquisadores diretamente envolvidos com a implementação e manutenção de redes comunitárias. A próxima reunião presencial do DC3 acontecerá em dezembro, por ocasião do IGF 2016 na cidade de Guadalajara, México, quando o grupo deve apresentar sua "declaração sobre a conectividade comunitária".[26]

Na versão temporária do documento que institui princípios e definições para redes comunitárias, estas são caracterizadas por seis "pontos". O primeiro deles diz respeito a apropriação coletiva, e indica que "a infraestrutura de rede é de propriedade da comunidade em que é implementada". Em seguida o documento institui que tal infraestrutura deve ser (2) "governada e operada pela comunidade" o que pressupõe que (3) "os detalhes de implementação da rede são públicos e acessíveis a todos" e que (4) "qualquer um está autorizado a estender a rede, desde que esteja de acordo com seus princípios e seu design". A rede (5) "deve oferecer reciprocidade" em acordos de *free peering* e pode servir como meio de trânsito entre redes com as quais têm acordos desse tipo. Por fim, mas não menos importante, uma rede comunitária é também caracterizada por (6) "considerar questões de segurança e privacidade no *design* e na operação da rede".

Ainda que as redes comunitárias carreguem de maneira mais explícita a bandeira da conectividade, da expansão dos meios de informação e comunicação, sua potência mais liberadora está na

apropriação local da infraestrutura. Isso passa pela afirmação do direito de uma comunidade em construir seus próprios meios de comunicação quando não há interesse de mercado; ou ainda quando o mercado não dá conta dos anseios da comunidade, por exemplo, no que diz respeito a qualidade do serviço, segurança da informação ou proteção da privacidade. Nesse texto, é o ponto sobre segurança e privacidade que interessa particularmente. É preciso notar, no entanto, que ele consta mais como uma preocupação/recomendação do que como algo que é completamente colocado em prática pelas redes comunitárias. Mas, é de se supor que, uma vez que a comunidade de usuários tenha se apropriado da infraestrutura local, tanto em sua implementação quanto em sua gestão e governança, tornam-se mais efetivas as práticas de proteção à privacidade porque podem ser implementadas *by design* desde a camada de conexão. ** Acima, já demos o exemplo das redes *Mesh* cuja arquitetura e modo de funcionamento podem favorecer o anonimato dos usuários, mas, na pratica, isso varia de acordo com o modo como a rede é implementada. Outra possibilidade de implementação que favorece a privacidade em redes locais sem fio é a randomização dos endereços MAC, dispositivo cujo padrão que está sendo desenvolvido pelo IETF em conjunto com o IEEE 802[27].

Retornamos ao argumento que abre o texto e que também servirá para encerrá-lo. Se há uma "virada para a infraestrutura" na governança da internet, trata-se de reconhecer que apropriar-se da infraestrutura e tomar decisões sobre seu funcionamento é a maneira mais eficaz de fazer prevalecer quaisquer princípios políticos e morais na rede. Isso necessariamente passa por modular sua evolução e influenciar sua tomada de forma. E se existem limites que são impostos pela extensão da infraestrutura, e as redes locais comunitárias podem apenas garantir um grau de autonomia que é relativo, limitado, por outro lado essa autonomia pode servir de base para um exercício ampliado de liberdade, especialmente no contexto em que nos encontramos, de alta concentração de poder na rede. É preciso que essas comunidades, que não se submetem aos interesses de mercado ou não são servidas adequadamente por ele, tenham acesso as condições necessárias para construir e governar suas próprias redes de informação e comunicação. Nessa direção o campo da Governança da Internet, em fóruns como o DC3, pode trazer uma contribuição interessante em nível global se garantir que iniciativas locais gozem de legitimidade e dos meios necessários para definir sua própria infraestrutura de informação e comunicação.

NOTAS

* Doutor em Sociologia, UNICAMP, professor da Fundação Escola de Sociologia e Política de São Paulo (FESPSP). Contato: djvicentin@gmail.com

1. Sobre a definição de ciberespaço, concordamos com Bruce Sterling (1992), para quem esse espaço é uma espécie de "fronteira eletrônica" criada a partir da invenção do telefone, e que ganhou luz e profundidade visual com a invenção da Internet. "Ciberespaço é o 'lugar' onde a conversação telefônica acontece. Não dentro do seu telefone real, o aparelho de plástico na sua mesa. Também não está dentro do telefone da outra pessoa, em alguma outra cidade. É o lugar entre os telefones. Um lugar indefinido lá fora, onde vocês dois, dois seres humanos, realmente se encontram e se comunicam" (Sterling, 1992:XII) [tradução minha]

2. A *web* é uma aplicação da Internet, mais especificamente aquela baseada na linguagem de hipertexto (HTML) cujo acesso acontece a partir do *web browser* (navegador), e a partir do modelo de comunicação comumente chamado de "cliente-servidor". É relativamente comum que a Internet e a web sejam tratadas como sinônimos, ou como instâncias intimamente associadas, isso acontece sobretudo porque a expansão da Internet comercial veio acompanhada da popularização das aplicações *web*.

3. *World Wide Web Consortium* (W3C) é o fórum de padronização que define os protocolos básicos de funcionamento da *web*. Foi fundado por Tim Berners-Lee em 1994 e hoje reúne entre seus membros grandes atores da economia digital.

4. Ver: http://www.nytimes.com/2016/06/08/technology/the-webs-creator-looks-to-reinvent-it.html [último acesso: 03/07/2016]

5. Ver: Sterling, 2012, 26m30s-35m00s. XSW2012. The Ultimate Bruce Sterling Talk. Disponível em: https://huffduffer.com/solle/70031 [último acesso: 03/07/2016].

6. O termo "*legacy network* ", utilizado por Sterling, é uma forma genérica de se definir a redes que já não são mais utilizadas porque sua tecnologia tornou-se obsoleta e caiu em desuso. O termo é comum na engenharia de redes e pode-se dizer que surgiu a partir de protocolos ancestrais à Internet e ao TCP/IP que, também por serem proprietários e fechados, tornaram-se rapidamente obsoletos.

7. A topologia de rede dá conta do modo como os diferentes nodos de uma determinada rede estão distribuídos e interconectados, seja em sua camada física ou lógica. Essa distribuição, claro, não se dá de maneira uniforme (seja ao longo do espaço e/ou do tempo) produzindo diferenças que se expressam em termos de concentração e dispersão. "A Internet é de fato uma rede sem escala (*scale free network*), o que significa que a conectividade entre os nodos não se mantém estável na medida em que a rede cresce; de modo contrário, alguns nodos atraem com mais força os novos nodos ('ligação preferencial') e assim criam uma conectividade maior com os nodos que já são poderosos. De tal modo, todo novo website será mais rapidamente conectado ao Google que a qualquer outro nodo, o que aumenta a centralidade do Google na rede como um todo." (Boullier, 2013:00) [tradução minha]

8. Agência de Segurança Nacional (National Security Agency) dos EUA. Principal órgão envolvido nas denúncias de espionagem dos EUA sobre sua própria população e sobre outros países, inclusive países considerados aliados pelos EUA, como Brasil e Alemanha. (Greenwald, 2014)

9. Os três projetos colocam empresas que atuam na camada de aplicações, como Google e Facebook, na disputa pelo mercado de conexão, especialmente em locais onde a Infraestrutura de conexão é ausente ou insuficiente. Daí a promessa um tanto descabida de prover conexão via balões e drones, caso do Google Loon e do projeto Aquila (Facebook). Ver: https://fiber.google.com/about/; https://x.company/intl/pt-BR_br/loon/; https://www.facebook.com/notes/mark-zuckerberg/the-technology-behind-aquila/10153916136506634/ [último acesso: 03/11/2016]

10. Em conjunto as empresas *América Móvil* e *Telefônica* concentram mais de 70% de todas as linhas ativas de telefonia móvel de toda a América Latina. Ver: http://www.teleco.com.br/operadoras/amovil.asp [último acesso: 03/07/2016]

11. A prática denominada de *zero-rating* consiste num acordo entre uma empresa provedora de aplicações e uma ou mais operadoras de rede, de tal modo que o usuário final não pague pelo acesso a aplicações

específicas da internet, como o Facebook e seus parceiros (programa Free Basics). Tais acordos não são transparentes e não se sabe exatamente qual é a compensação que os provedores de aplicação concedem aos provedores de conexão. Se a compensação não é financeira, podemos esperar que seja algo relacionado ao compartilhamento dos rastros de navegação dos usuários. A validade desses acordos está sendo questionada pela sociedade civil, especialmente porque quebra o princípio da neutralidade da rede. A India, por exemplo, recentemente proibiu a prática de *zero-rating*, ver: http://www.thehindu.com/opinion/op-ed/Free-Basics-now-through-the-backdoor/article14471120.ece [último acesso: 01/12/2016]

12. Ver o exemplo da AT&T nos EUA: https://www.technologyreview.com/s/428989/att-looks-to-outside-developers-for-innovation/
E ainda: https://www.technologyreview.com/s/513016/how-wireless-carriers-are-monetizing-your-movements/ [último acesso: 01/12/2016]

13. Ver: https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules [último acesso: 01/12/2016]

14. Além das referências que já foram mobilizadas ao longo do texto na construção do argumento, gostaria ainda de sugerir: Assange, Appelbaum & Muller-Maguhn, 2012; Marsden, 2010; Morozov, 2011; 2013; Mueller, 2010.

15. Uma arquitetura P2P ou *peer-to-peer*, como indica Musiani (2015:24): "tem uma definição técnica relativamente simples: trata-se de um modelo de rede informática estruturado de maneira descentralizada de tal modo que as comunicações ou trocas ocorrem entre nodos dotados de responsabilidades iguais dentro do sistema" [*tradução minha*]. Esse tipo de arquitetura sugere um "modelo organizacional" baseado na troca, no compartilhamento, na cooperação não-hierarquizada e, portanto, na autonomia. Além disso, o P2P é um princípio de funcionamento do protocolo TCP/IP que serviu de base para a fundação da Internet (Galloway, 2004:47).

16. Como oposição ao modo de vida imposto pelo complexo militar-industrial que caracteriza o período da guerra fria, nos EUA, a década de 1960 viu surgir a contracultura, que defende modelos comunitários de vida. Assim, naquele período multiplicou-se o número de comunas ao longo da costa oeste dos EUA. Turner (2005) relata o surgimento de uma das primeiras "comunidades virtuais" a partir desse contexto e como desdobramento de uma publicação que se dedicava justamente aos temas de interesse das comunas. Tal publicação (*Whole Earth Catalog*) assentou as bases para "uma sociabilidade geograficamente distribuída" (Turner, 2005:511) que ajudaria a formar as "comunidades virtuais", claro, em associação com a computação em rede. As "comunidades virtuais" e as "redes comunitárias" certamente compartilham traços adquiridos da contracultura, mas, são modos distintos de atualização do encontro entre comunidade e computação. As ressonâncias e dissonâncias entre esses dois modos de atualização certamente ainda precisam ser bem trabalhadas. No entanto, podemos apontar timidamente que as "redes comunitárias" se dedicam necessariamente à infraestrutura básica que garante o acesso ao ciberespaço, ou seja, à infraestrutura de conexão que possibilita a existência das "comunidades virtuais".

17. O livro de Schuler intitulado "*New Community Networks, wired for change* ", de 1996, está disponível para leitura online no seguinte endereço: http://www.scn.org/ncn/ [último acesso: 03/07/2016]

18. Ver: http://www.scn.org/ [último acesso: 03/07/2016]

19. Schuler (1996) é abertamente influenciado pelo trabalho do sociólogo Robert D. Putnam que desenvolve sua versão do conceito de "capital social", especialmente ligado à vida comunitária, como uma forma de "estoque" de confiança comum e compartilhada entre os membros de uma determinada comunidade. Ver: Putnam, 2002.

20. Segundo dados da pesquisa TIC domicílios de 2015, 16% dos domicílios com acesso à Internet no Brasil fazem uso de uma conexão que é compartilhada com um ou mais domicílios vizinhos. Esse número sobe para 21% considerando apenas áreas rurais e para 23% entre os domicílios com renda de até 1 salário-mínimo. A pergunta foi aplicada de tal modo que a informação relevante dá conta de saber se a conexão é ou não compartilhada com outro domicílio, sem especificar o modo como isso é feito e quem arca com os custos da conexão. Ver: http://cetic.br/tics/usuarios/2015/total-brasil/A13/ [último acesso: 03/07/2016]

21. Guia sobre o funcionamento básico das redes *mesh*: http://tecnologia.hsw.uol.com.br/rede-mesh-sem-fio.htm [último acesso: 03/07/2016]

22. A *Internet Society* (ISOC), por exemplo, vem promovendo debates e iniciativas ligadas à conectividade comunitária ao menos desde 2010. Ver: http://www.internetsociety.org/what-we-do/where-we-work/asia/south-asia/wireless-communities; [último acesso: 03/07/2016]

23. O Fórum de Governança da Internet (IGF, em inglês) foi instituído pelo ONU em 2005 no contexto da Cúpula Mundial da Sociedade da Informação (*World Summit on Information Society*, WSIS). Trata-se de uma reunião anual, com representação multissetorial, que promove debates sobre temas sensíveis à governança da Internet visando promover recomendações sobre seu modo de funcionamento e gestão. Apesar da visibilidade que o fórum adquiriu e de sua importância como meio de pautar a agenda da governança da Internet, suas recomendações não tem poder normativo. Ver: Mueller, 2010; Rosa & Vicentin, 2016.

24. O DC3 é resultado mais objetivo do *workshop* "Community Networks: a Revolutionary Paradigm" realizado no IGF (Internet Governance Forum) de 2015, em João Pessoa (PB).

25. Cf. *The Internet Governance Forum (IGF), Dynamic Coalition on Community Connectivity (DC3)* https://www.intgovforum.org/cms/175-igf-2015/3014-dynamic-coalition-on-community-connectivity-dc3 [último acesso: 03/07/2016]

26. O documento está sendo preparado pelos membros do grupo e está aberto a contribuições no seguinte endereço: https://pad.codigosur.org/GuadalajaraDeclaration [último acesso: 15/11/2016]

27. Ver: https://standards.ieee.org/events/iot/presentations/ieee_e2e_trust_and_security_workshop_for_iot_-_wi-fi_privacy.pdf [último acesso: 15/11/2016]

REFERÊNCIAS

Abdo, A. H. (2015). Descentralização e criptografia no combate à vigilancia e controle. Em *Anais do 3o Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territórios*. Rio de Janeiro, Brasil.

Assange, J. Appelbaum, J. & Muller-Maguhn, A. (2012). *Cypherpunks: freedom and the future of the Internet*. Times Group Books.

Bode, K. (2015). After A Decade Of Waiting ForVerizon, Town Builds Itself Gigabit Fiber For $75 Per Month. *Techdirt*. URL: https://www.techdirt.com/articles/20151215/07583533085/after-decade-waiting-verizon-town-builds-itself-gigabit-fiber-75-per-month.shtml

Boullier, D. 2014. Le «hard» du «soft»: la matérialité du réseau des réseaux. *CERISCOPE Puissance*. Disponível em: http://ceriscope.sciences-po.fr/puissance/content/part2/le-hard-du-soft-la-materialite-du-reseau-des-reseaux.

Brodkin, J. (2015). How a Group of Neighbors Created Their Own Internet Service. *ArsTechnica*. URL: http://arstechnica.com/information-technology/2015/11/how-a-group-of-neighbors-created-their-own-Internet-service/

Coleman, E. G. (2013). *Coding Freedom: the ethics and aesthetics of hacking*. Princeton and Oxford: Princeton University Press.

DeFilippi, P. (2015). Community Mesh Networks: citzens' participation in the deployment of smart cities. In A. Vesco, & F. Ferrero, *Handbook of Research on Social, Economic, and Environmental Sustainability in the Development of Smart Cities Hershey*, (pp. 296-312), Paris: IGI Global.

Defilippi, P., Tréguer, F. (2014). Expanding theInternet Commons: The Subversive Potential of Wireless Community Networks. *Journal of Peer Production*. Disponível em http://peerproduction.net/wp-content/uploads/2015/01/De-Filippi-Tr%C3%A9guer-Expanding-the-Internet-Commons-with-Community-Networks.pdf

Deleuze, G., e Guattari, F. (1997). *Mil Platôs: capitalismo e esquizofrenia.* Vol. 5. Rio de Janeiro: Ed. 34.

Echaniz, N. (2015). Redes comunitárias: Internet desde la primera milla. In *Frida 10 años contribuyendo al desarrollo en américa Latina y el Caribe*. Cidade do México, LACNIC. Disponível em http://lacnic.net/frida/FRIDA-book2015-es.pdf

Galloway, A. R. (2004). *Protocol: how control exists after decentralization*. Cambridge: MIT Press.

Greenwald, G. (2014). *No place to hide*. Nova Iorque: Metropolitan Books.

Kanashiro, M. M., Bruno, F., Evangelista, R. A., Firmino, R. J. (2013). Maquinaria da privacidade. *Rua* (UNICAMP), 1, 22.

Marsden, C. (2010). *Net Neutrality: towards a Co-regulatory Solution*. London; New York, N.Y.: Bloomsbury Academic.

Meinrath, S. D. (2005). Wirelessing the World: The Battle over (Community) Wireless Networks. In R. McChesney (ed) *The Future of the Media: Resistance and Reform in the 21st Century*, (pp. 219-42). New York: Seven Stories Press.

Morozov, E. (2011). *The NetDelusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Morozov, E. (2013). *To save everything click here. The folly of technologial solutionism.* New York: PublicAffairs.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: The MIT Press.

Mumford, L. (1970). *The Myth of the Machine: the pentagon of power*. Nova Iorque: Columbia University Press.

Mumford, L. (1979). *Interpretations and Forecasts: 1922-1972*. Mariner Books.

Musiani, F. (2015). *Nains sans géants, architecture decentralisée et services Internet.* Paris: Presses des Mines.

Musiani, F., Cogburn, D.L., Denardis, L. y Levinson, N.S. (Eds.) (2016). *The Turn to Infrastructure in Internet Governance*. UK: Palgrave Macmillan.

Powell, A. (2006). *"Last Mile" or Local Innovation? Canadian Perspectives on Community Wireless Networking as Civic Participation.* Disponível em http://papers.ssrn.com/abstract=2103713.

Putnam, R. D. (2002). *Comunidade e Democracia: a experiência da Itália moderna*. 3 ed. Rio de Janeiro:FGV.

Rosa, F. R. e Vicentin, D. (2016). Governança da Internet e suas implicações para políticas publicas. *CROLAR (Critical Reviews on Latin America Research)*, 5, 67-77.

Sandvig, C. (2004). An Initial Assessment of Cooperative Action in WiFi Networking. *Telecommunications Policy,* 28(7/8), 579-602.

Schuler, D. (1996). *New Community Networks*. Disponível em: http://www.scn.org/ncn/.

SILVEIRA, S. A. (2007). Comunicação digital, redes virais e espectroaberto. *Líbero*,10(19). Disponível em: http://www.revistas.univerciencia.org/index.php/libero/article/view/3193/3003

Sinnreich, A., Graham, G., & Trammel, A. (2011). Weaving a New 'Net: A Mesh-Based Solution for Democratizing Networked Communications. *The Information Society* 27(5): 336–345.

Sterling, B. (2012). "The Ultimate Bruce Sterling Talk". Disponível em: https://huffduffer.com/solle/70031.

Turner, F. (2005). Where the counterculture met the new economy. The WELL and the origins of virtual community. *Technology and Culture,* 46(3), 485-512.

Wu, T. (2012). *Impérios da comunicação: do telephone à Internet, da AT&T ao Google.* Rio de Janeiro: Zahar.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, 75–89.

ESTRATÉGIAS DE CONTRAVIGILÂNCIA E RESISTÊNCIA DURANTE AS MANIFESTAÇÕES DE 2013 NO BRASIL

Resumo: Tendo em vista as manifestações de 2013, que ocorreram nas ruas das principais capitais do Brasil, iremos realizar uma cartografia das diversas estratégias de contravigilância e resistência à vigilância governamental produzidas pelos ativistas engajados na mobilização dos protestos. Em junho de 2013, o Brasil viu crescer, exponencialmente, o número de pessoas nas ruas protestando, num primeiro momento, contra o aumento da tarifa do transporte público e, num segundo momento, com pautas variadas. O Facebook se tornou um ator importante nesse processo, pois serviu de lugar para a propagação de ideias, divulgação dos atos e troca de experiências entre os ativistas. Por isso mesmo, transformou-se em uma poderosa fonte de informação para a mídia, em seu trabalho de formular reportagens, e para a polícia, em seu trabalho de ordenar a movimentação nas ruas e combater atos violentos durante os protestos, como depredação de prédios e queima de ônibus. Com a prisão de alguns ativistas, o monitoramento digital realizado pelo governo ficou evidente, provocando medo e fazendo os ativistas se preocuparem com a própria segurança de modo mais efetivo, lançando mão de algumas estratégias de resistência. A partir da análise da conexão entre ativistas e Facebook, de reportagens publicadas em jornais e revistas e de entrevistas com três ativistas, cinco policiais, um jornalista e dois advogados, foi possível cartografar algumas formas de resistência, desde a não participação no Facebook até a formulação de uma cultura de segurança.

Palavras chave: Vigilância, Resistência, Manifestações.

LUCIANA SANTOS GUILHON ALBUQUERQUE*
ROSA MARIA LEITE RIBEIRO PEDRO**

Estrategias contra la vigilancia y la resistencia durante las manifestaciones en Brasil 2013

Resumen: Teniendo en cuenta los acontecimientos de 2013, que tuvo lugar en las calles de las principales ciudades de Brasil, llevaremos a cabo un mapeo de las diversas estrategias de contravigilancia y resistencia a la vigilancia gubernamental producida por activistas que participan en la movilización de las protestas. En junio de 2013, Brasil ha visto crecer de forma exponencial, el número de personas en las calles protestando, al principio, en contra del aumento en la tarifa del transporte público y, en segundo lugar, con diferentes agendas. Facebook se ha convertido en un jugador importante en este proceso, ya que sirve como un lugar para la difusión de las ideas, la difusión de las acciones y el intercambio de experiencias entre los activistas. Por lo tanto, se ha convertido en una poderosa fuente de información para los medios de comunicación, en su trabajo para la formulación de informes y la policía en su trabajo para ordenar el movimiento en las calles y combatir los actos violentos durante las protestas, como la depredación de los edificios y autobús en llamas. Con la detención de algunos activistas, la vigilancia digital por el gobierno fue evidente, causando miedo y haciendo activistas se preocupan por su propia seguridad de manera más eficaz, haciendo uso de algunas estrategias de resistencia. A partir del análisis de conexión entre los activistas y Facebook, los artículos publicados en periódicos y revistas y entrevistas con tres activistas, cinco policías, un periodista y dos abogados, fue posible mapear algunas formas de resistencia, ya que ningún juego en Facebook para formulación de una cultura de seguridad.

Palabras clave: Vigilancia, Resistencia, Manifestaciones.

Strategies against surveillance and resistance during the 2013 demonstrations in Brazil

Abstract: Given the events of 2013, which took place in the streets of the main cities of Brazil, we will conduct a mapping of various countersurveillance strategies and resistance to government surveillance produced by activists engaged in mobilizing the protests. In June 2013, Brazil has seen grow exponentially, the number of people on the streets protesting, at first, against the increase in public transport fare and, second, with varying agendas. Facebook has become an important player in this process because it served as a place for the spread of ideas, dissemination of actions and exchange of experiences among activists. Therefore, it has become a powerful source of information for the media, in their work to formulate reports and the police in their work to order the movement in the streets and combat violent acts during the protests, as depredation of buildings and bus burning. With the arrest of some activists, the digital monitoring by the government was evident, causing fear and doing activists worry about his own safety more effectively, making use of some strategies of resistance. From the connection analysis between activists and Facebook, articles published in newspapers and magazines and interviews with three activists, five policemen, one journalist and two lawyers, it was possible to map some forms of resistance, since no stake in Facebook to formulation of a safety culture.

Keywords: Surveillance, Resistance, Demonstrations.

INTRODUÇÃO

Junho de 2013 ficou marcado na história recente do Brasil como um mês de intensas manifestações nas ruas das principais cidades do país, que se prolongaram por algum tempo. Começaram em São Paulo, mobilizadas pelo aumento da passagem de ônibus e se espalharam rapidamente pelo resto do país, ampliando o número de pessoas nas ruas e das pautas reivindicadas.

Além da participação da mídia mais tradicional, a Internet foi um ator importante nesse processo, pois os atos foram marcados e divulgados por meio de redes sociais, especialmente o Facebook. Debates acalorados, exibição de videos, troca de ideias, formação de coletivos e outras tantas ações também tiveram lugar na rede virtual. O ativismo no Brasil parece ter fortalecido sua conexão com a Internet durante esse período. Por isso mesmo, tornou-se um lugar de proliferação de informações interessantes para as outras mídias tradicionais e, principalmente, para as polícias, em seus diferentes papeis.

No Brasil, temos a Polícia Militar que atua no policiamento ostensivo nas ruas e a Polícia Civil, responsável pelo trabalho investigativo. Nesse período, a Polícia Militar foi responsável por acompanhar e garantir a segurança das manifestações nas ruas, enquanto a Polícia Civil investigou a autoria dos atos de depredação de prédios públicos e privados e de incêndio a ônibus.

A Polícia Militar era, tradicionalmente, avisada sobre o trajeto de qualquer ato público. No entanto, nesse período, isso muitas vezes não aconteceu, por uma atitude de questionamento das instituições do governo e porque algumas vezes o trajeto era decidido durante o próprio percurso. Juntamente com um trabalho de infiltração nas ruas e nas assembleias, os policiais acessaram as redes sociais, principalmente Facebook e Mídia Ninja[1], a fim de acompanhar as decisões e obter informações relevantes sobre o trajeto e os manifestantes.

A Polícia Civil, já acostumada a usar o Facebook na investigação de crimes cibernéticos, juntou as informações coletadas na rede com testemunhos de pessoas envolvidas nos atos e mandados de busca e apreensão autorizados pela justiça. Montou um processo que culminou com a prisão de vinte e três ativistas, causando grande comoção e uma onda de medo e paranoia, relatada por eles[2].

Essas prisões fizeram ampliar nos ativistas a consciência da vigilância exercida pelo governo. Muitos já carregavam certa preocupação adotando táticas seguras de comunicação via Internet, mas a grande maioria parecia bem despreocupada, agindo com bastante liberdade na expressão e divulgação de ideias, fotos e vídeos. Com as prisões, as consequências dessa exposição e visibilidade na rede parecem ter ficado mais claras, gerando a busca de novas táticas de resistência.

ALGUMAS DIRETRIZES TEÓRICAS SOBRE RESISTÊNCIA

Para falar de resistência, entendemos que resgatar Foucault é fundamental, pois é um dos autores que desenvolveu essa ideia em seu trabalho sobre as relações de poder. Em seu pensamento, poder não possui uma dimensão concreta nem se refere a uma substância ou algo que se possui ou se perde, muito menos se remete à ideia de repressão. Poder implica ação, ele se exerce nas relações humanas, inclusive nas mais cotidianas; é uma relação de força, que se refere à "relação em que cada um procura dirigir a conduta do outro" (Foucault, 2010: 277), ou seja, em agir sobre a ação do outro. Poder não quer dizer dominação de um ou uns sobre os outros, como algo que se detém, mas ele se exerce em rede.

> Nas suas malhas os indivíduos não só circulam, mas estão sempre em posição de exercer esse poder e de sofrer sua ação; nunca são o alvo inerte ou consentido do poder, são sempre centros de transmissão. [...] O indivíduo é um efeito do poder e simultaneamente, ou pelo próprio fato de ser um efeito, é seu centro de transmissão (Foucault, 1979: 183/184).

Portanto o indivíduo não é passivo frente ao poder, mesmo sofrendo seus efeitos também o transmite na sua relação com os outros. Por isso não podemos falar de repressão pura e simples, mas só podemos admitir a existência de relações de poder se os indivíduos forem livres para

agir e é na hora da escolha de que ação tomar que podemos observar os efeitos de poder. Sempre existe possibilidade de resistência nas relações de poder. Na medida em que os indivíduos são livres para agir e refletir essas forças que o atingem, várias possibilidades de ação são possíveis, inclusive a resistência à força e a produção de algo novo, não previsto e que se oponha à corrente que predomina.

Para o autor (Foucault, 2010), as relações de poder são móveis e podem ser reversíveis. No entanto, é possível encontrar situações de dominação em que essas relações de poder estão há muito tempo fixadas de modo assimétrico e com uma margem de liberdade mínima. Ainda assim, acredita ser possível criar ações de resistência a essa força.

Desse modo, entendemos resistência como uma força, inserida numa relação de poder, que se opõe a outra força, resistindo à sua ação:

> Portanto, para que se exerça uma relação de poder, é preciso que haja sempre, dos dois lados, pelo menos uma certa forma de liberdade. [...] Isso significa que, nas relações de poder, há necessariamente possibilidade de resistência, pois se não houvesse possibilidade de resistência –de resistência violenta, de fuga, de subterfúgios, de estratégias que invertam a situação-, não haveria de forma alguma relações de poder (Foucault, 2010: 277).

No entanto, resistência não se refere a uma força meramente reativa, dizer não é apenas uma forma de resistir. Dentro do pensamento Foucaultiano podemos apontar para sua dimensão positiva e criativa, que afirma outras possibilidades de ser e estar no mundo. Nesse sentido, entendemos que as estratégias dos ativistas para escapar da vigilância não se configuram apenas como uma reação à ação do governo, mas como uma tentativa de afirmação de outras formas de vivência coletiva e organização política, contrárias à ordenação social predominante.

Como indivíduos, não estamos fora das relações de poder, mas somos atravessados por esse jogo, que Foucault (2004) caracteriza como uma luta. Uma vez dentro, sempre é possível mudar a situação, senão viveríamos sob o jugo da obediência simplesmente. A seu ver "A resistência vem em primeiro lugar, e ela permanece superior a todas as forças do processo, seu efeito obriga a mudarem as relações de poder" (Foucault, 2004: 268).

Se entendermos o monitoramento como uma das estratégias utilizadas pelo governo na tentativa de ordenar o social, ou seja, de dar uma ordem à instabilidade causada pelo questionamento promovido pelas manifestações, podemos resgatar também a reflexão de John Law (1992). O autor sustenta que todo esforço de ordenamento encontra resistências. Toda tentativa de apaziguar as forças em disputa e criar uma ordem ou uma estabilização precisa vencer certas resistências. Dessa maneira, ações de resistência seriam aquelas que oferecem obstáculos e desafios ao monitoramento ou tentariam se opor a ele, encontrando saídas para escapar de seu alcance.

CARTOGRAFIA DAS RESISTÊNCIAS

Nesse exercício de cartografar as estratégias de resistência, criadas pelos ativistas, frente à crescente vigilância digital exercida pelo governo, encontramos algumas práticas. Em primeiro lugar, sempre existe a possibilidade de não ter conta no Facebook.

> P: Mas qual divergência, assim, qual razão mais forte você diria para não ter o perfil?
>
> E: Olha, acho que tem tudo a ver com todo esse aparato de vigilância que está se montando dos Estados associados a algumas grandes corporações, no caso o Facebook (Entrevistado 4, ativista)[3].

No entanto, essa alternativa traz problemas. Abre-se mão de usufruir das vantagens que essa rede social pode promover, no sentido da comunicação imediata e propagação de ideias, e sempre há a perspectiva de participar da rede contra a própria vontade, quando outras pessoas que possuem perfil postam fotos e informações de si. Dentro dessa ideia, há a busca por meios de comunicação alternativos ao Facebook, como panfletagem, blog etc. A questão é que acabam sendo menos eficientes, pois não têm um alcance tão grande.

Seguindo essa linha de pensamento, outras tecnologias de comunicação consideradas vulneráveis ao monitoramento vão sendo deixadas de lado, para a discussão de assuntos mais delicados. Conversas face a face, sem mediação tecnológica, voltam a ganhar importância num mundo em que o virtual apresenta riscos. Não se abre mão completamente da tecnologia, no entanto uma reflexão sobre como usá-la de modo mais seguro é feita. O conteúdo discutido e a forma como se fala ao usar telefone, e-mail e Internet vai ganhando novos contornos.

