

## **Estado de vigilância** Surveillance state

**José Adércio Leite Sampaio**<sup>1</sup>

*Pontifícia Universidade Católica de Minas Gerais*

**Christiane Costa Assis**<sup>2</sup>

*Universidade do Estado de Minas Gerais*

**Sumário:** 1. Introdução. 2. A hipervigilância como traço da sociedade digital. 3. Vigilância e securitização. 4. A vigilância massiva em exemplos. 5. Vigilância em massa – A situação no Brasil. 6. Considerações finais. Referências.

**Reusmo:** A “revolução” da tecnologia da informação tem produzido reflexos em todos os domínios da existência humana. Prenuncia-se a emergência de uma nova sociedade do mundo digital e pós-alfabético. As ambivalências desse prenúncio e sociedade ainda não foram adequadamente compreendidas pela epistemologia, menos ainda pelo Direito. Na novidade o que se tem de certo é o velho instrumento de controle: a vigilância. A economia é cada vez mais uma economia de vigilância. O Estado, antigo protagonista da técnica de vigia, é cada vez mais também um Estado de vigilância. As comodidades da vida são o argumento da economia. A “pax social”, a promessa desse velho novo Estado. O constitucionalismo da Modernidade e suas garantias parecem uma arqueologia da política e do Direito. Em seu lugar, instaura-se um constitucionalismo da concórdia civil, em última instância, do mercado.

**Palavras-chave:** Estado de vigilância; Sociedade digital; Constitucionalismo digital; Big data; Informação.

**Abstract:** The “revolution” of information technology has had repercussions in all areas of human existence. The emergence of a new society in the digital and post-alphabetic world. The ambivalences of this foreshadowing and society have not yet been properly understood by epistemology, still less by law. In the novelty, what is certain is the old instrument of control: surveillance. The economy is increasingly an economy of surveillance. The State, the former protagonist of the watching technique, is also increasingly a State of surveillance. The comforts of life are the case for economics. The “pax social”, the promise of this old new state. The constitutionalism of Modernity and its guarantees seem like an archeology of politics and law. In their place, a constitutionalism of civil concord, ultimately, of the market, is established.

---

<sup>1</sup> Pós-Doutor em Direito pela Universidad de Castilla-La Mancha (Espanha). Doutor e Mestre em Direito pela Universidade Federal de Minas Gerais. Professor da Pós-graduação *Stricto Sensu* em Direito da Pontifícia Universidade Católica de Minas Gerais e da Escola Superior Dom Helder Câmara. Procurador da República.

<sup>2</sup> Doutoranda em Direito pela Universidade Federal de Minas Gerais. Mestre em Direito pela Pontifícia Universidade Católica de Minas Gerais. Professora da Universidade do Estado de Minas Gerais.

**Keywords:** State of surveillance; Digital society; Digital Constitutionalism; Big data; Information.

## 1. Introdução

O desenvolvimento da tecnologia de informação tem causado uma série de transformações no diversos domínios de existência e reprodução humana. As pessoas nunca estiveram tão conectadas umas com as outras, mas, paradoxalmente, tão distantes. O próprio conceito de distância pode vencer o paradoxo. Do ponto de vista virtual, nunca existiu tanta proximidade como hoje nem faltam os afetos entre os que vivem a milhares de quilômetros de distância física. Distâncias físicas evaporadas por monitores eletrônicos; afetos expressos em símbolos como “emojis” que parecem expressar um retorno à linguagem pictórica. A economia se torna cada vez um território de algoritmos e de dados, num outro tipo de mineração e de comércio que se alia à política, a velha política de Estado, que, na busca de prevenir os novos (velhos) inimigos sociais, os criminosos e o terrorismo, esforça-se por intensificar seus olhos e ouvidos. O controle do mercado e o controle social se tornam, no mundo virtual, sócios do mesmo projeto, às vezes com interesses iguais; às vezes com interesses distintos.

Parece haver uma emergência de um novo tipo de cultura, de um novo tipo de economia, de um novo tipo de sociedade, de um novo tipo de política. Se for isso verdade e não ilusão da ótica do contemporâneo que não enxerga bem o real e menos ainda o virtual, por seu cristalino cognitivo já dá sinais de catarata, os aparatos epistemológicos e as formas de lidar com a realidade, por meio dos antigos símbolos, podem estar a viver sua obsolescência. Estaria havendo o alvorecer de um tempo pós-alfabético, um tempo, por assim dizer, digital? Se, de novo, assim for, quais os efeitos para os sistemas regulatórios, especialmente o direito? Note-se que, do pouco que foi dito, no esforço de estimular à leitura do que se segue no texto, duas coisas parecem seguir a velha lógica: o mercado e o Estado. A técnica que se mencionou, a vigilância, tradicionalmente foi uma ferramenta usual de controle do Estado, tendo sido mais recentemente apropriada pelo mercado de modo central. O Estado e o capitalismo se valem da vigilância para seus fins, o controle da sociedade e o controle do mercado. Esses elementos do velho mundo invadem os novos horizontes, abrindo, de modo intencional ou de rebote, as clareiras de compreensão. É preciso tentar entender o que está acontecendo, ainda que com o cristalino embaçado.

As estruturas constitucionais e seus sistemas de garantias podem estar sendo corroídos de dentro, pelo Estado que, numa leitura termidoriana da histórica, autolimitou-se para deixar que as autonomias se pudessem expressar na esfera privada, principalmente, no mercado. E, pelo mercado, na exteriorização de uma intenção antes deliberadamente latente de moldar, controlando com o Estado, a sociedade. Os sinais são ambíguos sobre a emergência de um novo digital, teoria, práxis, teoria em práxis, práxis em teoria.

O presente artigo busca, na revisão da bibliografia sobre o tema, discutir o suposto fenômeno da “mutação digital”, identificando, mais por dedução do que por indução, talvez um vezo de uma episteme caduca, os traços que a caracterizam. O leitor notará que se faz uma associação entre o novo e o velho, esse binômio complicado, como espelho imperfeito do virtual e do analógico, do digital e do alfabético, com o antigo discurso de segurança ou “pax social”, garantido primeiramente pela vigilância. E esse realmente é o novo de novo, não no sentido da recauchutagem, a não ser do pretexto ou justificativa, mas de sua hiperpotencialização pelas tecnologias da informação. A estrutura do artigo tenta ela mesma denunciar essa dualidade ou contradição com o debate em torno do tempo digital e suas confusões de sentido, mas que tem a hipervigilância como território mais explorado, em primeiro lugar, pelo mercado, e em seguida pelo Estado. Uma sequência de sentidos e não uma cronologia de intenções. Após a discussão, tenta-

se a relevar o que se encontra expresso no debate e subentendido na prática: uma vigilância estatal massiva. O abuso da dicotomia novo/velho serve de alerta para que se tente, ao menos, tente-se imaginar em que lugar se situam as “velhas” ferramentas e os “antigos” institutos que, por meio do direito, especialmente, constitucional tentavam por freios ao Estado e ao mercado.

## **2. A hipervigilância como traço da sociedade digital**

Os indivíduos vivem sob intensa vigilância, pretensamente para sua comodidade e seus projetos de felicidade. A hipervigilância é, sobretudo, uma “datavigilância” ou, por tributo à sua cunhagem original, uma “dataveillance”<sup>3;4</sup>. Querem-se os dados que estão no histórico ou no armazenamento dos dispositivos eletrônicos, mas que também trafegam entre eles ou se alojam nas nuvens; alguns que são postos à disposição em perfis de redes sociais como ofertas (ou “dados”)<sup>5</sup> ou capturados pelos diversos instrumentos de coletas e monitoramento, visíveis ou clandestinos, legais ou não, de imagens, vídeos, sons, fichários, registros<sup>6</sup>. Dados e metadados<sup>7</sup>. A datavigilância combina o mundo dos negócios com os interesses de Estados e governos, se é que se pode separar tão claramente os dois domínios. O capitalismo, na sua ânsia e ambição de “construir” o(s) futuro(s) e dele(s) se apropriar<sup>8</sup>, migrou para o mundo digital.

As poderosas empresas “.com” e “de plataformas” estão entre as mais valiosas do mundo<sup>9;10;11</sup>. Sua mercadoria principal são exatamente os dados e seus métodos, a vigilância em seus múltiplos aspectos, coleta, armazenamento, mineração, filtragem, análise, emprego e disseminação. Uma vigilância que, todavia, provoca os indivíduos a serem vigiados, recombina-os em ajustes e agrupamentos, estimulando-os a interações e comportamentos individuais ou de manada<sup>12;13;14</sup>. O volume de dados coligidos e tratados cresce exponencial e

<sup>3</sup> CLARKE, R. A.. “Information, Technology and Dataveillance”. *Communications of the ACM*, v. 37, n. 5, 1988, p. 498-512.

<sup>4</sup> VAN DIJCK, J. “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology”. *Surveillance & Society*, v. 12, n. 2, 2014, p. 197-208.

<sup>5</sup> LEMOS, A.. “Cibercultura como Território Recombinante” em (Martins, C. D.; Silva, D. C.; Motta, R. Orgs.), *Territórios recombinares: arte e tecnologia - debates e laboratórios*, Instituto Sérgio Motta, São Paulo, 2007, p. 35-48.

<sup>6</sup> MAYER-SCHONBERGER, V.; CUKIER, K. *Big Data: A Revolution that Will Change How We Live, Work and Think*. John Murray, London, 2013, p. 150 e ss.

<sup>7</sup> VAN DIJCK, J. “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology”. *Surveillance & Society*, v. 12, n. 2, 2014, p. 205.

<sup>8</sup> SANTOS, L. G. “A informação após a virada cibernética”, em (Santos, L. G.; Kehl, M. R.; Kucinsk, B. eds), *Revolução tecnológica, internet e socialismo*, Fundação Perseu Abramo, São Paulo, 2003, p. 9-33.

<sup>9</sup> FORBES. “The World's Most Valuable Brands”, 30/4/2020. Disponível em: <<https://www.forbes.com/powerful-brands/list/>>. Acesso em: 3 mai. 2020.

<sup>10</sup> STATISTA. “Brand value of the 25 most valuable brands in 2020”, 30/4/2020. Disponível em: <<https://www.statista.com/statistics/264875/brand-value-of-the-25-most-valuable-brands/>>. Acesso em 3 mai. 2020.

<sup>11</sup> Em agosto de 2019, as dez maiores empresas de tecnologia do mundo valiam algo em torno de US\$ 5,7 trilhões. DIVINE, J., “The 10 Most Valuable Tech Companies in the World The world”, *US News*, 16/08/2019. Disponível em: <<https://money.usnews.com/investing/stock-market-news/slideshows/the-10-most-valuable-tech-companies-in-the-world>>. Acesso em: 3 mai. 2021.

<sup>12</sup> GILLESPIE, T. “The relevance of algorithms”, em (Gillespie, T.; Boczkowski, P. J.; Foot, K. A. Eds), *Media technologies: Essays on communication, materiality, and society*, The MIT Press, Cambridge, 2014, p. 167-194.

<sup>13</sup> ROUVROY, A.; BERNS, T. “Governamentalidade algorítmica e perspectivas da emancipação: o dispar como condição de individuação pela relação?”, *Revista Eco-Pós*, v. 18 (Tecnologia e Vigilância), n. 2, 2015, p. 40-41.

