

UNIVERSIDADE DO VALE DO RIO DOS SINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL DOUTORADO

ELIAS JACOB DE MENEZES NETO

SURVEILLANCE, DEMOCRACIA E DIREITOS HUMANOS: OS LIMITES DO ESTADO NA ERA DO BIG
DATA

São Leopoldo
2016

Elias Jacob de Menezes Neto

SURVEILLANCE, DEMOCRACIA E DIREITOS HUMANOS: OS LIMITES DO ESTADO NA ERA DO BIG
DATA

Tese apresentada como requisito parcial
para a obtenção do título de Doutor em
Direito, pelo Programa de Pós-Graduação
em Direito da Universidade do Vale do Rio
dos Sinos - UNISINOS

Orientador: Prof. Dr. Jose Luis Bolzan de Moraes

São Leopoldo

2016

J15s Jacob de Menezes Neto, Elias
Surveillance, democracia e direitos humanos: os limites do Estado na era do big data / por Elias Jacob de Menezes Neto. -- 2016.
293 f. ; 30cm.

Tese (Doutorado em Direito) -- Universidade do Vale do Rio dos Sinos - Unisinos. Programa de Pós-Graduação em Direito, São Leopoldo, RS, 2016.

Orientação: Prof. Dr. Jose Luis Bolzan de Moraes.

1. Direitos humanos. 2. Surveillance. 3. Vigilância. 4. Crise do Estado. 5. Internet. I. Título. II. Moraes, Jose Luis Bolzan de.

CDU 342.7

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
NÍVEL DOUTORADO

A tese intitulada: **“SURVEILLANCE, DEMOCRACIA E DIREITOS FUNDAMENTAIS: OS LIMITES DO ESTADO NA ERA DO BIG DATA”**, elaborada pelo doutorando **Elias Jacob de Menezes Neto**, foi julgada adequada e aprovada por todos os membros da Banca Examinadora para a obtenção do título de DOUTOR EM DIREITO.

São Leopoldo, 28 de junho de 2016.

Prof. Dr. **Leonel Severo Rocha**,

Coordenador do Programa de Pós-Graduação em Direito.

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dr. Jose Luis Bolzan de Morais

Membro: Dr. Wilson Engelmann

Membro: Dr. Leonel Severo Rocha

Membro: Dra. Ruth Maria Chittó Gauer

Membro: Dr. Márcio Ricardo Staffen

Ao ciclista que, em um final de tarde de uma primavera qualquer, colapsou universos.

AGRADECIMENTOS

Esta foi uma tese escrita nas alturas. Seja na dos aviões, pelas dezenas de milhares de quilômetros viajados durante sua escrita, seja na do estado de espírito extremamente elevado que só uma força arrebatadora como o amor pode proporcionar. O amor foi o elemento inicial da reação em cadeia que culminou neste trabalho. Em um mundo eletronicamente hiperconectado, este sentimento é a ponte imaterial que conecta tudo e todos. Por isso, sou extremamente grato pelas conexões abaixo:

M. Medeiros, a *startup neutron source* desta reação em cadeia (e de tantas outras). Chris Martin sempre teve razão: *without you it's a waste of time*.

S. Couto, pelo eterno amor, incondicional apoio e infinita fé.

M. Soares, por um dos amores mais genuínos e puros que existem, daqueles que simplesmente dá sem esperar absolutamente nada em troca.

R. Barreto, pelo amor do qual eu tenho certeza que sente.

C. Grieffenhagen, pela amizade verdadeira, fiel e forte.

F. Murakami, pela amizade que, mesmo distante, permaneceu inabalável.

J. Bolzan, pela excelente parceria, amizade, dedicação e ativa participação na elaboração e orientação deste trabalho.

W. Engelmann e L. Rocha, pela cuidadosa leitura e valiosas sugestões no aprimoramento da tese.

M. Kayser, pelo carinho, cuidado e amizade desde a minha chegada no RS.

I. Vedovatto, pelo auxílio na lapidação deste trabalho e pelas agradáveis conversas.

C. Cassini, pela ajuda crucial na canalização de forças extremamente poderosas, capazes de materializar o intangível.

T. Prucha, pela amizade, carinho e conversas que levarei sempre comigo.

M. Moura, A. Andrighetto, M. Veras, B. Costa, Z. Lopes, D. Lima, T. Squeff, C. Rego, V. Fortes, T. Gervasoni, F. Nunes, juristas extremamente talentosos e pessoas adoráveis que tive o prazer de conhecer durante o mestrado e doutorado.

S. Cordeiro, M. Queiroz, V. Chaves, F. Resende, R. Pinheiro, F. Araújo, G. Emídio, A. Santana, novos e queridos amigos que chegaram com tudo.