> [...] é, acho que tem uma preocupação maior com segurança, assim, da informação em geral, né, a gente mesmo passa a ter uma preocupação. [...] por exemplo, coisas que a gente falaria até pelo, pelo, pelo, não pelo Facebook né, mas por Telegram, a gente prefere falar pessoalmente (Entrevistado 6, advogado).

Refletir sobre nossa relação com a tecnologia e criar outras formas de conexão com ela também são formas de resistência, que escapam de um caráter meramente negativo. Apresentam-se em seu caráter afirmativo e propositivo de atitudes, que desafiam qualquer tentativa de controle e carregam certa singularidade, apontando para a novidade e a possibilidade de que algo novo surja e surpreenda a ordem estabelecida. Nesse sentido, resistir é afirmar outros modos de existência, outras possibilidades de subjetivação que não impliquem a rejeição à tecnologia, mas possam se conectar a ela de forma criativa, apontando para pontos de fuga a partir de ações que enfraqueçam o controle (Pedro e Chevitarese, 2002).

Outra estratégia utilizada, na medida em que a visibilidade porta certo risco, é buscar a invisibilidade por meio das máscaras, a fim de proteger a própria identidade. Pudemos traçar três sentidos que a conexão entre manifestantes e máscaras assumiu durante as manifestações. O primeiro remete à ideia de disfarce e proteção. Diz respeito a essa busca pelo anonimato, que almeja a sensação de proteção sustentada pela invisibilidade. Num mundo que nos incita à transparência, a exposição de si está cada vez mais naturalizada e a visibilidade tende a nos deixar vulneráveis e submetidos

a uma constante vigilância. Com a multiplicação de tecnologias de captura, produção e circulação de imagens, o uso posterior dessas imagens escapa a qualquer controle, podendo levar a efeitos danosos para os sujeitos. No caso das manifestações, a máscara foi um artifício usado pelos manifestantes para se proteger da vigilância policial, uma vez que certas atitudes poderiam ser consideradas criminosas e a identificação dos autores poderia levar à prisão. Nesse sentido, a máscara se configurou como um obstáculo que fez resistência a esse monitoramento e, por isso, incomodou o governo do Estado do Rio de Janeiro, que conseguiu aprovar uma lei proibindo seu uso[4].

A busca da invisibilidade vem acompanhada de uma ação para colocar o outro que vigia em cena. Utilizar celulares para fotografar e filmar a atitude de policiais durante as manifestações foi uma forma encontrada de deixar os "algozes" na berlinda, uma vez que tornar o outro visível pode significar torná-lo mais vigiado, controlado, ameaçado e vulnerável. Em muitos momentos, os policiais também saíram às ruas com os rostos cobertos ou sem identificação na farda. O problema, percebido por meio das entrevistas, é que o alvo alcançado por essa dinâmica foram os policiais individualmente, que sofreram as consequências dessa exposição. A instituição e sua forma de atuar, apesar de alguns questionamentos, permaneceram fortes e intactas.

O segundo sentido busca a criação de uma identidade coletiva, tensionando a ideia de que as ações são individuais. É uma forma de não pessoalizar a luta política, de não ligar uma ideia a um indivíduo específico e de diluir o protagonismo individual numa massa. O trabalho da polícia era identificar indivíduos responsáveis pelos "crimes de vandalismo", enquanto isso, os coletivos envolvidos nas manifestações procuravam diluir a centralidade do poder em sua organização interna, a fim de tornar a ação maior que os indivíduos. Mais uma vez, essa atitude funcionou como resistência ao trabalho policial.

O terceiro sentido aponta para a força de empoderamento que a máscara pode trazer. Ao vesti-la muitos se sentiram confortáveis para agir de forma mais solta, livre e expressiva, o que não quer dizer violenta. Usar máscara produziu diferença na forma de atuar no mundo, possibilitando a ampliação da ação, a adoção de atitudes inéditas e a expressão de emoções de forma mais eloquente. Nesse sentido a máscara não esconde o verdadeiro eu, mas potencializa sua ação. O eu se constrói ao colocar a máscara, que surge como um ator que ajuda a compor uma forma de ser e atuar no mundo. Nessa conexão, o eu e a máscara ganham novos sentidos. A resistência se atualiza, nesse caso, como uma possibilidade de construir uma imagem e uma atuação no mundo mais potentes e menos constrangidas pelas forças de monitoramento. A máscara possibilita ao manifestante operar na visibilidade ao invés de tentar se esconder dela.

Tomar a visibilidade como lugar da disputa política, da defesa de ideias e da afirmação de si pode ser apontado como mais um movimento de resistência. Transformando seu sentido e se apropriando da sua força, o manifestante pode agir se fazendo ouvir ao mesmo tempo em que se protege. Um dos caminhos para isso foi escolher de forma mais cautelosa o que deve e pode ser visto, refletindo e medindo as publicações, por meio de um controle com a exposição no Facebook, evitando fornecer muitas informações sobre si. Esse é um caminho em que não é necessário abrir mão

completamente do Facebook como ferramenta de comunicação, mas que incorpora uma preocupação em fomentar uma cultura de segurança e uma cautela maior com a adoção de determinadas medidas que visam certo anonimato na rede.

As postagens deixam de ser realizadas de modo livre e descuidado, para passarem por uma reflexão e crivo, pontuados por um automonitoramento a partir do que se imagina que a polícia irá considerar como suspeito. A exposição deixa de ser um ato despreocupado para ser atravessado por um cuidado em não fornecer elementos que possam ser transformados em indícios de crime ou que sirvam para contar uma história, que sustente uma acusação formal da polícia.

A ideia da Internet como um lugar onde as pessoas podem navegar livremente, se conectar com um mundo de possibilidades e interagir com uma variedade de pessoas vem sendo problematizada. Por isso não podemos imaginar que as tecnologias possuem um sentido próprio e estável, mas sua ação no mundo, conectada com humanos, vai se transformando e ganhando outros sentidos.

Em entrevista a Antonio Martins (2016), Rafael Evangelista e Rafael Zanatta discorrem sobre as mudanças que podem ser observadas nos últimos tempos. Citam, por exemplo, como o Facebook regula os conteúdos publicados por seus usuários por meio de algoritmos, estabelecendo categorizações do que deve ou não ser mais popular, sem explicitar como esse mecanismo funciona, ferindo certo princípio de igualdade de divulgação de notícias e ideias, que antes caracterizava a Internet. É como se a nossa navegação estivesse sendo cada vez mais regulada e restringida por grandes empresas privadas como Facebook e Google.

O surgimento dos celulares com Internet também é apontado na entrevista como um ator que ajudou nessa limitação da navegação mais livre pela rede, por conta dos aplicativos que restringem nosso espaço de circulação. Outra maneira de exercer certa regulação, apontada na entrevista, é desenvolver algorítimos para capturar a atenção do usuário, para que ele fique cada vez mais preso naquele ambiente. O que leva à questão de pensar o quanto nós limitamos a essas ferramentas toda nossa fonte de informação.

O incômodo com o Facebook, por pertencer a uma grande empresa privada, apareceu nas falas dos ativistas, ocasionando tensões e questionamentos dentro dos coletivos. A procura por outras formas de comunicação sempre é levantada, mas é muito difícil abrir mão dessa rede, pela potência que ela ainda preserva. O Facebook acaba sendo considerado um “mal necessário”.

Outra forma de continuar usando as ferramentas tecnológicas e suas vantagens foi conectando -se a elas a partir de alguns princípios de segurança, como fazer um perfil falso no Facebook ou adotando plataformas mais seguras. É uma forma de usar a ferramenta sem oferecer a contrapartida esperada: grande quantidade de dados pessoais. Dessa maneira, é possível continuar aproveitando as vantagens que as tecnologias de comunicação permitem, mas de uma forma mais invisível ou mais anônima.

> Mas aí, curiosamente, no meio das manifestações eu resolvi fazer um*fake* pra justamente poder operar e utilizar a ferramenta Facebook de distribuição de informação, né, e de organização também. [...] Seria uma forma de tentar utilizar a ferramenta, mas sem dar os dados pra ferramenta, sem você participar desse jogo de ter que se expor totalmente ali (Entrevistado 4, ativista).

As dificuldades e desafios desse caminho são a necessidade de um conhecimento técnico sobre a Internet e o custo financeiro muitas vezes envolvido para proporcionar a segurança almejada. Para pensar em estratégias de resistência ao monitoramento digital é preciso conhecer o sistema, estudá-lo, o que demanda interesse e disponibilidade de tempo. Muitas vezes aqueles que têm um pouco mais de conhecimento compartilham o que sabem, a fim de tentar aumentar a segurança digital do coletivo em geral. Além disso, para se munir de ferramentas mais seguras, como utilizar criptografia, é necessário investimento financeiro, o que nem sempre é fácil. De qualquer forma, parece estar no horizonte dos ativistas a possibilidade de encontrar formas de usar plataformas de comunicação mais colaborativas e menos dependentes de empresas privadas, como o Facebook.

> Panfletagem, blog, um blog numa plataforma um pouco mais segura, que não dependa de um policial chegar e falar: 'pare, fecha esse blog', aí vai e fecha. Facebook você tem que cumprir. A plataforma, esse pessoal da luta internacional que tem criado essas plataformas pra minimizar isso, dar segurança. Permitir que você faça uso do sistema internacional de computadores, sem ser identificado né, tem a privacidade (Entrevistado 2, ativista).

> Eu acho que a gente deve se empoderar de ferramentas mais seguras, buscar comunicações criptografadas, se cercar de questões, que a gente não conseguiu fazer ainda essa transição, porque isso requer investimentos. [...] Eu não vejo, exatamente, uma maneira como um objetivo superar essas ferramentas. De repente, seja possível, no futuro, plataformas que não dependam de multinacionais e de empresas, e sejam plataformas colaborativas que não nos deixe com essa dependência. Seria mais desejável (Entrevistado 5, advogado).

Por fim, alguns entrevistados apontaram os próprios atos nas ruas como uma forma de resistência. Apesar de todo o monitoramento e ações policiais em decorrência dele, como as prisões, há pessoas que resistiram e continuam a apostar nas manifestações de rua como um meio legítimo de protestar. Junto a isso, temos o trabalho de assistência jurídica que alguns advogados e organizações de direitos humanos fazem, ao acompanhar os manifestantes e o trabalho da polícia na rua, como uma estratégia de apoio aos movimentos sociais e às vozes que tentam contrabalançar o discurso mais hegemônico.

CONSIDERAÇÕES FINAIS

Diante desse quadro, acreditamos que as possibilidades de resistência não irão se produzir fora da rede tecnológica. O caminho não parece ser se afastar da Internet e das redes sociais, mas se aproximar, conhecer seus meandros e seus mecanismos para poder construir outras formas de se conectar.

Guattari e Rolnik (1999) já apontavam as habilidades do capitalismo globalizado em capturar tudo aquilo que surge de singular na esfera social e minimizar seu potencial de transformação. As redes sociais, como o Facebook, são a grande fonte de dados que alimenta a comercialização

de produtos e potencializam o poder de ação das grandes empresas e, consequentemente, do mercado financeiro. A linguagem e o modelo de negócios têm invadido a vida cotidiana e colonizando espaços.

Durante as manifestações de 2013 no Brasil, foi possível perceber como uma ferramenta relativamente nova de comunicação serviu para potencializar e unir vozes contrárias ao governo para questionar certas práticas, com a mobilização da população para a participação de atos nas ruas. E esse parece ser um legado ainda visível hoje em dia. Alguns entrevistados apontaram para esse potencial de mobilização que se estendeu para além de 2013, mesmo que em menores proporções.

Por outro lado, essa mesma ferramenta foi sendo apropriada por órgãos do governo, a fim de dar instrumentos para um melhor controle da população. Na entrevista a Antonio Martins (2016), Rafael Zanatta e Rafael Evangelista apontam como essa ligação entre governo e tecnologia, ao aumentar o controle sobre a população, vai tornando as práticas sociais menos democráticas, indo de encontro a certo otimismo anterior que apostava na Internet como um veículo de emancipação e desenvolvimento da democracia.

Nesse sentido, a tecnologia pode operar no sentido de alavancar um poder emancipatório, contribuindo para o jogo democrático, quanto pode participar do jogo corporativo e medidas autoritárias. Dentro dos próprios coletivos que participaram da mobilização para os atos de rua, essa é uma controvérsia presente. Pois o Facebook por um lado colabora com a conexão entre as pessoas, a divulgação de ideias e ações, mas por outro provoca ruídos na comunicação que dificultam que decisões coletivas sejam tomadas e que o funcionamento democrático almejado se fortaleça.

Uma das apostas é a criação de plataformas colaborativas em que mais pessoas participem das decisões e formulem as regras de funcionamento, para que isso não fique na mão de um grupo pequeno de proprietários de empresas privadas e governos. O caminho, portanto, não parece ser tentar achar uma possibilidade de ficar fora da rede e das artimanhas da tecnologia, mas se associar a ela para potencializar ações mais coletivas e de resistência à colonização da vida social pela lógica do capital.

NOTAS

* Professora substituta do Instituto de Psicologia/ UFRJ; Doutora em Psicologia/UFRJ – luguilhon@yahoo.com.br.

** Professora associada do Instituto de Psicologia/UFRJ; Doutora em comunicação e cultura/UFRJ; rosapedro@globo.com

1. A Mídia Ninja é um grupo de mídia alternativa que ganhou visibilidade durante as manifestações de 2013, apostando numa atuação colaborativa. Funcionou como um espaço bem ativo de comunicação e decisão entre os manifestantes Como eles mesmos se definem: “Somos a Mídia NINJA Narrativas Independentes, Jornalismo e Ação. Uma rede de comunicadores que produzem e distribuem informação em movimento,

agindo e comunicando". Para saber mais, acesse: https://ninja.oximity.com/partner/ninja/about.

2. Esse trabalho é resultado da tese de doutorado "Facebook, ativismo, vigilância: conexões e controvérsias vividas nas manifestações de 2013" que investigou a vigilância no Facebook durante as manifestações de 2013. Para a pesquisa foram entrevistados 3 ativistas, 5 policiais, 2 advogados e 1 jornalista.

3. P: pesquisadora; E: entrevistado.

4. A lei foi sancionada pelo governador da época, Sérgio Cabral, em setembro de 2013. Para acessar o conteúdo da lei, ver: http://alerjln1.alerj.rj.gov.br/contlei.nsf/4734bd1980be7a200325 6b2a0061e644/953948338 46e60a583257be5005ec84a?OpenDocument

REFERÊNCIAS

Foucault, M. (1979). *Microfísica do Poder.* Rio de Janeiro: Edições Graal.

Foucault, M. (2004). Michel Foucault, uma entrevista: sexo, poder e a política da identidade. *Verve*, 5, 260-277.

Foucault, M. (2010) *Ética, sexualidade, política. (Ditos e Escritos volume V).* Rio de Janeiro: Forense Universitária.

Guattari, F., e Rolnik, S. (1999). *Micropolítica: Cartografias do desejo*. Petrópolis: Vozes.

Law, J. (1992). Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity". *Systems Practice*, 5(4), 379-393.

Martins, A. A. (2016, ago, 10). Internet tragada pelo Capitalismo de Vigilância? Rafael Evangelista e Rafael Zanatta, entrevistados por Antonio Martins. [Arquivo de vídeo] Recuperado de: http://outraspalavras.net/posts/a-internet-tragada-pelo-capitalismo-de-vigilancia/

Pedro, R. M. L., e Chevitarese, L. (2002). Da sociedade disciplinar à sociedade de controle: a questão da liberdade por uma alegoria de Franz Kafka, em O Processo, e de Phillip Dick, em Minority Report. *Estudos de Sociologia*, 1(8), 129-162.

DEFEZAP E NÓSPORNÓS: USOS, OPERACIONALIZAÇÕES E EFEITOS DOS APLICATIVOS DE CONTRAVIGILÂNCIA

Resumo: O presente trabalho tem como objetivo analisar a utilização de aplicativos de contra-vigilância, na publicização de ações perpetradas por autoridades policiais e outros agentes estatais. Concomitante ao contexto de "gestão militarizada do espaço urbano", observa-se no Brasil a presença histórica de práticas policiais de traços autoritários e seletivos em relação à parcela jovem, pobre e negra da população. Assim, diante do desenvolvimento de tecnologias na área de segurança pública, diferentes atores têm se apropriado de aplicativos e plataformas, os quais podem ser definidos tanto como construto tecnocultural (artefatos que produzem relações entre os atores sociais) quanto como estrutura econômica (manifestando -se nas relações de poder entre produtos institucionais e consumidores individuais). A presente investigação atém-se sobre a dimensão tecnocultural de aplicativos de contravigilância e se fundamenta nas seguintes questões: Quem desenvolve e quais os usos pretendidos para os aplicativos de contra-vigilância no Brasil? Como operam esses aplicativos e quais seus usos efetivos? Quais os efeitos produzidos pelos aplicativos sobre a lógica de gestão do espaço público? Como objeto empírico, foram selecionados os aplicativos DefeZap e NósporNós. O Defezap é caracterizado como "um sistema de autodefesa contra esculachos do Estado". O serviço funciona na região metropolitana do Rio de Janeiro e recebe vídeos-denúncia que demonstrem violências cometidas por agentes do Estado. O NósporNós também é um aplicativo adstrito à região metropolitana do Rio de Janeiro e criado para acolher denúncias de violência policial e constituir uma rede de apoio e proteção a eventuais vítimas. Metodologicamente, optou-se por: analisar os aplicativos (funcionalidades, usuários, usos e conteúdos) e entrevistar os atores responsáveis pelo desenvolvimento dos aplicativos. Identifica-se que tecnologias digitais como o DefeZap e o NósporNós inserem-se na *netwar* com a pretensão de questionar a assimetria de detenção de informação entre Estado e sociedade civil.

Palavras-chave: Contra-vigilância, Aplicativos digitais, Gestão do espaço urbano.

BRENDA ESPINDULA*
EDUARDO GEORJÃO FERNANDES**

Defezap y NósporNós: usos, operacionalización y los efectos de las aplicaciones de contravigilancia

Resumen: Este estudio tiene como objetivo analizar el uso de las aplicaciones de contra-vigilancia para la difusión de los actos cometidos por la policía. Concomitante con el contexto de "gestión militarizada del espacio urbano", no Brasil se observa la presencia histórica de prácticas autoritarias y selectivas por parte de la policía, en relación con los sectores negros, jóvenes y pobres de la población). Delante del desarrollo de tecnologías en materia de seguridad pública, los distintos actores hacen uso de diferentes aplicaciones y plataformas, las cuáles pueden definirse tanto como constructos tecnoculturales (artefactos que producen las relaciones entre los actores sociales), así como estructuras económicas (por meio das cuales se manifiestam las relaciones de poder entre los productos institucionales y los consumidores individuales). Esta investigación es sobre la dimensión tecnocultural de aplicaciones de contra vigilancia y se basa en las siguientes cuestiones: ¿Quién los desarrolla y cuales los usos previstos para las aplicaciones de contra vigilancia en Brasil? Cómo estas aplicaciones funcionan y cuáles son sus usos reales? ¿Cuáles son los efectos producidos por las aplicaciones en la lógica de gestión del espacio público? Como objetos empíricos, fueron seleccionados las aplicaciones DefeZap y NósporNós. El Defezap se caracteriza como "un sistema de defensa personal contra 'escraches' del Estado". El servicio funciona en la región metropolitana de Río de Janeiro y recibe vídeos de denuncia que muestran la violencia cometida por agentes del Estado. El NósporNós también es una aplicación que activo en la zona metropolitana de Río de Janeiro y fué creado para recibir denuncias de violencia policial y construir una red de apoyo y protección a las víctimas potenciales. Metodológicamente, se decidió analizar las aplicaciones (características, los usuarios, los usos y contenidos) y entrevistar a los actores responsables para el desarrollo de las aplicaciones. Se considera que las tecnologías digitales como DefeZap y NósporNós son parte de la guerra en red con la intención de cuestionar la asimetría de información entre el Estado de detención y la sociedad civil.

Palabras clave: Contra-vigilancia, Aplicaciones digitales, Gestión del espacio urbano.

Defezap and NósporNós: uses, operationalization and effects of countersurveillance applications

Abstract: This study aims to analyze the use of counter-surveillance applications over actions perpetrated by police. Hand to hand with the "new military urbanism", is observed in Brazil the historical presence of authoritarian and selective police practices directed to the young, poor and black part of the population. In the face of the development of technologies in public safety, diverse actors have incorporated the use of applications and platforms, which can be defined both as technocultural construct (artifacts that produce relations between social actors) and as economic structure (manifesting itself in power relations between institutional products and individual consumers). This investigation is related to the technocultural dimension of counter-surveillance applications and is based on the following questions: Who develops and what are the intended uses for the counter -surveillance applications in Brazil? How these applications operate and what their actual use? What are the effects produced by these applications on the logic of public space management? As empirical object, the applications DefeZap and NósporNós were selected. Defezap is characterized as "a self-defense system against state violence". The service works in the metropolitan region of Rio de Janeiro and receives complaint videos showing violence committed by state agents. NósporNós is also an application that operates on the metropolitan area of Rio de Janeiro. It was created to receive complaints of police violence and to build a network support and protection to potential victims. Methodologically, the authors opted to analyze the applications (features, users, uses and content) and to interview the actors responsible for the development of the applications. It finds that digital technologies like DefeZap and NósporNós are part of the netwar with the intention of questioning the information detention asymmetry between state and civil society.

Keywords: Counter-surveillance, Digital applications, Urban space management.

INTRODUÇÃO

O presente trabalho tem como objetivo analisar a utilização de aplicativos de contra-vigilância na coleta e publicização de informações sobre ações perpetradas por autoridades policiais e outros agentes estatais. A relevância e a atualidade da temática estão vinculadas ao contexto

em que se inserem tais aparatos tecnológicos. Stephem Graham (2011) aponta que o contexto ocidental pós-11 de setembro é marcado, em grandes metrópoles, pelo desenvolvimento de lógicas, práticas e tecnologias próprias de guerra, motivo pelo qual o autor desenvolve o conceito de "gestão militarizada do espaço urbano". Especificamente na cidade do Rio de Janeiro, a realização de megaeventos (Copa do Mundo 2014 e Jogos Olímpicos 2016) constitui a possibilidade de desenvolvimento de novas concepções de gestão do espaço urbano, fenômeno identificado conceitualmente a partir da ideia de cidade de exceção (Vainer, 2011). Ainda, no Brasil, a literatura aponta a presença histórica de práticas policiais de traços autoritários e seletivos em relação à parcela jovem, pobre e negra da população. No contexto do desenvolvimento de tecnologias na área de segurança pública, diferentes atores têm se apropriado de aplicativos e plataformas, os quais podem ser definidos tanto como construto tecnocultural (artefatos que produzem relações entre os atores sociais) quanto como estrutura econômica (manifestando-se nas relações de poder entre produtos institucionais e consumidores individuais) (Van Dijck, 2013).

A presente investigação atém-se sobre a dimensão tecnocultural de aplicativos de contra-vigilância e se fundamenta nas seguintes questões: Quem desenvolve e quais os usos pretendidos para os aplicativos de contra-vigilância no Brasil? Como operam esses aplicativos e quais seus usos efetivos? Quais os efeitos produzidos pelos aplicativos sobre a lógica de gestão do espaço público? Como objeto empírico, foram selecionados os aplicativos *DefeZap* e *NósporNós*. O *DefeZap* é caracterizado como "um sistema de autodefesa contra esculachos do Estado". O serviço funciona na região metropolitana do Rio de Janeiro e recebe vídeos-denúncia que demonstrem violências cometidas por agentes do Estado. O *NósporNós* também é um aplicativo adstrito à região metropolitana do Rio de Janeiro e criado para acolher denúncias de violência policial e constituir uma rede de apoio e proteção a eventuais vítimas.

Como estratégia metodológica, optou-se por analisar os aplicativos do ponto de vista das funcionalidades, usuários, usos e conteúdos, seguindo as dimensões propostas por Van Dijck (2013) para o estudo de mídias sociais. Como procedimentos de investigação, a fim de dar conta da estratégia citada, definiu-se a realização de entrevistas semiestruturadas com os desenvolvedores das iniciativas selecionadas, a utilização dos aplicativos no papel de usuários e a análise de conteúdo e análise de rede das páginas do Facebook que promovem e divulgam os aplicativos estudados. Cabe salientar que a coleta de dados ainda não foi finalizada, já que as entrevistas com os responsáveis pelo aplicativo NósporNós ainda estão sendo articuladas, o que contudo não inviabilizou o início do processo de análise dos outros dados já coletados.

As tecnologias digitais de contra-vigilância e a gestão do espaço urbano

Importante formulação teórica é o conceito de novo urbanismo militar, de Stephem Graham (2011). Em sua obra, o autor identifica a existência contemporânea de aparatos tecnológicos e conceituais que transformam a cidade no local e no meio de concretização da guerra. A utilização de gramáticas bélicas na gestão dos conflitos urbanos, a disseminação de discursos de medo e

de insegurança, o desenvolvimento de uma indústria da vigilância, a formação de enclaves privados, em conjunto, demonstram, segundo autor, que a cidade tem sido habitada pela lógica da militarização, como espaço de rotinização de uma "guerra irregular, assimétrica ou de baixa intensidade" (Graham, 2011:15).

Essa construção teórica insere-se em estudos que visualizam a cidade em seu aspecto conflitivo. Segundo Graham (2011), a emergência do espaço urbano como *locus* de concentração da população mundial no século XXI opera-se concomitantemente à eclosão de uma série de transformações tecnológicas, as quais tiveram como plano de fundo a expansão das formas de capitalismo, com a passagem de modelos industriais para as atuais configurações do neoliberalismo.

Dentre as tecnologias desenvolvidas nesse contexto, destacam-se os sistemas de vigilância, que buscam classificar e demarcar fronteiras, com vistas ao estabelecimento de áreas pouco permeáveis a situações de desordem social. Nesse sentido, os atores sociais, uma vez identificados como potencialmente danosos à manutenção da ordem, tornam-se objetos das tecnologias de controle. Estas atuam para a produção de bancos de dados, nos quais perfis individuais são traçados e mantidos sob vigilância (Bloomfield, 2001).

As transformações pelas quais as configurações do espaço urbano têm passado não são, porém, recebidas de modo passivo pelos atores sociais. Assim, têm se desenvolvido uma série de ações "em reação às transformações globais em curso nos espaços e recursos públicos" (Monahan, 2006: 01). Dentre essas reações, interconectada à "guerra urbana" que habita as cidades contemporâneas, deslinda-se, com a difusão e apropriação das tecnologias da informação, uma "guerra de informação". Essa guerra é denominada por Arquilla e Ronfeldt (2001) como *netwar*.

No espaço de disputas da *netwar*, um dos modos de resistência possíveis operacionaliza-se a partir do conceito de "mídias táticas" (Garcia e Lovink, 2003). Estas se sustentam sobre dois pontos centrais: um formal, ligado ao desenvolvimento de plataformas em rede, nas quais a informação circula de maneira descentralizada; um material, referente ao fato de que o conteúdo produzido explicita o posicionamento político dos sujeitos, grupos e organizações responsáveis pela manufatura da informação (Lara, 2008).

Um dos modos de utilização tática das TICs é a contra-vigilância. Esta pode ser definida como o uso intencional e tático "de tecnologias de vigilância para desafiar as assimetrias do poder institucional" (Monahan, 2006: 01). Em outros termos, a contra-vigilância consiste em um ato de inversão, em uma tentativa de utilização de aparatos tecnológicos contra o poder institucional de controle. A ideia consiste em tornar os próprios vigilantes objetos da vigilância (Serisier & Wilson, 2010).

É interessante situar a emergência e o uso de tecnologias digitais na forma de aplicativos colaborativos, e as possibilidades de contra-vigilância ou resistências contra os "excessos das forças da ordem" mediadas e materializadas por meio delas, na disputa sobre os modos como os espaços urbanos são produzidos e administrados. Telles (2015:36) nos ajuda nesse desafio ao

enfatizar que "é nesse registro, dos atritos, fricções e conflitos com a lei e o poder que talvez possamos identificar as transversalidades e ressonâncias presentes nas diversas territorialidades urbanas", já que eles seriam indicativos da experiência urbana ou dos modos de viver e habitar a cidade, trazendo à tona os conflitos da apropriação dos seus recursos.

Por esse pressuposto, investigar e problematizar o porquê na cidade do Rio de Janeiro e no seu entorno metropolitano diferentes iniciativas de desenvolvimento de aplicativos de contra-vigilância são apresentadas e passam a envolver um conjunto múltiplo de atores sociais, tanto na concepção e proposição, quanto na utilização e apropriação dessas tecnologias digitais. Vale ressaltar que, para além dos casos do Defezap e NósporNós estudados nesse artigo, a Anistia Internacional, organização não-governamental com atuação na área dos Direitos Humanos, também propôs e desenvolveu o aplicativo "Fogo Cruzado", apresentado como uma ferramenta digital para dar visibilidade à rotina de tiroteios e violência armada com a qual convivem os moradores e outras pessoas que circulam nesses territórios. Nele qualquer cidadão registra a ocorrência de tiroteios em seu bairro, sendo que essa informação coletada é processada pela organização em um mapa cartográfico da região metropolitana do Rio, em que pode-se inferir sobre a prevalência e a distribuição geográfica e social da violência armada na região.

Por isso, cabe agregar à análise a proposição de Vainer (2011), o qual aborda sobre a noção de cidade de exceção para qualificar a gestão urbana do Rio de Janeiro, a partir da realização dos megaeventos esportivos, a Copa do Mundo e, em especial, os Jogos Olímpicos. O autor sugere que seria uma forma nova de regime urbano, em que

> (...) não obstante o funcionamento (formal) dos mecanismos e instituições típicas da república democrática representativa, os aparatos institucionais formais progressivamente abdicam de parcela de suas atribuições e poderes. A lei torna-se passível de desrespeito legal e parcelas crescentes de funções públicas do estado são transferidas a agências "livres de burocracia e controle político". (Vainer, 2011: 10).

Nesse sentido, "os excessos das forças da ordem", materializados nas ações perpetradas por autoridades policiais e por outros agentes estatais, passam a tornar-se mais visíveis pelas possibilidades de uso dos aplicativos colaborativos de contra-vigilância? Em que medida essas iniciativas de aplicativos de contra-vigilância têm efeitos para a disputa sobre os modos como os espaços urbanos são produzidos e administrados? Assim, por meio dessas problematizações, pretende-se analisar os casos de aplicativos colaborativos de contra-vigilância selecionados para a pesquisa.

Os casos do *DefeZap* e de *NósporNós*

A seguir, são descritas duas iniciativas de contra-vigilância atualmente em uso na região metropolitana do Rio de Janeiro: *DefeZap* e *NósporNós*. A descrição, fundamentada na concepção de construto tecnocultural de Van Dijck (2013), busca ressaltar elementos empíricos a fim de pensar duas dimensões estruturantes das iniciativas: projeto e implementação/apropriação. Na concepção da autora, as plataformas de mídias sociais são consideradas estruturas socioeconômicas

que podem vigiar os usuários, através da coleta, armazenamento e mineração automatizada de dados. Entretanto, a própria autora discute em que medida essa disposição pode ser problematizada na medida em que se pressupõe, em diálogo com Michel Certeau, que:

> as pessoas usam 'táticas para negociar' as estratégias direcionadas a elas pelas organizações e instituições, sendo que é exatamente isso que acontece no desenvolvimento de plataformas de mídias sociais e aplicativos projetadas de cima para baixo: os usuários 'negociam' se irão utilizar e como os utilizarão nos seus hábitos cotidianos (Van Dijck, 2013: 06).

Nesse sentido, para dar vazão a ideia de que plataformas e aplicativos são um conjunto de relações que precisam ser constantemente exercidas por diferentes atores, que o fazem atribuindo interpretações e materializando práticas particulares, Van Dijck (2013) sugere dissecar: 1. as funcionalidades do artefato digital, como a operação da tecnologia digital configura a atividade social sob a forma de uma arquitetura computacional; 2. os usuários e os usos, a agência dos usuários e os usos decorrentes situam-se entre uma participação implícita (o que se pode fazer por meio da arquitetura computacional) e uma participação explícita (como os usuários interagem com a plataforma ou aplicativo); e 3. os conteúdos, como a manifestação da relação entre a tecnologia e a agência do usuário. Seguindo essas dimensões, bem como levando em conta os dados coletados até agora pela pesquisa, procura-se apresentar as aproximações analíticas dos casos investigados.