<sup>14</sup> As técnicas nem precisam de tanta sofisticação e estão incorporadas no cotidiano dos usuários da internet. “APIs” e “feed” permitem que conteúdos publicados pelos indivíduos

continuamente, e em altíssima velocidade, podendo ser criado em tempo real<sup>15</sup>. É o tempo dos “big data” e dos dados como “commodities” ou “um novo petróleo”, todavia, renováveis<sup>16;17</sup>, empregados e vendidos no rico e quase inesgotável mercado digital. A “Google” oferta em sua prateleira eletrônica, de modo ativo ou passivo, inúmeros serviços e produtos de multiusos, tanto no ambiente “online”, quanto “offline”, sendo provavelmente a maior exploradora e tratadora de informações obtidas na rede mundial de computadores<sup>18</sup>. Há um bilionário mercado de “intermediários de dados” ou “data brokers”, como a Acxiom (LiveRamp), a CoreLogic, a Datalogix, a Epsilon e a Experian (e seu braço no Brasil, a Serasa

---

sejam coletados automaticamente. Programas como “Radian6”, “Scup” e “Brandwatch” monitoram, por filtros de palavras ou indexadores, os conteúdos públicos na web. O “Klout PeerIndex” e similares medem o grau de influência de perfis, podendo orientar tanto negócios como a política, o “engajamento” e a perseguição. SILVA, T. “Web 2.0, Vigilância e Monitoramento: entre funções pós-massivas e classificação social”, Congresso Luso Afro Brasileiro de Ciências Sociais, Salvador, 2011. Disponível em: <<https://www.slideshare.net/tarushijio/web-20-vigilancia-e-monitoramento-entre-funcoes-posmassivas-e-classificacao-social-9661816>>

<sup>15</sup> O volume de dados digitais duplica-se a cada dois anos, o que pode ser incrementado ainda mais com novos sistemas de armazenamento “International Data Corporation (IDC)”. SAMPAIO, A. C. *Data brokers: um novo modelo de negócios baseado em vigilância de dados*, Dissertação de Mestrado. Campinas: Unicamp, 2017. Disponível em: <[http://repositorio.unicamp.br/bitstream/REPOSIP/322483/1/Sampaio\\_AliceCastaldi\\_M.pdf](http://repositorio.unicamp.br/bitstream/REPOSIP/322483/1/Sampaio_AliceCastaldi_M.pdf)>. Acesso em 20 abr. 2021, p. 22.

<sup>16</sup> HIRSCH, D. D., “The glass house effect: Big Data, the new oil, and the power of analogy”. *Maine La Review*, v. 66, 2013, p. 373-395.

<sup>17</sup> Os big data são caracterizados ainda pela (a) diversidade, a incluir os ditos dados “estruturados”, disponíveis ao armazenamento; os “semiestruturados”, como os “sms”; e “não estruturados” ou “sujos”, na pluralidade de arquivos de texto, de áudios, imagem e vídeos coletados; (b) exaustividade em seu alcance, tanto em sentido objetivo – dos dados em si –, quanto subjetivamente – dos seus produtores, buscando capturar populações ou sistemas inteiros; (c) refinabilidade de seu conteúdo –, em busca de categorizações e individualizações; (d) relacionabilidade das informações, assim, obtidas, a envolver, prévia ou posteriormente, nexos ou relações entre os perfis e dados, gerando novas e mais refinadas associações. As técnicas de “perfilização” (“profiling”) e de “mineração” (“mining”) conseguem extrair informes e correlações não triviais, em geral, desconhecidas ou implícitas, dotados de capacidade de prever em bases probabilísticas ou mesmo estimular condutas e acontecimentos; (e) extensionalidade de seus propósitos, proporcionada pela capacidade de adaptação a novas ou incidentes demandas e a inclusão de novos domínios; e (f) escalabilidade ou exponenciabilidade de sua produção. FRAWLEY, W. J.; PIATETSKY-SHAPIO, G.; MATHEUS, C. J., “Knowledge discovery in databases: an overview”, *AAAI Magazine*, Palo Alto, v. 13, n. 3, 1992, p. 57-70; BOUNSAYTHIP, C.; RINTA-RUNSALA, E., “Overview of data mining for customer behavior modeling”, *VTT Information Technology Research Report*, v. 1, 2001, p. 1-53; RUBINSTEIN, I. S.; LEE, R. D.; SCHWARTZ, P. M., “Data mining and Internet profiling: Emerging regulatory and technological approaches”, *University of Chicago Law Review*, v. 75, 2008, p. 261-185; BRUNO, F., “Rastrear, classificar, performar”, *Ciência e cultura*, São Paulo, v. 68, n. 1, 2016, p. 34-38; MAYER-SCHONBERGER, V.; CUKIER, K. *Big Data: A Revolution that Will Change How We Live, Work and Think*. John Murray, London, 2013, p. 19 e ss.; KITCHIN, R., “Big Data, new epistemologies and paradigm shifts”, *Big Data & Society*, [S.l.], 2014, p. 1-22. Disponível em: <<http://bds.sagepub.com/content/1/1/2053951714528481>>. Acesso em: 1º jul. 2016; SAMPAIO, A. C. *Data brokers: um novo modelo de negócios baseado em vigilância de dados*, Dissertação de Mestrado. Campinas: Unicamp, 2017. Disponível em: <[http://repositorio.unicamp.br/bitstream/REPOSIP/322483/1/Sampaio\\_AliceCastaldi\\_M.pdf](http://repositorio.unicamp.br/bitstream/REPOSIP/322483/1/Sampaio_AliceCastaldi_M.pdf)>. Acesso em 20 abr. 2021, p. 24.

<sup>18</sup> ZUBOFF, S., “Big other: surveillance capitalism and the prospects of an information civilization”, *Journal of Information Technology*, v. 30, n. 1, 2015, p. 75-89. Disponível em: <<http://link.springer.com/article/10.1057/jit.2015.5>>. Acesso em: 25 abr. 2021.

Experian), em que se negocia uma gigantesca base de dados coligida da internet e de fontes secundárias, com ou sem o conhecimento dos usuários e titulares<sup>19; 20; 21</sup>.

O Estado também possui e desenvolve seu aparato tecnológico, de modo a capturar, tratar e usar os "big data", procurando imprimir a seu trabalho a desenvoltura das empresas privadas, embora seja mais comum buscar com elas a cooperação, em vez da competição. As empresas a ela se submetem por pressão ou conveniência<sup>22; 23; 24</sup>. A "National Security Agency – NSA" estadunidense, por exemplo, tem estreita relação com diversas delas, incluindo a AT&T, Google, Yahoo e Microsoft<sup>25; 26; 27</sup>. Vê-se no quadro dessa combinação que o mundo da "dataficação" é um território de controle e fora de controle. A assimetria de informação que domina nesse mundo transfere o poder dos titulares dos dados para os controladores, privados e públicos<sup>28; 29</sup>. Capitalismo e vigilância, Estado e mercado se autodefinem

<sup>19</sup> RODERICK, L., "Discipline and power in the digital age: The case of the US consumer data broker industry", *Critical Sociology*, v. 40, n. 5, 2014, p. 729-746.

<sup>20</sup> ZUBOFF, S., *Google as a Fortune Teller: the secrets of surveillance capitalism*. *Frankfurter Allgemeine*, 2016. Disponível em: <<http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>>. Acesso em: 12 mar. 2020.

<sup>21</sup> Segundo a própria Acxiom, ele teria informações de cerca de 10% da população mundial. Em 2010, ela teria adquirido a brasileira "GoDigital". Essas intermediárias violam direitos e podem trazer sérios riscos à democracia. A interferência da Cambridge Analytica nas eleições presidenciais dos Estados Unidos e no "Brexit" britânico só foi possível pelos dados de que dispunha. De acordo com ela mesma, havia em seus arquivos os perfis psicológicos de 220 milhões de cidadãos norte-americanos. DOMENICO, T., *Big Data and the Computable Society: Algorithms and People in the Digital World*, World Scientific, New Jersey, 2019, p. 59; BUSINESSWIRE, *Acxiom Expands into South America with Acquisition of GoDigital*, 12/05/2010. Disponível em:

<<https://www.businesswire.com/news/home/20100512006274/en/Acxiom-Expands-South-America-Acquisition-GoDigital>>. Acesso em: 11 abr. 2021; KRISHNAN V, G., "Aadhaar in the hand of spies Big Data, global surveillance state and the identity project", *Fountain Ink Magazine*, 03/06/2017. Disponível em: <<https://fountainink.in/reportage/aadhaar-in-the-hand-of-spies->>. Acesso em: 11 mar. 2021; WARD, K., "Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting", *Journal of media ethics*, v. 33, n. 3, 2018, p. 133-148.

<sup>22</sup> SUSKIND, R., *One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11*, Simon and Schuster, New York, 2006, p. 35.

<sup>23</sup> MICHAELS, J. D. "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror", *California Law Review*, v. 96, 2008, p. 914-915.

<sup>24</sup> A atitude das empresas de plataformas em relação aos órgãos estatais é ambivalente. Quando lhes convém, requerem adoção de políticas públicas e leis. Outras vezes, queixam-se do excesso de regulamentação, reivindicando a efetividade da autorregulação. BROWN, B.; CHUI, M.; MANYIKA, J., "Are you ready for the era of 'big data'?", *Trend Report McKinsey Global Institute*, 2011. Disponível em: <<https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/are-you-ready-for-the-era-of-big-data#>>. Acesso em: 11 fev. 2021; SCHMIDT, E.; COHEN, J., *The New Digital Age. Reshaping the Future of People, Nations and Business*, Knopf, New York, 2013; VAN DIJCK, J., "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology". *Surveillance & Society*, v. 12, n. 2, 2014, p. 205.

<sup>25</sup> BAGLEY, A. W., "Don't be evil: The Fourth Amendment in the age of Google, national security, and digital papers and effects", *Albany Law Journal of Science & Technology*, v. 21, 2011, p. 153-191.

<sup>26</sup> KOSCIEJEW, M., "The Individual and Big Data", *Felicitier*, v. 59, n. 6, 2013, p. 32-35, Disponível em: <<https://www.highbeam.com/doc/1P3-3158119951.html>>. Acesso em: 15 mar 2020.

<sup>27</sup> VAN DIJCK, J., "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology", *Surveillance & Society*, v. 12, n. 2, 2014, p. 205-206.

<sup>28</sup> SCHNEIER, B., "Metadata = Surveillance", *IEEE Security & Privacy*, v. 12, n. 12, 2014, p. 84. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6798571>>. Acesso em: 20 abr. 2020.

<sup>29</sup> ZUBOFF, S., "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, v. 30, n. 1, 2015, p. 75-89. Disponível em:

no ambiente de uma cultura que, epistêmica e praticamente, promove por diversos giros, sendo também por eles promovidos. O “giro matemático” ou “numérico”, a contagiar com racionalidade matemática a visão de mundo e as ciências sociais, a lógica, a filosofia da linguagem<sup>30</sup>, e o próprio direito<sup>31</sup>. Ou o correlato “giro computacional”, especialmente das humanidade, seduzidas pelas técnicas e metodologias da ciência da computação, a valer-se da multiplicidade de fontes e dados, seu tratamento, sua mineração e seu gerenciamento, para entender-se a si e ao mundo, numa imbricada “datificação” do saber e da cultura<sup>32</sup>. Além de um “giro pós-humano”, que abandona a ilusão da descontinuidade do humano com o seu meio (em seu viés ecocêntrico)<sup>33;34;35;36</sup>, e com as máquinas que fabrica (viés cibernético e transhumanista)<sup>37;38</sup>.

O “giro normogênico” tem moldado os sistemas regulatórios em direção de uma diversidade de fontes supra e infraestatais, caracterizadas por normativas fluidas, tanto estatais, quanto decorrentes de autorregulações privadas, na maioria dos casos, dominadas pela lógica de indicadores econométricos de eficiência<sup>39</sup>. A Constituição jurídico-política há de ser, nesse ambiente, um ordenamento polimorfo, a resultar mais dos experimentos sociais e do sentido da frustração de validade (ou de vigência) de expectativas de direitos, mesmo, fundamentais<sup>40</sup>. Seu papel seria ordenar o quanto possível essa “governança mista” público-privada<sup>41;42</sup>, sendo, paradoxalmente, dela emergida ou, menos paradoxal, a ela se adaptando continuamente, por ser, ao fim, resultado de “constituições civis”<sup>43</sup>. É dizer que,

---

<<http://link.springer.com/article/10.1057/jit.2015.5>>. Acesso em: 25 abr. 2021, p. 73; p. 83 e ss.

<sup>30</sup> BOCHNER, S., “Mathematical reflections”, *The American Mathematical Monthly*, v. 81, n. 8, 1974, p. 827-852.

<sup>31</sup> AMARILES, D. R. “The mathematical turn: l’indicateur Rule of Law dans la politique de développement de la Banque Mondiale”, en (Fryman, B.; Van Waeyenberge, A. Dir.). *Gouverner par les standards et les indicateurs: de Hume au rankings*, Bruylant, Bruxelles, 2018, p. 193-234.

<sup>32</sup> HALL, G., “Towards a post-digital humanities: cultural analytics and the computational turn to data-driven scholarship”, *American Literature*, v. 85, n. 4, 2013, p. 781-809.

<sup>33</sup> CHAGANI, F., “Critical political ecology and the seductions of posthumanism”, *Journal of Political Ecology*, v. 21, n. 1, 2014, p. 424-436.

<sup>34</sup> BRAIDOTTI, R., “Posthuman critical theory”, en (Banerji, D.; Paranjape, M. R. Eds). *Critical posthumanism and planetary futures*, Springer, New Delhi; San Francisco, 2016, p. 13-32.

<sup>35</sup> CHAGANI, F., “Critical political ecology and the seductions of posthumanism”, *Journal of Political Ecology*, v. 21, n. 1, 2014, p. 424-436.

<sup>36</sup> BRAIDOTTI, R., “Posthuman critical theory”, en (Banerji, D.; Paranjape, M. R. Eds). *Critical posthumanism and planetary futures*, Springer, New Delhi; San Francisco, 2016, p. 13-32.

<sup>37</sup> MAZLISH, B., *The Fourth Discontinuity The Co-Evolution of Humans and Machines*, Yale University Press, New Haven, 1995.

<sup>38</sup> HUXLEY, J., “Transhumanism”, *Ethics in Progress*, v. 6, n. 1, 2015, p. 12-16; JAUVERT, V. “Cooment la France écoute (aussi) le monde”, *L’Obs*, juillet 2015. Disponível em: <<https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html>>. Acesso em 14 abr. 2020.

<sup>39</sup> Há quem chame a essa reviravolta de “giro empresarial” ou “do governo à governança”. MORAIS, J. L. B., “O fim da geografia institucional do estado. A “crise” do estado de direito”, en “Oliveira, C. M. Org), *Novos direitos: a interdisciplinaridade do direito na sociedade contemporânea*, CPOI/UFSCar, São Carlos, 2017, p. 21.

<sup>40</sup> TEUBNER, G., *Fragmentos constitucionais: constitucionalismo social na globalização*, Saraiva, São Paulo, 2016, p. 231.

<sup>41</sup> FITZGERALD, B., “Software as discourse? A constitutionalism for information society”, *Alternative Law Journal*, v. 24, n. 3, 1999, p. 144-149.

<sup>42</sup> SUZOR, N. P., *Digital constitutionalism and the role of the rule of law in the governance of virtual communities*. PhD Thesis, Queensland University of Technology, 2010. Disponível em: <<https://eprints.qut.edu.au/37636/>>. Acesso em: 20 mar. 2020.

<sup>43</sup> TEUBNER, G., “Societal Constitutionalism; Alternatives to State-Centred Constitutional Theory?” en (Joeges, C.; Sand, I. J.; Teubner, G. Eds.), *Transnational Governance and*

mesmo com ideias remanescentes do “velho” constitucionalismo de Estado, não inteiramente aceitas nem renunciáveis<sup>44;45</sup>, guias da arqueologia alfabético-jurídica, a “constituição digital” seria mais produto da “maieutica” social de normogênese ou do confronto ou das sínteses de regulação dos diversos segmentos da sociedade<sup>46;47</sup>. Tudo a somar-se (e, talvez, resumir-se) num “giro digital”, a compreender-se como uma “ratio” e mente pós-analógicas e mesmo pós-alfabéticas<sup>48;49</sup>. A tecnologia e cultura do hipertexto<sup>50;51</sup> produziram uma ruptura que se move a tornar obsoletas a mente alfabética e as ferramentas que a modernidade construiu para tentar conhecer, ordenar e mesmo comandar o mundo<sup>52</sup>.

A queda da razão alfabética teria tornado o mundo ilegível ou incompreensível, criando um caos cognitivo e de discernimento sobre a verdade, a correção e a estética. O direito e sua arquitetura institucional e retórica não acharam ainda seu lugar<sup>53</sup>. Não se sabe se em decorrência da transição ainda entre o analógico pleno e o digital completo<sup>54</sup>, certo é que foram aumentadas as incertezas e os riscos<sup>55</sup>, gerando um campo propício ao discurso securitário, sobretudo, pelo Estado<sup>56</sup>. A paz que abençoa, por seu turno, o mercado.

### 3. Vigilância e securitização

A vigilância encontra na hiperconectividade a ampliação de seus velhos poderes de controle social, com a reprodução do medo generalizado<sup>57</sup>, mas também do “personal fear”, o medo individualizado ou direcionado. Os algoritmos, essas ferramentas poderosas do mundo e tempo digitais, são capazes de, com um número relativamente pequeno de informações e rastros eletrônicos, identificar que tipo de temor ou de ameaça mais sensibiliza ou (i)mobiliza os indivíduos, bombardeando-o

---

*Constitutionalism. International Studies in the Theory of Private Law*, Hart, Oxford; Portland, 2004, p. 3-28.

<sup>44</sup> RODOTÀ, S., “Una Costituzione per Internet?”, *Politica del diritto*, v. 3, 2010, p. 337-351.

<sup>45</sup> ZICCHITTU, P., “I movimenti “antisistema” nell’agorà digitale: alcune tendenze recenti”, *Liber per Amicorum Pasquale Costanzo*, 5/3/ 2020. Disponível em: <[http://www.giurcost.org/LIBERAMICORUM/zicchittu\\_scrittiCostanzo.pdf](http://www.giurcost.org/LIBERAMICORUM/zicchittu_scrittiCostanzo.pdf)>. Acesso em: 22 abr. 2020.

<sup>46</sup> KARAVAS, V., “Governance of Virtual Worlds and the Quest for a Digital Constitution” en (Graber, C. B.; Burri-Nenova, M. Eds), *Governance of Digital Game Environments and Cultural Diversity Transdisciplinary Enquiries*, E. Elgar, Cheltenham, 2010, p. 167-168.

<sup>47</sup> O grande problema é que nem a internet como um todo nem os algoritmos ou as plataformas são neutras, como se tentou demonstrar no texto. GILLESPIE, T., “The relevance of algorithms”, en (Gillespie, T.; Boczkowski, P. J.; Foot, K. A. Eds.), *Media technologies: Essays on communication, materiality, and society*, The MIT Press, Cambridge, 2014, p. 167-194.

<sup>48</sup> WESTERA, W., *The digital turn: How the internet transforms our existence*, AuthorHouse, Bloomington, 2012.

<sup>49</sup> RICCIARDI, M., “La Costituzione del digitale”, *DigitCult*, v. 3, n. 3, 2018, p. 41-60.

<sup>50</sup> DELANY, P.; LANDOW, G. *Hypermedia and Literary Studies*, MIT Press, Cambridge, 1991.

<sup>51</sup> LÉVY, P., *Cibercultura*, Ed. 34, São Paulo, 2000.

<sup>52</sup> HAVELOCK, E. A., *The Muse Learns to Write: Reflections on Orality and Literacy from Antiquity to the Present*, Yale University Press, New Haven, 1986.

<sup>53</sup> CELESTE, E., “Digital constitutionalism: a new systematic theorization”, *International Review of Law, Computers & Technology*, v. 33, n. 1, 2019, p. 76-99.

<sup>54</sup> RICCIARDI, M., “La Costituzione del digitale”, *DigitCult*, v. 3, n. 3, 2018, p. 45.

<sup>55</sup> O’NEIL, C., *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown Publisher, New York, 2016, p. 161.

<sup>56</sup> OMAND, D., *Securing the State*, Hurst and Company, London, 2010.

<sup>57</sup> FUCHS, C., “Como podemos definir vigilância”, *Matrizes*, n. 1, 2011, p. 129. Disponível em: <<https://www.revistas.usp.br/matrizes/article/download/38311/41154#:~:text=A%20vigil%C3%A2ncia%20%C3%A9%20o%20poder,de%20ver%20sem%20ser%20visto.>>. Acesso em: 20 abr. 2020.

com notícias e mensagens direcionadas<sup>58;59</sup>. As subjetividades se converteram em meros objetos de manipulação privada e pública, na suposição de deterem um livre poder de decisão<sup>60</sup>. Essa estratégia de convencimento se dá de maneira intensiva e transversal nos diversos domínios da vida. As interações sociais passam a ser induzidas pelos próprios algoritmos, de modo a tanto criarem ou estimularem direcionadamente nichos ou enclaves ideológicos, que se alimentem reciprocamente dos medos compartilhados; quanto a expandir num universo de usuários ampliados a verossimilhança dos riscos e das ameaças<sup>61;62</sup>. É preciso que se proteja a segurança dos indivíduos, dos grupos, da política, da economia, da nação<sup>63</sup>. A narrativa da securitização é um apelo estratégico de ativação do sistema límbico social<sup>64</sup>. E ganha a musculatura de uma necessidade social e de um valor constitucional com a mobilização, pelo Estado, do medo e da violência simbólica<sup>65</sup>. Hobbes nunca esteve tão em moda<sup>66;67</sup>.

Esse é o campo fértil de convencimento individual e coletivo de que a hipervigilância é necessária, ordinarizando o que seria extraordinário; normalizando e rotineirizando o que seria emergencial ou exceção, justificando ações que pareceriam fora dos quadrantes jurídicos e das fronteiras da política<sup>68</sup>. É nesse ambiente polimorfo ou atípico que se situam as legislações sobre o tema. Em geral, são diversas as fontes legais, criando-se um emaranhado de normas de complicada hierarquização. As suas enunciações costumam ser semanticamente abertas e repletas de lacunas interpretativas, deixando um amplo espaço de

<sup>58</sup> BUZAN, B.; WAEVER, O.; DE WILDE, J., *Security: A New Framework for Analysis*, Lynne Rienner Publishers Inc., Boulder, 1998, p. 211-212.

<sup>59</sup> O'NEIL, C., *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown Publisher, New York, 2016, p. 68 ss; p. 179 e ss.

<sup>60</sup> ZUBOFF, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile, 2019, p. 34

<sup>61</sup> FOGG, B. J., "Creating persuasive technologies: an eight-step design process", en (Chatterjee, S. Ed) *Proceedings of the 4th international conference on persuasive technology*, Association for Computing Machinery, 2009, p. 1-6. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/1541948.1542005>>. Acesso em: 12 mar. 2020; FOGG, B. J., "Persuasive technology: using computers to change what we think and do", *Ubiquity*, v. 3, n. 44, 2002, p. 89-120. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/764008.763957>>. Acesso em: 12 mar. 2020.

<sup>62</sup> Esse, aliás, é um dos empregos mais usuais nas redes sociais de oferta de contatos e perfis que aproximem os que pensam parecido ou tenham preferências similares. BOYD, D. M.; ELLISON, N. B., "Social Access Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, v. 13, n. 1, 2007. Disponível em: <<https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2007.00393.x?scrollTo=references>>. Acesso em 11 mar. 2021, p. 02.

<sup>63</sup> PORTER, G., "Environmental security as a national security issue", *Current History*, v. 94, n. 592, 1995, p. 218-222.

<sup>64</sup> BUZAN, B.; WAEVER, O.; DE WILDE, J., *Security: A New Framework for Analysis*, Lynne Rienner Publishers Inc., Boulder, 1998, p. 211-212.