DefeZap

A plataforma *DefeZap* foi lançada em 09 de maio de 2016, sendo um *software* desenvolvido pela rede Meu Rio, com o apoio de uma rede de apuração colaborativa formada por voluntários. Conforme a página de apresentação[1], os princípios que embasam a rede Meu Rio são o apartidarismo, o pacifismo, embasamento e respeito aos direitos humanos. A rede Meu Rio foi desencadeada a partir da organização Nossas, a qual apresenta-se como uma

> organização sem fins lucrativos que atua sob a missão de armar e articular a potência para reinventar e reconstruir a política, todos os dias. Para cumprir esta missão, Nossas desenvolve tecnologias de ponta para armar atores da potência com ferramentas ativistas e fomenta redes de mobilização para articular estes atores, aumentando seu potencial de impacto.[2]

Em relação à dimensão da tecnologia, na página da plataforma Defezap, visualiza-se, na tela inicial, uma barra superior com as seguintes opções: "Quem somos"; "Privacidade"; "Quem paga"; "Blog"; "*Facebook* "; "Contato". Em "Quem somos", consta: "*DefeZap* é um sistema de autodefesa contra esculachos do Estado e produção de informação jornalística com sigilo garantido. O serviço permite o envio de vídeos-denúncias que mostrem violência ilegal cometida por agentes do Estado...".

Além disso, informa-se o que o serviço permite e quais os encaminhamentos adotados a partir dos materiais enviados. Quanto à "Privacidade", o *site* da plataforma comunica que a pessoa que envia vídeos para o *DefeZap* não precisa identificar-se, resguardando-se o anonimato da denúncia.

A identificação ocorre apenas em casos excepcionais, com a devida anuência do(a) informante, nos seguintes casos: se a pessoa é parente da vítima; se a pessoa conhece outra testemunha do ocorrido; se a pessoa aceita falar com a imprensa sobre o fato; se a pessoa aceitaria testemunhar em órgãos policiais e judiciais sobre o ocorrido; se a pessoa deseja saber o que será feito com o vídeo enviado.

No tópico "Quem paga", é informado que a rede "Nossas Cidades", à qual está vinculado o *DefeZap*, não aceita dinheiro de governos ou partidos políticos. O aporte de recursos para desenvolvimento do projeto foi realizado pela *Open Society Foundation*, instituição que financia projetos de defesa de direitos humanos no mundo. A manutenção do *DefeZap* é feita pelo "Meu Rio", que recebe doações.

No painel central da página inicial do *DefeZap*, constam três opções: "Envie agora seu vídeo"; "Inscreva-se agora"; "Acesse o Boletim DefeZap". "Envie agora seu vídeo" é opção de envio de vídeos com denúncias de violência estatal. É possível fazer *upload* de arquivo ou enviar um *link*. Não são solicitados dados de identificação do informante.

Em "Inscreva-se agora", é possível realização de cadastro como voluntário da rede. A inscrição permite as seguintes ações: colaboração para elucidar alguns casos, através de pesquisa e apuração de dados; participação de atividades de formação em segurança pública e direitos humanos; participação em ações de divulgação do *DefeZap* na região metropolitana do Rio de Janeiro. Os dados dos voluntários são anônimos.

A opção "Acesse o Boletim *DefeZap* " dá acesso ao *blog* da plataforma. O *blog* constitui um espaço no qual são publicadas matérias e opiniões a respeito dos casos recebidos pelo *DefeZap* e dos temas da segurança pública e dos direitos humanos.

A página de *Facebook* do projeto produz conteúdo de divulgação do *DefeZap*, posta textos e eventos relacionados às temáticas de segurança pública e direitos humanos e publiciza determinados vídeos de violência estatal. Ao total, a página, criada em 09 de maio de 2016, tem 5215 curtidas (dado de 13/10/2016).

NósporNós

O aplicativo NósporNós foi lançado em março de 2016 como iniciativa do Fórum de Juventudes do Rio de Janeiro. Conforme a página do Fórum no Facebook[3], essa organização apresenta-se como "um espaço de articulação e participação de jovens (principalmente jovens negr@s, pobres periféric@s e favelad@s), organizações, coletivos, redes e pessoas que lutam pela garantia dos direitos das juventudes". Segundo a apresentação na página do Facebook, o Fórum foi criado no ano de 2003 e a trajetória de atuação envolve a participação em espaços como o Conselho Estadual de Juventude no Estado do Rio de Janeiro, o Conselho Nacional de Juventude, bem como de comissões parlamentares de juventudes e fóruns internacionais de juventudes, pela qual enfatizam que "o Fórum foi um dos protagonistas na concepção e elaboração do que hoje chamamos de

campo das PPJs (Políticas Públicas para as Juventudes no Brasil)". Entretanto, ainda na apresentação da página, enfatizam que o Fórum, "a partir de espaços de diálogo, principalmente com as juventudes negras, pobres periféricas e faveladas, tem tido um posicionamento de não participação dos espaços como conselhos e conferências, por acreditar que são espaços de uma pseudo participação e que pouco ou quase nada impacta na vida dessas juventudes", sendo que a prioridade "é o processo de formação e mobilização da base" por meio das "bandeiras de luta" como "o fim da violência contra as mulheres; o fim do genocídio da juventude negra pobre e periférica e favelada; a desmilitarização da segurança pública; o fim da homofobia; o direito à cidade; e o direito à comunicação" e de atividades como "ocupação das ruas e conversando com a população, em especial as juventudes; realizando festivais de juventudes, luau, saraus,cursos de formação, cine debates e rodas de conversas; ações de incidência política e produzindo uma comunicação própria".

O aplicativo está disponível para *download* gratuito pela loja da *Google Play* e é voltado para usuários que utilizam *smartphones* com o sistema operacional *Android*. A loja virtual indica como desenvolvedor do aplicativo o projeto chamado Rebaixada (não tendo-se clareza sobre as relações desse projeto com o Fórum de Juventudes do RJ). Na primeira tela do aplicativo observa-se a frase "Denuncia a violência policial - as juventudes negras, pobres e faveladas querem viver!" e um menu com *links* para as seguintes opções: "Denuncie"; "Rede de apoio"; "Conheça seus direito"; "Mapeamento". A partir do link "Denuncie", é possível fazer uma denúncia, pela qual o/a usuário/a insere um endereço físico, data, hora; indica quem fez a violação, selecionando opções preestipuladas no aplicativo (Polícia Civil, Polícia Militar, Polícia Federal, Governo Municipal, Exército-Marinha-Aeronáutica); indica também "o que aconteceu" a partir da seleção de opções preestipuladas no aplicativo (abuso de poder, agressão física, homicídio, tortura, prisão ilegal, racismo, machismo, homofobia, ocultação de identidade policial, extorsão, invasão de domicílio, censura de meios de comunicação); insere um arquivo de mídia já capturado (vídeo ou fotografia) ou captura diretamente no aplicativo um vídeo ou fotografia; e, ainda, o/a usuário /a pode contar o que aconteceu no campo de texto "Ocorrência". Todos esses campos são de preenchimento obrigatório, sendo que os campos "Nome", "email" e "telefone", que seguem após os campos acima mencionados, são de preenchimento opcional. Ou seja, é possível não identificar quem está fazendo a denúncia; contanto, não foi examinado se os dados de navegação do usuário são rastreados pelo aplicativo.

A partir do *link* "Rede de apoio", são listados endereços e contatos de "organizações e comissões que podem colaborar com você", bem como endereços e contatos de "redes de comunidades e movimentos contra a violência". Já no *link* "Conheça seus direitos", há dois blocos de informações: o primeiro são respostas à pergunta "o que não pode?", incluindo as ações que caracterizam a violência policial, e o segundo bloco refere-se à questão "como deve ser?", sendo descrito com deve ser a abordagem policial por lei.

Por fim, no *link* "Mapeamento", abre-se um mapa cartográfico da base do *Google Maps*, em que as denúncias são georreferenciadas, podendo-se ter noção em que bairros e ruas as violações

aconteceram. Quando se clica no ponto da denúncia, somente a categoria inserida no tipo de violação aparece, quais sejam, abuso de poder, agressão física, homicídio, tortura, prisão ilegal, racismo, machismo, homofobia, ocultação de identidade policial, extorsão, invasão de domicílio e censura de meios de comunicação. Os pontos são rotulados com o tipo de violência, e nada mais pode ser sabido sobre a denúncia.

CONSIDERAÇÕES FINAIS

A partir das dimensões tecnologia e usos da plataforma e aplicativos, podem ser delineados resultados parciais do estudo. Destaca-se, primeiramente, a similaridade do objetivo concebido para as duas tecnologias, sendo ambas dirigidas à denúncia de violência por parte de autoridades policiais e outros agentes estatais. Identifica-se, ainda assim, diferença de linguagem, pois enquanto o *DefeZap* trata de "violência ilegal cometida por agentes do Estado", *NósporNós* utiliza a expressão "violência policial" para definir seu alvo. Entretanto, infere-se que a plataforma Defezap teria maior disposição para a recepção de denúncias de violência perpetradas para todo e qualquer agente do Estado, para além das autoridades policiais e dos servidores públicos diretamente vinculados com a política de Segurança Pública.

Quanto ao público ao qual são destinados, *NósporNós* explicita, na descrição do aplicativo, a defesa às "juventudes negras, pobres e faveladas". A descrição do *Defezap*, por outro lado, não indica, a princípio, quem seria o alvo de proteção da plataforma. De qualquer modo, ambas tecnologias buscam garantir o anonimato do usuário que faz a denúncia, resguardando os dados pessoais de quem registra as informações na plataforma e no aplicativo. Entretanto, se o usuário do Defezap quiser identificar-se para ter apoio e proteção na apuração da denúncia, é possível pelo aplicativo, o que no caso do NósporNós não é explícito. Fora isso, em relação à garantia do anonimato pleno no uso, não tem-se clareza se ambas tecnologias digitais suportam integridade total dos dados pessoais dos usuários, já que os dados de navegação são transmitidos e armazenados, tanto na plataforma, quanto no aplicativo, podem ser rastreados por quem tiver essa intenção.

Identifica-se que o conteúdo de ambas as tecnologias compõe-se, além das denúncias recebidas em vídeo, de informações (matérias, opiniões, boletins informativos, georreferenciamento de denúncias) sobre as temáticas da segurança pública e dos direitos humanos. Destaca-se, também, que nos dois casos analisados, outras mídias sociais e aplicativos (*Facebook, blogs, Whatsapp*) fazem parte da iniciativa, seja para promoção e divulgação do Defezap e do NósporNós ou para dar desdobramento à apuração das denúncias realizadas.

Cabe enfatizar as diferenças entre os atores sociais que desencadearam ambas as iniciativas e problematizar o quanto essas diferenças têm implicações tanto para o projeto concebido quanto para a forma de implementação das iniciativas e, propriamente, a apropriação das tecnologias. No caso do Defezap, quem propôs foi uma rede de pessoas que, para além de acreditar na "tecnologia de ponta" para mobilizar pessoas e "reconstruir a política", têm como princípio de ação a promoção e o respeito aos Direitos Humanos. Isso explicita-se, em grande medida, com

a ideia do nome do aplicativo, orientado para a defesa de alguém por outrém, o que pode ter desdobramentos para a forma em que a tecnologia é apropriada e como ela é concebida, bem como os seus efeitos para a contra-vigilância. Da mesma maneira, no aplicativo NósporNós, ecoa a ideia de quem ninguém "fala" ou "faz" pelos desenvolvedores da iniciativa, mas sim eles mesmos. Ou seja, a concepção sobre as tecnologias digitais e seus efeitos de contravigilância ganha outro status em relação à plataforma Defezap.

Esses apontamentos, em conjunto, delineiam a possibilidade da mobilização do conceito de vigilância distribuída (Bruno, 2013), para caracterização da descentralização de atores e da multiplicidade de conteúdos, na disseminação de informações de controle sobre a ação do Estado. Em meio à disputa identificada como *netwar*, tecnologias como o *DefeZap* e o *NósporNós* inserem -se com a pretensão de questionar a assimetria de detenção de informação entre Estado e sociedade civil. Cabe avançar na coleta e na análise dos dados, a fim de pensar sobre os efeitos da utilização dessas tecnologias na disputa sobre os modos de produzir e administrar o espaço urbano, bem como tensionar a reflexão sobre as dificuldades enfrentadas pelos desenvolvedores na implementação dos fins a princípio projetados. Como continuidade da investigação, faz-se necessária, ademais, a coleta e a análise de uma quantidade massiva de dados, seja para a identificação qualitativa do conteúdo de rastros digitais, seja para a operacionalização de outros instrumentos metodológicos, como a análise de redes.

NOTAS

* Doutoranda do Programa de Pós-Graduação em Sociologia (PPGS), Universidade Federal do Rio Grande do Sul (UFRGS) - Brasil, licenciada em Ciências Sociais e mestre em Sociologia pela mesma universidade. Email: bespindula@gmail.com.

** Doutorando do Programa de Pós-Graduação em Sociologia (PPGS), Universidade Federal do Rio Grande do Sul (UFRGS) – Brasil, bacharel em Psicologia pela PUC-RS, bacharel em Ciências Sociais e Jurídicas e mestre em Sociologia pela UFRGS. Email: eduardo.g.fernandes@gmail.com.

1. No link `http://www.meurio.org.br/`, com acesso em 13/10/2016.

2. Extraído na página da organização, no link `http://www.fundadores.nossas.org/#block-2190`, com acesso em 13/10/2016.

3. Extraído no link `https://www.facebook.com/pg/forumdejuventuderj/about/?ref=page_internal`, com acesso em 13/10/2016.

REFERÊNCIAS

Arquilla, J. e Ronfeldt, D. (2001). *Networks and Netwar:* The Future of Terror, Crime and Militancy. RAND'S National Security Research Division.

Bloomfield, B. (2001). In the right place at the right time: Electronic tagging and problems of social order/ disorder. *Sociological Review*, 49(2), 174-202.

Bruno, F. (2013). *Máquinas de ver, modos de ser.* Vigilância, tecnologia e subjetividade. Porto Alegre: Sulina.

Garcia, D., e Lovink, G. (2003). *O ABC da Mídia Tática.* Disponível em: https://arquivodeemergencia.wordpress.com/anotacoes/abc-da-midia-tatica/.

Graham, S (2011). *Cities Under Siege: The New Military Urbanism*. London: Verso.

Lara, P. J. O. M. (2008). *Fragmentos das táticas da cultura: técnica e política dos usos de mídia.* (Dissertação de Mestrado) Faculdade de Sociologia, Universidade Estadual de Campinas. Campinas.

Monahan, T. (2006). Counter-surveillance as Political Intervention? *Social Semiotics*, 16(4), 515-534.

Serisier, T. & Wilson, D. (2010). Video Activism and the Ambiguities of Counter-Surveillance, *Surveillance & Society*, 8(2), 166-180.

Telles, V. (2015). Cidade: produção de espaços, formas de controle e conflitos. *Revista de Ciências Sociais*, 46(1), 15-41.

Vainer, C. (2011). Cidade de exceção: reflexões a partir do Rio de Janeiro. *Anais do Encontro Nacional da ANPUR14*, Rio de Janeiro. Disponível em: http://www.anpur.org.br/site/anais/ena14/ARQUIVOS/GT1-1019-633-20110106150243.pdf

Van Dijck, J. (2013). *The culture of connectivity: a critical history of social media*. Oxford: Oxford University Press. "...people use tactics to negotiate the strategies that are arranged for them by the organizations or institutions. That is precisely what happened with the development of social media platforms and the apps built on top of them: users "negotiate" whether and how to appropriate them in their quotidian habits." (tradução nossa)

COMPARAÇÃO DE APLICATIVOS MÓVEIS DE COMUNICAÇÃO SEGURA

Resumo: Esse trabalho fará a comparação de três aplicativos móveis de comunicação, notáveis tanto pela vasta popularidade, facilidade de uso e adesão, em diferentes graus, às boas práticas de segurança – WhatsApp, Signal e Telegram –, levando-se em conta aspectos como: modelo de negócio de suas companhias; garantias de segurança prometidas; adequação ao modelo de software livre; protocolos de criptografia; e relatos de falhas de segurança, sanadas ou não. Será analisada a documentação relativa aos protocolos de segurança, bem como seus componentes individuais, e suas vulnerabilidades encontradas na literatura. Uma análise crítica desses aplicativos é especialmente relevante uma vez que são ferramentas essenciais para ativistas, jornalistas e demais indivíduos e organizações que requerem alto nível de segurança durante o trânsito de informações. O trabalho conclui com uma exposição acerca da inadequação de todos os três aplicativos enquanto candidato sólido a aplicativo padrão de troca de mensagens seguras –usandose a filosofia da distribuição de Android denominada Securegen como parâmetro–, descrevendo os problemas encontrados em cada um, e possíveis soluções a alguns desses problemas.

Palavras-chave: Aplicativos, Criptografia, Telefonia móvel, Contravigilância.

Comparación de aplicaciones móviles de comunicación segura

Resumen: Este trabajo compara tres aplicaciones de comunicación móvil, notables por su gran popularidad, facilidad de uso y adhesión, a diferentes niveles, a las buenas prácticas de seguridad – WhatsApp, Signal y Telegram – teniendo en cuenta aspectos como: modelo de negocio de sus empresas; garantías de seguridad prometidas; adecuación al modelo de software libre; la documentación relativa a los protocolos de criptografía; y informes de defectos de seguridad, corregidos o no. Será analizada la documentación de los protocolos de seguridad, así como sus componentes individuales, y las vulnerabilidades encontradas en la literatura. Un análisis crítico de esas aplicaciones es especialmente relevantes ya que son esenciales a los activistas, periodistas y demás personas y organizaciones que requieren un alto nivel de seguridad durante el tránsito de información. El documento concluye con una exposición acerca de la insuficiencia de todas las tres aplicaciones como candidato sólido para aplicación estándar de cambio de mensajería segura – tomando como parámetro la filosofía de la distribución de Android llamada Securegen –, describiéndose los problemas encontrados en cada uno, y posibles soluciones a algunos de estos problemas.

Palabras clave: Aplicaciones, Criptografía, Telefonía móvil, Contravigilancia.

Comparison of secure mobile communication applications

Abstract: This paper will compare three mobile message applications, notable for their huge popularity, ease of use and adherence, to varying degrees, to best safety practices – WhatsApp, Signal, and Telegram –, taking into account aspects such as: business model of their respective companies; promised security guarantees; suitability to the free software model; encryption protocols; and reports of security flaws, fixed or not. It will examine the documentation related to their security protocols – both the architecture and the individual components – and respective vulnerabilities as found on literature. A critical analysis of those applications is especially relevant since they are essential tools for activists, journalists and other individuals and organizations that require a high level of security during the exchange of information. The paper concludes that all three selected applications fail as a solid candidate for standard secure mobile message application – using the philosophy behind Android distribution called Securegen as parameter –, describing issues found in each, and possible ways to solve some of these problems.

Keywords: Applications, Cryptography, Mobile phones, Countersurveillance.

LEONARDO PICCIONI DE ALMEIDA*
MÁRCIO MORETTO RIBEIRO**

INTRODUÇÃO

As denúncias feitas em junho de 2013 pelo ex-funcionário da Agência Nacional de Segurança (NSA) estadunidense, Edward Snowden, sobre o esquema de vigilância em massa efetuado pela agência e seus parceiros, trouxe à tona o debate sobre gargalos da segurança da informação na comunicação digital (Greenwald, MacAskill & Poitras, 2013).

Em particular o programa PRISM indicou que o governo dos EUA tem acesso direto, seja consentido ou não, aos dados das grandes empresas de comunicação via web (Greenwald & MacAskill, 2013).

A concentração de dados vulneráveis nos servidores dessas empresas, portanto, seria um desses gargalos. Como resposta a essa ameaça, ou como oportunidade de negócios, não tardou a surgirem aplicativos de comunicação móvel que prometiam proteger o usuário desse tipo de vigilância.

Arcabouço teórico

Com o objetivo de auxiliar usuários a escolher entre esses aplicativos, a Electronic Frontier Foundation (EFF, 2016) propôs sete critérios úteis, mas não necessariamente suficientes, a serem analisados. Os critérios em si são, aqui, mais relevantes do que os conceitos dados pela EFF a cada aplicativo, principalmente porque não se distingue aplicativos que implementam bem ou mal tais critérios.

O primeiro critério é a "criptografia em trânsito", que evita a decifração da mensagem, caso seja interceptada a caminho do destinatário da mensagem ou de um servidor intermediário.

O segundo critério, mais sofisticado, é a chamada "criptografia ponta a ponta", ou "criptografia fim a fim", ou seja, a inviabilidade de qualquer servidor intermediário de decifrar a mensagem. Num esquema de criptografia ponta a ponta, idealmente, apenas remetente e destinatário têm acesso às mensagens. Além de preservar a privacidade do usuário, tal atitude evita a existência de um "ponto único de falha": o acesso ao servidor intermediário por indivíduos ou organizações maliciosos pode resultar no vazamento do conteúdo de bilhões de mensagens.

O terceiro critério é a capacidade de um usuário verificar a identidade de um outro usuário. Na prática, isso significa que remetente e destinatário – mas não necessariamente terceiros – podem verificar a identidade um do outro, afastando a possibilidade de fraude.

O quarto critério é a "*perfect forward secrecy*", isso é, a impossibilidade de decifrar todas as mensagens de uma conversa caso o segredo usado para decifrar uma mensagem específico seja descoberto.

O quinto critério se refere à possibilidade de auditoria independente do código-fonte. Uma generalização desse critério é o conceito de software livre, proposto por Stallman (2015:3), que prevê quatro direitos (as chamadas "quatro liberdades") ao usuário: o direito de utilizar o

programa para qualquer fim; o direito a estudar – o que inclui auditar – o software e modificá-lo; o direto de distribuir independentemente o software; e o direito de distribuir quaisquer modificações que o usuário tenha feito no mesmo.

A possibilidade de auditoria independente permite verificar se, e como, os mecanismos de segurança são implementados. Combinada com a noção de software livre, possibilita ao usuário distribuir versões do software original que corrija quaisquer vulnerabilidades de segurança encontradas.

Completam a lista de critérios o sexto, relacionado a uma documentação abrangente dos mecanismos de segurança, e o sétimo, que avalia se houve uma auditoria recente do código.

É importante ressaltar que o placar da EFF previa apenas o cumprimento ou não dos critérios, não havendo graduação dentro de cada nível ou outra maneira de mensurar as mazelas de cada aplicativo (Zorz, 2016). Tal debilidade é, inclusive, razão pelo abandono do placar, ainda sem substituto (EFF, 2016).

No último placar atualizado, os três principais aplicativos de comunicação móvel apresentavam os seguintes conceitos: Signal apresentou conceito máximo; WhatsApp não pontuou no quinto critério; e o Telegram apresentou nota máxima em sua versão criptografada ponta a ponta, enquanto que o modo padrão do Telegram não pontuou do segundo ao quarto critérios. Contudo, como o trabalho pretende demonstrar, todos os aplicativos apresentam mazelas que o inviabilizam como solução para os sete critérios.

SIGNAL

O aplicativo Signal, originalmente chamado TextSecure, surgiu como um aplicativo de troca de SMS /MMS criptografados, mas seu foco mudou ao longo do tempo. Desde 2015, as mensagens são enviadas criptografadas ponta a ponta através de rede de telefonia celular, se o destinatário possui Signal instalado; ou através de SMS/MMS não criptografado, caso contrário (Marlinspike, 2015).

O aplicativo é mantido pela organização não governamental Open Whisper Systems (OWS), mantida por doações, financiamento governamental e, possivelmente, ganhos da venda de sua empresa antecessora, a *start-up* Whisper Systems, adquirida pelo Twitter (Greenberg, 2011).

O código-fonte, tanto dos aplicativos clientes quanto dos servidores, é disponibilizado como software livre. O aplicativo possui clientes para Android e iOS, bem como uma extensão para Google Chrome/Chromium.

O aplicativo implementa o protocolo Signal (anteriormente conhecido como Axolotl ou TextSecure), desenvolvido pelo fundador da OWS, Moxie Marlinspike, mas aberto ao público e de ampla adoção – softwares proprietários que afirmam implementar o protocolo incluem WhatsApp, Facebook Messenger e Google Allo.

Pode-se entender o protocolo Signal como uma evolução do protocolo OTR (*off-the-records*), apresentando aprimoramentos em relação a esse, como maior plausibilidade de negação (Marlinspike, 2013b) e segurança retroativa ("*future secrecy*") (Marlinspike, 2013a).

Arquitetura do protocolo

Para efeitos de clareza e concisão, considere um cenário em que Alice pretende iniciar uma comunicação com Bob[1].

Para poderem se comunicar em segurança, Alice e Bob precisam compartilhar um segredo, que será usada para cifrar e decifrar as mensagens. Porém, o canal de comunicação usado para a trocas desse segredo pode ser inseguro – por exemplo, grampeado. Dessa forma, Alice e Bob necessitam de um artifício para que, mesmo que o segredo não trafegue às claras pelo canal, ambos – e, necessariamente, nenhum terceiro – obtenham o mesmo segredo ao final. O mais usado desses artifícios é o protocolo de Diffie-Hellman, usado pelo Signal.

Além das chaves privadas transmitidas de maneira opaca pelo protocolo de Diffie-Hellman, é necessário que Alice e Bob tenham uma chave pública cada, únicas e disponíveis para consulta por todos. Após Alice requisitar ao servidor a chave pública de Bob, ela consegue obter três segredos distintos: um combinando a chave pública dela e a chave privada de Bob, um com a chave privada dela e a chave pública dele, e um com as chaves privadas de ambos.

Uma característica desse arranjo particular é que, uma vez que Bob possa checar a chave pública de Alice e ambos obtenham os mesmos três segredos, Bob pode se assegurar da autenticidade de Alice. Contudo, como um terceiro não pode provar que as chaves privadas enviadas por Diffie -Hellman não tenha sido forjadas, não é possível garantir que a conversa como um todo não tenha sido forjada – essa garantia é a chamada "plausibilidade de negação".

Esses três segredos serão combinados para a produção de uma "chave raiz". Junto à primeira chave raiz, Alice enviará uma nova chave privada, que será usada na geração da próxima chave raiz e uma "chave corrente".

A chave corrente será usada para a geração da próxima chave corrente, bem como de uma "chave mestra".

A partir da chave mestra, é possível gerar outros dois segredos: o primeiro será usado para cifrar a mensagem; o segundo para se gerar um MAC (*message authentication code*) a partir da cifra, usado para se garantir a autenticidade da mensagem.

Junto com sua primeira resposta a Alice, Bob enviará uma nova chave privada, que será usada para gerar a próxima chave raiz e as chaves conseguintes. Analogamente, durante toda a comunicação, novas chaves privadas serão enviadas cada vez que um dos lados enviar um conjunto de mensagens e, partindo delas, serão obtidas novas chaves raiz, etc.

Esse esquema de geração de chaves, que pode parecer à primeira vista supérfluo, é útil pois permite que, uma vez que a chave mestra seja gerada, as chaves corrente e raiz que a antecederam possam ser descartadas sem prejuízos.

Como o algoritmo de geração de chaves é irreversível, uma vez que uma chave mestra tenha sido corrompida, ela não pode ser usada para a geração de outras chaves correntes e raiz – portanto, provendo ao protocolo *future secrecy*. Portanto, para se decifrar outras mensagens, as únicas informações que Alice precisa armazenar é sua última chave privada enviada a Bob, a última chave raiz e a chave mestra das mensagens ainda não decifradas – a comunicação celular é assíncrona, de modo que as mensagens nem sempre chegam na ordem em que foram enviadas.

Além das maneiras descritas acima, a autenticidade de Alice e Bob podem ser conferidas presencialmente, através do conferimento de um *fingerprint* de suas chaves.

Primitivas criptográficas

Primitivas criptográficas são algoritmos básicos, confiáveis e bem documentados, que podem ser combinados de forma a se obter um protocolo de criptografia.

Para a troca de chaves, o protocolo Signal utiliza o protocolo de Diffie-Hellman, ou de Diffie-Hellman-Merkle. Considerando a a chave privada de Alice e b a chave privada de Bob, uma troca de chaves de Diffie-Hellman consiste no envio de g e g^a por Alice, seguidas pelo envio de g^b por Bob, de forma que $(g^a)^b = (g^b)^a = g^{ab}$. Se não for factível formar gab apenas com g, g^a e g^b, Alice e Bob podem usar g^{ab} como segredo para um esquema de criptografia simétrica (Menezes, van Oorschot & Vanstone, 1997: 515).

Para se garantir que não seja factível obter g^{ab} a partir de g, g^a e g^b, é necessário que g, a e b pertençam a um conjunto de números em que o problema da fatoração seja computacionalmente difícil – no caso do Signal, o conjunto utilizado é a curva elíptica Curve25519, proposta por Bernstein (2006).

A geração de chaves usa ora HMAC, ora HKDF, a depender da quantidade de chaves a serem geradas a cada passo. HMAC (*hash-based MAC*) é um algoritmo originalmente utilizado para geração de MACs, mas que pode ser usado para gerar entropia. HKDF (*HMAC-based key derivation function*) é um algoritmo que utiliza HMAC para geração de chaves seguras de tamanho arbitrário. Ambos os algoritmos são irreversíveis e considerados confiáveis tanto por desenvolvedores quanto por acadêmicos.

O HMAC e, consequentemente, o HKDF do protocolo Signal está baseado no uso do algoritmo SHA-256, também conhecida como SHA-2, desenvolvida pela NSA e recomendada pelo *National Institute of Standards and Technology* estadunidense (NIST, 2012). Atualmente, não há ataques conhecidos contra o algoritmo completo, mas apenas contra algumas simplificações.

As mensagens são cifradas e decifradas utilizando a cifra de bloco AES (*Advanced Encryption Standard*), também conhecida como *Rijndael* – outro padrão NIST (2001) –, em modo contador (Diffie & Hellman, 1979). Atualmente, não há ataques conhecidos com ganhos significativos sobre a força bruta. Para a geração de MACs, também é utilizado o algoritmo HMAC.

O protocolo Signal utiliza a consagrada tática *encrypt-then-mac* – isso é, cifrar a mensagem para, em sequência, obter um MAC da mensagem cifrada. Segundo Bellare & Namprempre (2000), essa estratégia comprovadamente providencia autenticidade, indistinguibilidade e não maleabilidade à mensagem cifrada.

WHATSAPP

WhatsApp é o aplicativo de troca de mensagens mais popular do mundo, somando mais de um bilhão de usuários. Desde 2014, o aplicativo pertence ao gigante das redes sociais Facebook. Possui versões para todas as principais plataformas para aparelhos celulares, bem como algumas legadas, e também versão para navegadores.

Seu código-fonte é fechado e proprietário, e o aplicativo lucra através da exploração da privacidade dos usuários, repassando dados, inclusive, para sua companhia mãe.

O WhatsApp implementa o protocolo Signal desde abril de 2016 (Marlinspike, 2016). Sua implementação do protocolo, supostamente, é bastante parecida com a do aplicativo Signal (WhatsApp, 2016). Contudo, é impossível analisar satisfatoriamente a implementação, uma vez que o código fonte do aplicativo é fechado.

Diferenças em relação à implementação no aplicativo Signal serão tratadas na subseção seguinte.

Protocolo

Na implementação do WhatsApp, Bob deve carregar um lote de "pré-chaves" no servidor do WhatsApp. Cada pré-chave é descartada após um único uso e, como cabe a Bob ativamente reenviar outro lote de pré-chaves cada vez que o lote anterior tenha se esgotado, é possível que, por determinados períodos de tempo, o servidor contenha nenhuma de suas pré-chaves.

Ao iniciar as trocas de chave com Bob, Alice recebe, além das chaves pública e privada de Bob, uma de suas pré-chaves, se disponível. Se Alice não receber nenhuma pré-chave de Bob, a geração da primeira "chave raiz" ocorre tal como na implementação do aplicativo Signal. Em caso contrário, a pré-chave é utilizada, junto com os outros três segredos compartilhados, para a geração da chave raiz.

TELEGRAM

O Telegram é um aplicativo sem fins lucrativos, mantido pela fortuna de seu fundador, o multimilionário russo Pavel Durov, também fundador e ex-CEO da rede social VK (originalmente,

Vkontakte). No entanto, o aplicativo não rejeita a possibilidade de sobreviver de doações ou funcionalidades pagas após o fim das reservas monetárias de Durov.

Durov decidiu fundar o Telegram após se negar, repetidas vezes, a entregar dados de oposicionistas políticos, usuários do VK, a autoridades russas (Salomão, 2015). A criptografia utilizada pelo Telegram, supostamente, seria usada como forma de tornar os dados de seus usuários opacos à inteligência russa e de outros países. Desde 2014, Durov vive exilado em São Cristóvão e Névis, no Caribe.

O aplicativo possui clientes, oficiais ou não oficiais, para quase todas as maiores plataformas, sejam *desktop* ou móvel, e também para navegadores. Os clientes oficiais são disponibilizados como software livre. O código do servidor, no entanto, é fechado – sua publicação não é considerada prioridade, atualmente.

O Telegram utiliza um protocolo próprio, o MTProto, desenvolvido por funcionários da empresa sem treinamento prévio em criptografia, de maneira que o protocolo sofreu algumas alterações ao longo de sua curta história, corrigindo problemas assim que encontrados. O Telegram oferece prêmios em dinheiro para quem conseguir quebrar a criptografia do aplicativo, mas as regras do concurso são consideradas muito restritas (Hornby, 2013).

O protocolo MTProto vem em dois sabores: com ou sem criptografia ponta a ponta. Por padrão, as conversas do Telegram não apresenta criptografia de ponta a ponta, mas apenas durante trânsito. No caso de conversas em grupo, criptografia ponta a ponta não é atualmente disponível.

Arquitetura do protocolo

O protocolo MTProto (Telegram, 2016a; 2016b) é considerado significativamente mais simples que o Signal, mas também mais heterodoxo. A explicação a seguir considera a versão criptografada ponta a ponta, teoricamente mais segura.

Para iniciar a conversa, Alice e Bob começam a compartilhar um segredo, enviando suas chaves secretas, de maneira opaca, utilizando-se o protocolo de Diffie-Hellman.

O MAC da mensagem é calculado a partir da mensagem. A partir do MAC e do segredo compartilhado, é gerada outra chave, que será usada para cifrar a mensagem. Então, a mensagem cifrada e seu MAC são enviadas para o canal.

Para prover *perfect forward secrecy*, uma nova troca de chaves de Diffie-Hellman ocorre a cada uma semana ou cem mensagens, o que ocorrer primeiro, exceto se a chave não tenha sido usada nenhuma vez.

A única forma de se conferir a identidade de Alice ou Bob é através de verificação de *fingerprint*, presencialmente.

Primitivas criptográficas

Diferentemente do protocolo Signal, que utiliza uma curva elíptica, o gerador utilizado pelo MTProto para a troca de chaves de Diffie-Hellman é um gerador de números primeiros de alta ordem. Há relatos de manipulação pela NSA na implementação de geradores de números primos (Adrian et al., 2015), o que, na prática, tornaria o uso de Diffie-Hellman pouco efetivo.

O MAC é gerada utilizando-se o SHA-1, um antecessor do SHA-2, atualmente considerado vulnerável (Schneier, 2004). Contudo, o uso original do SHA-1 é cifragem, e não geração de MAC, o que torna incerto a relevância das vulnerabilidades conhecida – tal qual a descrita em Stevens (2012).

A geração da chave de cifragem a partir do segredo compartilhado por Diffie-Hellman utiliza uma função de derivação de chaves desenvolvida pelos próprios desenvolvedores do protocolo, sendo pouco estudada e praticamente não utilizada por nenhum outro protocolo.

A cifragem também utiliza AES. Contudo, diferentemente do protocolo Signal, ela utiliza um modo bem mais raro, o IGE (*Infinite Garble Extension*). Até por ser raramente usado e estudado, não há vulnerabilidades conhecidas em relação à forma como o protocolo utiliza IGE.

Uma característica particular do modo IGE é que a alteração da mensagem cifrada necessariamente causará alterações na decifração da mensagem, o que pode ser utilizado como indício da autenticidade da mensagem. Contudo, esse uso do modo IGE não apresenta todas as propriedades comprovadas pelo paradigma *encrypt-then-mac*, não adotado pelo MTProto.

CONCLUSÃO

Securegen (2016) é uma distribuição Android, focada em três pilares valiosos para aqueles que necessitam comunicar-se seguramente em dispositivos móveis: software livre, uso de criptografia forte e máximo respeito à privacidade do usuário.

Ao analisar os três aplicativos apresentados, contudo, pode-se perceber que nenhum deles adota satisfatoriamente esses três pilares.

A solução pelo WhatsApp é, talvez, a hipótese mais facilmente descartada. Por ser software fechado, não é possível uma auditoria pública do código e, se fosse necessário, correção do mesmo por qualquer usuário. Não é possível falar de comunicação móvel segura sem apelar para as liberdades do software. O WhatsApp também é notavelmente débil em relação à privacidade do usuário, coletando muito mais metadados dos usuários e mensagens do que o aplicativo Signal (Lee, 2016), e pouco se sabe sobre como o Facebook utiliza os mesmos.

O Signal, por sua vez, é campeão do respeito à privacidade do usuário, e possui o protocolo mais sólido e consolidado – praticamente não apresenta alterações desde 2014, quando o suporte a mensagens SMS/MMS criptografadas foi removido. Problemas de implementação existem, mas

são raros e, quando descobertos, rapidamente resolvidos. Exemplos passados incluem um *bug* que fazia com que as mensagens fossem mandadas em texto plano, ou seja, sem uso de criptografia (OWS, 2014a), e outro que permite a leitura das mensagens decifradas na tela de bloqueio do aparelho (OWS, 2014b).

Seu uso enquanto software livre, todavia, é prejudicado: apesar de exemplarmente disponibilizar seu código como software livre tanto o código do servidor quanto do cliente – situação única entre os três –, sua instalação na plataforma Android requer o uso de serviços fornecidos pelo Google, o que obriga seus usuários nessa plataforma a aceitar os nebulosos termos de serviço daquela companhia, inviabilizando, por exemplo, sua distribuição junto a projetos como o Securegen.

Uma solução possível para esse impasse seria uma versão do protocolo Signal que substituísse o uso dos serviços do Google nessa implementação por outras tecnologias. Tentativa nesse sentido incluíram o LibreSignal (n.d.), que utilizava o padrão aberto WebSocket para comunicação. Contudo, seu desenvolvimento foi abandonado em definitivo.

Apesar de o código do servidor Telegram ser fechado, ele fornece uma bem documentada API pública, que permite o desenvolvimento de clientes não oficiais com relativa facilidade. O código de seus clientes oficiais são abertos e livres.

O protocolo do Telegram, apesar de simples, é bastante heterodoxo: sua escolha por primitivas obscuras ou obsoletas, a decisão de não usar o paradigma *encrypt-then-mac* e, no caso da derivação de chaves, praticamente "reinventar a roda" usando um algoritmo próprio, sem qualquer justificação teórica ou empírica, em vez de uma primitiva criptográfica em que se pudesse confiar, são motivos mais que suficientes para requerer cautela a qualquer usuário. Apesar de o uso do protocolo MTProto não ter ainda sido descartado para comunicação segura, pouco há para se confiar em suas decisões de projeto.

Devido a relativa imaturidade do protocolo, ainda é comum se encontrar vulnerabilidades no protocolo, com reações distintas por parte do Telegram. Dois ataques teóricos, descritos por Jakobsen & Orlandi (2015), que comprometem a indistinguibilidade do texto cifrado (IND-CCA), foi desconsiderado pela equipe de engenheiros, porque ainda não afeta a segurança prática do protocolo. Nas palavras do próprio Telegram (2016a):

> Um funcionário do correio pode escrever 'Haha' (usando tinta invisível!) no lado de fora de um envelope selado que ele entrega para você. Isso não impede o envelope de ser entregue, isso não permite-o alterar o conteúdo do pacote, e isso não permite-o ver o que há do lado de dentro.

O próprio esquema de *fingerprints* do Telegram, utilizado para garantir a identidade dos usuários, já sofreu um ataque teórico, descrito por Rad (2015). O ataque partia das premissas de que, como o *fingerprint* é apenas um "resumo" da chave, e não a chave em si, é muito mais fácil encontrar colisões entre *fingerprints* do que entre chaves – 2^{-65} contra 2^{-128}. Desde então, o Telegram alterou a forma como obtém os *fingerprints* (Telegram, 2015), tornando o ataque infactível perante o

poder computacional atual. Ataques dessa natureza, causados pela má escolha de primitivas pelo Telegram, têm chances altas de se repetirem, o que poderiam ter sido evitado pela formulação de um protocolo mais ortodoxo, a princípio.

Outro ataque do Telegram, este aqui ainda não resolvido e com claras implicações práticas, ocorre porque a vasta maioria dos usuários do aplicativo não utilizam autenticação em dois passos. Como, no Telegram, a autenticação entre aparelhos ocorre a partir de envio de mensagens SMS, alguém com poder sobre a rede SMS – como governos e companhias de telefonia – poderiam interceptar um SMS de autenticação requisitado por Alice, ou até se passar por ela, e ter acesso a todas as suas conversas Rad (2015). Esse ataque pode ser contornado com autenticação de dois passos, mas pouco foi feito para se encorajar tal prática.

É preciso ponderar, ainda, quão prudente é lançar o código de um protocolo em pleno desenvolvimento ao público, onde pode ser acessado e estudado por indivíduos e órgãos mal intencionados.

Outro problema do Telegram é referente à grande quantidade de metadados enviados aos seus servidores, por padrão, que podem ser utilizados para rastrear um usuário, comprometendo sua privacidade (Flisbäck, 2015).

Contudo, suas boas vindas em relação ao desenvolvimento de aplicações derivadas torna o Telegram um candidato para aplicações que pretendem melhorar a segurança dos usuários. Alguns problemas que impedem um uso mais abrangente do usuário é o fato de que, por padrão, as conversas são criadas sem criptografia ponta a ponta e autodestruição – o que seria perfeitamente possível de se consertar no cliente –, a indisponibilidade de conversas criptografadas ponta a ponta para grupos e a não obrigatoriedade da autenticação em dois passos.

Conclui-se, dessa forma, que nenhum dos três aplicativos cumprem, no estado atual, todos os requisitos postos pelo Securegen. No entanto, soluções para alguns desses problemas podem ser achadas. O campo de aplicativos móveis seguros ainda necessitam muito da solução de muitos impasses colocados pelo *status quo* atual.

NOTAS

* Aluno do bacharelado em Sistemas de Informação da EACH-USP (leopiccionia@gmail.com).

** Professor doutor da EACH-USP (marciomr@usp.br).

1. Esta seção é baseada em OWS (2015).

REFERÊNCIAS

Adrian, D. et al. (2015). Imperfet Forward Secrecy: How Diffie-Hellman Fails in Practice. In *Proceeding of the 22nd ACM SIGSAG Conference on Computer and Communications Security*, pp. 5-17. ACM. Retrieved from https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

Bellare, M., & Namprempre, C. (2000). Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology – ASIACRYPT 2000*, pp. 531-545. Springer Berlin Heidelberg. Retrieved from http://cseweb.ucsd.edu/mihir/papers/oem.pdf

Bernstein, D. J. (2006). Curve25519: new Diffie-Hellman speed records. In *Proceedings of PKS 2006, to appear*. Retrieved from http://cr.yp.to/papers.html#curve25519

Diffie, W., & Hellman, M. E. (1979). Privacy and authentication: An introduction to cryptography. *Proceeding of the IEEE*, 67(3), 397-427.

Electronic Frontier Foundation. (2016). *Secure Messaging Scorecard*. Retrieved from https://www.eff.org/node/82654

Flisbäck, O. (2015). *Stalking anyone on Telegram*. Retrieved from https://oflisback.github.io/telegram-stalking/

Greenberg, A. (2011, Nov 28). Twitter Acquires Moxie Marlinspike's Encryption Startup Whisper Systems. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2011/11/28/twitter-acquires-moxie-marlinspikes-encryption-startup-whisper-systems

Greenwald, G., & MacAskill, E. (2013, Jun 07). NSA Prism program taps in to user data of Apple, Google and Others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., MacAskill E., & Poitras, L. (2013, June 11). Edward Snowden: the whistleblower behind NSA surveillance revelations. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Hornby, T. (2013, Dec 19). Telegram's Cryptanalysis Contest. *Crypto Fails* [Blog post]. Retrieved from http://www.cryptofails.com/post/70546720222/telegrams-cryptanalysis-contest

Jakobsen, J. B., & Orlandi, C. (2015). *A practical cryptanalysis-of-the Telegram messaging protocol*. Master Thesis. Aarhus University. Retrieved from http://cs.au.dk/jakjak/master-thesis.pdf

Lee, M. (2016, Jun 22). Battle of the Secure Messaging Apps: How Signal Beats WhatsApp. *The Intercept*. Retrieved from https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/

LibreSignal. (n.d.). LibreSignal: the truly private and Google-Free messenger for Android. *GitHub.* Retrieved from https://github.com/LibreSignal/LibreSignal

Marlinspike, M. (2013a, Nov 26). Advanced cryptographic ratcheting [Blog post]. *Open Whisper Systems*. Retrieved from https://whispersystems.org/blog/advanced-ratcheting/

Marlinspike, M. (2013b, Jul 27). Simplifying OTR deniability [Blog post]. *Open Whisper Systems*. Retrieved from https://www.whispersystems.org/blog/simplifying-otr-deniability/

Marlinspike, M. (2015, Mar 06). Saying goodbye to encrypted SMS/MMS [Blog post]. *Open Whisper Systems.* Retrieved from https://whispersystems.org/blog/goodbye-encrypted-sms/

Marlinspike, M. (2016, Apr 05). WhatsApp's Signal Protocol Integration is now complete [Blog post]. *Open Whisper Systems*. Retrieved from https://whispersystems.org/blog/whatsapp-complete/

Menezes, A. J., van Oorschot, P. C, & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. US: CRC Press.

National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES)*. Springfield, VA. Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

National Institute of Standards and Technology. (2012). *Secure Hash Standard (SHS)*. Gaithersburg, MD. Retrieved from http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

Rad, A. (2015, Jan 09). *A 264Attack On Telegram, and Why a Supper Villain Doesn't Need It To Read Your Telegram Chats* [Blog post]. Retrieved from https://www.alexrad.me/discourse/a-264-attack-on-telegram-and-why-a-super-villain-doesnt-need-it-to-read-your-telegram-chats.html

Salomão, K. (2015, Dec 20). Pavel Durov, o polêmico fundador do aplicativo Telegram. *Exame*. Retrieved from http://exame.abril.com.br/negocios/pavel-durov-o-polemico-fundador-do-aplicativo-telegram/

Schneier, B. (2004, Aug 19). Opinion: Cryptanalysis of MD5 and SHA: Time for a new standard [Blog post]. *Computerworld.* Mountain View, CA. Retrieved from http://www.computerworld.com/article/2566208/security0/opinion--cryptanalysis-of-md5-and-sha--time-for-a-new-standard.html

Securegen. (2016). Página inicial. Retrieved from http://securegen.org/

Stallman, R. M. (2015). *Free Software, Free Society* (3rd ed.). Boston, MA: Free Software Foundation.

Stevens, M. (2012). *Attacks on Hash Functions and Applications*. Amsterdam. Retrieved from https://marc-stevens.nl/research/papers/PhD Thesis Marc Stevens - Attacks on Hash Functions and Applications.pdf

Open Whisper Systems. (2014a). Forward SMS not being encrypted when not touching text. *GitHub*. Retrieved from https://github.com/WhisperSystems/Signal-Android/issues/1073

Open Whisper Systems. (2014b). Reading “Encrypted” Messages without Password. *GitHub*. Retrieved from https://github.com/WhisperSystems/Signal-Android/issues/1716

Open Whisper Systems. (2015). ProtocolV2. *GitHub*. Retrieved from https://github.com/JavaJens/TextSecure/wiki/ProtocolV2

Telegram. (2015, Apr 08). *Active Sessions and Two-Step Verifications* [Blog post]. Retrieved from https://telegram.org/blog/sessions-and-2-step-verification

Telegram. (2016a). *FAQ for the Technically Inclined*. Retrieved from https://core.telegram.org/techfaq

Telegram. (2016b). *MTProto Mobile Protocol*. Retrieved from https://core.telegram.org/mtproto

WhatsApp. (2016). *WhatsApp Encryption Overview*. Retrieved from https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Zorz, Z. (2016, Aug 11). How the EFF was pushed to rethink its Secure Messaging Scorecard. *Help Net Security.* Retrieved from https://www.helpnetsecurity.com/2016/08/11/eff-secure-messaging-scorecard/

O PROCESSO DE IMPLEMENTAÇÃO DE SALAS DE VIODEOMONITORAMENTO NO BRASIL

Resumo: O presente trabalho tem como objetivo reconstruir analiticamente o processo de implementação de salas de videomonitoramento (CCTV) no contexto brasileiro recente, no bojo da realização de megaeventos (Copa do Mundo 2014 e Olimpíadas 2016). Especificamente, busca-se mapear quais dimensões convergem para a legitimação desses sistemas de vigilância, por meio do mapeamento de atores, instituições e dispositivos legais envolvidos no processo de implementação e de operacionalização dos Centros Integrados de Comando e Controle (CICC) no país. Metodologicamente, foi (a) pesquisada e organizada sistematicamente a legislação que regula o tema no Brasil; em seguida, foram (b) realizadas entrevistas com autoridades políticas e policiais envolvidas na adoção das políticas nacionais de videomonitoramento; for fim, realizaram-se (c) observações no Centro Integrado de Comando e Controle da cidade de Canoas/RS, para verificação do modo como são operacionalizadas as propostas legais em âmbito municipal. Em nível teórico, o trabalho dialoga com as obras de Foucault e Agamben, a partir dos conceitos de práticas discursivas e biopolítica. Como resultado, aduz-se que, ao menos, seis dimensões convergem para a legitimação das propostas de implementação dos CICC: uma internacional; uma econômica; uma material; uma jurídica; uma discursiva; uma espacial. Dentre tais dimensões, os atores entrevistados salientam a construção do discurso do "medo" da cidade como fator decisivo para implementação de sistemas de videomonitoramento, embora não haja, no Brasil, qualquer estudo que indique a eficiência desses sistemas para a redução de taxas de criminalidade. A despeito de a ideia de "segurança" constituir o elemento discursivo que legitima a adoção dessas práticas, a operacionalização dos CICC não se atém à área da segurança pública, atuando como dispositivo biopolítico na gestão de uma ampla gama de elementos do espaço urbano.

Palavras-chave: Vigilância, Videomonitoramento, Centros integrados de comando e controle, Processo de implementação.

EDUARDO GEORJÃO FERNANDES*

El proceso de implementación de salas de videovigilancia en Brasil

Resumen: El presente trabajo tiene como objetivo reconstruir analíticamente el proceso de implementación de salas de videovigilancia (CCTV) en el contexto brasileño reciente, de realización de megaeventos (Copa del Mundo 2014 y Juegos Olímpicos 2016). Específicamente, se busca mapear cuales son las dimensiones que convergen a la legitimidad de estos sistemas de vigilancia, por medio del mapeo de atores, instituciones y dispositivos legales envueltos en el proceso de implementación y de operación de los Centros Integrados de Comando e Controle (CICC) en el país. Metodológicamente, ha sido (a) investigada y organizada de forma sistemática la legislación que regula el tema en el Brasil; en la secuencia, fueran (b) realizadas entrevistas con autoridades políticas y policiales envueltas en la adopción de la videovigilancia; por fin, se realizaron (c) observaciones en el Centro Integrado de Comando e Controle en la ciudad de Canoas/RS, para comprobar la forma que se tornan operativas las propuestas legales a nivel municipal. A nivel teórico, el trabajo dialoga con las obras de Foucault y Agamben, a partir de los conceptos de prácticas discursivas y biopolítica. Como resultado, se aduce que, por lo menos, seis dimensiones convergen para la legitimación de las propuestas de implementación de los CICC: una internacional; una económica; una material; una jurídica; una discursiva; una espacial. Entre estas dimensiones, los actores investigados resaltan la construcción del discurso del "miedo" de la ciudad como un factor decisivo para la implementación de sistemas de videovigilancia, aunque, en Brasil, no haya cualquier estudio que indique la eficiencia de estos sistemas para la reducción de los índices de criminalidad. A pesar de la idea de "seguridad" construir el elemento discursivo que legitima la adopción de estas prácticas, la operación de los CICC no se sostiene a la zona de la seguridad pública, actuando como un dispositivo biopolítico en la gestión de una amplia gama de elementos del espacio urbano.

Palabras-clave: Videovigilancia, Centros integrados de comando e controle, Proceso de implementación.

The implementation of video surveillance rooms in Brazil

Abstract: This work aims to analytically reconstruct the process of implementation of video surveillance rooms (CCTV) in the recent Brazilian context, related to the realization of mega-events (2014 World Cup and 2016 Olympics). Specifically, it seeks to identify which dimensions converge to the legitimacy of these surveillance systems, through the mapping of actors, institutions and legal mechanisms involved in the process of implementation and operationalization of the Integrated Command and Control Centers (ICCC) in the country. Methodologically, (a) the legislation regulating the issue in Brazil was systematically researched and organized; (b) the author interviewed political and police authorities involved in the adoption of national video surveillance policies; finally, (c) the author researched police practices in the Integrated Command and Control Centre of the city of Canoas/RS, to check how legal proposals are operationalized at the municipal level. At a theoretical level, the work dialogues with the works of Foucault and Agamben, based on the concepts of discursive practices and biopolitics. As a result, the author concludes that at least six dimensions converge to the legitimacy of the implementation of ICCC: an international dimension; an economic dimension; a material dimension; a legal dimension; a discursive dimension; a spatial dimension. Among these dimensions, the interviewed actors emphasize the construction of the discourse of the "fear" of the city as a decisive factor for the implementation of video surveillance systems, although there isn't, in Brazil, any study indicating the efficiency of these systems to reduce crime rates. Despite the idea of "security" as the discursive element that legitimizes the adoption of these practices, the operationalization of the ICCC is not restricted to security, acting as a biopolitical device in managing a wide range of urban space elements.

Keywords: Surveillance, CCTVs, Implementation.

INTRODUÇÃO

O presente trabalho tem como objetivo produzir uma reflexão acerca da construção da vigilância como objeto de estudos no Brasil, sob uma perspectiva sociológica. Busca-se demonstrar a contemporaneidade do fenômeno da vigilância no contexto brasileiro, ao mesmo tempo em que se propõe o desenvolvimento e a consolidação de uma agenda de estudos sobre o tema.

A justificativa para a realização dessa pesquisa fundamenta-se na constatação de que a vigilância é um fenômeno relevante nas atuais configurações das sociedades ocidentais[1] e constitui objeto de diversos estudos europeus e norte-americanos. Na França, há uma tradição que segue os estudos de Foucault (2002); no Reino Unido, mais recentemente, a intensa proliferação de câmeras de vigilância é estudada desde os trabalhos inaugurais de Clive Norris e Armstrong (1999). Nos Estados Unidos, destaca-se, como ponto de partida, o estudo clássico de James B. Rule (1973).

Ainda assim, verifica-se que a temática não assumiu centralidade nas agendas de pesquisa brasileiras e, mais amplamente, latino-americanas. Em outros termos, a vigilância não assume uma significância relevante no debate teórico latino-americano. Conforme Botello (2012) assevera, estudos sobre Segurança Pública têm se consolidado na América Latina, desde os anos 1990, principalmente para análise de contextos políticos pós-ditaduras militares. As pesquisas da região em Segurança Pública têm, de modo geral, abordado quatro questões centrais: o policiamento e o controle social, em diferentes níveis e escalas; a segurança em processos de rupturas com lógicas tradicionais de convívio; a expansão de novas formas de subjetivação quanto ao tema da violência; a análise das formas como o crime e a insegurança atuam sobre o espaço urbano. Em todas essas linhas de análise, a vigilância é adotada como epifenômeno, como uma dimensão periférica e complementar a ser estudada, e não como o centro da análise (Botello, 2012). Configura-se, portanto, uma lacuna teórica a ser enfrentada.

Para tratar dessa questão, subdivide-se o trabalho em três momentos: primeiramente, busca-se contextualizar a implementação de dispositivos de vigilância (com ênfase empírica sobre o caso dos sistemas de videomonitoramento) no Brasil, principalmente em um período recente; em segundo lugar, apontando-se dimensões que convergem para a consolidação desses dispositivos; em terceiro lugar, a partir de pesquisa exploratória realizada no Centro Integrado de Comando e Controle (CICC) da cidade de Canoas/RS, são analisadas, dentre as dimensões apontadas, aquelas que os atores identificam como os principais fundamentos para a implementação desses dispositivos, bem como é analisada a operacionalização do CICC sobre a gestão do espaço urbano.

Metodologicamente, foi, em um primeiro momento, realizada uma revisão da literatura e da legislação que regula a implementação de CICC's no Brasil. Foram, em seguida, realizadas entrevistas com o ex-comandante geral da Brigada Militar do Rio Grande do Sul, com o atual e um antigo Secretário de Segurança Pública da cidade de Canoas/RS e com o atual analista do CICC de Canoas. Ainda, realizaram-se observações no referido CICC.

A EMERGÊNCIA DA VIGILÂNCIA COMO FENÔMENO BRASILEIRO: DIMENSÕES EM CONVERGÊNCIA

Eventos disparadores do debate: o ciclo de manifestações de 2013 e os megaeventos no Brasil

Um fenômeno catalisador de uma série de processos sociais recentes no Brasil é ciclo de manifestações de 2013. Esse ciclo trouxe à tona diversas questões sobre as quais há um esforço teórico de análise ainda em desenvolvimento (Maricato et al., 2013; Cattani, org., 2014). A partir dos acontecimentos observados, foram realizados estudos sobre temas como os processos de engajamento e organização dos atores das manifestações (Silva, 2014), a conjuntura socioeconômica que permitiu a eclosão dos protestos (Žižek, 2013), os conflitos violentos ocorridos entre manifestantes e policiais (Tavares dos Santos; Teixeira, 2014) e o papel desempenhado pelas mídias que cobriram os atos (Lima, 2013).

O presente trabalho postula que um dos temas que as manifestações de 2013 colocaram em pauta é o modo como se dá a gestão de conflitos urbanos no país. Nesse sentido, uma das especificidades dos protestos de 2013 reside no fato de que, embora estudos demonstrem que o Estado brasileiro seja caracterizado por adotar uma tradição de práticas militarizadas no espaço urbano, com o uso político da polícia para controle das classes populares (Pinheiro; Izumino y Fernandes, 1991; Wacquant, 2003), aquele período de manifestações realizou-se em condições específicas: os atos de protestos ocorreram, majoritariamente, em espaços urbanos centrais, com o protagonismo de atores não advindos das periferias das cidades brasileiras (Singer, 2013; Tavares dos Santos e Teixeira, 2014) e com a paralela utilização de novas tecnologias de informação por manifestantes (Silva, 2014).

As características supracitadas, em conjunto, criaram um espaço propício à visibilização das ações das polícias em diversas regiões do Brasil. Nesse contexto, é possível destacar o papel de coletivos como, por exemplo, a Mídia Ninja,[2] a qual realizou a cobertura em tempo real de protestos no país, e o uso instrumental de *smartphones* e das redes sociais na disseminação de vídeos, imagens e textos a respeito dos protestos. Assim, diferentemente do que ocorre quando operam na periferia (Manning, 2008; Goldsmith, 2010), as ações policiais tornaram-se amplamente publicizadas.

Ao mesmo tempo, o contexto das manifestações, somado à realização da Copa do Mundo no Brasil, em 2014, foi catalisador para a concretização de investimentos em tecnologias policiais. Dentre tais investimentos, podem ser mencionados a utilização de câmeras de vigilância para a identificação de manifestantes, o uso de bancos de dados para acesso ao perfil criminal de ativistas e o desenvolvimento de *softwares* de rastreamento de perfis em redes sociais.[3] Tais tecnologias foram incorporadas aos Centros Integrados de Comando e Controle (CICC), constituídos por salas de monitoramento de âmbito estadual, instaladas nas capitais de todos os estados em que foram realizados jogos da Copa do Mundo de 2014, para controle de situações de "risco" durante o evento.

Segundo Kopittke (2015), o impacto dos megaeventos para a gestão do espaço urbano no Brasil data da realização dos Jogos Panamericanos de 2007, na cidade do Rio de Janeiro. Embora neste evento a Secretaria Nacional de Segurança Pública (SENASP) tenha implantado estratégias vinculadas à construção de programas sociais com jovens de comunidades periféricas da cidade, a preparação para os megaeventos seguintes (Copa do Mundo de 2014 e Olimpíadas de 2016) não seguiu o mesmo modelo. Kopittke (2015) relata que, para estes eventos, criou-se uma Secretaria específica (Decreto n. 7.538, de 1º de agosto de 2011), coordenada por Delegados da Polícia Federal. Após disputas institucionais, a presidenta à época, Dilma, optou que o Ministério da Justiça, o Ministério da Defesa e o Gabinete de Segurança Institucional formassem um triunvirato para tratar das questões de segurança na Copa do Mundo de 2014. Sobre a gestão da segurança na Copa do Mundo de 2014, afirma, em entrevista, o atual Secretário de Segurança Pública de Canoas/RS: "A proposta do Governo Federal então se reduziu ao Centro de Comando e Controle. A 12 Centros de Comando e Controle".

Essa dinâmica complexa, em que órgãos estatais de controle dispõem de aparatos tecnológicos para visibilização e armazenamento de dados sobre situações conflitivas (ao mesmo tempo em que tecnologias são apropriadas por atores da sociedade civil, como nas manifestações de 2013), traz à tona o debate sobre os usos de tecnologias para fins de vigilância no Brasil. A tradução desse fenômeno empírico em objeto teórico constitui procedimento necessário para a compreensão do tema.

As dimensões para a implementação de dispositivos de vigilância no Brasil

No percurso analítico entre a detecção de que práticas de vigilância fazem-se presentes no contexto brasileiro e o desenvolvimento de um debate teórico sobre o tema, é necessário que se questione: *como a temática da vigilância tem se inserido enquanto fenômeno relevante no contexto brasileiro?* Com vistas a entender o processo de implementação de dispositivos de vigilância no país, foram mapeadas dimensões que, em convergência, têm atuado para a produção desse fenômeno. Foram detectadas, nesse sentido, ao menos seis dimensões relevantes: uma relacionada ao contexto internacional; uma econômica; uma material; uma jurídica; uma discursiva; e, por fim, uma espacial. Essas dimensões foram isoladas para fins analíticos, embora, na realidade, encontrem-se interligadas e mutuamente implicadas.

A primeira dimensão, muito apontada como relevante pela literatura, é relacionada à conjuntura *internacional*. A grande maioria dos atuais estudos sobre vigilância toma como ponto de inflexão os acontecimentos decorrentes de 11 de setembro de 2001 para uma reconfiguração das políticas internacionais de segurança (Wood, 2009). Isso porque após o episódio do *World Trade Center*, o governo norte-americano passa a adotar uma série de providências contra o "terrorismo", como o *Patriot Act*,[4] e legitima discursivamente a "Guerra ao Terror". A união entre uma concepção específica de segurança e o desenvolvimento tecnológico de instrumentos de controle é denominada por Stpehem Graham (2011) "gestão militarizada do espaço urbano". Trata-se da

entrada, na cidade, de lógicas e tecnologias militarizadas na gestão dos conflitos ("guerra irregular, assimétrica ou de baixa intensidade"), de modo que os próprios habitantes do espaço urbano são entendidos como potenciais ameaças à garantia da ordem. Graham (2015) demonstra que diversas tecnologias utilizadas em situações de guerra (como é o caso dos *drones*) passam a colonizar o cotidiano da cidade.