<sup>65</sup> WALT, S. M., "The renaissance of security studies", *International Studies Quarterly*, v. 35, n. 2, 1991, p. 213-214.

<sup>66</sup> DEBRIX, F.; BARDER, A. D. "Nothing to fear but fear: Governmentality and the biopolitical production of terror", *International Political Sociology*, v. 3, n. 4, 2009, p. 398-413.

<sup>67</sup> CEYHAN, A., *Surveillance as biopower*, Routledge, New York, 2012, p. 38-45.

<sup>68</sup> BUZAN, B.; WAEVER, O.; DE WILDE, J., *Security: A New Framework for Analysis*, Lynne Rienner Publishers Inc., Boulder, 1998, p. 211-212.

discrecionalidade ou de indefinição entre a licitude e o seu contrário<sup>69;70;71</sup>. Os tribunais que as aplicam, especializados ou não, têm dificuldades práticas de compreensão dos limites de atuação, dada a sua complexidade técnica; quanto não são também envolvidos no próprio discurso de securitização e do medo<sup>72;73</sup>. A ambivalência da prática, das normas e dos juízos revela a parcial substituição da lógica jurídica dos juízos assertórios do normativamente devido pelos juízos de probabilidades ou de mera possibilidade de riscos a serem mitigados, sem se dar conta dos próprios e talvez igualmente sérios riscos que cria. Nesse território de indeterminação, os próprios serviços de inteligência tentam se autoprogredir, levando junto seus instrumentos de controle<sup>74</sup>.

É a “ratio” da digitalização que se mostra nos domínios do controle político e que não encontra ainda a resposta jurídica de um regime de contenção adequado. O pensamento jurídico “análogo” tenta se atualizar num programa de submissão quase incondicional a uma mentalidade e funcionamento que desconhece, abrindo mão de garantias que lhe parecem ultrapassadas. Em troca de nada ou muito pouco<sup>75;76</sup>. São necessários momentos de rupturas, provocados por escândalos, para se ter ideia de que o “virtual” mundo digital já é realidade, que relativiza os aparelhos de proteção que o mundo autoproclamado real detinha, quando não passava mesmo de uma simples virtualidade.

#### **4. A vigilância massiva em exemplos**

As revelações de Edward Snowden sobre a extensão do monitoramento realizado, principalmente, pela Agência de Segurança Nacional (NSA) nos Estados Unidos levantaram a poeira de uma dúvida e suspeita que assombravam muitos estudiosos, estrategistas e políticos, mas que eram desdenhadas pelo direito. Havia um sistema de vigilância intensiva e de escala planetária, empreendida por um conjunto de programas de coleta, de armazenamento, de análise e ao compartilhamento de informações digitais. A pretexto de combate ao terrorismo e da defesa da segurança interna, estava-se coletando clandestinamente um grande número de informações de pessoas várias, anônimas e famosas, representações diplomáticas e instalações militares, incluindo o quartel-general da Organização do Tratado do Atlântico Norte (OTAN); empresas, autoridades e governantes, incluindo

---

<sup>69</sup> JAUVERT, V. “Comment la France écoute (aussi) le monde”, *L’Obs*, juillet 2015. Disponível em: <<https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html>>. Acesso em 14 abr. 2020.

<sup>70</sup> MOREL, C., “Stratégie maritime – Le réseau mondial de câbles sous-marins: une toile dans la Toile”, *Revue Défense Nationale*, v. 2015/9, n. 784, 2015, p. 117-120.

<sup>71</sup> TARROW, S., *War, states, and contention: A Comparative Historical Study*, Cornell University Press, Ithaca, 2015, p. 165-166.

<sup>72</sup> BALZACQ, T., “The three faces of securitization: Political agency, audience and context”, *European journal of international relations*, v. 11, n. 2, 2005, p. 171-201.

<sup>73</sup> DIXIT, P., “Securitization and terroristization: analyzing states’ usage of the rhetoric of terrorism” en (Koch, B. Ed.) *State Terror, State Violence: Global Perspectives*, Springer, Wiesbaden, 2016, p. 31-50.

<sup>74</sup> CAPARINI, M., “Controlling and Overseeing Intelligence Services in Democratic States”, en (Born, H.; Caparini, M. Eds.), *Democratic Control of Intelligence Services. Containing Rogue Elephants*, Ashgate, Aldershot, 2007, p. 3-24.

<sup>75</sup> RODOTÀ, S., “Una Costituzione per Internet?”, *Politica del diritto*, v. 3, 2010, p. 337-351.

<sup>76</sup> ZICCHITTU, P., “I movimenti “antisistema” nell’agorà digitale: alcune tendenze recenti”, *Liber per Amicorum Pasquale Costanzo*, 5/3/ 2020. Disponível em: <[http://www.giurcost.org/LIBERAMICORUM/zicchittu\\_scrittiCostanzo.pdf](http://www.giurcost.org/LIBERAMICORUM/zicchittu_scrittiCostanzo.pdf)>. Acesso em: 22 abr. 2020.

os de países como Alemanha, Brasil, França e México, além do Secretário-Geral das Nações Unidas e o Papa<sup>77; 78; 79</sup>.

Os Estados Unidos da América eram centrais, mas não estavam sozinhos. Havia uma rede de parceiros, distribuídos em níveis de importância. Em primeiro plano, estava a “aliança dos cinco olhos”, composta pelos norte-americanos, australianos, canadenses, britânicos e neozelandeses, que compartilhavam suas informações de modo abrangente<sup>80</sup>. Entre os “sócios” de segundo nível estavam países como Alemanha, Arábia Saudita, Argélia, Áustria, Bélgica, Cingapura, Coreia do Sul, Dinamarca, Emirados Árabes Unidos, Espanha, Finlândia, França, Hungria, Índia, Israel, Itália, Japão, Jordânia, Noruega, Países Baixos, Paquistão, Polônia, República Tcheca, Romênia, Suécia, Tailândia, Taiwan e Turquia<sup>81; 82</sup>. Muitos deles foram “vítimas” da própria vigilância norte-americana ou dos “five eyes”, o que

<sup>77</sup> BALL, J., “NSA monitored calls of 35 world leaders after US official handed over contacts”, *The Guardian*, 25 Out 2013. Disponível em: <<https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>>. Acesso em: 27 mar 2020.

<sup>78</sup> GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Henry Holt and Company, New York, 2014, p. 146, 152.

<sup>79</sup> Em outubro de 2018, uma decisão proferida pela Corte estadunidense da FISA (“Foreign Intelligence Surveillance Court”), especializada em conceder autorizações para vigilâncias, revelou que o FBI era, nos Estados Unidos, o mais prolífico vigilante e minerador em massa de dados de nacionais ou estrangeiros legalmente estabelecidos lá. Em 2017, o FBI realizara aproximadamente 3,1 milhões de buscas relacionadas a essas pessoas, incluindo seus próprios agentes (uns aos outros), enquanto a CIA e a NSA fizeram juntas cerca de 7.500 buscas. Muitas das buscas do FBI foram ilegais, segundo a Corte. Teriam sido usados dados de vigilância em massa para investigar testemunhas e informantes em potencial que não eram suspeitos de crimes nem estavam envolvidos com atividades que ameaçassem a segurança nacional. Havia também indicativos de que estivesse usando a chamada “construção paralela” de provas, para inserir aquelas colhidas pelo programa de vigilância em massa da NSA em processos criminais. A vigilância permite que se busquem mandados apenas para legalizar a prática de obtenção de provas. ESTADOS UNIDOS. *Foreign Intelligence Surveillance Court, Memorandum Opinion and Order*, 18/10/2018. Disponível em: <<https://www.documentcloud.org/documents/6464604-2018-FISC-Ruling-Shows-How-FBI-Abused-NSA-Mass.html>>. Acesso em: 20 mar. 2021; NATIONAL SECURITY AGENCY – NSA. Snowden’s Papers. *NSA Strategic Partnerships*, 13/05/2014, Data de publicação. Disponível em: <<https://edwardsnowden.com/2014/05/15/nsa-strategic-partnerships/>>. Acesso em: 22 abr. 2021; SAVAGE, C., “F.B.I. Practices for Intercepted Emails Violated 4th Amendment, Judge Ruled”, *The New York Times*, 08/10/2019. Disponível em: <<https://www.nytimes.com/2019/10/08/us/politics/fbi-fisa-court.html>>. Acesso em: 04 nov. 2021.

<sup>80</sup> NATIONAL SECURITY AGENCY – NSA. Snowden’s Papers. *FY2013 Foreign Partner Review*, 01/01/2013. Disponível em: <<https://edwardsnowden.com/2014/06/14/fy2013-foreign-partner-review/>>. Acesso em: 22 abr. 2020.

<sup>81</sup> NATIONAL SECURITY AGENCY – NSA. Snowden’s Papers. *FY2013 Foreign Partner Review*. 01/01/2013. Disponível em: <<https://edwardsnowden.com/2014/06/14/fy2013-foreign-partner-review/>>. Acesso em: 22 abr. 2020.

<sup>82</sup> A literatura identifica camadas de parcerias. Os “Nove Olhos” são integrados pelos “Cinco Olhos” mais a Dinamarca, França, Holanda e Noruega. Os “Quatorze Olhos” são constituídos pelos mesmos países dos “Nove Olhos”, além da Alemanha, Bélgica, Itália, Espanha e Suécia. O nome real desse grupo é “SIGINT Seniors Europe (SSEUR)”, tendo por objetivo a coordenação do intercâmbio de inteligência de sinais militares entre seus membros. BIGO, D. “Beyond national security, the emergence of a digital reason of state(s) led by transnational guilds of sensitive information: the case of the Five Eyes Plus network”, em (Wagner, B.; Kettemann, M. C.; Vieth, K. Eds). *Research Handbook on Human Rights and Digital Technology Global Politics, Law and International Relations*, Edward Elgar Publishing, Cheltenham/Northampton, 2019, p. 33-52.

demonstrava que o lema da NSA de “saber tudo, coletar tudo, processar tudo, explorar tudo”<sup>83</sup> não poupava nem os aliados<sup>84</sup>.

A parceria com os Estados Unidos indicava que a vigilância intensiva era uma prática rotineira nos países, democráticos ou não. Investigações feitas, na França, revelaram que, no início de 2008, o presidente Nicolas Sarkozy autorizara a agência francesa de inteligência, a “Direction générale de la Sécurité extérieure” (DGSE), a espionar as comunicações internacionais que passavam pelos cabos submarinos que conectavam a Europa ao resto do mundo, com a ajuda da operadora de telefonia “Orange” e do grupo Alcatel-Lucent. A DGSE firmou uma série de acordos de inteligência com outros pares no exterior, assim como fez o próprio governo francês<sup>85;86</sup>. Na Alemanha, a “Bundesnachrichtendienst (BND)”, a agência de inteligência alemã, coletou, armazenou e tratou metadados da internet e de comunicações telefônicas, coligidos de pessoas dentro e fora do País<sup>87</sup>. Dois exemplos de países que criticaram publicamente a investida norte-americana e a defesa dos direitos violados dos seus cidadãos, mas que também eles, na clandestinidade, realizavam as mesmas práticas e também os violaram<sup>88;89</sup>. A vítima, o algoz e o veneno se confundiam na retórica da securitização, legitimando com o apelo ao escândalo e ao esconderijo das práticas o atentado ao Estado de Direito e aos direitos fundamentais<sup>90</sup>.