À dimensão internacional soma-se um aspecto de natureza *econômica*. O pós-11 de setembro instaura a possibilidade de desenvolvimento de uma indústria multinacional de vigilância. Ou seja, a vigilância passa a ser um negócio lucrativo. Nesse sentido, a gestão pública do espaço urbano (representada por órgãos estatais de controle social) mescla-se a uma lógica privada, e diversas empresas passam a concorrer pela ocupação do mercado da vigilância. A literatura aponta que o investimento de grandes empresas está diretamente ligado à expansão dos sistemas de vigilância no mundo (Graham, 2011).

A seguir, há uma dimensão denominada *material*, que se traduz na possibilidade de implementação de novas tecnologias em espaços específicos. Trata-se do conjunto de tecnologias (atores não-humanos) que compõe o espaço da cidade. No caso do Brasil, como já citado, a ocorrência de megaeventos (Copa do Mundo de 2014 e Olimpíadas de 2016) é central para o aporte de recursos na implementação de um pacote tecnológico de vigilância. A literatura de megaeventos considera esses pacotes de segurança como uma das principais (senão a principal) "heranças" desses eventos (Gaffney, 2016). No caso do Brasil, a estratégia de segurança adotada para a Copa do Mundo consistiu primordialmente na instalação de Centros Integrados de Comando e Controle em todos os estados que receberam jogos. Esses centros são compostos por salas de controle, interconectadas a um conjunto de câmeras. As câmeras, voltadas para a filmagem do espaço urbano, são controladas por agentes estatais. Atualmente, após a ocorrência da Copa do Mundo, esses centros estão ainda em funcionamento. Se, à época do evento, o objeto da vigilância eram eventuais "ameaças terroristas" (dado o contexto internacional que atravessa a instalação desses dispositivos), no momento atual são os habitantes das cidades brasileiras os sujeitos que passam a ser controlados.

Uma característica específica desses sistemas de vigilância é traduzida pelo conceito operacional de "vigilância distribuída" (Bruno, 2013). Por meio desse conceito, busca-se demonstrar que atualmente esses dispositivos de segurança não estão necessariamente ligados a um sistema central para o qual convergem as informações (modelo Panóptico – Foucault [2002]), mas sim está distribuída, de modo que diversos atores convergem na assunção do papel de "vigilante".

Interconectada a essas dimensões, existe uma dimensão *jurídica*, relativa a uma série de instrumentos legais que permite e incentiva a disseminação de políticas de vigilância. No caso do Brasil, recentemente foi aprovada a Lei Antiterrorismo (13.260/2016), que segundo a presidenta (suspensa) Dilma é uma lei especificamente voltada para a segurança das Olimpíadas, mas que terá seus efeitos aplicados mesmo posteriormente aos jogos olímpicos. Além disso, no Brasil não existe regulamentação de proteção a dados pessoais, de modo que a privacidade não é, de

fato, elevada à condição de direito. Além disso, está em andamento na Câmara dos Deputados a CPI dos Crimes Cibernéticos,[5] que estabelece uma série de restrições ao uso da *Internet*, em oposição aos princípios estabelecidos no Marco Civil da *Internet*.

A seguir, é possível identificar uma dimensão *discursiva*. Esse elemento é central, pois ele está ligado à construção de um aparato discurso que justifica e legitima a necessidade de implementação de sistemas de vigilância. Nesse âmbito, é fundamental a oposição entre a o "medo da cidade" e a "eficiência da tecnologia". Em outros termos, constroi-se, por um lado, a ideia de que a cidade é um território a ser temido, um espaço perigoso, no qual o "risco" e a "insegurança" são preponderantes (Souza, 2008). Por outro lado, apesar de não haver nenhum estudo que comprove a eficácia do uso de novas tecnologias para a diminuição de índices de criminalidade, a tecnologia é vista, segundo a literatura, como um meio eficaz de resolução dos conflitos no espaço urbano (Byrne & Marx, 2011). Além disso, a palavra "segurança" é utilizada discursivamente como um "significante vazio", que também se autolegitima. "Em nome da segurança" tudo é feito, sem que se questionem as consequências potencialmente perversas da expansão do controle (Agamben, 2014).

Por fim, uma dimensão relevante para o entendimento do fenômeno da vigilância é o aspecto *espacial*. É necessário, nesse sentido, refletir até que ponto a políticas de vigilância reconfiguram o espaço urbano, atuando nas fronteiras de delimitação entre o público e o privado. Há uma série de estudos que se vincula a uma perspectiva urbanista, na reflexão sobre as consequências da vigilância, ou seja, sobre os modos como os dispositivos tecnológicos de vigilância atuam diante dos espaços das cidades no Século XXI (Graham, 2011; Lippert y Wood, 2012).

Implementação dos CICC's: entre a demanda por segurança e a gestão do espaço urbano

A partir de entrevistas e observações realizadas no CICC da cidade de Canoas/RS, podem ser apontados alguns resultados parciais da presente pesquisa. Primeiramente, todas as falas dos entrevistados convergem para a centralidade da demanda pela implementação tecnologias para gestão da segurança no espaço urbano. O atual Secretário de Segurança Pública de Canoas, quando perguntado sobre as demandas por segurança na cidade, afirma: "eu tinha muita gente pedindo câmera. Todo mundo pedindo câmera. [...] Todo mundo quer câmera".

A demanda por dispositivos de tecnologia evidencia a relevância da dimensão discursiva para implementação dos CICC's. Como já afirmado, às câmeras de vigilância está atrelado o discurso da eficácia (Byrne & Marx, 2011). Em um contexto no qual o espaço urbano é reconhecido como *locus* do medo (Souza, 2008), as alternativas que são operadas com base na vigilância desse espaço são legitimadas socialmente. Ainda assim, o próprio Secretário de Segurança Pública da cidade afirma: "Eu não conheço nenhuma evidência, nenhuma pesquisa que tenha demonstrado a relação entre câmeras e redução de criminalidade". A dissonância entre a demanda por tecnologias de vigilância como política de segurança pública (com a ausência de debates sobre

as implicações de tais dispositivos sobre a esfera da privacidade) e a não comprovação da eficácia das câmeras na redução da criminalidade consiste em um ponto central, a ser investigado de forma aprofundada.

Como consequência da demanda por tecnologia, verifica-se, no CICC de Canoas, a proliferação de uma série de aparatos tecnológicos: 180 câmeras, espalhadas pela cidade e operadas por policiais militares aposentados; dispositivos de detecção facial; aparelhos de leitura de placas de carro; detectores de tiros; alarme em prédios públicos; *Whatsapp* comunitário; alarme comunitário. Assim, verifica-se uma amplificação de dispositivos, os quais não se restringem a câmeras de vigilância, multiplicando-se a quantidade e o formato de dados armazenados no CICC.

Ademais, a operacionalização do CICC de Canoas não se restringe à área da segurança pública. Além do controle sobre a criminalidade, o CICC buscar operacionalizar a detecção de prevenção de catástrofes ambientais, regular o tráfego terrestre na cidade, fiscalizar serviços públicos (serviços de iluminação, por exemplo), entre outros. Segundo o analista do CICC, diversos órgãos convergem na operacionalização do centro de controle. Portanto, apesar de a demanda por segurança ser o elemento central que justifica a implementação do CICC, a gestão operacionalizada pelo centro transcende a área da segurança e se constitui como mecanismo biopolítico (Foucault, 1999), abrangendo uma ampla gama de aspectos do espaço urbano. As consequências da irradiação de dispositivos tecnológicos sob controle do Estado, na gestão dos espaços urbanos, constitui tema a ser explorado.

CONSIDERAÇÕES FINAIS

Conclusivamente, podem ser apontados alguns desafios para a continuidade da presente pesquisa. Uma questão a ser enfrentada não apenas no contexto brasileiro, mas também nos estudos internacionais sobre vigilância, é o desenvolvimento de abordagens e técnicas que confiram rigor metodológico. Diversos estudos sobre vigilância consistem em especulações teóricas, as quais, apesar de sua indiscutível importância, não realizam um cotejamento entre o abstrato e o empírico (Walby, 2005).

Para tanto, é necessário, a um só tempo, o investimento em pesquisas empíricas, a utilização de mecanismos que confiram rigor metodológico e verificabilidade aos resultados encontrados (Spink e Lima, 2013) e a assunção de posturas criativas, que primem pela imaginação e pela inventividade. Quanto a este último ponto, exatamente por serem os estudos em vigilância uma área de recente desenvolvimento, há um espaço aberto para que sejam criadas novas formas de coleta e de análise de dados. Em outros termos: não há um manual sobre como estudar vigilância ou um método único a ser utilizado. Diferentes abordagens e técnicas estão sendo testadas (é o caso, por exemplo, da etnografia institucional no estudo de salas de videomonitoramento – Walby, 2005), e há construções ainda a serem propostas.

Ademais, há poucos estudos que tratam da vigilância de acordo com as especificidades do espaço urbano brasileiro. Nesse ponto, destacam-se os estudos de Bruno (2013) e Kanashiro (2008) pela percepção da relevância que as condições nacionais de produção da vigilância possuem. Mesmo a partir da matriz foucaultiana que domina a área, é inevitável refletir sobre as relações de poder implícitas aos dispositivos de vigilância. No caso do Brasil (e da América Latina, de modo geral) os contextos pós-ditadura (com os resquícios, na atuação policial, de posturas autoritárias), as exclusões socioeconômicas e as desigualdades são elementos centrais, sem os quais não podem ser entendidos os efeitos da vigilância. Em outros termos, as tecnologias de vigilância atuam em contextos caracterizados por assimetrias na distribuição do poder e, no limite, podem servir para a potencialização dessas assimetrias.

Por fim, segundo Lyon (2007), a pesquisa em vigilância é um projeto necessariamente interdisciplinar. Assumir a vigilância como uma área interdisciplinar, para além de uma construção meramente retórica, exige que se leve a sério tal questão. Essa temática pode ser tratada a partir de diversas perspectivas, como a sociologia da violência, o urbanismo, a geografia, a sociologia da ciência e da tecnologia, o direito, a psicologia, as relações internacionais, dentre outras. Assim, é importante que se atente para as diversas dimensões que atuam, em conjunto, na produção da vigilância, assim como se deve evitar a disputa para delimitação da vigilância como objeto de uma área específica (sob o risco de se perder a complexidade da temática).

NOTAS

* Universidade Federal do Rio Grande do Sul (UFRGS), aluno de Doutorado e Mestre em Sociologia pela UFRGS, e-mail: eduardo.g.fernandes@gmail.com.

1. Diversas denominações, como “sociedade tecnológica”, “sociedade de informação” e “sociedade de conhecimento”, buscam produzir uma interpretação abrangente sobre o contexto atual das sociedades ocidentais (Knorr-cetina, 1999).

2. A Mídia Ninja é definida, em seu *site*, nos seguintes termos: “Uma rede de comunicadores que produzem e distribuem informação em movimento, agindo e comunicando. [...] Nossa pauta está onde a luta social e a articulação das transformações culturais, políticas, econômicas e ambientais se expressa.” Disponível em: `https://ninja.oximity.com/partner/ninja/about`;. Acesso em: 20/06/2015.

3. Em entrevista, ex-comandante da Brigada Militar do Rio Grande do Sul referiu o seguinte: “Nós usamos *software* de identificação. Eu tinha uma viatura, um veículo que a câmera passava, identificava o rosto da pessoa, e essa identificação ia para um banco de dados que dizia “olha, esse aqui é procurado, esse aqui não é delinquente, esse aqui não tem nada, esse aqui tem lesão corporal, esse aqui tem homicídio, esse aqui é traficante”, entende? Então nós tínhamos isso durante a Copa do Mundo”.

4. O *Patriot Act* é um decreto assinado por George W. Bush em 26 de outubro de 2001. O decreto estipula medidas (como a intercepção telefônica e de e-mails) que o governo norte-americano adotar contra pessoas suspeitas de práticas “terroristas”.

5. Para mais informações sobre a CPI dos Crimes Cibernéticos e sobre a legislação que regula a vigilância no Brasil, é possível acessar o dossiê "Da Cibersegurança à Ciberguerra – o desenvolvimento de políticas de vigilância no Brasil", do Artigo 19. Fonte: http://artigo19.org.greenhostpreview.nl/. Acesso em: 10/07/2016.

REFERÊNCIAS

Agamben, G. (2014). *Como a obsessão por segurança muda a democracia*. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1568.

Botello, N. A. (2012). Surveillance Studies: An Agenda for Latin America. *Surveillance & Society,* 10(1), 5-17.

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina.

Byrne, J. & Marx, G. (2011). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. *Cahiers Politiestudies*, 3(20), 17-40.

Cattani, A. D. [org.]. (2014). *#protestos*: *análises das ciências sociais*. Porto Alegre: Tomo Editorial.

Foucault, M. (1999). *Em defesa da sociedade: curso no Collège de France* (1975-9176). São Paulo: Martins Fontes.

Foucault, M. (2002). *Vigiar e Punir*: *nascimento da prisão*. Petrópolis: Vozes.

Gaffney, C. (2016). Segurança Pública e os Megaeventos no Brasil. Em O. A. dos Santos Júnior, C. Gaffney e L. C. de Q. Ribeiro (orgs.). *Brasil: os impactos da Copa do Mundo 2014 e das Olimpíadas 2016.* Rio de Janeiro: Observatório das Metropoles.

Graham, S. (2011). *Cities Under Siege*: The New Military Urbanism. London: Verso.

Graham, S. (2015). O bumerangue de Foucault: o novo urbanismo militar. Em B. Kucinski et al. *Bala perdida: a violência policial no Brasil e os desafios para sua superação.* São Paulo: Boitempo.

Goldsmith, A. (2010). Policing's New Visibility. *British Journal of Criminology*, 50(5), 914-934.

Kanashiro, M. (2008). Surveillance Cameras in Brazil: exclusion, mobility regulation, and the new meanings of security*, Surveillance & Society*, 5(3), 270-289.

Knorr-cetina, K. (1999). A comunicação na ciência. First publ. Em: F. Gil (ed.). *A Ciência tal qual se faz.* (pp. 375-393). Lisboa: Edições João Sá da Costa.

Kopittke, A. (2015). *Segurança pública e democracia no Brasil:* uma história de desencontros. (Tese). Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, Rio Grande do Sul, Brasil.

Lima, V. A. de. (2013). Mídia, rebeldia urbana e crise de representação. Em E. Maricato et al. *Cidades rebeldes: Passe Livre e as manifestações que tomaram as ruas do Brasil.* São Paulo: Boitempo: Carta Maior.

Lippert, R. K. & Wood, D. M. (2012). The New Urban Surveillance: Technology, Mobility, and Diversity in 21st Century Cities. *Surveillance & Society*, 9(3), 257-262.

Lyon, D. (2007). *Surveillance Studies: an Overview.* Cambridge: Polity Press.

Manning, P. (2008). A view of surveillance. Em S. Leman-Langois *Technocrime: Technology, crime and social control*. Cullompton: Willan.

Maricato, E. et al. (2013). *Cidades rebeldes: Passe Livre e as manifestações que tomaram as ruas do Brasil.* São Paulo: Boitempo: Carta Maior.

Norris, C. & Armstrong, G. (1999). *The Maximum Surveillance Society*: The Rise of CCTV. Oxford: Berg.

Pinheiro, P. S.; Izumino, E. A. e Fernandes, M. C. J. (1991). Violência fatal: conflitos policiais em São Paulo (1981-1989), *Revista USP*, (9), 95-112.

Rule, J. B. (1973). *Private Lives, Public Surveillance: Social Control in the Information Age*. London: Allen Lane.

Silva, M. K. (2014). #vemprarua: o ciclo de protestos de 2013 como expressão de um novo padrão de mobilização contestatória? Em: A. D. Cattani (org.). *#protestos: análises das ciências sociais*. Porto Alegre: Tomo Editorial.

Singer, A. (2013). Brasil, junho de 2013: classes e ideologias cruzadas. *Revista Novos Estudos*, ed. 97.

Spink, M. J. e Lima, H. (1999). Rigor e visibilidade: a explicitação dos passos da interpretação. Em M. J. Spink (org.). *Práticas discursivas e produção de sentidos no cotidiano; aproximações teóricas e metodológicas.* (pp. 93-122). São Paulo: Cortez.

Souza, M. L. de. (2008). *Fobópole: O Medo Generalizado e a Militarização da Questão Urbana.* Rio de Janeiro: Bertrand Brasil.

Tavares dos santos, J. V. e Teixeira, A. N. (2014). Atores sociais jovens nos protestos de 2013. Em A. D. Cattani (org.).# protestos: análises das ciências sociais. Porto Alegre: Tomo Editorial.

Wacquant, L. (2003). Toward a Dictatorship of the Poor? Notes on the Penalization of Poverty in Brazil, *Punishment & Society*, 5(2), 197-205.

Walby, K. T. (2005). Institutional Etnography and Surveillance Studies: An Outline For Inquiry. *Surveillance & Society*, 3(2/3), 158-172.

Wood, D. M. (2009). Situating Surveillance Studies. *Surveillance & Society*, 19, 52-61.

Žižek, S. (2013). Problemas no Paraíso. Em: E. Maricato et al. *Cidades rebeldes: Passe Livre e as manifestações que tomaram as ruas do Brasil.* São Paulo: Boitempo: Carta Maior.

EJE 9

ARTE, VIGILANCIA Y TECNOLOGÍA

CONTRALAB NA NUVEM: O LABORATÓRIO TÁTICO ANTIRREPRESSÃO COMO INICIATIVA DE RESISTÊNCIA

Resumo: O presente artigo tem como objeto oContralab- Laboratório TáticoAntirrepressão, realizado pelohacklab Nuvem, uma estação rural que abriga projetos que se encontram na intersecção entre arte e tecnologia em Visconde de Mauá (RJ). OContralabfoi idealizado no contexto das manifestações de 2013, desencadeadas pelo aumento da tarifa do transporte público em diversas grandes cidades brasileiras, que ganhou corpo às vésperas da realização de um grande evento, a Copa do Mundo. Considerando o laboratório como uma iniciativa de resistência à violência e à vigilância, principalmente policial, esse trabalho apresenta uma tentativa de entendimento das ideias e motivações mobilizadas para organização, produção e disseminação de estratégias de comunicação segura, proteção de dados e coleta de evidências em casos de abuso por parte da polícia na segunda edição, o Contralab:reboot, realizada em 2016.

Palavras-chave: Arte etecnologia, Repressão, Violência, Laboratório tático.

Contralab en Nuvem: Laboratorio Táctico Anti Represión como Iniciativa de Resistencia

Resumen: Este artículo está sobre el Contralab - laboratorio táctico anti represión en poder de hacklab Nuvem, un hacklab rural que alberga los proyectos que están en la intersección entre el arte y la tecnología en Visconde de Mauá (RJ). El Contralab fue concebido en el contexto de las manifestaciones de 2013 contra el aumento en la tarifa del transporte público en varias de las principales ciudades de Brasil, que ganó volumen a la víspera de un evento importante, la Copa del Mundo. Teniendo en cuenta el laboratorio como una iniciativa de la resistencia a la violencia y la vigilancia, principalmente la policial, este trabajo presenta un intento de entender las ideas y motivaciones movilizados para la organización, producción y difusión de estrategias de comunicación seguros, protección de datos y la recogida de pruebas en casos abuso por parte de la policía en la segunda edición, el Contralab: reboot, celebrada en 2016.

Palabras clave: Arte y tecnología, Represión, Violence, Laboratório táctico.

Contralab at Nuvem: Tactical Anti-Repression Laboratory as an Iniciative of Resistance

Abstract: This article has as its object the Contralab - Tactical Laboratory Anti-repression held by hacklab Nuvem, a rural station that houses projects that are at the intersection between art and technology in Visconde de Mauá (RJ). The Contralab was conceived in the context of the 2013 demonstrations, triggered by the increase in public transport fare in several major Brazilian cities, which gained strenght at the eve of a major event, the World Cup. Considering the laboratory as an initiative of resistance to violence and surveillance this work presents an attempt to understand the ideas and motivations mobilized for the organization, production and dissemination of secure communication strategies, data protection and collection of evidence in cases of police abuse in the second edition, the Contralab: reboot, held in 2016. The research maps the ideas and motivations based on the ideology concept from Wolf (1999) followed by a discussion guided by Malinowski's propositions (1978).

Palavras-chave: Art and technology, Repression, Violence, Tactical lab.

CAMILA MONTAGNER*

A NUVEM E O CONTRALAB

O presente trabalho mapeia as formas de resistência que encontraram espaço no Contralab:reboot, laboratório tático antirrepressão organizado pela Nuvem, estação rural que atua na intersecção entre tecnologia, ciência e arte. A pesquisa acompanha quais foram as ideias e motivações mobilizadas a partir do conceito de ideologia de Wolf (1999) e discute a partir de uma observação de campo guiada a partir das premissas de Malinowski (1978). Paralelamente a isso, o artigo também aborda como a forma de organização e disseminação do trabalho dentro do laboratório antirrepressão idealizado pela Nuvem converge para práticas do movimento software livre.

Pensada para ser um espaço autônomo que recebe projetos ligados à arte, ciência e tecnologia, a Nuvem fica em uma região turística da serra fluminense. Desde 2012, a casa promove anualmente residências de verão, que duram 30 dias nos quais os participantes se revezam de forma que a casa chega a receber até 30 pessoas no período. Nos anos de 2012 e 2013 foram realizadas também residências de inverno, com instrutores para instruir os residentes, que eram selecionados e permaneciam um mês na casa, ao final do qual faziam uma apresentação final do que foi produzido. Além dessas atividades regulares, o hacklab também realiza encontros e laboratórios eventuais.

Por meio da Lei de Inventivo à Cultura, a Nuvem, idealizada por Cinthia Mendonça e Bruno Vianna recebeu o patrocínio da Vivo Telecomunicações, integrando o programa Vivo Arte.mov durante os dois primeiros anos de atividade. A partir de 2014, com a mudança na política de patrocínios da Vivo e a dissolução do programa Vivo Arte.Mov, o projeto procura autonomia experimentando com formas alternativas de financiamento, como vaquinhas e a colaboração pontual dos participantes para cobrir despesas básicas. O desligamento de Luciana Fleishman, que tinha sido chamada para a coordenação da iniciativa, também se deu em 2014, deixando Cinthia Mendonça e Bruno Vianna como únicos responsáveis pelas atividades do hacklab. Também foi em 2014 que se deu a primeira edição do Contralab, financiada com vaquinha e divisão de custos entre participantes.

Em 2016, a Nuvem passou a ter novas fontes de financiamento, entre elas a Fundação Ford, e também passou por uma reorganização interna. A justificativa apresentada na chamada para o Interactivos?'16 é a seguinte:

> Inaugurando seu 5º ano de trabalho e diante da necessidade de atualizar-se enquanto projeto colaborativo e autogestionado, a Nuvem - Estação Rural de Arte e Tecnologia investe em parcerias eum novo formato de coordenação que se biparte em frentes de trabalho autônomas. A finalidade dessa partição é expandir o alcance das atividades, garantir objetivos específicos para cada uma das partes e realizar novas associações e colaborações.
>
> (...)
>
> Ambas as coordenações estão comprometidas com a inclusão tecnológica, assim como a valorização de saberes populares e o uso de licenças livres.[1]

A segunda edição do Contralab teve sua chamada lançada quase que simultaneamente ao anúncio da mudança na organização feito no site da Nuvem, em maio de 2016. O laboratório antirrepressão

se deu entre os dias 10 e 17 de julho de 2016, período no qual estive na Nuvem fazendo trabalho de campo. Atuei como colaboradora e, ao mesmo tempo, realizei observação participante e entrevistas com os residentes tentando deixar o mais claro possível quais eram meus objetivos ali. Os registros recolhidos foram analisados conforme as três vias descritas por Malinowski (p. 36, 1978) para alcançar o objetivo de compreender o ponto de vista dos atores observados, "a sua relação com a vida, perceber a sua relação com o seu mundo".

O CONTRALAB:REBOOT

A segunda edição do Contralab foi um evento da frente Atividades Territoriais, que atua "promovendo o acesso às tecnologias e o intercâmbio com pessoas e projetos nessa comunidade" ,[2] coordenada por Bruno Vianna. Em 2014, a Nuvem ainda não havia se reorganizado – de forma que Cinthia, que hoje coordena a frente Feminismos e Deslocamentos, teve atuação direta no primeiro laboratório, e não esteve presente no segundo. Dois convidados (que já haviam estado na Nuvem anteriormente – um deles como proponente do Contralab de 2014), cinco proponentes e dez colaboradores passaram pela casa na edição de 2016.

Os colaboradores, que seriam divididos em grupos de até três pessoas por projeto, foram aceitos conforme ordem de inscrição e poderiam participar do(s) projeto(s) que desejassem, independentemente de seus conhecimentos técnicos. Os convidados foram chamados para selecionar os proponentes entre os vinte inscritos para o Contralab:reboot e também passaram a semana na Nuvem. Embora tenham atuado como consultores em alguns momentos, a intenção era de que os projetos sofressem o mínimo de interferência possível, uma vez que se tratam de propostas de pessoas atuantes politicamente e autônomas.[3]

Como um dos proponentes não compareceu, todos os projetos acabaram com mais de três colaboradores. Também havia a possibilidade de proponentes poderem colaborar com até dois projetos. Os projetos "Se a democracia fosse nossa" e o "Diretório de ações e coletivos políticos", acabaram se fundindo, por decisão de seus proponentes. As proponentes de "Ferramentas coletivas para organização comunitária contra as violências" e "Hybris_Latinoamerica", pensaram em fazer o mesmo, mas desistiram ao longo da semana. O "Jogo do Golpe" começou a ser desenvolvido antes do início do Contralab e contou com a participação de colaboradores atuando remotamente.

PRODUÇÃO EM LABORATÓRIO

Entre convidados, colaboradores e proponentes, quatro já haviam participado de atividades realizadas pela Nuvem anteriormente como o encontro de Tecnomagia, de Agrofloresta, o EnkkontrADA e o próprio Contralab. Remanescentes de coletivos da rede internacional Indymedia, assim como representantes de casas coletivas, filiados a partido político, um ativista de direitos digitais e um ex-funcionário público federal que também é voluntário do empacotamento de

software livre Debian também estavam entre os participantes do Contralab:Reboot.

Enquanto os colaboradores são convidados a se apropriarem dos projetos com o fim de fazer dos mesmos produções coletivas, os proponentes se mostram desprendidos da questão da autoria. O reconhecimento é desejado, porém negociável em nome do potencial impacto de não restringir a circulação, uso e modificação do que foi produzido[4] (ainda que a marcação de autoria não restrinja a circulação em termos de licenças livres). Isso, em grande parte, se deve ao já citado compromisso da Nuvem com o uso de licenças livres. Uma exceção discutida pelo grupo nesse laboratório em particular seria a preservação da identidade do proponente e colaborador caso essas informações se inserissem em um escopo daquilo que deve ser mantido em segredo por razões táticas.

Assim como a Nuvem não se caracteriza pela prática política tradicional, defendendo sua posição em palanques, mas pela produção técnico-científica e artística, a maior parte de seus participantes também se coloca prioritariamente como produtores. Um dos poucos momentos de conflito durante a semana foi justamente quando uma colaboradora expressou seu desejo de que o produto do laboratório não fosse usado por um partido político. Como candidato à Câmara de Vereadores de sua cidade, um dos proponentes respondeu que sua intenção é que o resultado do seu trabalho ali pudesse ser usado por qualquer pessoa ou organização, e que ele não seria carimbado com o selo de sua legenda, que se encontra à esquerda do espectro político.

Como esse trabalho de campo faz parte de uma pesquisa de mestrado que tem como objetivo investigar as manifestações de ideias do movimento software livre na Nuvem é inevitável estabelecer algumas conexões entre o que se passou durante o laboratório antirrepressão e o meu objeto de estudo enquanto aluna regular do curso de Divulgação Científica e Cultural da Universidade Estadual de Campinas. Tomemos como referência afirmação do software livre como movimento social feita por Evangelista (2010), que identifica duas correntes políticas principais - free e open - que têm em comum a oposição às licenças proprietárias, ou seja, licenças que não garantem as liberdades de usar o software sem qualquer restrição; de ler e estudar o código-fonte; de alterar o código-fonte para produzir uma versão diferente; e, por último, o direito de fazer cópias do software e distribuí-las. Já a principal divergência entre os dois grupos é que o grupo free defende que não deve haver diferenças entre produtores e consumidores de software. Apesar dessas diferenças políticas, os dois grupos praticam um agnosticismo verbal, cuja performance facilita sua penetração em outros campos que não o da programação.

> Because the practices of F/OSS challenge economic incentive theory – assumptions that buttress intellectual property law – it works as a form of cultural critique, tacit assumptions converted to an explicit state of affairs. The moment that "any set of values, and material forms comes to be explicitly negotiable," observe Comaroff and Comaroff (1992, 29), signals "the end of its naturalized state." (COLEMAN, 2013, p. 200)

Coleman (2013, p. 196) também registra a aproximação entre seus membros e midiativistas da rede internacional de mídia independente. A ressalva feita pela colaboradora em relação ao uso do projeto, por sua vez, pode ser colocada em perspectiva na medida em que ela entra em conflito

com uma das características do software livre, a de não discriminação. A lógica de não restringir as possíveis explorações do software corresponde às "noções mais liberais de liberdade e equidade" (COLEMAN, 2013, p. 195) intrínseca às licenças livres. Vale destacar aqui que o proponente em questão delineou o seu projeto dentro do escopo de ideias que se colocam mais à esquerda do espectro político (que inclui, entre outras coisas, o seu partido), mas não pretendia impor uma restrição prévia em relação aos possíveis usos e distribuições do que seria produzido ou colocar a "assinatura" do partido no projeto.

Dois dos projetos, o "Ferramentas" e o "Jogo do Golpe", foram formulados de maneira que se conformassem a uma determinada visão política. O primeiro, voltado para casas coletivas e espaços compartilhados, busca auxiliar no combate à violência nesses ambientes. O segundo, voltado para jovens, tem como objetivo ser um board game educativo que ajuda a entender o funcionamento do senado em um contexto específico: a votação do impeachment, que aconteceria algumas semanas depois do laboratório. Apesar de ser um consenso dentro do grupo que o processo de impedimento da presidente Dilma Rousseff não foi legítimo e tinha contado com o apoio da mídia tradicional, grande parte do esforço investido no jogo foi feito para que os dois lados – pró e contra a perda de mandato – tivessem a mesma chance de vencer o jogo, com os jogadores se dividindo em igual número entre eles. O "Jogo do Golpe" acabou sendo renomeado "Efeito 55", fazendo referência ao número de senadores que foram a favor do impeachment na primeira votação, que configura o cenário inicial do jogo.

Tanto o "Hybris" quanto o "Diretório", no entanto, foram formulados de maneira que abrangessem uma diversidade maior de manifestações políticas – o primeiro como plataforma de articulação e o segundo como suporte. "Hybris" se insere no âmbito da manifestação política individual, que trabalha entre o fluxo das dinâmicas incidem sobre o sujeito e o uso do corpo como instrumento de manifestação política. O diretório tem como foco grupos que se articulam difusamente e/ou centralizam suas manifestações públicas em redes sociais, principalmente o Facebook. A ideia do diretório é oferecer uma alternativa que permita aos movimentos driblar a plataforma e sua aversão ao anonimato que exige que o usuário abra mão uma grande quantidade de dados em nome do acesso à sua base de relacionamentos – acesso esse que também é controlado de forma totalmente opaca, configurando uma assimetria e facilitando a repressão. Nesse último caso, foi discutida a possibilidade de estabelecer uma linha editorial para justificar a retirada de manifestações xenofóbicas, machistas e racistas, por exemplo. A plataforma ainda não foi ao ar.

MODOS DE PENSAR E RESISTIR NO CONTRALAB

Como a grande maioria dos participantes do Contralab:Reboot já atuava em grupos de ativistas, vindo das mais variadas linhas de atuação para estar ali como residentes temporários da Nuvem -assim como outros grupos com outros antecedentes estiveram ali antes- cabe aqui deixar claro que não se pretende com esse trabalho encaixar os participantes do laboratório em determinados modelos ou categorias já estabelecidas, sejam elas nacionais ou estrangeiras com reflexos locais. O trabalho de Wolf (1999) oferece um referencial que interessa a este trabalho no sentido em

que indica um caminho para a investigação da conexão entre ideias e poder. Esse percurso consiste em "tentar identificar os significados instrumentais, organizacionais e ideológicos que mantém os costumes e subscreve a busca por coerência" (WOLF, 1999, p. 66). O conceito de ideologia, nesse caso, diz respeito ao sentido dado às ações a partir de um conjunto de ideias, de uma chave de significação que, por sua vez, também é influenciada pelo sistema de produção de valor vigente, legitimando o que é desejável e que é indesejável na caracterização grupos e pessoas.

Os conceitos descritos aqui farão parte de um esforço que busca apontar para as expressões características do movimento software livre dentro do grupo, e não conformar o objeto a correspondências e relações para cercá-lo. A distinção entre pintura e desenho feita por Ingold (2011, p. 220) como metáfora de práticas antropológicas do século XX que buscavam compor uma figura completa e a proposta do autor - de uma aproximação entre o trabalho antropológico e o traçado que se preocupa mais com sua própria continuidade que com o arranjo geral, respectivamente - pode ser empregada para ilustrar o que se espera realizar com esse estudo. Enquanto a pintura busca a completude, o desenho manifesta em suas linhas uma história do "vir a ser", mais que uma imagem do que "é".

Apesar de cada um trazer para o Contralab motivações que perpassam sua experiência em agências individuais e coletivas para a convivência em um pequeno período, é possível reconhecer algumas das referências culturais compartilhadas que se cristalizaram durante esse breve encontro. As empresas tradicionais de mídia como a Globo e a Folha de S.Paulo eram apontadas como vilãs no sentido de que tendem a fazer uma cobertura parcial e enviesada da política, dando respaldo a ações policiais violentas e ao impeachment da presidente Dilma Rousseff – uma visão que se aproxima muito da motivação que teceu a rede internacional de midiativistas do Indymedia. Nas cartas de "movimentos sociais" do Efeito 55, por exemplo, aparecem manifestações e ações que foram retratados por outros veículos que não os convencionais, que estabelecem um equilíbrio na pontuação, tornando possível que os jogadores sorteados para tentar barrar o impeachment e seus adversários tenham iguais chances de ganhar. Além da mídia tradicional, Facebook e Google também são vistos com desconfiança, uma vez que recolhem uma grande quantidade de dados dos usuários para deles extrair informações de interesse comercial.

> Em paralelo às redes tradicionais de produção e comercialização, surgem grupos de artistas e profissionais das novas tecnologias de informação e comunicação que se organizam, às vezes à margem do próprio capitalismo, tendo em vista a criação de outros sistemas de trocas. O digital permite a criação de sistemas distribuídos de trabalho visando a construção coletiva de produtos de mesma natureza que os colocados pelo mercado tradicional. (EVANGELISTA, 2010, p. 24)

Wolf (2001, p. 395), destaca que o estudo de grupos, na maior parte dos casos, precisa levar em consideração que seus desenvolvimentos se devem a processos que se originam externamente a eles e têm um alcance que vai além deles – e assim como a cristalização dos grupos depende desses processos, eles passam a se inserir neles e afetá-los.

Retomemos aqui a referência a sistemas centralizados, como a mídia tradicional, ou ainda empresas de tecnologia que atuam com base em práticas de negócios cada vez mais comuns nas

quais "as empresas sabem mais sobre os consumidores que os consumidores sobre eles mesmos" (PALMAS, 2011, p. 349). A ideia do "Diretório", por exemplo, se delineia como uma proposta de alternativa para divulgação das ações de ativistas que sem que eles precisem fornecer dados que possam servir para alimentar essa relação assimétrica que é também vista como potencial facilitadora da repressão.

Vale lembrar que o primeiro Contralab aconteceu em 2014, um ano depois dos primeiros vazamentos de informação da Agência Nacional de Segurança (NSA) feitos pelo ex-agente da CIA Edward Snowden,[5] ou seja, momento a partir do qual a associação entre vigilância e consumo se cristalizou e se tornou conhecida.

No Brasil, ainda que a cooperação entre empresas de tecnologia e Estado não opere, pelo menos por enquanto, na mesma intensidade que a cooperação no caso norte-americano, as informações que os usuários expõem no uso cotidiano da rede para comunicação e expressão são apropriadas pelo governo (ALBUQUERQUE E PEDRO, 2013, p. 7). Outros dados, que a rede recolhe e o usuário fornece de modo privado também podem ser solicitadas por ordem judicial. A solicitação de dados já resultou em embates entre empresas e governo, levando à prisão do vice-presidente do Facebook na América Latina.[6] No entanto, os ativistas também usufruem da visibilidade proporcionada pela rede para fazer circular imagens de policiais cometendo abusos e transgressões, por exemplo. Albuquerque e Pedro (2015), em uma reflexão sobre o uso das máscaras por Black Blocks e o Anonymous, apontam para uma tensão no uso do Facebook pelos seus membros.

> A preocupação com a vigilância não é o único motivo e mesmo que ela esteja presente não será sempre um impeditivo para a exposição, uma vez que a visibilidade traz vantagens, ainda que haja algum risco. A maioria dos coletivos parece ver as vantagens nessa exposição que a Internet e uma rede social podem oferecer, tornando suas ideias públicas e mais conhecidas, ampliando, assim, suas conexões e seu poder de ação. Essa escolha, no entanto, não deixa de ser sem tensões, principalmente após as prisões de alguns indivíduos (...) (ALBUQUERQUE E PEDRO, 2015, p. 13)

As pesquisadoras destacam a possibilidade do Facebook e a internet serem usados como modo de proteção e resistência, uma vez que se permite "operar na própria visibilidade". Assim como as máscaras, que não são usadas apenas como proteção e esconderijo, mas também para descentralizar a origem da ação – que não se dá na escala do indivíduo, mas pela agência do coletivo – e dessa forma "ampliar a atuação na visibilidade", se expor mais intensamente (ALBUQUERQUE E PEDRO, 2015, p. 13). Foi cogitada a mobilização de estratégias como essa, por exemplo, na elaboração do "Diretório", que seria organizado prioritariamente em páginas para expressão de grupos de ativistas, e não de indivíduos, dos quais seria requisitado uma quantidade minimamente viável de dados. No Facebook, os usuários só podem se manifestar usando seus nomes verdadeiros, o que os torna responsabilizáveis e vigiáveis pelas forças públicas de segurança que utilizam o método de apropriação dos perfis construídos na rede.

Apesar de o neoliberaberalismo alçar os direitos individuais, se manifestar contra monopólios e a favor de um mundo livre das limitações reguladoras dos governos, a sua prevalência depende

da intervenção ativa do estado, da legislação e da exploração sem concorrentes de mercado (COLEMAN, 2013, p. 73). A partir da cooperação entre estado e corporações que se cristaliza na legislação, se faz relevante a questão levantada por Coleman (2013, p. 183) de até que ponto adquirir conhecimentos legais de maneira informal é algo útil para atores sociais que combatem esse regime.

O aconselhamento legal foi uma constante durante o Contralab:reboot, não só a partir da troca de conhecimentos sobre o texto da lei, mas também de experiências com questões dessa alçada. Participaram do laboratório tanto pessoas que se articulam ativamente em torno de questões regulatórias e direitos digitais, mas também sujeitos que já sofreram processos e ainda aqueles que procuram saber sobre a legislação para servir às suas necessidades ativistas.

A troca de conselhos legais, no entanto, não foi o único modo de atuação contra essa dinâmica entre estado e empresas de tecnologia posto em discussão durante a semana de laboratório. Talvez porque a capitalização financeira capta a realidade social mais rapidamente que outras organizações sociais, um outro tipo de resistência, mais integrada ao desenvolvimento técnico -científico, também teve lugar. O uso de habilidades técnicas para evitar que o cerceamento legal do estado sobre articulações com base na rede sufoque os movimentos que se colocam contra o regime de cooperação entre essas duas esferas de poder também foi colocado como uma possibilidade para torna-los mais resilientes. Dentro da formulação dos modos de resistência no contexto do Contralab, a vigilância foi um tema importante que motivou a mobilização de preocupações e estratégias entre os participantes.

CONSIDERAÇÕES FINAIS

Ao fazer uma breve apresentação dos sentidos atribuídos às formas de resistir encontradas no Contralab:reboot, esse trabalho buscou fazer um compilado dos modos de sentir e pensar dentro desse contexto. O registro de formas de resistência que podem ser incisivos ou não se deu em um ambiente que se inscreve na intersecção entre tecnologia, arte e ciência, a Nuvem, em um laboratório que teve sua primeira edição em 2014. Nesse mesmo ano, 23 pessoas foram presas preventivamente acusadas de violência em protestos como resultado de uma investigação fundamentada no monitoramento de telefonemas e emails entre os manifestantes.[7]

Para a identificação de manifestações bases culturais comuns em um curto período de tempo, foram traçados alguns paralelos entre grupos que se baseiam em laços sociais mais fortes como os midiativistas do Indymedia, os membros do movimento software livre e outras articulações que performam uma crítica cultural. Esse trabalho mapeou que entre os modos de resistência que encontraram espaço no Contralab:Reboot se colocam a proposição da construção de uma rede social alternativa, o tratamento do momento político de forma lúdica com objetivos educativos, a exploração das possibilidades de uso do corpo para manifestações políticas que dizem respeito à dinâmicas de poder que incidem sobre o sujeito e instrumentos de organização coletiva contra as violências. A vigilância foi identificada como uma questão que aparece na

formulação de resistências mapeadas no evento, assim como também é um tema importante dentro de outros grupos ativistas. Além disso foram traçados paralelos entre o modo de organização e disseminação do trabalho no Contralab:reboot aquelas encontradas dentro do movimento software livre.

Por fim, alguns caminhos possíveis para o aprofundamento de algumas das questões que atravessam esse trabalho seriam estudos que abordem os tensionamentos entre o desenvolvimento técnico-científico e os direitos digitais, assim como o embate entre individualismo e cooperação social dentro do contexto de resistência às atuais dinâmicas de associação entre vigilância e consumo.

NOTAS

* Mestranda em Divulgação Científica e Cultural na Universidade Estadual de Campinas (camilamontagnerfama@gmail.com)

1. http://interactivos16.info/

2. http://nuvem.tk/?coordenacoes/

3. Entrevista com Bruno Vianna – 14/07/2016

4. Entrevistas com proponentes

5. Greenwald, Glenn; MacAskill, Ewen and Poitras, Laura. Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian. Hong Kong, 11 de jun de 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance Acesso em 10 de out. de 2016.

6. Gonçalves, Matheus. O cabo de guerra entre o Facebook e a Justiça brasileira. Tecnoblog. 25 de fev de 2016. Disponível em: https://tecnoblog.net/192283/facebook-justica-brasileira-cabo-de-guerra/. Acesso em 10 de out. de 2016.

7. Ramalho, Sérgio. Relatório da polícia diz que ativistas preparavam ação com bombas para marcar final da Copa. O Globo, 21 de jul 2015. http://oglobo.globo.com/rio/relatorio-da-policia-diz-que-ativistas-preparavam-acao-com-bombas-para-marcar-final-da-copa-13323218 Acesso em 10 de out de 2016.

REFERÊNCIAS

Albuquerque, L., Pedro, R. (2015). Vigilância e visibilidade nas manifestações de 2013. *Seminários temáticos da V Reunião de Antroplogia da Ciência e da Tecnologia*. Porto Alegre, maio. Disponível em: https://ocs.ige.unicamp.br/ojs/react/article/view/1360. Acesso em 13 de out. de 2016.

Albuquerque, L., Pedro, R. (2013). Facebook como dispositivo de vigilância e visibilidade: algumas controvérsias

em questão. *Trabalho apresentado no dia 17 de outubro, no Grupo de Trabalho 9 – Tecnologia, visualidade e subjetividade.* Disponível em: http://files.dirppg.ct.utfpr.edu.br/ppgte/revistatecnologiaesociedade/revEdEspecialTE%20CS0C2013/revEdEspecialTECS0C2013_a08.pdf. Acesso em 13 de out. de 2016.

Coleman, E. (2013). *Coding freedom: The ethics and aesthetics of hacking*. Princeton: Princeton University Press.

Evangelista, R. (2010). *Traidores do movimento: política, cultura, ideologia e trabalho no software livre*. Tese (Doutorado em Antropologia Social). Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas.

Deleuze, G. (1994). Post-Scriptum das sociedades de controle. En *Conversações*. São Paulo: Editora 34.

Ingold, T. (2011). *Being Alive: Essays on Movement, Knowledge and Description*. Nova York: Routledge.

Malinowski, B. (1978). *Argonautas do pacífico ocidental: Um relato do empreendimento e da aventura dos nativos nos arquipélagos da Nova Guiné melanésia*. São Paulo: Abril Cultural.

Palmas, K. (2011). Predicting what you'll do tomorrow. *Surveillance & Society*. Vol. 8, n. 3, 338-354.

Wolf, E. (1999). *Envisioning Power*. Berkeley: University of California Press.

Wolf, E. (2001). Culture: Panacea or Problem? *American Antiquity*, Vol. 49, No. 2, 393-400.

APORTES PARA UNA ESTÉTICA DEL CONTROL

Resumen: El presente trabajo tiene como propósito el estudio de la “apropiación” sobre materiales de los discurso audiovisual construidos por los Circuitos Cerrados de Tv (C.C.TV). Es una crítica y subversión del uso original de los dispositivos de vigilancia. El concepto de vigilancia se encuentra muy presente en los inicios del videoarte y se aceleró en las últimas décadas.

Partimos de que vivimos en la “sociedades de control”, está proponen nuevas lógicas, que se sintetiza en el entramado conceptual del panoptismo y la vigilancia como consumo a partir del entretenimiento-espectáculo (pos-panóptico). El papel de la imágenes, como “big data” desde la “híper presencia de lo visible”, a partir de las tecnología de la representación automatizadas; cámaras de vigilancia, las web cam, gps, drones, construyen el punto de partida de esta investigación.

Desde el campo del arte podemos identificar casos específicos que (re)presentan el entramado de esta sociedad, desde una visión crítica, reflexiva, sobre el fenómeno de la vigilancia. Este enfoque no se limita únicamente a la capacidad práctica del modo de control, sino que esboza desde la especificidad del arte un modo de análisis del fenómeno de la vigilancia. Podemos afirmar que este modo de análisis, tiene la particularidad de desarmar del “adentro” hacia el “afuera”, las prácticas sociales de la observación, involucrando al espectador a partir de las sensaciones y los sentidos.

Las películas “Der Riese” (1982-1983) de Michael Klier, o la sinfonía urbana “Stopover in Dubai” 2011 de Chris Marker, la autobiografía de ciencia-ficción de “Faceless” de Manu Luksch y los aportes de Farocki nos dan elementos para pensar Si existe una estética de la resistencia a la vigilancia.

La fundación Rodríguez plantea la videovigilancia como género, ¿se puede reconocer una estética de control?, este análisis aportará elementos para la estética del (des)control.

Palabras claves: C.C.TV, Arte panóptico, Vanguardia, Vigilancia, Estética de control.

JUAN MANUEL ZALDUA*

Aportes para uma estética do controle

Resumo: O presente trabalho tem como propósito do estudo da "apropriação" sobre materiais dos discursos audiovisuais construidos pelos Circuitos fechados da TV (c.c..TV). É uma critica e subverção do uso original dos dispositivos de vigilancia. O conceito de vigilância se esteve constantemente presente nos inicios da videoarte e se acelerou nas ultimas décadas.

Partimos de que vivemos em uma "sociedade de controle", este propõe novas lógicas, que sintetiza em uma estrutura conceitual do panoptismo e a vigilância como consumo a partir do entretenimento-espetáculo (pos-panóptico). O papel das imagens como "big data" desde a "hiper presença do visivel", a partir das tecnologías da representação automatizada; câmera de vigilância, as web cam, gps, drones, constroem o ponto de partida dessa investigação

Desde o campo da arte podemos identificar casos específicos que (re)apresentam a estrutura desta sociedade, desde uma visão critica, reflexiva, sobre o fenômeno da vigilancia. Este enfoque não se limita únicamente na capacidade prática do modo de controle, senão que esboça desde a especificidade da arte um modo de analises do fenômeno da vigilancia. Podemos afirmar que este modo de analises, tem a particularidade de desarmar de "dentro para fora", as práticas sociais da observação, envolvendo o espectador a partir das sensações e dos sentidos.

Os filmes de "Der Riese" (1982-1983) de Michael Klier, ou a sinfonia urbana "Stopover in Dubai" 2011 de Chris Marker, a autobiografía de ciencia-ficção de "Faceless" de Manu Luksch e os aportes de Farocki nos dão elementos para pensar se existe uma estética da resistencia a vigilância.

A fundação Rodriguez plantea a video vigilância como gênero. Pode-se conhecer uma estética de controle? Esta análise aportará elementos para a estética do (des)controle.

Palavras chaves: C.C.TC, Arte panóptico, Vanguarda, Vigilancia, Estética do controle.

Contributions for an esthetic of control

Abstract: The aim of this work is to study the "appropriation" of the materials of audiovisual discourse built by the Closed TV Circuits (C.TV.C.). It is a critic and subversion of the original use of the surveillance devices. The concept of surveillance is quite present in the beginnings of videoart and it has rapidly gone in depth in the last decades.

The starting point is that we live in the "societies of control" which suggest new logics that are synthesized in the panopticism and surveillance conceptual framework as a consumable entertainment-spectacle (post-panoptic). The role of images as "big data" from the "hyper-presence of the visible", from the automatized technology of representation: surveillance cameras, webcams, GPS, drones, provide the point of departure for this research.

Situated in the art field, it is possible to identify specific cases that (re)present the framework of this society from a critic and reflexive version about the surveillance phenomenon. This perspective is not only limited up to the practical capacity of the control type, but it also outlines, from the art specificity, an analytical way on the surveillance phenomenon. We can assure that this way of analysis has the distinctive feature of deconstruct, from the "inside" to the "outside", the social practices of observation, involving the observer's feelings and senses.

The movies "Der Riese" (1982-1983) by Michael Klier, or the urban symphony "Stopover in Dubai" 2011 by Chris Marker, the science-fiction autobiography of "Faceless" by Manu Luksch, and the contributions by Farocki give us resources for thinking whether exist or not an esthetic of resistance to surveillance.

The Rodriguez Foundation sets out the video-surveillance as a genre. Is it possible to recognize an esthetic of control? This analysis will contribute elements to the esthetic of (non-)control.

Keywords: C.TV.C., Panoptic art, Avant-garde, Surveillance, Esthetic of control.

APORTES PARA UNA ESTÉTICA DE CONTROL: LAS IMÁGENES DE LA RESISTENCIA

"Tan pronto como hay una relación de poder, hay una posibilidad de resistencia[...]
No el lugar del rechazo, alma de la revuelta, foco de todas las rebeliones,
ley pura del revolucionario, sino algunas resistencias [...]
posibles, necesarias, improbables,
espontáneas, salvajes, solitarias, concertadas,
deslizantes, violentas irreductibles, prontas al compromiso,
interesadas o sacrificadas." Michel Foucault.

SUJETO DE MIRADA. EN EL MUNDO CONTEMPORÁNEO.

El arte y la tecnología siempre fueron parejas complementarias. Las prácticas de la mirada o la observación son elementos constitutivos de la disciplina estética, podemos afirmar más aún de las artes audiovisuales, ya que esta se presenta como el arte de la escucha y la mirada. Esta investigación tiene el objetivo de hacer una breve reseña histórica sobre cierto tipo de tecnología y arte, que se presentan orientadas al control, para llegar a las de nuestra época. Donde reconocemos que existe un pasaje de la mirada y la observación, un cambio de espectador, síntoma de una tipo de sociedad. Luego nos centraremos en experiencias que realizan una subversión del uso original de los dispositivos de control, desde la resistencia a estos tipos de prácticas.

Para lograr esto, necesitamos entender el rol de la mirada y al escucha en sociedad contemporánea. A fines de la época del 60 y principio del 70, se construyeron dos paradigmas, que se entendía como opuesto, hoy son complementarios. Estos dos postulados son muy recurrentes y comunes, pero fundamentales para un análisis de este tipo. Lo que Guy Debord llamó "la sociedad del espectáculo", en esta se entiende al rol de las imágenes audiovisual como sujeción y dominación sobre los espectadores (). El otro postulado no afecta directamente a las imágenes audiovisuales, sino a toda la cultura. Esta noción pertenece más al orden de la vigilancia, propuesta por Michel Foucault en "Vigilar y Castigar". Parte desde los aspectos arquitectónicos (vale aclarar que la arquitectura es un arte) de la cárcel y las relaciones que construye para hacer una analogía con las relaciones sociales, por ende la cultura, el rol de lo visible como ejercicio de poder nos permite profundizar sobre la relación con la mirada, el saber y el espectador.

El audiovisual se ve afectado por estas dos aspectos desde sus inicios, sustentada en la cultura del espectáculo que logra el asombro y a la fascinación de las ilusiones (teatro de sombras, fantasmagoria, linternas mágicas, diorama, panorámicas, entre otras), pero también la cultura de la vigilancia, por esa cuestión de la máquina que hace al mundo visible, como registro, almacenamiento y proyección, como forma de cierto tipo control desde las imágenes y los sonidos.

En relación con la estética en la misma época, el reconocimiento de la cultura visual encontrando elementos de los estudios culturales, la historia del arte, las teoría crítica, la antropología y la filosofía, que nos permiten reconocer el rol de la imagen como fundamental en nuestra cultura. Este enfoque rompe con los cánones del arte en cuanto a la autentico, el artista genio creador, el arte de elite, o el análisis de aspectos formales de las obras, para proponer pensar el rol social del arte como formador de cultura, reconociendo un arte popular, entre lo más relevante.

El psicoanalista Gérard Wajcman (2011) nos plantea que más allá de la cultura visual, el reconoce una cultura de la mirada. Este cambio de repensar las imágenes y la cultura, nos permite pensar que las imágenes audiovisuales nos miran y nos vigilan. Es en este momento de la historia, las pantallas nos miran y nos escuchan, con sus cámaras web y parlantes, o nos localizan con sus gps, o nos persiguen en el supermercado o en las calles. Ya nadie está libre de ser un objeto de

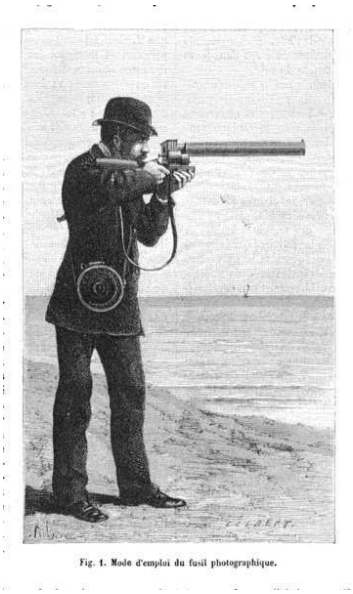
miradas del otro. El caso más significativo para entender la conformación de los sujetos de la mirada de control, es el nacimiento de un bebé. Explica Wajcama (2011), el embrión es objeto de mirada antes que sea sujeto, ya que por medio de la ecografía a las pocas semanas de vida, cuando a partir de imágenes y auriculares podemos reconocer la vida de bebé, escuchamos los latidos del corazón y nos llevamos la primer foto muy particular, que se asemeja más a infografía de uso tecnológico que a un ser humano. Allí los síntomas del embarazo se convierte en afirmaciones, las parejas comienzan a construir el cuerpo deseado del bebé. Podemos decir que tiene vida porque hay imagen, hemos vigilado a partir de la audiovisión que allí vive un bebé. Aquí subyace una afirmamos que el control provoca sensación de seguridad, nosotros nos proponemos discutir, imposible de cerrar la discusión en este trabajo, sino solo dejar en claro que esta sensación de seguridad no es puesta sobre el sujeto que lo miran sino al que mira, afirmando la relaciones de saberes que Foucault planteó a la hora del ejercicio del poder.

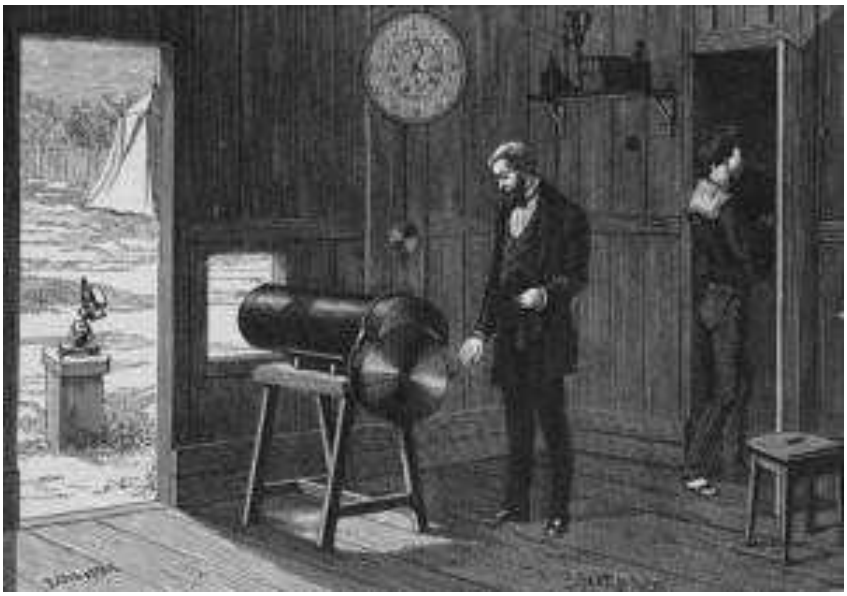
MÁQUINA DE VISIÓN, ARMAS DE DESTRUCCIÓN.

La fascinación por lograr aparatos que permitan observar y registrar el mundo o muchas veces hasta más allá de la propia visión humana (como el espacio o el interior de los seres humanos), ha provocado bastos avances tecnológicos. La dialéctica constante de que todo avance destruye otra cosa, sumado a que los mayores avances surgen en el sector armamentístico con usos militares o científicos, nos hace pensar que en sí mismo la noción de vigilancia y control son la esencia de estos avances y productos. En estas múltiples funciones que comienza a tener los artefactos se piensan desde el pasado con el fin de pensar un mundo mejor, la encrucijada del mundo mejor, se provoca por el uso de estos aparatos para mantener el estatus del sistema capitalista.

Desde los esfuerzos de los inicios de los artefactos de la visión, se ve un esfuerzo de registrar para conocer, y conocer para operar en un campo concreto. Los avances de la cronografía de Etienne-Jules Marey que partían del *revólver astronómico* de Janssen (figura 1), es posible repensar el sentido del control y la relación fisiológica de los aparatos con armas de guerra. Este revólver fotografiaba el paso de Venus delante del sol, se registran 48 imágenes sobre un disco de 25 cm de diámetro. El mismo artefacto con un par de modificaciones, pensado para captar los vuelos de los pájaros fue el *revólver fotográfico* (figura 2) o escopeta fotográfica de Marey. Este fusil consistía en registrar en una placa única las diferentes fases del movimiento. Para conseguir esto ideó un sistema que suponía fotografiar con una misma placa por separado, las distintas fases del movimiento sobre un fondo completamente negro. Este dispositivo para capturar imágenes obtenía con el disparo de su gatillo series de doce fotografías sucesivas con exposición de 1/720 de segundo, sobre un soporte circular que giraba como el tambor de un revólver, ante el cañón-objetivo.

FIGURA 1 Y 2.
El revólver astronómico de Janssen y El *revólver fotográfico de* Marey.





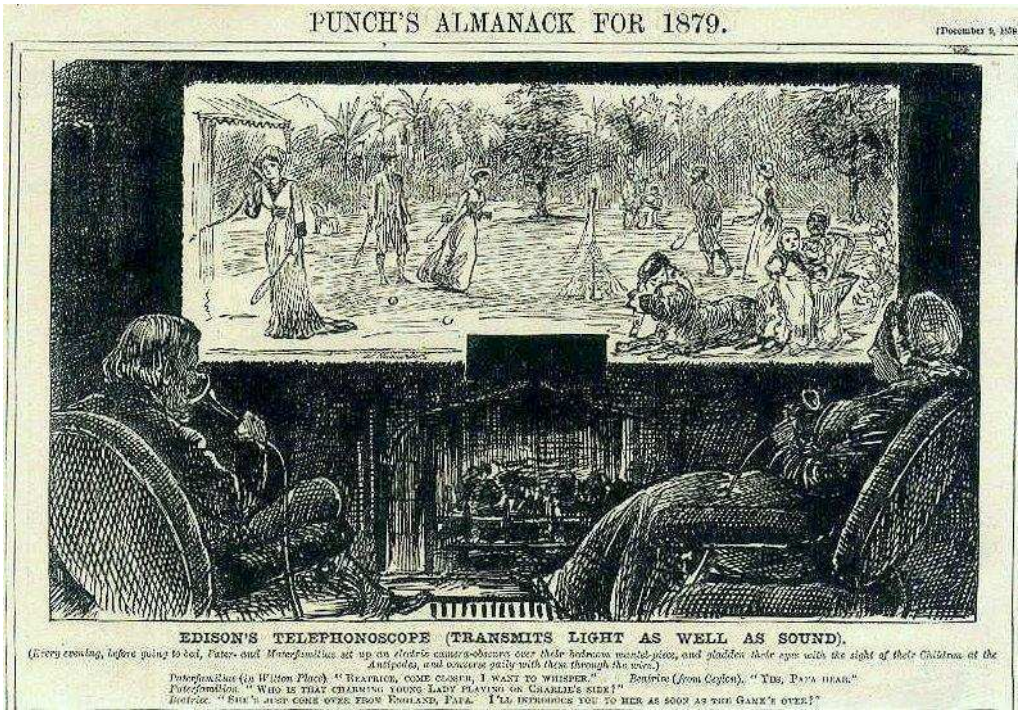
Desde estos avances claves del desarrollo científico se encuentra imágenes de cuerpo humano, anatomía, deportistas, naturaleza y campos de batallas, el discípulo e inventor Lucien Bull trabajo en el seno del ejército francés con cámaras de alta velocidad y sus equipos de detección sonora para localizar artillería enemiga en la Primer Guerra Mundial. En Alemania, un inventor con los mismos intereses sobre registros fue Ottomar Anschutz quien produjo lo que se reconoce como la primera fotografía en el campo de batalla.

Los que se proponen estos inventos es aplicar la experiencia de la observación más detallada, detenida en el tiempo con finalidades operativas, aquello que se movía, era lo que se quería control, se lograba a partir de estos instrumentos aniquilando el movimientos. Los inicios del cine se ven como continuadores de esta cultura masiva del espectáculo pero también como dimensión orientada a proveer un conocimiento a la tecno ciencia, esta doble función se encuentra en varias máquinas de la visión, por ejemplo la televisión que con el cine son inventos del siglo XIX.

La idea de los avances tecnológicos sobre la televisión es muy parecida al cine. La particularidad de este medio es que en vez de la química y la física, se usa la electricidad como forma de comunicación. El telégrafo reemplazó los sistemas de señal óptica de semáforos diseñados por Chappe para el ejército francés, convirtiéndose en la primera forma de comunicación eléctrica. El funcionamiento del mismo consta del uso de un código que se transmite por mensaje de texto codificado, como el código Morse, mediante líneas alámbricas y radiales. Las invenciones del pantèlegrafo de Giavanni Caselli continúa con esta forma de comunicación, en este caso provoca la transmisión de dibujos y palabras, que luego tuvieron lugar para uso comercial de la industria publicidad. Estos avances tratan de observar lo que está pasando en otro lugar, al mismo tiempo, una extensión de la visión a distancia, sin involucrar al cuerpo del observador. Claramente la noción del control aparece inscrita en esta práctica, tener un saber por la mirada desde observación

a distancia con una finalidad operativa, de monitoreo. En este caso la electricidad facilitaba el contacto visual "instantáneo". Un caso muy relevante y recurrente es el telefonoscopio de Thomas Alva Edison y la ilustración de George Du Maurier (figura 3), donde podemos ver una pareja de un living de una familia burguesa, frente a una pantalla que simula ser una venta, ubicada en un hogar de leña (lugar que luego ocupó el televisor). En las manos tiene unos conos que permiten intercomunicarse a través del sonido con quienes ven en la pantalla. En la pantalla una joven posee el mismo tele comunicador no se sabe si ella los ve a los sujetos del living. En esta se ve un campo de producción, podemos pensar que es un campo inglés de proyectos de té. La comunicación entre el campo y la ciudad, los burgueses controlan y monitorean sus producciones, estos nos permite pensar que la función más inmediata de la televisión fueron pensadas en el marco del monitoreo, la vigilancia y el control por medio de cámaras y pantallas.