Embora essas práticas tivessem sido condenadas por órgãos da União Europeia como o Conselho da União Europeia<sup>91</sup>, a Comissão Europeia de Direitos Humanos<sup>92</sup> e a Comissão das Liberdades Cívicas Justiça e Assuntos Internos do Parlamento Europeu<sup>93</sup>, a própria União estava envolvida em vigilâncias controversas. Em nome do controle de fronteiras, foi criada uma vasta rede de centros de controle e bancos de dados. O Sistema Europeu de Vigilância de Fronteiras (Eurosir) interliga diversos bancos de dados, como aqueles da Agência Europeia de Segurança Marítima

---

<sup>83</sup> NATIONAL SECURITY AGENCY - NSA. Snowden's Papers. *New Collection Posture*. 2011, Disponível em: < <https://edwardsnowden.com/2014/05/13/new-collection-posture/>>. Acesso em: 22 abr. 2020; NATIONAL SECURITY AGENCY - NSA. Snowden's Papers. *Boundless Informant. Describing mission capabilities from Metadata records*. 13/07/2012, Disponível em: <<https://edwardsnowden.com/2013/06/08/boundless-informant-slides/>>. Acesso em: 22 abr. 2020.

<sup>84</sup> GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Henry Holt and Company, New York, 2014.

<sup>85</sup> JAUVERT, V. “Cooment la France écoute (aussi) le monde”, *L'Obs*, juillet 2015. Disponível em: <<https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html>>. Acesso em 14 abr. 2020.

<sup>86</sup> MOREL, C., “Stratégie maritime – Le réseau mondial de câbles sous-marins: une toile dans la Toile”, *Revue Défense Nationale*, v. 2015/9, n. 784, 2015, p. 117-120.

<sup>87</sup> SCHALLER, C., “Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden”, *German Law Journal*, v. 19, n. 4, 2018, p. 941-980.

<sup>88</sup> SCHULZE, M., “Patterns of surveillance legitimization. The German discourse on the NSA scandal”, *Surveillance & Society*, v. 13, n. 2, 2015, p. 197-217.

<sup>89</sup> BAINÉE, O.; NICOLAS, F., “Security, Terror, and Freedom: The Dynamics of Public Opinion in the French Surveillance Debate”, *Journalism and the NSA Revelations: Privacy, Security and the Press*, Reuters Institute/IB Tauris, London, 2017 p. 91-112.

<sup>90</sup> SCHULZE, M., “Patterns of surveillance legitimization. The German discourse on the NSA scandal”, *Surveillance & Society*, v. 13, n. 2, 2015, p. 197-217.

<sup>91</sup> UNIÃO EUROPEIA, *Democratic and effective oversight of national security services*, Council of Europe, Strasbourg, 2015. Disponível em: <<https://rm.coe.int/1680487770>>. Acesso em: 11 mar. 2020.

<sup>92</sup> UNIÃO EUROPEIA, *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU: Mapping member states' legal frameworks (2015)*, Publications Office of the European Union, Luxembourg, 2015.

<sup>93</sup> UNIÃO EUROPEIA. *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*, 21 February 2014. Disponível em: <<https://www.europarl.europa.eu/sides/getDoc.do?reference=A7-2014-0139&type=REPORT&language=EN&redirect>>. Acesso em: 11 abr. 2020.

(EMSA), dos Centros Nacionais de Coordenação (NCCs), Frontex, e do Centro de Satélites da União Europeia (SatCen), possibilitando o intercâmbio de informações entre todos os estados membros da UE<sup>94;95</sup>. O Eurosur assegura que as informações trocadas não incluem dados pessoais. Há dúvidas, todavia, pois a Frontex está vinculada ao centro de operações EU-LISA, que gerencia os três principais sistemas de tecnologia da informação que lidam com vistos, solicitações de asilo e troca de informações para garantir a segurança do espaço Schengen<sup>96</sup>. Esses repositórios de dados armazenam informações de cerca um milhão de pessoas procuradas pela polícia, trinta e dois milhões de solicitantes de visto e mais de cinco milhões de requerentes de asilo<sup>97</sup>.

Nota-se que são práticas típicas dos Estados autoritários ou com regimes mistos como a China e a Rússia. O método e a lógica de vigilância, ancorados no discurso securitista, estão espalhados entre, praticamente, todos os Estados, ricos, emergentes ou pobres. O que diferencia é o maior ou menor grau de sofisticação dos instrumentos jurídicos e técnicos empregados. Os escândalos se sucedem, mas as práticas continuam. A legalidade fluida do mundo digital é o recurso usual de legitimidade das práticas, segundo os discursos de necessidade pública. Os serviços de inteligência da Índia requisitou às empresas de telecomunicações o envio de todos os registros de dados de chamadas de seus usuários. O governo estaria criando um “banco de dados de 360 graus” para rastrear a vida de todos os indianos. Nenhuma das medidas parece ter previsão legal nem segue o devido processo legal<sup>98</sup>.

## 5. Vigilância em massa – a situação no Brasil

O Brasil também foi vítima da vigilância da Agência norte-americana. Servidores da NSA coletavam e processavam intensivamente dados da internet e da telefonia no Brasil. Calcula-se que foram coletados 2,3 bilhões de dados de comunicação no Brasil<sup>99;100</sup>. Entre tantos alvos, estava a embaixada do Brasil em Washington e a representação do País junto à ONU, em Nova York. O caso ganhou maior repercussão com a notícia de monitoramento das comunicações de autoridades brasileiras, incluindo a então Presidente Dilma Rousseff e seus assessores mais

<sup>94</sup> UNIÃO EUROPEIA, *Frontex EUROSUR*, 2017. Disponível em: <<http://frontex.europa.eu/intelligence/eurosur/>>. Acesso em: 10 abr. 2020.

<sup>95</sup> UNIÃO EUROPEIA, 6215/18 ADD 1 FRONT 34 COMIX 57. Brussels, 15/12/2018. Disponível em: <<http://data.consilium.europa.eu/doc/document/ST-6215-2018-ADD-1/en/pdf>>. Acesso em: 11 mar. 2020.

<sup>96</sup> UNIÃO EUROPEIA, *EU-LISA Operational Management*, 2017. Disponível em: <<http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/CoreActivities/Pages/OperationalManagement.aspx>>; Acesso em: 10 abr. 2020.

<sup>97</sup> SIMANTKE, E.; SCHUMANN, H., “Surveillance without limits – How Europe creates a dysfunctional border regime”, *Investigate Europe*, 22/12/2016.

<sup>98</sup> SUBRAMANIAN, N. “The government has stopped even trying to justify mass surveillance as necessary for the public good”, *ScrollIn*, 05/03/2020. Disponível em: <<https://scroll.in/article/956586/the-government-has-stopped-even-trying-to-justify-mass-surveillance-as-necessary-for-the-public-good>>. Acesso em: 25 mar. 2020.

<sup>99</sup> GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Henry Holt and Company, New York, 2014.

<sup>100</sup> O então diretor da Agência de Segurança Nacional (NSA) e comandante do Comando Cibernético dos Estados Unidos, General Keith Alexander, negou que estivesse realizando monitoramento das pessoas no Brasil, quando muito, usando metadados, não apenas no País, mas ao redor do mundo com vistas a identificar atividades terroristas. ALEXANDER, K., “Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War”, *Aspen Security Forum*, Press department, 18/07/2013. Disponível em: <<https://www.intelligence.gov/index.php/ic-on-the-record-database/results/40-clear-and-present-danger-cyber-crime-cyber-espionage-cyber-terror-and-cyber-war-video>>. Acesso em: 21 abr 2021.

próximos<sup>101</sup>. Os indícios eram de que teria havido uma atenção maior às informações sobre a tecnologia de exploração em águas profundas da camada pré-sal. Não foi possível saber a extensão da espionagem, tampouco se houve acesso às informações armazenadas nos computadores da Petrobrás. Em resposta protocolar, a NSA negou que roubasse segredos corporativos para benefício de empresas norte-americanas, limitando-se a coletar informações econômicas destinadas a prevenir crises financeiras e suas repercussões nos mercados internacionais<sup>102;103</sup>.

No Senado Federal, foi instalada uma comissão parlamentar de inquérito, mais conhecida como a "CPI da Espionagem". O relatório dessa CPI considerou improvável a comprovação da materialidade dos crimes de espionagem, duvidando do êxito do inquérito instaurado pela Polícia Federal<sup>104</sup>, o que fez os senadores darem maior atenção ao "aprimoramento dos sistemas de segurança das comunicações e de contrainteligência"<sup>105</sup>. O tráfego de dados, originado e terminado no Brasil, pode ter seu roteamento realizado fora do País, principalmente em Miami, nos Estados Unidos, onde se concentram os servidores centrais da internet. Pouco adiantava, portanto, o fato de a infraestrutura física da "infovia" que atende aos órgãos governamentais ser operada pelo Serpro. Seus dados transitavam pelos Estados Unidos<sup>106</sup>.

O relatório sugeriu uma série de medidas com o objetivo de reduzir a notável vulnerabilidade do País, definidas em quatro eixos: tecnológico, pessoal, processual e institucional. Dentre as medidas estavam o estabelecimento de uma Política Nacional de Inteligência de Sinais, a criação de uma agência para segurança cibernética, a aprovação de normas que dessem respaldo à atividade e ao pessoal de inteligência e que proteja o conhecimento sigiloso sob a guarda dos serviços secretos, e a determinação de que todo tráfego de internet originado e terminado no Brasil fosse trocado localmente<sup>107</sup>.

Algumas constatações da CPI davam alertas para o limbo em que se encontrava a política de inteligência. Além de um estrutura pública descoordenada e de uma agência central, a Agência Brasileira de Inteligência (ABIN), sem poderes jurídicos e instrumentais para o exercício de suas atividades, havia inúmeras empresas que realizavam "inteligência privada", tudo, atividades privadas ou públicas, sem mecanismos efetivos de controle<sup>108</sup>. A ABIN não dispunha de poderes jurídicos para interceptar comunicações telefônicas nem telemáticas. A Lei

---

<sup>101</sup> BBC BRASIL. *EUA espionaram Petrobras, dizem papeis vazados por Snowden*, 08/09/2013. Disponível em: <[https://www.bbc.com/portuguese/noticias/2013/09/130908\\_eua\\_snowden\\_petrobras\\_dilm\\_a\\_mm](https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilm_a_mm)>. Acesso em 11 fev. 2020.

<sup>102</sup> G1. *Petrobras foi espionada pelos EUA, apontam documentos da NSA*, 08/09/2013. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>>. Acesso em: 11 fev. 2020.

<sup>103</sup> O Ministério das Minas e Energia também teria sido espionado, mas pela "parceira", Agência Canadense de Segurança em Comunicação [Communications Security Establishment Canada (CSEC)]. SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020, p. 17.

<sup>104</sup> SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020., p. 131.

<sup>105</sup> SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020, p. 141.

<sup>106</sup> SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020, p. 284-285.

<sup>107</sup> SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020, p. 117, 132ss.

<sup>108</sup> SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020, p. 84, 87, 96.

9296/1996 não a incluiu entre os órgãos autorizados a realizar interceptação telefônica<sup>109</sup>. O art. 3º da Lei 9883/1999, que criou a ABIN, determina que as atividades de inteligência se desenvolvam, “no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado”<sup>110</sup>. Não lhe é dada, portanto, legalmente, competência para monitorar pessoas, suas comunicações físicas ou eletrônicas, suas redes sociais.

A realidade, porém, parece bem outra. Segundo investigações jornalísticas, a ABIN teria monitorado redes sociais como o Twitter, o Facebook, o Instagram e o WhatsApp das pessoas, diante dos protestos de rua que ocorreram no Brasil em 2013<sup>111</sup>. Procurava-se avaliar diariamente a probabilidade de protestos de rua e, se fosse o caso, antecipar o itinerário e o tamanho dos protestos, infiltrações de grupos políticos e supostas fontes de financiamento dos eventos. Para tanto, valiam-se do “Sistema Georreferenciado de Monitoramento e Apoio à Decisão da Presidência da República” ou “GEO-PR”, um grande sistema de dados integrados com diversas áreas do governo, cujas informações de interesse eram catalogadas em um menu chamado “Mosaico de Segurança Institucional”, um sistema online de acompanhamento de cerca de 700 temas definidos pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI)<sup>112; 113</sup>. Segundo o próprio Gabinete, a ABIN, quando necessário, “realiza pesquisas em fontes abertas, incluindo mídias sociais, para eventual subsídios aos seus trabalhos”. Reconhecia-se, portanto, o monitoramento<sup>114</sup>.