FIGURA 3.
El Telefonoscopio de Edison.



En la segunda guerra mundial, por medio del radar con su función de basa, donde se emite un impulso de radio, que se refleja en el objetivo y se recibe típicamente en la misma posición del emisor. Profundizar esta noción de la vigilancia a distancia, construyendo máquinas de destrucción teledirigidas, poder monitorear el lanzamiento y los resultados. En 1942 La sociedad de aparatos electro-acústico y mecánic en Alemania utilizaba el radar para detectar los barcos y aviones, lo mismo hicieron los Ingleses al poco tiempo. El realizador Farocki habla que la primer imagen capturada por una cámara puesta en un proyectil es un misil de prueba HS 293 D sobre un buque cerca de Peenemünde. Las imágenes fueron transmitidas por radiofrecuencias al avión después

de que arrojaba la bomba. El misil fue guiado sobre el blanco con un control de mando muy parecido a los joystick. Esta tecnología no llegó a utilizarse en la segunda Guerra Mundial pero la miniaturización de la cámara de televisión fue un gran paso tecnológico. Este hecho se lo reconoce como el primer acercamiento al dispositivo C.C.TV circuito cerrado de televisión. (Farocki 2015) La primera comercialización de este tipo de sistemas fue en 1949 a través de la empresa Vericon, por aquel entonces, al no disponer de sistemas de grabación de imagen, la monitorización se hacía de forma continuada. Y no fue hasta 1951 que apareció el primer sistema para poder almacenar las imágenes en una cinta de vídeo VTR. En América Latina, se reconoce en México y Argentina el uso de este dispositivo en las pruebas de ensayo para lo que después fue la experiencia de la televisión, pero en estos países no se fomento el uso que luego tendría.

La transmisión de la llegada del humano a la luna a partir de este sistema, es un hecho histórico que da cuenta de la nueva época que se avecina, la comunicación con C.C.Tv conectados a satélites con alcances globales, deseo conquistado por la internet.

Para terminar con este breve recorrido histórico entre la conexión de medios, visón y control, recordaremos el inicio de las pantallas interactivas, que hoy abundan en nuestro cotidiano. Estas pantallas son posibles a través de grandes computadoras *mainframe* dedicada a uso militar. El autor Lev Manovich realiza una descripción cuando intenta hacer una genealogía de la pantalla y se sitúa en los inicios de los 90, con la categoría de *new media*, en este reconoce que el principio de las pantalla interactivas fue dispuesta para el sistema de detección aérea de las fuerzas armadas estadounidenses bautizado como Semi Autimatic Ground Envirinment. (Manovich, 2005). Esta tecnología que surge en contexto de la guerra fría desde el instituto tecnológico de Massachusetts, la corporación IBM y el pentágono, hacen que los monitoreos de la computadora tenga una doble función, la transmisión en tiempo real, y permiten cuando un objeto entraba en la zona monitoreada daré instrucciones al aparato de defensa para preparar la intercesión del intruso aéreo. Como se aprecia en la época del 60 en guerra fría hasta los inicios de los 90 se trata de un periodo de complejización de las pantallas y dispositivos de la visión, ya lo usos no son los del espectáculo, la información, el documento de lo real, o fines educativos, sin operaciones concretas en el control y de logística.

Hoy en día, el dispositivo C.C.Tv está en gran parte de los espacios públicos, centros de monitoreo urbanos unidos por un tinglado de fibra óptica generan una red de control sobre la población civil y espacio público. La cámaras son los ojos de los operadores que vigilan día a día la vida cotidiana de los ciudadanos. Podemos afirmar los postulados de Gérard Wajcman la cultura de la mirada en una época de híper presencia de lo visible, la sensación de la transparencia es el concepto soberano de la mirada (Wajcman 2011), nosotros solo nos encargamos de controlarnos, depositamos nuestros propios datos en las máquinas. Es el término Synoptico donde entra en debate una lógica inversa, todos, o un conjunto impreciso y dinámico por la impresión colectiva de tener en la mirada a uno, o unos pocos. El caso extremo es el programa de entretenimiento Gran Hermanos, producido por Endemol en 42 países.

Pero, ahora bien, nos surgen preguntas en relación al campo del arte, ¿cómo es tomada estas situaciones desde el arte? ¿Hay un arte de esta época, se encuentra un cambio en relación a la estética?.

RESISTIR DESDE LA PANTALLA Y LA IMAGEN.

Entendemos que existe un tipo de arte, que trabaja con el control, y que tiene el procedimiento de apropiarse de este tipo de imágenes audiovisuales para subvertir el uso original, logrando una crítica a la sociedad de control, estas son las obras seleccionadas. Vemos que el fenómeno de la vigilancia no se limita únicamente a la capacidad práctica del modo de control, sino que también se perciben rasgos estéticos del fenómeno de la vigilancia, que permite ser apropiados por los artistas a partir de la poética, la metáfora, para construir nuevos sentidos en relación a la vigilancia.

El primer país en tener un sistema de monitoreo de vigilancia fue Alemania, en plena guerra fría, en un contexto de espionaje favoreció a este tipo de prácticas. La película *La vida de los otros* (Henckel von Donnersmarck, 2006), da cuenta el clima de la época y la utilización de estos dispositivos de espionajes constante, se calcula que de cada 10 ciudadanos 8 eran de servicio de inteligencia o informantes. En este contexto, se produce la película *Der Riese (Michel Klier 1982-83)*, esta obra se convirtió en un hito del video arte y de la técnica del material encontrado y de apropiación. Hecha en su totalidad con un montaje de materiales del registro de las cámaras de vigilancia, iniciado un procedimiento híbrido entre las imágenes electrónicas con estrategias cinematográficas. En los títulos de la película el autor deja en claro este posicionamiento cuando escribe *Ein Film* y no *Ein video*, que para la época eran conceptos muy discutibles, hoy discusión ya saldada. Esta obra es citada por el crítico Virilio que justifica que luego de verla le surgió la necesidad de escribir *Máquinas de visión*. La película se compone en un pasaje de imágenes de la ciudad observada por las cámaras y un operador que manipula los encuadres a partir de los zoom digitales y las elecciones de las cámaras. Imágenesde video de baja resolución, en blanco y negro, con movimientos automatizados de paneos y zoom, se acompañada por una banda sonora que por momentos es ambientes y en otros fragmentos de música clásica orquestal (de Richar Strauss, Aram Khachaturi, Richard Wagner, entre otros.). Dan un clima dramático, con elementos de los *film noir,* un *thriller* o un films de espionaje, que se reafirma cuando el operador aparece en escena. Una vez visto la película es inevitable remontarse a las *sinfonías urbanas* de los años 20 y 30, y encontrar reminiscencia con *Berlín, sinfonía de una ciudad (1926)* de Walther Ruttman.

La narrativa del film no lineal, se presenta a modo de segmentos o micros relatos, no se reconoce una cadena causa efecto, sino causal, que se sustentan por la tensión, que propone mirar las imágenes de otros modo, a partir de su montaje ensaya sobre el sentido de la mirada, nuestra mirada espectador sobre un otro en pantalla, un cuerpo objeto de mirada ejerciendo el control. Es posible pensar esta metáfora como la revisión que hace Foucault sobre el panoptismo de Bentham y más aún si lo pensamos que son contemporáneos en época de difusión. Pero los aporte de Arlindo Machado en su ensayo *la cultura de la vigilancia* y su revisión con Maquinas

de vigilancia, utilizan este ejemplo para hablar de un estado pos-panóptico, entendiéndose como una experiencia bisagra entre la visión panóptica y otro tipo de visón, que no necesita un espacio determinado, arquitectónico, sino encontrar formas de control que se acerca a la idea de la malla, las redes, muchos puntos simultáneos, en diferentes capas.

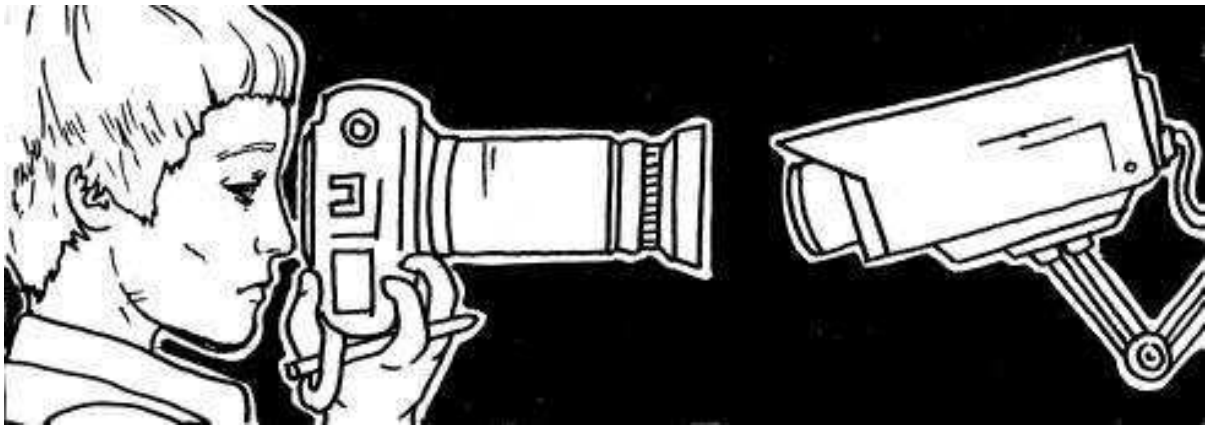
Es interesante pensar como aquí comienza un debate impulsado por los estudios de la vigilancia (surveillance Studies) como referente David Lyon, de si vivimos en un pos-panóptico o un superpanóptico electrónico. En fin las dos dan cuenta de una profundización del modelo de las relaciones de control por los avances de la tecnología.

En lo que respecta a la estética, la fundación Rodríguez toma como objeto de estudio las nuevas narrativas a partir de la vigilancia, en sus artículos reconoce este fenómeno como generadora de un género.

> (...)Las imágenes que proporcionan esas cámaras son capaces de conformar percepciones subjetivas y elucubraciones friccionantes, participando cada vez con mayor peso en el universo mediático y en el imaginario social. La videovigilancia se transforma así en un género narrativo con subgéneros que van desde el humor hasta el suspenso y el horror (Fundación Rodríguez, 2007: 65).

Entonces, se podría afirmar, que existen rasgos temáticos, enunciativos y retóricos, que permiten pensar el fenómeno como un género en sí mismo, y además nos habilitan a pensar en una estética propia, esta afirmación no la podemos resolver en este artículo, pero sí acercarnos a pensarla.

(*Imagen ilustrativa de estas nueva estética, entre la imágenes operativas y imágenes productos de las sujetos* https://zaboujojo.wordpress.com/tag/london/.)



Una película relevante es *imágenes de prisión* (Gefängnisbilde de Farocki), están realizadas por la expropiación de las imágenes de un C.C.Tv localizado en una prisión.

La película recopila imágenes de instituciones de encierro y se repiensa de cómo el cine a lo largo de su historia, ha representado a la institución carcelaria. Tiene una visión de la institución centrada en la disciplina, haciendo hincapié en los dispositivos de visibilidad, en un primer momento arquitectónicos.

Las imágenes de las cárceles en la actualidad, percibe un cambio, gracias a la implementación de un sistema electrónico de control –que va acompañado de chip en los presos, gases lacrimógenos automatizados, pantallas gráficas que individualizan la posición de los presos-. La vigilancia está en todo el espacio, atraviesa los sujetos, sus cuerpos, no en un espacio físico, volvemos aquí a la idea de la profundización del control. El director a partir de su relato, visibiliza un nuevo rol social de las imágenes, las imágenes operativas; "(…) Estas imágenes que no están hechas para entretener ni para informar (ojo/máquina, Berlin, 2001). Imágenes que no buscan simplemente reproducir algo, sino que son más bien parte de una operación". (Farocki 2015: 153).

Otra artista que se apropia de las imágenes provista por el C.C.Tv es Manu Luksch con su película *Faceless*. La autora, residente en Gran Bretaña, a partir de la ley protección de datos, que rige en este país, pudo obtener las imágenes de ellas recorriendo, en su vida cotidiana, lugares de la ciudad. Debido a la ley, los sujetos registrados, tienen acceso a una copia de la base de datos. La película tiene la cualidad de presentar todo rostro que aparece con un cuadro negro, dándole un carácter plástico muy particular, con reminiscencia a las obras plásticas de René Magritte *The son of Man* o *the lovers (Figura 5).*

FIGURA 5.
Comparación entre la plástica de "Faceless" y las pinturas de René Magritte.

La obra parte de modo documental pero por su poética y apropiación de las imágenes, narrada por voz en off a cargo de Tilda Swinton resignifica el sentido de las imágenes construye una narrativa de un mundo distópico, con rasgos del documental y la ciencia ficción, podríamos afirmar un documental surrealista. La metáfora de la sociedad de control se construye por desplazamiento en los rasgos estéticos, de puntos de vistas, cualidad de las imágenes de vídeo, movimientos de cámaras, carencia de cuadros, entre los más relevantes. Comienza

> tiempo nuevo la nueva máquina. En la existe un sueño singular. Esta es la historia de una mujer cazada por los eco de una memoria, un sueño dislocado donde el pasado deja ver el futuro. Ella no entiende las imágenes que la revisitar las que la sacan del tiempo real, fuera de la ficción de la nueva máquina, solo después ella la reconoce como nostalgia y el presentimiento (Luksch 2007. 40" del inicio).

Esta obra lleva consigo la construcción de un manifiesto sobre la realización de C.C.Tv que promueve a la producción de más obras con estas características, dando cuenta de la necesidad de trabajar estos temas desde la resistencia y la apropiación de los dispositivos.

En esta película se pone en debate los derechos de la imágenes, la identidad de las personas, dando cuenta que existe una base de datos de las actividades de los ciudadanos. Las esferas de lo público y lo privado están en discusión y re organización, para la vigilancia y el control que no posee ética, ni límite, que se encuentra en todas partes.

La reciente película *Best of luck with the wall* (Josh Begley 2016) que retrata un viaje a través de la frontera entre Estados Unidos y México, a partir de 200.000 imágenes de satélite de google earth, nos re piensa en el terreno del poder de la imágenes audiovisuales para controlar las frontera, el territorio y los cuerpos que habitan. Creemos en el potencial de esta forma de arte de apropiarse de la máquina, parafraseando a Manu Luksch

> un (...) sueño dislocado donde el pasado deja ver el futuro, la necesidad de pensar los avances del pasado para saber porque estamos en esta nueva forma de vigilancias. Continua (...) las imágenes que la revisitar las que la sacan del tiempo real, fuera de la ficción de la nueva máquina, es esta cultura de la mirada, (...) solo después ella la reconoce como nostalgia y el presentimiento. (Luksch 2007. 50" del inicio).

Entendemos que la nostalgia del presente, no puede ser el pesimismo apocalíptico, es necesario organizar la resistencia, por eso al presentimiento de los avances, la salida es por la pantalla o la imagen audiovisual, el terreno en disputa.

Por último, solo decir bien fuerte. Por una estética del descontrol.

NOTAS

* Prof. en Artes Audiovisuales. Tesista de grado en Lic. en Teoría y Critica en Artes Audiovisuales. Universidad Nacional de La Plata. Email: Zalduajuanmanuel@gmail.com

REFERENCIAS

Bauman, Z., Lyon, D. (2013). *Vigilancia Liquida*. Barcelona: Paidós.

Farocki, H. (2014). *Desconfiar de las imágenes*. Buenos Aires: Caja negra.

Foucault, M. (1975). *Vigilar y castigar*. México: Siglo Veintiuno.

Fundacion Rodriguez, Zemos98. (2007). *Panel de control. Interruptores críticos, para una sociedad vigilada*. Andalucía: Asociación Cultural, Hapaxmedia.net.

Lyon, D. (1994). *El ojo electrónico. El auge de la sociedad de la vigilancia*. Madrid: Alianza.

Machado, A. (2000). Maquina de vigilar. En *El paisaje mediático. Sobre el desafío de las poéticas tecnológicas.* pp. 289-300. Buenos Aires: Universidad de Buenos Aires. Libros del Rojas.

Manovich, L. (2005). *El lenguaje de los nuevos medios de comunicación*. Barcelona: Paidós.

Russo, E. (2016). La mirada del cine en la sociedad de control. En *Arkadin* (Nº5). Vigilancia, Found Footage y resistencia. pp. 20-36.

Wajcman, G. (2011). *El ojo absoluto*. Buenos Aires: Manantial.

PELÍCULAS

Begley, Josh (2016). Best of luck with the wall. Field of Vision.

Farocki, Harun (2001). “imágenes de prisión”. “Gefängnisbilde”.

Klier, Michel (1982-83).“Der Riese”. Alemania.

Luksch, Manu (2007). Faceless. Amour fou filmproduktion.

Henckel von Donnersmarck (2006).” La vida de los otros”. Alemana.

COMO NOS VÊ O QUE NOS OLHA?

Resumo: O objetivo deste trabalho é, ao perceber a vigilância como dispositivo de referência na arte, investigar o deslocamento dos modos de vigiar para um regime cada vez mais regido por algoritmos. Em concisa apreciação de exemplos de artistas, em especial latino-americanos, problematizamos como o crescente automatismo das imagens gradativamente dissipa a ideia antropocentrista de olhar, transformando o estatuto do observador, as relações entre visível e invisível, opacidade e transparência, bem como, os modos de prestar atenção na cultura contemporânea. Em jogo, nos parece, uma investigação sobre o reposicionamento das formas de monitoramento, cujo foco não mais reside em identificar indivíduos, mas interpretar padrões de dados, antecipar atos, intervir em tempo presente e performar comportamentos. Buscamos, enfim, questionar como obras que exploram estéticas da vigilância, ao posicionar o humano como um corpo de dados poroso ao escrutínio interpretativo dos olhares maquínicos, apontam para a transformação da nossa percepção do mundo e de nós mesmos em relação aos objetos e processos tecnológicos. Em regime clássico de vigilância, diante das câmeras, indagávamos: como vemos o que nos olha? Em regime algorítmico, cujas imagens têm se destinado progressivamente menos ao olhar humano, retorna pergunta especulativa sobre a relação observador-máquina-imagem: como nos vê o que nos olha? Obras como Retablo (2016), do uruguaio Fernando Velazquez; Zoom Pavilion (2015), do mexicano Rafael Lozano-Hemmer, Modular Solution for Corridor Installations (2009) do colombiano Andrés Burbano e 4 Walls (2000-2003) do brasileiro Lucas Bambozzi convocam as possibilidades técnicas e estéticas de sensores e câmeras regidos por uma gestão algorítmica que se organizam em tecnologias de observação antes do fato. Quais experiências espaço-temporais, perceptivas e subjetivas emergem do reordenamento entre quem vê e o que é visto no monitoramento contemporâneo?

Palavras-chave: Estéticas da vigilância, Vigilância algorítmica, Arte, Subjetividade.

ANNA BENTES*
PAULO FALTAY**

¿Cómo nos ven lo que nos mira?

Resumen: El objetivo de este trabajo es, al mirar la vigilancia como un dispositivo de referencia en el arte, investigar el desplazamiento de las formas de vigilar en un régimen cada vez más regulado por algoritmos. A partir de los ejemplos de artistas, especialmente los latinoamericanos, hablamos de cómo la creciente automatización de las imágenes disipa gradualmente la idea antropocéntrica de mirar. Eso cambia la condición del observador, las relaciones entre visible y invisible, la opacidad y la transparencia, así como las maneras de la atención en la cultura contemporánea. O sea, nosotros estamos investigando la nueva posición de las formas de control, cuya mirada ya no pasa por la identificación de los individuos, sino que por la interpretación de los patrones de datos, anticipando las acciones, interviniendo en el tiempo presente y llevar a comportamientos. Nosotros buscamos, por último, preguntar cómo obras que exploran la estética de la vigilancia, al poner el ser humano como un cuerpo de datos porosos al escrutinio interpretativo de las miradas de las máquinas, apuntan para la transformación de nuestra percepción del mundo y de nosotros mismos en relación a los objetos y procesos tecnológicos. En el régimen clásico de vigilancia, ante las cámaras, nosotros nos preguntábamos: cómo vemos lo que nos mira? En el régimen algorítmico, cuyas imágenes son progresivamente cada vez menos dirigidas para el ojo humano, podemos decir que la pregunta especulativa vuelve diferente acerca de la relación observador-máquina-image: ¿cómo nos ven lo que nos mira? Trabajos como Retablo (2016), del uruguayo Fernando Velázquez; Zoom Pavilion (2015), del mexicano Rafael Lozano-Hemmer, Modular Solution for Corridor Installations (2009), del colombiano Andrés Burbano y 4 Walls (2000-2003), del brasileño Lucas Bambozzi convocan las posibilidades técnicas y estéticas de sensores y cámaras gobernadas por una gestión algorítmica que se organizan en las tecnologías de observación antes del hecho. ¿Cuáles experiencias espacio-temporales, perceptivas y subjetivas emergen de la reordenación entre quien ve y lo que é visto en el monitoreo contemporáneo?

Palabras clave: Estética de la vigilancia, Vigilancia algorítmica, arte, Subjetividad.

How does what gazes at us see?

Abstract: This study aims to investigate how surveillance practices are increasingly characterized by a regime governed by algorithms. Starting off with a discussion of contemporary artworks, mostly by Latin America artists, that address surveillance technologies, we analyze how the increasing automatism of images gradually dissipates an anthropocentric idea of gaze. This dissipation, we defend, transforms the status of the observer, the forms of attention and the relations between visibility and invisibility and opacity and transparency in contemporary culture. These artworks highlight a shift among ways of monitoring which no longer aim at identifying individuals, but at interpreting data patterns, foreseeing actions, intervening in real time and performing behaviors. Finally, as these works explore surveillance aesthetics by means of regarding the human as a body of data and display its vulnerability to the scrutiny of the machinic gaze, we seek to discuss how they point out to a transformation in our perception of the world and of ourselves with respect to the technological objects and processes. In a classic surveillance regime, once facing the camera, we used to inquire: how do we see what look at us? In an algorithmic regime, in which images are progressively less addressed to the human gaze, returns a speculative question on the observer-machine-image relation: How does what gazes at us see? Works as Retablo (2016), by Uruguayan Fernando Velazquez; Zoom Pavilion (2015), by Mexican Rafael Lozano-Hemmer, Modular Solution for Corridor Installations (2009) by Colombian Andrés Burbano and 4 Walls (2000-2003) by Brazilian Lucas Bambozzi notably summon the technical and aesthetical possibilities of sensors and cameras which are ruled by an algorithmic management set up by before-the-fact observation technologies. What temporal, perceptive and subjective experiences emerge from the rapport between those who see and those who are seen amidst contemporary monitoring mechanisms?

Keywords: Surveillance aesthetics, Algorithmic surveillance, art, Subjectivity.

APRESENTAÇÃO

Radares com câmeras para gestão do trânsito, equipamentos de circuito interno nos cantos das paredes, o cínico alerta acompanhado de um rosto sorridente “Sorria, você está sendo filmado”, um painel reunindo as imagens destas câmeras destinado ao olhar de guardas, funcionários de lojas ou trabalhadores de portaria. Cenários e elementos de regimes de monitoramento que progressivamente se naturalizaram e se tornaram banais no cotidiano, ao mesmo tempo que,

com o crescente aumento da fauna tecnológica em todos os espaços e aspectos da vida, se mostram insuficientes para abarcar as investigações de como a vigilância contemporânea modula formas de olhar, subjetivações e socializações.

A propagação destas tecnologias se soma a uma ecologia do olhar vigilante ainda mais complexa, espraiada e vestigial efetivado pela criação e captura de rastros digitais das ações ou da presença, seja por imagens ou atos no espaço físico e/ou nas redes de comunicação. O monitoramento de e por rastros digitais é parte das promessas da computação ubíqua que, em sua mais recente fase conhecida como Internet das Coisas, se apresenta como ambiente em que microprocessadores e chips de trocas de informações vão se tornando cada vez menores, mais baratos, com eficácia expandida e encravados em objetos ordinários como relógios, bilhetes de transporte público, coleiras de animais de estimação e artigos esportivos.

Estes aparelhos deslocam temas como captura, produção e exibição de imagens, acesso e processamento de dados pessoais, conectividade e privacidade digital para uma gramática cotidiana, participando da regulação do nosso trabalho, lazer, identidades, interesses culturais, desejos e visões políticas. Produzem imagens operativas (Farocki, 2004) não necessariamente direcionadas à visão humana e que, muitas vezes, dispensam a visualidade em uma vigilância heterogênea, que envolve a agência e delegação de sentido a humanos e não-humanos, instituições estatais e/ou corporativas em uma assemblage da vigilância (Heggerty e Ericson, 2007-2010) ou vigilância distribuída (Bruno, 2013).

Definida por códigos (Lyon, 2007), a paisagem tecnológica contemporânea não somente aumenta o poder de captura em micromonitoramentos automatizados e permanentes, mas também o armazenamento e o processamento de volume exponencial de dados (Mayer-Schoenberger e Cukier, 2013, p.101), fenômeno conhecido pelo termo *Big Data*. Espaços urbanos são constituídos cada vez mais por ambientes inteligentes (*ambient intelligence*), que são mais performativos e estarão capacitados a responder ao estímulo de usuários de aparelhos tecnológicos e aos objetos em seu entorno (Thrift, 2005). Ao contrário das salas e painéis de controle clássicos, de um modelo mais próximo do panóptico (Foucault, 1987), os regimes de segurança progressivamente se assentam em câmeras e sistemas de rastreamento diversos que não necessitam da atenção e análise humana. Podem, por exemplo, focar em trajetórias consideradas suspeitas, reconhecer rostos e medidas biométricas e ler placas de carros automaticamente, com o bônus de nunca se distraírem ou adormecerem durante seu praticamente ininterrupto turno.

A comunicação M2M (*Machine to Machine*, ou máquina a máquina) e a ordem exponencial de grandeza das informações possíveis de serem coletadas pelas tecnologias digitais engendra uma nova modalidade de vigilância: a dos dados, ou *dataveillance*. Definida por Clarke (1998) como o "uso sistemático de sistemas de dados pessoais para investigar e monitorar as ações ou comunicações de uma ou mais pessoas"[1] (p. 500), a vigilância de dados é promovida através de utopia de eficiência e comodidade permitida pelos regimes de saber que estes dados promoveriam (Boyd e Crawford, 2011).

Se nas sociedades modernas, a eficácia da vigilância não estava assentada apenas em estruturas disciplinares e punitivas, mas também em ferramentas positivas de governo voltadas para a promoção de saúde, bem estar, segurança, educação e organização da vida (Foucault, 1987; 2000; 2008), as sociedades contemporâneas de controle (Deleuze, 1992) hipotecam grande parte de suas esperanças no processo de *datafication* e do governo de algoritmos, a governamentalidade algorítmica (Ziewitz, 2015). Ou seja, a crença nos supostos benefícios advindos da transformação de toda e qualquer ação em dados quantitativos através de rastreamento, muitas vezes em tempo presente, e posterior análise em modelos preditivos (Mayer-Schoenberger and Cukier, 2013).

Com efeito, a preocupação da vigilância digital diz menos respeito a um paradigma da evidência – ainda que coexista extensivamente –, isto é, apontar responsáveis por uma determinada ação já ocorrida; e mais a um paradigma do cálculo: o anseio em modular comportamentos, desejos e condutas. E como cálculo (Dubois, 2004), o real e a ação não são apenas percebidos ou representados, mas antes potencialmente criados através da gramática do código (Galloway, 2004).

Além de estar distribuída por uma variedade de tecnologias, práticas, processos, propósitos e funções, a vigilância participa de diferentes âmbitos de produção cultural e artística de nosso tempo. Incorporada no cinema, na arte, na literatura ou em formas de sociabilidade na vida online, a vigilância torna-se um elemento familiar em um campo abrangente de produção estética, participando da construção de imaginários e mobilizando circuitos de prazer e entretenimento. Ao modular nossos modos de ver e prestar atenção através de relações afetivo -sensoriais com um mundo, entendemos que um campo vasto de estéticas de vigilância está em formação e em disputa. Dupla herdeira da cinza maquinaria disciplinar e dos coloridos prazeres do espetáculo (Bruno, 2007), a vigilância contemporânea, em seu caráter multifacetado, impregna nosso campo sensível e perceptivo. Apesar de entendermos que esse amplo domínio de estéticas está, também, distribuído por diferentes esferas da cultura, aqui, concentramos o foco de nossa análise no campo da arte contemporânea.

Assim, buscamos reposicionar o questionamento dos regimes estéticos da vigilância, em que, diante das câmeras analógicas, indagávamos: como vemos o que nos olha? Em regime algorítmico, cujas imagens têm se destinado progressivamente menos ao olhar humano, retorna pergunta especulativa sobre a relação observador-máquina-imagem: como nos vê o que nos olha? Arriscamos que, com o crescente automatismo das imagens e a distribuição de funções e olhos vigilantes em cada sujeito do mundo, gradativamente é dissipada a ideia antropocentrista de olhar. Ainda, ultrapassando as retóricas do controle e da segurança e se imiscuindo em circuitos de prazer e comunicação, a governamentalidade algorítmica, opera mais uma reviravolta no olhar, reposicionando o humano como um corpo de dados porosos ao escrutínio interpretativo de outros olhos, que se organizam em tecnologias de observação antes do fato (Bogard, 1996).

Para tanto, obras como *Modular Solution for Corridor Reactive Installations* (2009) do colombiano Andrés Burbano, *4 Walls* (2000-2003) do brasileiro Lucas Bambozzi, *Level of Confidence* (2014), do mexicano Rafael Lozano-Hemmer, *Zoom Pavilion* (2015), também de Lozano-Hemmer, em

parceria com Krzysztof Wodiczko, e *Retablo* (2016), de Fernando Velázquez, nos auxiliam nas problematizações das possibilidades técnicas e estéticas de sensores e câmeras regidos por uma gestão algorítmica. Em jogo, nos parece, uma investigação sobre a transformação da nossa percepção do mundo e de nós mesmos em relação aos objetos e processos tecnológicos e o reposicionamento das formas de monitoramento, cujo foco não mais reside em identificar e interpretar indivíduos, mas processar a performatividade e o corpo humano enquanto padrões de dados, antecipar atos, intervir em tempo presente e modular comportamentos.

REGIME CLÁSSICO DE ESTÉTICAS DA VIGILÂNCIA

Segundo Anne-Marie Duguet (2009), nas décadas de 1960 e 1970, a partir de diversas formas de experimentações e articulações entre tecnologia, espaço e imagem, a vigilância torna-se um dispositivo de referência para a arte contemporânea. De acordo com a autora,

> ao mesmo tempo máquina e maquinação (no sentido de*méchanè* grega), todo dispositivo visa à produção de efeitos específicos. De início, esse "agenciamento dos efeitos de um mecanismo" é um sistema gerador que, a cada vez, estrutura a experiência sensível de maneira específica. Mais do que uma simples organização técnica, o dispositivo põe em jogo diferentes instâncias enunciadoras ou figurativas, e implica tanto situações institucionais quanto processos de percepção (DUGUET, 2009, p. 55).

Apropriações de filmagens por câmeras de vigilância, bem como seu uso nos circuitos fechados no espaço expositivo, possibilitava explorar métodos de produção da imagem e do próprio processo perceptivo do observador (Duguet, 2009). Além de remeter a outras máquinas de visão e representação, essas obras problematizam a relação do espectador com espaço, com a materialidade de seu corpo, sobre os limites entre o real e a ficção, sobre as fronteiras entre público e privado e o efeito de espetacularização das imagens. Dentre os artistas dessa geração estão: Dan Graham, Bruce Nauman, Peter Campus, Michael Snow, Andy Warhol, Bill Viola, Sophie Calle, etc.