Nunca se soube, ao certo, o grau de intrusão na esfera privada das pessoas, promovida por essas atividades. Tampouco se tem notícia, como relatado pela própria CPI, das ações por ela rotineiramente realizadas<sup>115</sup>. Algo que chama a atenção é o fato de a CPI não ter apurado o emprego do GEO-PR pela inteligência brasileiro. Esse sistema fora criado com o objetivo de processar os pedidos de concessão de exploração mineral em faixas de fronteira. Entretanto, ele passou a ser usado para monitorar assentamentos rurais, ONGs, greves, mobilizações e manifestações sociais, além de comunidades indígenas e quilombolas. Segundo informações do GSI, o sistema fora desativado em outubro de 2015, embora seus

<sup>109</sup> BRASIL. *Lei nº 9.296*, de 24 de julho de 1996. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/19296.htm](http://www.planalto.gov.br/ccivil_03/leis/19296.htm)>. Acesso em: 03 nov. 2021.

<sup>110</sup> BRASIL. *Lei nº 9.883*, de 7 de dezembro de 1999. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/LEIS/L9883.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm)>. Acesso em: 03 nov. 2021.

<sup>111</sup> JUNQUEIRA, D., “Para prever potencial de protestos, Abin vai monitorar Facebook, Twitter, Instagram e WhatsApp?”, *Gizmodo Brasil*, 20/07/2013. Disponível em: <<https://gizmodo.uol.com.br/para-prever-potencial-de-protestos-abin-vai-monitorar-facebook-twitter-instagram-e-whatsapp/>>. Acesso em: 20 mar. 2020.

<sup>112</sup> RIZZO, A.; MONTEIRO, T., “Abin monta rede para monitorar internet”, *O Estado de São Paulo*, 19/06/2013. Disponível em: <<https://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500>>. Acesso em 22 abr. 2020.

<sup>113</sup> FIGUEIREDO, L., “O Grande Irmão”, *The Intercept Brasil*, 05/12/2016. Disponível em: <<https://theintercept.com/2016/12/05/abin-tem-megabanco-de-dados-sobre-movimentos-sociais/>>. Acesso em 20 abr. 2020.

<sup>114</sup> MATSUKI, E.; PEDROSA, L., “Abin admite monitorar dados de redes sociais para investigações”, *Portal EBC*, 28/08/2013. Disponível em: <<https://www.ebc.com.br/tecnologia/2013/08/abin-monitora-dados-de-redes-sociais>>. Acesso em 11 fev. 2020.

<sup>115</sup> O controle que hoje existe da ABIN é exercido formalmente por uma comissão legislativa composta por 12 membros, sendo seis do Senado e seis da Câmara dos Deputados, conforme o art 6º da Lei 9883/1999. BRASIL. *Lei nº 9.883*, de 7 de dezembro de 1999. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/LEIS/L9883.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm)>. Acesso em: 03 nov. 2021.

arquivos tenham sido transferidos para a ABIN<sup>116;117</sup>. Em 2019, o ministro-chefe do GSI, Gen. Augusto Heleno, declarou, em documento oficial, que a Agência continuava a monitorar “determinados fenômenos” e a “acompanhar” movimento social, assentamentos rurais, comunidades indígenas e quilombolas, por meio de “fontes abertas”. O documento veio à luz, após suspeitas de que estivesse havendo espionagem de bispos da Igreja Católica na preparação do Sínodo da Amazônia que ocorreria no Vaticano entre os dias 6 e 27 de outubro de 2019<sup>118</sup>.

## 6. Considerações finais

As transformações sociais, epistemológicas, econômicas e políticas produzidas pela revolução digital parecem anunciar um mundo novo, sobre o que a racionalidade alfabética tem pouco ou nada a dizer. As ambivalências como real/virtual ou presença/ausência podem ser um elemento intrínseco a esse novo mundo anunciado ou apenas resultado da incompreensão dos contemporâneos. Olhar o passado e especular sobre o futuro são mais fáceis que compreender o presente. A filosofia de há muito lida com as suas contradições. O que aparece aos olhos de modo menos embaçado é a capacidade que as novas tecnologias da informação oferece ao Estado e ao mercado para vigiar as pessoas. Uma vigilância que não apenas observa, mas que induz e produz comportamentos. Se a emergência de uma nova sociedade digital parece ainda uma questão irresoluta, pelo menos, no sentido de um substituto mais que funcional, estrutural da sociedade alfabética, a afirmação de um Estado de vigilância, ancorado numa economia também de vigilância, está menos às sombras das óticas cognitivas.

A vigilância do mercado objetiva o que sempre objetiva o mercado: o lucro e o controle, a mercancia. Os dados se tornam uma “commodity” de primeira grandeza. As formas cada vez mais sofisticadas de os capturar se associa a algoritmos que provocam necessidades e desejos em escala exponencial. Os titulares dos dados se acham senhores, quando não passam, em verdade (uma verdade do virtual), de servos dos reais (uma realidade do virtual) senhores. A vigilância do Estado também busca o controle e a indução de comportamentos, também pela oferta de paz e segurança. A retórica securitista é seu grande álibi. As ameaças reais são ampliadas e estendidas a todos os domínios da vida. O medo é seu alimento e os episódios de terror suas justificativas. O Estado de Direito ainda requer um pouco de contenção,

---

<sup>116</sup> FIGUEIREDO, L., “O Grande Irmão”, *The Intercept Brasil*, 05/12/2016. Disponível em: <<https://theintercept.com/2016/12/05/abin-tem-megabanco-de-dados-sobre-movimentos-sociais/>>. Acesso em 20 abr. 2020.

<sup>117</sup> A ABIN teria feito, ao presidente do Tribunal Superior Eleitoral, em 2018, proposta de monitoramento amplo e abrangente dos metadados oriundos das mídias sociais e provedores de internet, sem autorização judicial, como forma de combater a disseminação de notícias falsas. A proposta teria sido recusada, por violar o Marco Civil da Internet. SERAPIÃO, F.; MOURA, R. M. “Abin propôs monitorar usuários na rede Sugestão da agência tem como argumento combate à disseminação de notícias falsas na internet”, *O Estado de São Paulo*, 08/07/2018. Disponível em: <<https://politica.estadao.com.br/noticias/eleicoes,abin-propos-monitorar-usuarios-na-rede,70002342417>>. Acesso em: 11 fev. 2021.

<sup>118</sup> O Presidente da República, Jair Bolsonaro, teria afirmado, porém, que a ABIN monitorava o próprio Sínodo, em virtude da influência política do evento. É sabido também que a Presidência da República contratou uma agência privada para monitorar as mídias digitais redes sociais, com relatórios diários sobre repercussões de atos do Planalto e falas de aliados e adversários. INSTITUTO HUMANITAS UNISINOS - IHU, “Bolsonaro diz que Sínodo da Amazônia é evento político e coloca Abin para monitorar bispos”, *Revista IHU Online*, 31/09/2019. Disponível em: <<http://www.ihu.unisinos.br/78-noticias/592207-bolsonaro-diz-que-abin-monitora-sinodo-da-amazonia>>. Acesso em 11 fev. 2021; TRINDADE, N., “Planalto monitora o 'humor' dos internautas”, *O Estado de São Paulo*, 01/04/2019. Disponível em: <<https://politica.estadao.com.br/noticias/geral,planalto-monitora-o-humor-dos-internautas,70002774927>>. Acesso em: 20 abr. 2020.

mas na forma de uma “Estado por Direito” ou, menos ambigualmente, um Direito para o Estado.

O alinhamento tático e estratégico entre os dois, Estado de vigilância e capitalismo de vigilância, conflituoso, como todo alinhamento se torna no começo e no processo, pelas diferenças de ênfases e velocidades, ficou muito mais incontroverso com as revelações de Edward Snowden. Grandes empresas da tecnologia de informação ajudaram os Estados, sob a liderança estadunidense, a vigiarem em massa seus cidadãos e os estrangeiros. A arquitetura jurídica, moldada em lacunas leis de autorização e em ineficazes mecanismos de supervisão, era uma espécie de casa de acomodação e legitimação de interesses. A grande inquietação surge ao perguntar-se se poderia ser diferente. O direito reivindicado pelos defensores da surgência da sociedade digital é ainda mais brando, mais convencional, menos estatal e mais produto de combinações atópicas ou sempre normogeneticamente ruidosas de constituições parciais.

As garantias “sólidas” de Estado de Direito e de direitos fundamentais se tornam regulações contingentes de acordos sociais sobre expectativas de validade de reivindicações individuais e sociais. A ser assim está declarada a dissolução do velho e político (por vezes demagogo) constitucionalismo da Modernidade em troca do novo e econômico (sempre assimétrico e fluido) constitucionalismo digital. O que se observa, por ora, é a submissão do funcionamento jurídico “analógico”, num esforço de atualização de programa, a uma mentalidade e funcionamento que, pelo menos, em parte, desconhece, abrindo mão de garantias que lhe parecem ultrapassadas. Em troca de nada ou muito pouco.

As transformações sociais, epistemológicas, econômicas e políticas produzidas pela revolução digital parecem anunciar um mundo novo, sobre o que a racionalidade alfabética tem pouco ou nada a dizer. As ambivalências como real/virtual ou presença/ausência podem ser um elemento intrínseco a esse novo mundo anunciado ou apenas resultado da incompreensão dos contemporâneos. Olhar o passado e especular sobre o futuro são mais fáceis que compreender o presente. A filosofia de há muito lida com as suas contradições. O que aparece aos olhos de modo menos embaçado é a capacidade que as novas tecnologias da informação oferece ao Estado e ao mercado para vigiar as pessoas. Uma vigilância que não apenas observa, mas que induz e produz comportamentos. Se a emergência de uma nova sociedade digital parece ainda uma questão irresoluta, pelo menos, no sentido de um substituto mais que funcional, estrutural da sociedade alfabética, a afirmação de um Estado de vigilância, ancorado numa economia também de vigilância, está menos às sombras das óticas cognitivas.

A vigilância do mercado objetiva o que sempre objetiva o mercado: o lucro e o controle, a mercancia. Os dados se tornam uma “commodity” de primeira grandeza. As formas cada vez mais sofisticadas de os capturar se associa a algoritmos que provocam necessidades e desejos em escala exponencial. Os titulares dos dados se acham senhores, quando não passam, em verdade (uma verdade do virtual), de servos dos reais (uma realidade do virtual) senhores. A vigilância do Estado também busca o controle e a indução de comportamentos, também pela oferta de paz e segurança. A retórica securitista é seu grande álibi. As ameaças reais são ampliadas e estendidas a todos os domínios da vida. O medo é seu alimento e os episódios de terror suas justificativas. O Estado de Direito ainda requer um pouco de contenção, mas na forma de uma “Estado por Direito” ou, menos ambigualmente, um Direito para o Estado.

O alinhamento tático e estratégico entre os dois, Estado de vigilância e capitalismo de vigilância, conflituoso, como todo alinhamento se torna no começo e no processo, pelas diferenças de ênfases e velocidades, ficou muito mais incontroverso com as revelações de Edward Snowden. Grandes empresas da tecnologia de informação ajudaram os Estados, sob a liderança estadunidense, a vigiarem em massa seus cidadãos e os estrangeiros. A arquitetura jurídica, moldada em lacunas leis de autorização e em ineficazes mecanismos de supervisão, era

uma espécie de casa de acomodação e legitimação de interesses. A grande inquietação surge ao perguntar-se se poderia ser diferente. O direito reivindicado pelos defensores da surgência da sociedade digital é ainda mais brando, mais convencional, menos estatal e mais produto de combinações atópicas ou sempre normogeneticamente ruidosas de constituições parciais.

As garantias “sólidas” de Estado de Direito e de direitos fundamentais se tornam regulações contingentes de acordos sociais sobre expectativas de validade de reivindicações individuais e sociais. A ser assim está declarada a dissolução do velho e político (por vezes demagogo) constitucionalismo da Modernidade em troca do novo e econômico (sempre assimétrico e fluido) constitucionalismo digital. O que se observa, por ora, é a submissão do funcionamento jurídico “análogo”, num esforço de atualização de programa, a uma mentalidade e funcionamento que, pelo menos, em parte, desconhece, abrindo mão de garantias que lhe parecem ultrapassadas. Em troca de nada ou muito pouco.

## Referências

- ALEXANDER, K., “Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War”, *Aspen Security Forum*, Press department, 18/07/2013. Disponível em: <<https://www.intelligence.gov/index.php/ic-on-the-record-database/results/40-clear-and-present-danger-cyber-crime-cyber-espionage-cyber-terror-and-cyber-war-video>>. Acesso em: 21 abr 2021.
- AMARILES, D. R. “The mathematical turn: l’indicateur Rule of Law dans la politique de développement de la Banque Mondiale”, en (Fryman, B.; Van Waeyenberge, A. Dir.). *Gouverner par les standards et les indicateurs: de Hume au rankings*, Bruylant, Bruxelles, 2018, p. 193-234.
- BAGLEY, A. W., “Don't be evil: The Fourth Amendment in the age of Google, national security, and digital papers and effects”, *Albany Law Journal of Science & Technology*, v. 21, 2011, p. 153-191.
- BAISNÉE, O.; NICOLAS, F., “Security, Terror, and Freedom: The Dynamics of Public Opinion in the French Surveillance Debate”, *Journalism and the NSA Revelations: Privacy, Security and the Press*, Reuters Institute/IB Tauris, London, 2017 p. 91-112.
- BALL, J., “NSA monitored calls of 35 world leaders after US official handed over contacts”, *The Guardian*, 25 Out 2013. Disponível em: <<https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>>. Acesso em: 27 mar 2020.
- BALZACQ, T., “The three faces of securitization: Political agency, audience and context”, *European journal of international relations*, v. 11, n. 2, 2005, p. 171-201.
- BBC BRASIL. *EUA espionaram Petrobras, dizem papeis vazados por Snowden*, 08/09/2013. Disponível em: <[https://www.bbc.com/portuguese/noticias/2013/09/130908\\_eua\\_snowden\\_petrobras\\_dilma\\_mm](https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilma_mm)>. Acesso em 11 fev. 2020.
- BIGO, D. “Beyond national security, the emergence of a digital reason of state(s) led by transnational guilds of sensitive information: the case of the Five Eyes Plus network”, en (Wagner, B.; Kettemann, M. C.; Vieth, K. Eds), *Research Handbook on Human Rights and Digital Technology Global Politics, Law and International Relations*, Edward Elgar Publishing, Cheltenham/Northampton, 2019, p. 33-52.
- BOCHNER, S., “Mathematical reflections”, *The American Mathematical Monthly*, v. 81, n. 8, 1974, p. 827-852.
- BOUNSAYTHIP, C.; RINTA-RUNSALA, E., “Overview of data mining for customer behavior modeling”, *VTT Information Technology Research Report*, v. 1, 2001, p. 1-53.

- BOYD, D. M.; ELLISON, N. B., "Social Access Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, v. 13, n. 1, 2007. Disponível em: <<https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2007.00393.x?scrollTo=references>>. Acesso em 11 mar. 2021.
- BRAIDOTTI, R., "Posthuman critical theory", en (Banerji, D.; Paranjape, M. R. Eds). *Critical posthumanism and planetary futures*, Springer, New Delhi; San Francisco, 2016, p. 13-32.
- BRASIL. *Lei nº 9.296*, de 24 de julho de 1996. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/l9296.htm](http://www.planalto.gov.br/ccivil_03/leis/l9296.htm)>. Acesso em: 03 nov. 2021.
- BRASIL. *Lei nº 9.883*, de 7 de dezembro de 1999. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/LEIS/L9883.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm)>. Acesso em: 03 nov. 2021.
- BROWN, B.; CHUÍ, M.; MANYIKA, J., "Are you ready for the era of 'big data'?", *Trend Report McKinsey Global Institute*, 2011. Disponível em: <<https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/are-you-ready-for-the-era-of-big-data#>>. Acesso em: 11 fev. 2021.
- BRUNO, F., "Rastrear, classificar, performar", *Ciência e cultura*, São Paulo, v. 68, n. 1, 2016, p. 34-38.
- BUSINESSWIRE, *Acxiom Expands into South America with Acquisition of GoDigital*, 12/05/2010. Disponível em: <<https://www.businesswire.com/news/home/20100512006274/en/Acxiom-Expands-South-America-Acquisition-GoDigital>>. Acesso em: 11 abr. 2021.
- BUZAN, B.; WAEVER, O.; DE WILDE, J., *Security: A New Framework for Analysis*, Lynne Rienner Publishers Inc., Boulder, 1998, p. 211-212.
- CAPARINI, M., "Controlling and Overseeing Intelligence Services in Democratic States", en (Born, H.; Caparini, M. Eds.), *Democratic Control of Intelligence Services. Containing Rogue Elephants*, Ashgate, Aldershot, 2007, p. 3-24.
- CELESTE, E., "Digital constitutionalism: a new systematic theorization", *International Review of Law, Computers & Technology*, v. 33, n. 1, 2019, p. 76-99.
- CEYHAN, A., *Surveillance as biopower*, Routledge, New York, 2012, p. 38-45.
- CHAGANI, F., "Critical political ecology and the seductions of posthumanism", *Journal of Political Ecology*, v. 21, n. 1, 2014, p. 424-436.
- CLARKE, R. A. "Information, Technology and Dataveillance". *Communications of the ACM*, v. 37, n. 5, 1988, p. 498-512.
- DEBRIX, F.; BARDER, A. D. "Nothing to fear but fear: Governmentality and the biopolitical production of terror", *International Political Sociology*, v. 3, n. 4, 2009, p. 398-413.
- DELANY, P.; LANDOW, G. *Hypermedia and Literary Studies*, MIT Press, Cambridge, 1991.
- DIVINE, J., "The 10 Most Valuable Tech Companies in the World The world", *US News*, 16/08/2019. Disponível em: <<https://money.usnews.com/investing/stock-market-news/slideshows/the-10-most-valuable-tech-companies-in-the-world>>. Acesso em: 3 mai. 2021.
- DIXIT, P., "Securitization and terroristization: analyzing states' usage of the rhetoric of terrorism" en (Koch, B. Ed.) *State Terror, State Violence: Global Perspectives*, Springer, Wiesbaden, 2016, p. 31-50.
- DOMENICO, T., *Big Data and the Computable Society: Algorithms and People in the Digital World*, World Scientific, New Jersey, 2019.
- ESTADOS UNIDOS. *Foreign Intelligence Surveillance Court, Memorandum Opinion and Order*, 18/10/2018. Disponível em: <<https://www.documentcloud.org/documents/6464604-2018-FISC-Ruling-Shows-How-FBI-Abused-NSA-Mass.html>>. Acesso em: 20 mar. 2021.

- FIGUEIREDO, L., "O Grande Irmão", *The Intercept Brasil*, 05/12/2016. Disponível em: <<https://theintercept.com/2016/12/05/abin-tem-megabanco-de-dados-sobre-movimentos-sociais/>>. Acesso em 20 abr. 2020.
- FITZGERALD, B., "Software as discourse? A constitutionalism for information society", *Alternative Law Journal*, v. 24, n. 3, 1999, p. 144-149.
- FOGG, B. J., "Creating persuasive technologies: an eight-step design process", en (Chatterjee, S. Ed) *Proceedings of the 4th international conference on persuasive technology*, Association for Computing Machinery, 2009, p. 1-6. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/1541948.1542005>>. Acesso em: 12 mar. 2020;
- FOGG, B. J., "Persuasive technology: using computers to change what we think and do", *Ubiquity*, v. 3, n. 44, 2002, p. 89-120. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/764008.763957>>. Acesso em: 12 mar. 2020.
- FORBES. "The World's Most Valuable Brands", 30/4/2020. Disponível em: <<https://www.forbes.com/powerful-brands/list/>>. Acesso em: 3 mai. 2020.
- FRAWLEY, W. J.; PIATETSKY-SHAPIO, G.; MATHEUS, C. J., "Knowledge discovery in databases: an overview", *AAAI Magazine*, Palo Alto, v. 13, n. 3, 1992, p. 57-70.
- FUCHS, C., "Como podemos definir vigilância", *Matrizes*, n. 1, 2011, p. 129. Disponível em: <<https://www.revistas.usp.br/matrizes/article/download/38311/41154#:~:text=A%20vigil%C3%A2ncia%20%C3%A9%20o%20poder,de%20ver%20se%20ser%20visto.>>. Acesso em: 20 abr. 2020.
- G1. *Petrobras foi espionada pelos EUA, apontam documentos da NSA*, 08/09/2013. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>>. Acesso em: 11 fev. 2020.
- GILLESPIE, T., "The relevance of algorithms", en (Gillespie, T.; Boczkowski, P. J.; Foot, K. A. Eds.), *Media technologies: Essays on communication, materiality, and society*, The MIT Press, Cambridge, 2014, p. 167-194.
- GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Henry Holt and Company, New York, 2014.
- HALL, G., "Towards a post-digital humanities: cultural analytics and the computational turn to data-driven scholarship", *American Literature*, v. 85, n. 4, 2013, p. 781-809.
- HAVELOCK, E. A., *The Muse Learns to Write: Reflections on Orality and Literacy from Antiquity to the Present*, Yale University Press, New Haven, 1986.
- HIRSCH, D. D., "The glass house effect: Big Data, the new oil, and the power of analogy". *Maine La Review*, v. 66, 2013, p. 373-395.
- HUXLEY, J., "Transhumanism", *Ethics in Progress*, v. 6, n. 1, 2015, p. 12-16;
- JAUVERT, V. "Cooment la France écoute (aussi) le monde", *L'Obs*, juillet 2015. Disponível em: <<https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html>>. Acesso em 14 abr. 2020.
- INSTITUTO HUMANITAS UNISINOS - IHU, "Bolsonaro diz que Sínodo da Amazônia é evento político e coloca Abin para monitorar bispos", *Revista IHU Online*, 31/09/2019. Disponível em: <<http://www.ihu.unisinos.br/78-noticias/592207-bolsonaro-diz-que-abin-monitora-sinodo-da-amazonia>>. Acesso em 11 fev. 2021.
- JAUVERT, V. "Cooment la France écoute (aussi) le monde", *L'Obs*, juillet 2015. Disponível em: <<https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html>>. Acesso em 14 abr. 2020.
- JUNQUEIRA, D., "Para prever potencial de protestos, Abin vai monitorar Facebook, Twitter, Instagram e WhatsApp?", *Gizmodo Brasil*, 20/07/2013. Disponível em: <<https://gizmodo.uol.com.br/para-prever-potencial-de-protestos-abin>>.