Ao utilizar o dispositivo eletrônico, esses trabalhos exploravam alguns princípios basilares da vigilância maquínica, tais como a onividência; a ininterrupção do registro; o automatismo do olhar; a invisibilidade do observador; e a dissociação entre ver e ser visto. Era frequente a constituição de mecanismos complexos de distribuição dos olhares, em que a presença física do espectador era convocada a perambular e ensaiar situações em espaços compartilhados com outros visitantes. A partir de finas modulações de temporalidade, criava-se ambientes imersivos de questionamento do próprio ato de visão. Deste modo, a arquitetura, espelhos, câmeras, monitores, corpos e as imagens põem em jogo diferentes aspectos dos princípios da vigilância, onde os espectadores são apreendidos em um estrutura autorreflexiva em que ora são sujeito e ora objeto do olhar (Duguet, 2009).

Neste tablado fértil de experimentações, portanto, configura-se a primeira geração que incorpora a vigilância como princípio de produção estética na arte, seja como tema central ou efeito secundário nos processos de criação. No que podemos caracterizar como regime clássico de

estéticas da vigilância (Bruno; Lins, 2010), é acentuado o uso das imagens em preto e branco em baixa resolução captadas de câmeras de circuito interno e a transmissão ao vivo em instalações com circuito fechado. Prevalecia, assim, uma problemática acerca da mirada visível e inverificável das tecnologias analógicas, convocando o sujeito perceptivo a prestar atenção no próprio gesto do olhar frente a esses dispositivos. *Como vemos o que nos olha?* Quais os efeitos dessa condição de visibilidade no ato perceptivo?

REGIME CONTEMPORÂNEO DE ESTÉTICAS DA VIGILÂNCIA

Ao entrar na sala escura do *Zoom Pavilion* (Figura 1), a pessoa pode ser tragada pela miríade de imagens exibidas em todas as paredes, projeções que cobrem, ao menos, oito metros de largura por seis de altura. Na principal, há um grande painel com as filmagens de 12 câmeras de segurança exibindo os rostos das e dos visitantes do espaço expositivo. As imagens são geradas pelo conjunto de sistemas de rastreamento e tecnologias biométricas formado por nove câmeras sensíveis à radiação infravermelha, câmeras térmicas que criam imagens a partir da faixa visível do espectro eletromagnético; três *robotic zoom cameras,* aparelhos automatizados capazes de identificar padrões de pixels, de reconhecimento facial, de seguir o movimento e de aumentar o zoom em até 35 vezes; dois iluminadores de visão noturna e três computadores.

FIGURAS 1 E 2

Zoom Pavilion (Rafael Lozano-Hemmer, 2015). Fonte: http://www.lozano-hemmer.com/zoom_pavilion.php

A obra anterior de Lozano-Hemmer, *Level of Confidence*, é formada por tecnologias biométricas que empregam algoritmos usados por forças policiais e militares na identificação de pessoas suspeitas (*Eigen*, *Fishe* e *LBPH*). *Retablo*, por sua vez, investiga as possibilidades estéticas e técnicas de aparelhos que escaneiam o ambiente a sua volta em três dimensões (*scanners 3D*), especificamente o *kinect*, sensor de movimento desenvolvido pela Microsoft para seus videogames.

Esta gradual incorporação às práticas artísticas dos correntes mecanismos de produção de imagem e dispositivos de monitoramento - câmeras de vídeo inteligentes,[2] webcams, sensores, algoritmos, software de reconhecimento facial, controle biométrico, smartphones - deslocam a

experiência da vigilância instituindo novas condições de visibilidade e modalidades de imagem. Assim, formas sensíveis vislumbram a constituição de um novo repertório de códigos visuais.

Diante disso, estendemos esses deslocamentos como princípios que marcam a formação de regime contemporâneo de estéticas da vigilância (Bruno; Lins 2010), que incita e problematiza as inserções entre arte e tecnologias digitais, especialmente, os cruzamentos entre mecanismos de dispositivos de monitoramento cada vez mais regidos por algoritmos e seus efeitos nas relações sociais. Ao explorar essas modulações de técnicas e propósitos vigilantes, somam-se tipos de imagem de diferentes vetores, qualidades, cores, formas, enquadramentos, movimentos (Bruno; Lins, 2010), bem como multiplicam-se instalações interativas que trazem à luz a capacidade reativa das máquinas para os espaços expositivos.

Neste contexto, a amplificação da vigilância enquanto questão em si – seja tema ou suporte nas práticas artísticas – vem impulsionando a curiosidade, pesquisa e experimentação dentro da *Surveillance art* ou *Artveillance* (Brighenti, 2010), menos um movimento artístico propriamente dito, mas um campo de investigação sobre a influência recíproca entre vigilância e arte. Contudo, fazem parte deste campo artistas e obras bem como produções teóricas (Brighenti, 2010, Schöny, 2007; Bruno; Barreto e Szafir, 2012) e exposições organizadas sobre esse eixo temático.[3] Segundo Brighenti (2010), a produção sob domínio da *Surveillance art* pode ser interpretado como uma tentativa de lidar com questões gerais sobre os regimes de visibilidade contemporâneos.

Neste novo repertório de códigos visuais, algumas modalidades de imagem digital ganham particular relevância. Em especial, as *imagens operativas* (Farocki, 2004) integram o imaginário da vigilância em nossas sociedades e são incorporadas em trabalhos artísticos a partir de diferentes estratégias. Conceituadas e amplamente exploradas na produção fílmica do artista e cineasta Harun Farocki, tais imagens não têm como finalidade a contemplação estética, pois exercem essencialmente operações no mundo. Produzidas para cumprir funções objetivas e específicas sobretudo técnicas, elas tornam-se sensíveis e reativas ao ambiente onde atuam. Assim, o olho -máquina automatiza a percepção e a atenção de modo a identificar no visível processos que o olho humano não seria capaz de detectar para, então, poder reagir antecipando eventos futuros e direcionar uma intervenção de acordo com protocolos determinados.

Portanto, ao perceber a vigilância como dispositivo de referência nas obras que surgem das interseções entre arte e tecnologia bem como de problematizações sobre os regimes de visibilidade, nos perguntamos: que deslocamentos dos modos de olhar e do sujeito surgem em um regime de interação e comunicação cada vez mais regido por algoritmos? Parte da produção neste regime contemporâneo de estéticas da vigilância, parece constantemente se indagar sobre a opacidade e invisibilidade dos mecanismos algorítmicos, bem como sua reatividade quando interagem com corpos e informações. Assim, a pergunta retórica *Como nos vê o que nos olha?* nos parece apropriada por convergir com as lógicas desses mecanismos algorítmicos exploradas em determinadas obras.

ENDEREÇAMENTO DAS IMAGENS E CORPOS DE DADOS

As telas de exibição, em *Zoom Pavilion*, são alimentadas por tudo o que ocorre na sala em tempo presente. Em um painel lateral (Figura 3), uma compilação de imagens são geradas por câmeras que reconhecem o formato das cabeças humanas, aumentam o zoom nos rostos, criando um contorno em formato de quadrado, similar ao que aparece em celulares para conferir melhor foco em *selfies*. Acompanham os semblantes projetados informações com a hora da captura e coordenadas de posicionamento dos corpos. Na outra parede lateral (Figuras 4 e 5), uma semelhante sequência de telas, estas apresentando uma visão aérea (*bird-eye-view*) da sala e tracejada por linhas que mostram a distância de uma pessoa a outra. O vetor é operado para, a depender da maior proximidade entre as pessoas, emitir um sinal de alerta, apontando-a como suspeita.

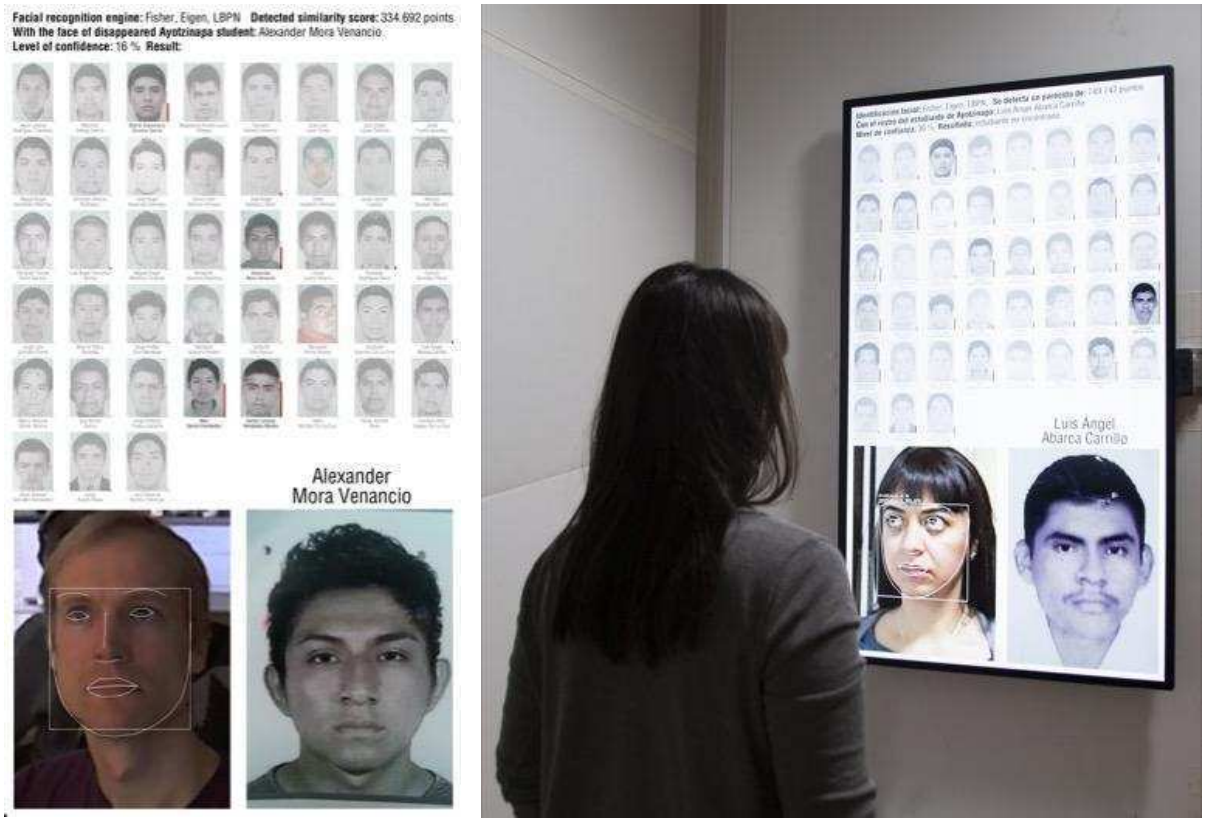
FIGURAS 3, 4 E 5

Paineis laterais de*Zoom Pavilion*. Fonte: `http://www.lozano-hemmer.com/zoom_pavilion.php`

A instalação desloca as imagens operativas para o espaço visível ocupado pelo observador, possibilitando, justamente, ao visitante poder ver como ele é visto aos olhos dessas tecnologias. Aquele que supostamente deveria ver, o espectador, é flagrado pela visão das câmeras e sensores que o capturam em uma estrutura autorreflexiva, que acumula camadas de fluxo de informação projetadas nas imagens. Entretanto, diferente dos ambientes criados por artistas nas décadas de 1960 e 1970, *Zoom Pavilion* e seus dispositivos algorítmicos são reativos e interpretativos a presença dos visitantes, modulando constantemente sua atividade de acordo com o movimento espontâneo no espaço expositivo. Deste modo, a obra faz ver a operacionalidade da visão maquínica sobre aqueles que são vistos.

Level of Confidence força o limite da própria estrutura técnica dos dispositivos de reconhecimento biométrico. Com algoritmos usados por forças policiais e militares na identificação de pessoas suspeitas (*Eigen*, *Fishe* e *LBPH*), o equipamento busca similitudes entre as e os visitantes e 43 estudantes que foram sequestrados e desapareceram em setembro de 2014, em Ayotzinapa, no México (Figuras 6 e 7). É dado, então, um nível de confiança de quão exata é a semelhança de alguma pessoa com os desaparecidos. Assim, o objetivo operacional do programa do dispositivo é, claro, destinado a fracassar em correspondência total.

FIGURAS 6 E 7:



Level of Confidence. Fonte: http://www.lozano-hemmer.com/level_of_confidence.php

A distribuição dos olhares e as trocas de visadas é ponto fundamental em *4 Walls*. Lucas Bambozzi cria uma instalação em que a personagem da projeção, através da programação algorítmica e do uso de sensores, é capaz de perceber quando é objeto do olhar do visitante e reage a essa situação. A personagem feminina encontra-se distante do espectador que a observa em uma espécie de janela (Figuras 8 e 9). À medida que o visitante se desloca pelo espaço, a figura interage com ele, mostrando um certo incômodo pelo olhar que a observa. Nesta obra, o artista inverte o olhar algoritmo da vigilância que monitora os indivíduos para o espectador que observa e vigia o algoritmo.

FIGURA 8 E 9:

Janela em*4 walls*. Fonte: http://pt.slideshare.net/lucasbambozzi/portfolio-2015-lucas-bambozzi-pdf

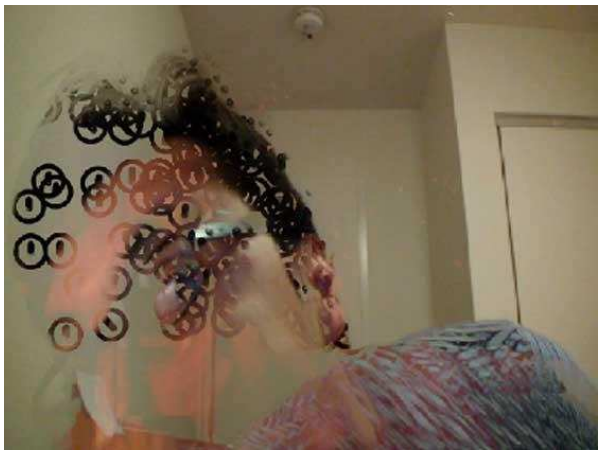
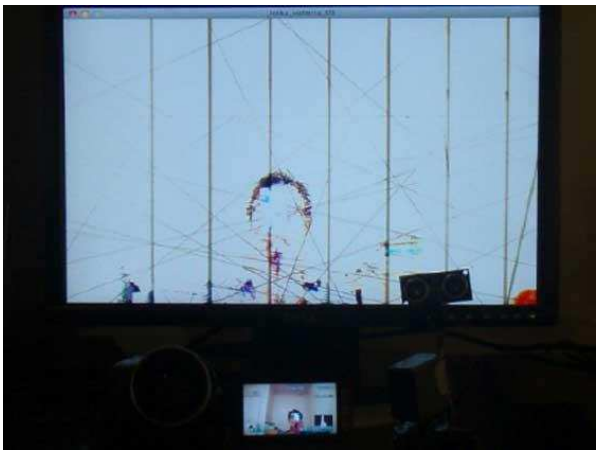
Já *Retablo* é uma instalação de arte digital com grande cotejo à pintura e escultura e que investiga o campo do retrato em tempos de imagens formadas por cálculos. O nome advém de estrutura de madeira ou de pedra colocada acima ou atrás dos altares de igrejas e que retratam, seja esculpidos ou pintados, temas sacros e figuras de santos. Em três grandes painéis (Figuras 10 e 11), a instalação interativa aposta nas experimentações luminosas e plásticas dos sensores de captura e de monitoramento para questionar, além da representação dos retratos e corpos, a condição espaço-temporal do contemporâneo, e os processos de subjetivações que, em ambiente progressivamente mais mediado por dispositivos tecnológicos, tornam-se visivelmente permeados e distribuídos entre uma constelação de agentes.

FIGURAS 10 E 11:

Visitantes em*Retablo*. Fonte: www.blogart.com

A relação entre a lógica algorítmica e a presença corpórea dos visitantes, com foco em sua dimensão motora, por sua vez, é problematizada em *Modular Solution for Corridor Reactive Installations (M S C R I)*, de Andres Burbano. Imagens capturadas por câmeras de circuito interno são misturadas através de uma ótica computacional que as projeta em uma sobreposição de quadros. Sensores de posição e distância e algoritmos pré-programados compõem as camadas de filtros que se acoplam às imagens, resultando em uma adição de máscaras pictóricas aos corpos (Figuras 11 e 12). Um mecanismo que "remete às chamadas "novas" gerações da vídeo-vigilância, que adicionam camadas algorítmicas às câmeras, tornando-as supostamente capazes de detectar padrões de movimento considerados suspeitos ou perigosos" (Bruno, Barreto e Szafir, 2012).

FIGURAS 11 E 12:

Imagens geradas em*M S C R I*. Fonte: http://www.manifesto21.com.br/ss_curatorship/burbano.html

Se para Foucault (2004), no século XIX, a humanidade adquire a dupla característica de ser sujeito e objeto do saber, a governamentalidade algorítmica apresenta novas possibilidades de associação, correlação e escrutínio de uma quantidade massiva de dados, expandindo-se das estatísticas normativas tradicionais do estabelecimento de médias. Na lógica da correlação, com a captura dos dados, os algoritmos estabelecem padrões (Kitchin, 2014), sem, entretanto, enquadrá -los em uma norma definida a priori. A comunicação *M2M* – em que a interação e os protocolos de processamento e análises de informações independe do fator humano, nos deslocando enquanto sujeitos e objetos de saber de outros agentes – contribui para a idealização de um suposto caráter objetivo e apolítico do governo de algoritmos.

Assim, obras que exploram estéticas da vigilância, como *Modular Solution for Corridor Reactive Installations (M S C R I), Zoom Pavilion, Level of Confidence, 4Walls* e *Retablo*, nos auxiliam na investigação do fenômeno que posiciona o humano como um corpo de dados poroso ao escrutínio interpretativo dos olhares maquínicos. Segundo Bruno (2013, p.58), o conhecimento advindo dos dados dos sujeitos para posterior criação de perfis computacionais, designação da ferramenta de *profiling*, "não segue processos dedutivos ou baseados em hipóteses previamente formuladas, mas sim processos indutivos baseados em algoritmos que extraem padrões e regras de correlação entre elementos", ou seja, as hipóteses são elas mesmas geradas a partir dos dados e informações que são capturados. São processos de subjetivação que não mais trabalham sobre os indivíduos, sobre os sujeitos, mas sobre as relações e associações criadas a partir da vigilância, entendida aqui em seu caráter de dispositivo de referência na arte e na cultura contemporânea.

Podemos perceber em *Zoom Pavilion* que os mecanismos de captura das imagens e de rastreamento não intentam detectar os visitantes em nível individual, bem dizer informações sobre as quais eles próprios observam e percebem sobre si, mas um saber advindo da elaboração de perfil, da relação de um indivíduo com outro(s) para a formação de um padrão. Na obra, a atenção dos mecanismos foca-se na proximidade espacial entre as pessoas. Não identificam os sujeitos que estão no espaço expositivo, mas mapeiam e registram esta distância para denunciar, apontar, o que seria um padrão considerado "suspeito". Segundo Bruno (2013), este conhecimento não revela características intrínsecas às pessoas, "mas padrões de conduta e escolha na presença de fatores que constituem uma circunstância (...) a inadequação ao perfil não representa um desvio, mas uma contingência, uma particularidade a ser, não corrigida, mas incorporada aos próprios cálculos futuros de definição do perfil" (p.160).

Essa forma de hipersegmentação, conforme Rouvroy e Berns (2015, p.44), se relaciona muito mais às ofertas comerciais e aos fluxos de capitais do que desejos e aspirações próprias de cada indivíduo. São processos de subjetivação que não mais trabalham sobre os indivíduos, sobre os sujeitos, mas sobre as relações, o que, desavisadamente poderia ser confundido com os "processos de individuação transindividual", como conceituados por Simondon (2007). Entretanto, dados que por si só não significam nada, tratados estatisticamente e negligenciadas todas as variáveis espaciais, temporais e linguísticas em direção a uma regulação supostamente objetiva, iria, ao contrário, impossibilitar todas as condições de individuações transindividuais, "(...) poupando

toda forma de "desvio" ou de "suspensão reflexiva" subjetiva entre os "estímulos" e suas "respostas-reflexo" (Rouvroy e Berns, p.44).

As obras também problematizam a cumplicidade entre os aparelhos de vigilância e as pessoas vigiadas, tematizando a ambiguidade e o caráter sedutor destas tecnologias. Vemos que a possível sujeição de ferramentas de controle e modulação de comportamentos se imiscuem em fins de prazer e exibicionismo, ao notar que, além de ter suas imagens projetadas, os visitantes de *Zoom Pavilion* também produzem imagens de si com seus celulares (Figura 13).

FIGURA 13:

Visitantes em*Zoom Pavilion*.
Fonte: http://www.lozano-hemmer.com/zoom_pavilion.php

Em *Retablo,* a ideia central reside no próprio corpo humano como um associação de dados, sendo performado nos fluxos de informação em redes sociotécnicas. Tornando possível, segundo Velázquez (2016)[4], "transformá-lo acrescentando dados inexistentes, ou simplesmente reduzi-lo ao mínimo de informação inteligível". Segundo Mol e Law (2004), todos sabemos que o corpo é tanto sujeito quanto objeto. Entretanto, os autores criticam a dicotomia estabelecida entre o corpo-objeto, elemento público, e o corpo-sujeito, esfera privada, deslocando a questão do corpo que somos e temos (*the body we are/ the body we have*) para o corpo que fazemos (*the body we do)*. Ou seja, o foco não seria no conhecimento, mas sim na ação/perfomatividade. Resumindo, na questão de cotejo foucaultiano que eles colocam: "o que *é* um corpo nas condições de possibilidade do começo do século XXI?"[5] (p. 3, grifo no original).

ENCAMINHAMENTOS FINAIS

Como vimos, a constituição de regimes estéticos de vigilância vem, mais especificamente a partir dos anos 1960 e 1970, em práticas e aparatos de visão e visualização que problematizam as

intersecções entre arte e tecnologia, deslocando os sentidos da integração de sistemas de controle e monitoramento nas relações sociais. Observamos também como a proliferação de tecnologias de vigilância vem compondo uma nova conjuntura de organização do visível cada vez mais automatizada e regida por algoritmos. Esse atual contexto, ainda em formação e disputa, torna-se referência para a pluralização de apropriações dos mecanismos e códigos visuais desses dispositivos no campo da arte.

Apesar de estarem distribuídos na gestão de diferentes setores de nossas vidas, o modo de funcionamento dos algoritmos ainda permanece bastante opaco e obscuro. Os exemplos aqui citados, pinçados de uma grande constelação de práticas e obras, exploram a criação de um repertório visual para processos tão pouco transparentes. Além disso, tais produções nos auxiliam a ver e investigar a capacidade sensitiva e reativa dessas tecnologias que, por sua vez, reposicionam o sujeito e objeto do olhar.

Enquanto o regime clássico de estéticas da vigilância colocava predominantemente em jogo a relação do corpo do observador no espaço com o dispositivo eletrônico, evidenciando e tensionando o próprio processo perceptivo, o regime contemporâneo questiona mais frontalmente o modo de percepção da máquina sobre aqueles que elas observam. Talvez, possamos arriscar, a capacidade autorreflexiva dessas obras seja um elemento de continuidade entre os dois regimes. Porém, no primeiro, a materialidade do corpo do observador é convocada a tornar-se sensível aos processos perceptivos e de produção da imagem; no segundo, acumula-se tanto a autorreflexividade do observador sobre si, quanto a percepção das máquinas sobre os espectadores. Assim, ao fazer ver a operação da lógica algorítmica, ou seus resultados, essas obras também ressignificam o estatuto do sujeito vigiado: sendo menos um corpo que vê e é visto, e mais um corpo de dados em fluxo incessante. Podemos marcar, ainda, mais um deslocamento em termos de temporalidade. Enquanto a vigilância analógica operava no interstício entre o presente e o passado, a vigilância algorítmica opera regida por um índice de devir, transformando o presente em cálculo para o futuro.

Portanto, se tais regimes estéticos tomam elementos e processos presentes em um regime de visibilidade mais amplo e os reorganizam, fazendo emergir novas camadas de visibilidade e sentido, o regime contemporâneo põe em jogo o deslocamento do estatuto do observador, da temporalidade e sentido do olhar. A lógica algorítmica transforma o observador em fluxos de dados e metadados que estão sempre sujeitos ao olhar maquínico capaz de reagir conforme seu programa. Em uma estrutura programada, e por isso limitada, os algoritmos tentam antever o sentido dos acontecimentos, e, assim, reduzir as incertezas e indeterminações, as repartições possíveis das ações e da realização de subjetivações, uma utópica e inverificável ação sem acontecimento, com "promessa de intervir proativamente sobre o que ainda não ocorreu" (Bruno, 2012). Futuro hipotecado que pretende apagar a "parte de incerteza, de virtualidade, de potencialidade radical que faz dos seres humanos processos livres para se projetar, relatar-se, tornar-se sujeitos, individuar-se, seguindo trajetórias relativamente e relacionalmente abertas" (Rouvroy e Berns, 2015).

As transformações da incorporação da gestão algorítmica das tecnologias acontece em uma temporalidade 24/7 (Crary, 2014) cujas mudanças sensíveis e perceptivas são de difícil apreensão. Assim, apostamos que os regimes estéticos podem ser uma arena fértil para observar esses processos ainda em disputa, cujas formações e trajetórias podem ser exploradas e testadas. *Como nos vê o que nos olha?* é a pergunta que permanece para despertar uma curiosidade acerca do funcionamento algorítmico e seu papel no governo das vidas.

NOTAS

* Mestranda do PPGCOM-UFRJ; annacbentes@gmail.com

** Doutorando do PPGCOM-UFRJ; pfaltay@gmail.com

1. Livre tradução para: "(...) the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".

2. Como observa Vidal Junior (2016), ao retomar o conceito de Belbachir (2010), estes aparelhos são conceituados como inteligentes porque "não apenas produzem imagens, mas também as entendem", que apesar da eficiência discursiva dessa assertiva, as noções e as relações entre inteligência, sistemas de visão e imagem e entendimento não são autoevidentes e necessitam ser mais exploradas e problematizadas.

3. Em uma lista incompleta dessas mostras, podemos apontar: *Rethorics of Surveillance: from Betham to Big Brother* (2001); *Exposed: voyerism, surveillance & the câmera* (2010); *Watching you, watching me* (2014); *Global Control and Censorship* (2015); *Big Bang Data* (2015).

4. http://www.blogart.com/Retablo

5. Livre tradução para: "(...)what *is* a body in the conditions of possibility at the beginning of the 21st century?

REFERÊNCIAS

Bogard, W. (1996). *The simulation of surveillance: hypercontrol in telematic societies*. Cambridge: Cambridge University Press.

Boyd, D., Crawford, K. (2011). Six Provocations for Big Data. In: *A Decade in Internet Time*: Symposium on the Dynamics of the Internet and Society. Simpósio conduzido em encontro no Oxford Internet Institute, Oxford, Reino Unido. Academic Press. Disponível em: http://dx.doi.org/10.2139/ssrn.1926431. Acesso em: 22/09/2015

Brighenti, A. M. (2010) Artveillance: at the crossroads of art and surveillance. *Surveillance & Society* issue on Surveillance, Performance and New Media Art, ed. John McGrath and Robert Sweeny, 7(2): 175-186.

Bruno, F. (2012). Contramanual para câmeras inteligentes: vigilância, tecnologia e percepção. *Galáxia* (São Paulo, Online), n. 24, p. 47-63.

Bruno, F. (2013) *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. 1a Edição. Porto Alegre, RS: Sulina.

Bruno, F., Barreto, P., Szafir, M. (2010). Surveillance Aesthetics in Latin America: Work in Progress. *Surveillance & Society* Vol 10(1): 83-89.

Candrall, J. (2010) *The Geospatialization of Calculative Operations*: Tracking, Sensing and Megacities. Theory, Culture & Society: 68-90. *DOI:* 10.1177/0263276410382027

Clarke, R. (2013) Introducion to dataveillance and information privacy and definition of terms. Disponível em: http://www.rogerclarke.com/DV/Intro.html. Acesso em: 18/07/2016.

Crary, J. (2012) *Técnicas do observador:* visão e modernidade no século XIX. Rio de Janeiro: Contraponto.

Crary, J. (2014) *24/7 – Capitalismo tardio e os fins do sono.* São Paulo: Cosac Naify.

Deleuze, G. (1992) *Pos-Scriptum: Sobre as sociedades de controle*. Conversações, 1972–1990. Rio de Janeiro: Ed.34.

Dubois, P. (2004) *O ato fotográfico e outros ensaios.* Campinas: Papirus.

Duguet, A. M. (2009) Dispositivos. In: Maciel, K. (org) *Transcinemas.* Rio de Janeiro, RJ: Contra Capa Livraria.

Farocki, H. (2004). *Phantom Images*. PUBLIC 29: 12-22.

Foucault, M. (1987) *Vigiar e Punir*: nascimento e prisão. Petrópolis: Vozes.

Foucault, M. (2000) *Em defesa da sociedade*: Curso no Collège de France (1975-1976), (trad. de Maria Ermantina Galvão). São Paulo: Martins Fontes.

Foucault, M. (2004) A ética do cuidado de si como prática da liberdade. In: Foucault, F. *Ditos e Escritos V. Ética, sexualidade e política*, p.264-287. Rio de Janeiro: Forense Universitária.

Foucault, M. (2008) *Segurança, Território, População*. São Paulo: Martins Fontes.

Galloway, A. R. (2004) *Protocol*: How Control Exists After Decentralization. Cambridge, Mass: MIT Press.

Haggerty, K., R. Ericson (2000) The surveillant assemblage. *British Journal of Sociology*, 51(4): 605-622.

Latour, B. (2000) Jamais fomos Modernos. Rio de Janeiro: editora 34.

Lyon, D. (2007) *Surveillance Studies* - An Overview, Cambridge, England, Polity Press.

Mayer-Schonberger, V.; Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Iorque Nova: Houghton Mifflin Harcourt.

Rouvroy, A.; Berns, T. (2015) *Governamentalidade algorítmica e perspectivas de emancipação*: o díspar como condição de individuação pela relação? Revista Eco-Pós (Online), v. 18, p. 36-56.

Schöny, R. (2007). *Within the apparatus of control. On the enduring fascination of surveillance aesthetics*. Disponível em: http://www.springerin.at/dyn/heft_text.php?textid=2127&lang=en Acesso em 15 de outubro 2016.

Thrift, N. (2005) *Knowing Capitalism*. Londres: Sage, 1a edição, 256p.

Vidal Junior, Í. F. (2016). *Invisibilidade, superficialidade e plasticidade*: três hipóteses sobre as câmeras inteligentes.

Galáxia (São Paulo. Online), v. 31, p. 156-167. Disponível em: http://dx.doi.org/10.1590/1982-2554201612427 0. Acesso em julho de 2016.

Ziewitz, M. (2015) *Governing Algorithms*: Myth, Mess, and Methods. Science, Technology & Human Values. Vol .41(1) 3-16. DOI: 10.1177/0162243915608948

CONFERENCIAS CENTRALES

Visão mediada por algoritmo: cidade, controle, tempo

FERNANDA BRUNO

Lógica económica de la vigilancia como fenómeno indisociable del capitalismo posindustrial

ENRIQUE CHAPARRO

Puede ver la conferencia haciendo click en el siguiente enlace:
https://youtu.be/rDA5wTvFkvc

Encountering and Engaging with Surveillance Culture

DAVID LYON

Closing the Circle?

JULIA POWLES

Puede ver la conferencia haciendo click en el siguiente enlace:
https://youtu.be/txS0Z7kxmpY

El poder escópico. Una mirada arqueológica de la vigilancia entre metafísica y Derecho

FABIÁN LUDUEÑA ROMANDINI

Genealogía de lo dividual

PABLO ESTEBAN RODRÍGUEZ & FERNANDA BRUNO

Pobreza, guerra civil mundial y sociedad de control

GUSTAVO CHIROLLA

Puede ver la conferencia haciendo click en el siguiente enlace:
https://youtu.be/yLkuRkTETlE

Vigilancia y esfera civil en América Latina

NELSON ARTEAGA BOTELLO

Algoritmo e vigilancia

DANILO DONEDA

Securitização, vigilância e territorialização em espaços públicos na cidade Neoliberal

RODRIGO FIRMINO

Puede ver la conferencia haciendo click en el siguiente enlace:
https://youtu.be/3QK-RSeOd5E