- vai-monitorar-facebook-twitter-instagram-e-whatsapp/>. Acesso em: 20 mar. 2020.
- KARAVAS, V., "Governance of Virtual Worlds and the Quest for a *Digital Constitution*" en (Graber, C. B.; Burri-Nenova, M. Eds.), *Governance of Digital Game Environments and Cultural Diversity Transdisciplinary Enquiries*, E. Elgar, Cheltenham, 2010, p. 167-168.
- KITCHIN, R., "Big Data, new epistemologies and paradigm shifts", *Big Data & Society*, [S.l.], 2014, p. 1-22. Disponível em: <<http://bds.sagepub.com/content/1/1/2053951714528481>>. Acesso em: 1º jul. 2016.
- KOSCIEJEW, M., "The Individual and Big Data", *Felicitier*, v. 59, n. 6, 2013, p. 32-35, Disponível em: <<https://www.highbeam.com/doc/1P3-3158119951.html>>. Acesso em: 15 mar 2020.
- KRISHNAN V, G., "Aadhaar in the hand of spies Big Data, global surveillance state and the identity project", *Fountain Ink Magazine*, 03/06/2017. Disponível em: <<https://fountainink.in/reportage/aadhaar-in-the-hand-of-spies->>. Acesso em: 11 mar. 2021.
- LEMOES, A., "Cibercultura como Território Recombinante" en (Martins, C. D.; Silva, D. C.; Motta, R. Orgs.), *Territórios recombinares: arte e tecnologia - debates e laboratórios*, Instituto Sérgio Motta, São Paulo, 2007, p. 35-48.
- LÉVY, P., *Cibercultura*, Ed. 34, São Paulo, 2000.
- MATSUKI, E.; PEDROSA, L., "Abin admite monitorar dados de redes sociais para investigações", *Portal EBC*, 28/08/2013. Disponível em: <<https://www.ebc.com.br/tecnologia/2013/08/abin-monitorea-dados-de-redes-sociais>>. Acesso em 11 fev. 2020.
- MAYER-SCHONBERGER, V.; CUKIER, K. *Big Data: A Revolution that Will Change How We Live, Work and Think*. John Murray, London, 2013.
- MAZLISH, B., *The Fourth Discontinuity The Co-Evolution of Humans and Machines*, Yale University Press, New Haven, 1995.
- MICHAELS, J. D. "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror", *California Law Review*, v. 96, 2008, p. 914-915.
- MORAIS, J. L. B., "O fim da geografia institucional do estado. A "crise" do estado de direito", en "Oliveira, C. M. Org), *Novos direitos: a interdisciplinaridade do direito na sociedade contemporânea*, CPOI/UFSCar, São Carlos, 2017.
- MOREL, C., "Stratégie maritime – Le réseau mondial de câbles sous-marins: une toile dans la Toile", *Revue Défense Nationale*, v. 2015/9, n. 784, 2015, p. 117-120.
- NATIONAL SECURITY AGENCY - NSA. Snowden's Papers. *Boundless Informant. Describing mission capabilities from Metadata records*. 13/07/2012. Disponível em: <<https://edwardsnowden.com/2013/06/08/boundless-informant-slides/>>. Acesso em: 22 abr. 2020.
- NATIONAL SECURITY AGENCY - NSA. Snowden's Papers. *FY2013 Foreign Partner Review*. 01/01/2013. Disponível em: <<https://edwardsnowden.com/2014/06/14/fy2013-foreign-partner-review/>>. Acesso em: 22 abr. 2020.
- NATIONAL SECURITY AGENCY - NSA. Snowden's Papers. *New Collection Posture*. 2011, Disponível em: < <https://edwardsnowden.com/2014/05/13/new-collection-posture/>>. Acesso em: 22 abr. 2020.
- NATIONAL SECURITY AGENCY - NSA. Snowden's Papers. *NSA Strategic Partnerships*, 13/05/2014, Data de publicação. Disponível em: <<https://edwardsnowden.com/2014/05/15/nsa-strategic-partnerships/>>. Acesso em: 22 abr. 2021.
- OMAND, D., *Securing the State*, Hurst and Company, London, 2010.
- O'NEIL, C., *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown Publisher, New York, 2016.
- PORTER, G., "Environmental security as a national security issue", *Current History*, v. 94, n. 592, 1995, p. 218-222.

- RICCIARDI, M., "La Costituzione del digitale", *DigitCult*, v. 3, n. 3, 2018, p. 41-60.
- RIZZO, A.; MONTEIRO, T., "Abin monta rede para monitorar internet", *O Estado de São Paulo*, 19/06/2013. Disponível em: <<https://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500>>. Acesso em 22 abr. 2020.
- RODERICK, L., "Discipline and power in the digital age: The case of the US consumer data broker industry", *Critical Sociology*, v. 40, n. 5, 2014, p. 729-746.
- RODOTÀ, S., "Una Costituzione per Internet?", *Politica del diritto*, v. 3, 2010, p. 337-351.
- ROUVROY, A.; BERNS, T.. "Governamentalidade algorítmica e perspectivas da emancipação: o díspar como condição de individuação pela relação?", *Revista Eco-Pós*, v. 18 (Tecnologia e Vigilância), n. 2, 2015, p. 40-41.
- RUBINSTEIN, I. S.; LEE, R. D.; SCHWARTZ, P. M., "Data mining and Internet profiling: Emerging regulatory and technological approaches", *University of Chicago Law Review*, v. 75, 2008, p. 261-185.
- SAMPAIO, A. C. *Data brokers: um novo modelo de negócios baseado em vigilância de dados*, Dissertação de Mestrado. Campinas: Unicamp, 2017. Disponível em: <[http://repositorio.unicamp.br/bitstream/REPOSIP/322483/1/Sampaio\\_AliceCastaldi\\_M.pdf](http://repositorio.unicamp.br/bitstream/REPOSIP/322483/1/Sampaio_AliceCastaldi_M.pdf)>. Acesso em 20 abr. 2021.
- SANTOS, L. G.. "A informação após a virada cibernética", em (Santos, L. G.; Kehl, M. R.; Kucinsk, B. eds), *Revolução tecnológica, internet e socialismo*, Fundação Perseu Abramo, São Paulo, 2003, p. 9-33.
- SAVAGE, C., "F.B.I. Practices for Intercepted Emails Violated 4th Amendment, Judge Ruled", *The New York Times*, 08/10/2019. Disponível em: <<https://www.nytimes.com/2019/10/08/us/politics/fbi-fisa-court.html>>. Acesso em: 04 nov. 2021.
- SCHALLER, C., "Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden", *German Law Journal*, v. 19, n. 4, 2018, p. 941-980.
- SCHMIDT, E.; COHEN, J., *The New Digital Age. Reshaping the Future of People, Nations and Business*, Knopf, New York, 2013.
- SCHNEIER, B., "Metadata = Surveillance", *IEEE Security & Privacy*, v. 12, n. 12, 2014, p. 84. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6798571>>. Acesso em: 20 abr. 2020.
- SCHULZE, M., "Patterns of surveillance legitimization. The German discourse on the NSA scandal", *Surveillance & Society*, v. 13, n. 2, 2015, p. 197-217.
- SENADO FEDERAL, *CPI da Espionagem, Relatório Final*. 2014. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 fev. 2020.
- SERAPIÃO, F.; MOURA, R. M. "Abin propôs monitorar usuários na rede Sugestão da agência tem como argumento combate à disseminação de notícias falsas na internet", *O Estado de São Paulo*, 08/07/2018. Disponível em: <<https://politica.estadao.com.br/noticias/eleicoes,abin-propos-monitorar-usuarios-na-rede,70002342417>>. Acesso em: 11 fev. 2021.
- SILVA, T. "Web 2.0, Vigilância e Monitoramento: entre funções pós-massivas e classificação social", Congresso Luso Afro Brasileiro de Ciências Sociais, Salvador, 2011. Disponível em: <<https://www.slideshare.net/tarushijio/web-20-vigilancia-e-monitoramento-entre-funcoes-posmassivas-e-classificacao-social-9661816>>
- SIMANTKE, E.; SCHUMANN, H., "Surveillance without limits – How Europe creates a dysfunctional border regime", *Investigate Europe*, 22/12/2016.
- STATISTA. "Brand value of the 25 most valuable brands in 2020", 30/4/2020. Disponível em: <<https://www.statista.com/statistics/264875/brand-value-of-the-25-most-valuable-brands/>>. Acesso em 3 mai. 2020.

- SUBRAMANIAN, N. "The government has stopped even trying to justify mass surveillance as necessary for the public good", *ScrollIn*, 05/03/2020. Disponível em: <<https://scroll.in/article/956586/the-government-has-stopped-even-trying-to-justify-mass-surveillance-as-necessary-for-the-public-good>>. Acesso em: 25 mar. 2020.
- SUSKIND, R., *One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11*, Simon and Schuster, New York, 2006.
- SUZOR, N. P., *Digital constitutionalism and the role of the rule of law in the governance of virtual communities*. PhD Thesis, Queensland University of Technology, 2010. Disponível em: <<https://eprints.qut.edu.au/37636/>>. Acesso em: 20 mar. 2020.
- TARROW, S., *War, states, and contention: A Comparative Historical Study*, Cornell University Press, Ithaca, 2015, p. 165-166.
- TEUBNER, G., "Societal Constitutionalism; Alternatives to State-Centred Constitutional Theory?" en (Joeges, C.; Sand, I. J.; Teubner, G. Eds.), *Transnational Governance and Constitutionalism. International Studies in the Theory of Private Law*, Hart, Oxford; Portland, 2004, p. 3-28.
- TEUBNER, G., *Fragmentos constitucionais: constitucionalismo social na globalização*, Saraiva, São Paulo, 2016.
- TRINDADE, N., "Planalto monitora o 'humor' dos internautas", *O Estado de São Paulo*, 01/04/2019. Disponível em: <<https://politica.estadao.com.br/noticias/geral,planalto-monitora-o-humor-dos-internautas,70002774927>>. Acesso em: 20 abr. 2020.
- UNIÃO EUROPEIA, 6215/18 ADD 1 FRONT 34 COMIX 57. Brussels, 15/12/2018. Disponível em: <<http://data.consilium.europa.eu/doc/document/ST-6215-2018-ADD-1/en/pdf>>. Acesso em: 11 mar. 2020.
- UNIÃO EUROPEIA, *Democratic and effective oversight of national security services*, Council of Europe, Strasbourg, 2015. Disponível em: <<https://rm.coe.int/1680487770>>. Acesso em: 11 mar. 2020.
- UNIÃO EUROPEIA, *EU-LISA Operational Management*, 2017. Disponível em: <<http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/CoreActivities/Pages/OperationalManagement.aspx>>; Acesso em: 10 abr. 2020.
- UNIÃO EUROPEIA, *Frontex EUROSUR*, 2017. Disponível em: <<http://frontex.europa.eu/intelligence/eurosur/>>. Acesso em: 10 abr. 2020.
- UNIÃO EUROPEIA, *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU: Mapping member states' legal frameworks (2015)*, Publications Office of the European Union, Luxembourg, 2015.
- UNIÃO EUROPEIA. *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*, 21 February 2014. Disponível em: <<https://www.europarl.europa.eu/sides/getDoc.do?reference=A7-2014-0139&type=REPORT&language=EN&redirect>>. Acesso em: 11 abr. 2020.
- VAN DIJCK, J., "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology". *Surveillance & Society*, v. 12, n. 2, 2014.
- WALT, S. M., "The renaissance of security studies", *International Studies Quarterly*, v. 35, n. 2, 1991, p. 213-214.
- WARD, K., "Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting", *Journal of media ethics*, v. 33, n. 3, 2018, p. 133-148.
- WESTER, W., *The digital turn: How the internet transforms our existence*, AuthorHouse, Bloomington, 2012.
- ZICCHITTU, P., "I movimenti "antisistema" nell'agorà digitale: alcune tendenze recenti", *Liber per Amicorum Pasquale Costanzo*, 5/3/ 2020. Disponível em: <[http://www.giurcost.org/LIBERAMICORUM/zicchittu\\_scrittiCostanzo.pdf](http://www.giurcost.org/LIBERAMICORUM/zicchittu_scrittiCostanzo.pdf)>. Acesso em: 22 abr. 2020.

- ZUBOFF, S., "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, v. 30, n. 1, 2015, p. 75-89. Disponível em: <<http://link.springer.com/article/10.1057/jit.2015.5>>. Acesso em: 25 abr. 2021.
- ZUBOFF, S., *Google as a Fortune Teller: the secrets of surveillance capitalism*. *Frankfurter Allgemeine*, 2016. Disponível em: <<http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>>. Acesso em: 12 mar. 2020.
- ZUBOFF, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile, 2019.