A. Moresco, H. Grunvalder, M. Aziz, B. Mayer, B. Orcina, S. Dreger, F. Pagel, F. Gottlieb, O. Martins, E. Johnny, N. González, F. Suárez, companheiros do Aikido que, juntos, dividiram a busca pelo 道.

E, claro, **Snowden** – o *Schnauzer*, não o humano – pelo ensinamento diário, sem palavras, de como a vida, em todas as suas formas, está surpreendentemente conectada.

Dividir este pedaço do espaço-tempo com cada um de vocês tem sido uma honra e um privilégio. Sem dúvidas, *it's louder than words*. **Obrigado!**

Sólo viviendo absurdamente se podría romper alguna vez este absurdo infinito.

(Julio Cortázar)

RESUMO

Esta tese resulta da necessidade de situar a proteção dos direitos humanos e da democracia diante dos fenômenos da *surveillance* e dos fluxos globais de dados, especialmente, levando-se em conta que a desterritorialidade e a fluidez desses fenômenos desafiam os mecanismos de controle jurídico, centrados, exclusivamente no Estado-nação. Demonstra como a soberania estatal passa a ser afetada pelas transformações oriundas da globalização, da modernidade líquida e da sociedade em rede. Delimita a categoria da *surveillance*, analisada como uma característica inerente à modernidade líquida com o objetivo de demarcar, de forma acertada, o papel do Estado e da democracia diante dos fluxos globais de dados. Para tanto, explica como a palavra *surveillance* não pode ser, diretamente, traduzida para o português sem que haja prejuízo semântico. Aborda, ainda, os limites dos modelos do panóptico e do Big Brother para elucidar a coleta de dados em massa na era do *big data*. Para tanto, analisa a expansão da *surveillance* no século XXI, bem como os efeitos do *big data* e dos algoritmos preditivos na construção do tempo e do espaço. Fundados na guerra ao terror, esses instrumentos buscam capturar o passado e analisar o presente com a finalidade de prever eventos futuros antes mesmo que aconteçam. Tais mecanismos permitem a desterritorialização das fronteiras e a sua transformação em espaço de controle de fluxos de pessoas consideradas indesejáveis. Por isso, demonstra que o Estado é palco fragilizado para a proteção dos direitos humanos violados pela *surveillance*, o que permite considerar as matrizes teóricas sistêmicas – inclusive a ideia de constitucionalismo híbrido – como adequadas para proteger direitos violados por corporações transnacionais ligadas à tecnologia da informação. Conclui que a proteção dos direitos humanos afetados pela *surveillance* não pode depender, exclusivamente, dos meios de regulação jurídica associados ao Estado, dada a sua impossibilidade de lidar com problemas que escapam à esfera da política e ao *container* territorial, o que torna imprescindível a participação da iniciativa privada.

Palavras-chave: Surveillance. Vigilância. Crise do Estado. Direitos humanos. Internet.

ABSTRACT

This thesis stems from the need to properly understand protection of fundamental rights and democracy under the effects of *surveillance* and global data flows, especially considering that these phenomena are deterritorialized and fluid and, hence, they challenge traditional legal control mechanisms based on the nation-state. For this, it shows how state sovereignty is now affected by the transformations of the nation-state caused by globalization, liquid modernity and the network society. It also explains that *surveillance* is intrinsic to liquid modernity, which is needed to properly understand the protection of fundamental rights and democracy against global data flows. Thus, it analyses how the word *surveillance* cannot be directly translated into Portuguese without losing its meaning. In addition, it explains why ideas such as panoptic and Big Brother aren't enough to understand surveillance in the age of *big data*. That why it deals with the expansion of surveillance in the twentieth first century and establishes how *big data* and predictive analytics change the meaning of time and space. Based in the war on terror, these techniques try to capture the past and analyse the present in order to predict future events even before they happen. Also, they allow the deterritorialization of nation-state borders, converting them in places to control undesired people flows. For this reason, it shows how the nation-state is weakened on its role of human rights guardian, especially those violated by surveillance, which is why system's theory and hybrid constitutionalism were considered capable to properly understand human rights violations by information technology transnational organizations. The conclusion points to the idea that human rights cannot be protected against surveillance by traditional legal control mechanisms as they are centered around the idea of the nation-state, which makes it impossible to handle issues that surpass its political system and territorial container, thus requiring private actor to take part in this discussion.

Keywords: Surveillance. Vigilance. Crisis of the nation-state. Human rights. Internet

RESUMEN

Esta tesis surge de la necesidad de presentar la protección de los derechos humanos y la democracia ante los fenómenos de la *surveillance* y de los flujos de datos globales, sobre todo teniendo en cuenta que la desterritorialización y la fluidez de estos fenómenos desafían los mecanismos legales de control que se centran exclusivamente en el Estado-nación. Muestra cómo la soberanía del Estado se ve afectada por las transformaciones ante la globalización, de la modernidad líquida y de la sociedad en red. Delimita la categoría *surveillance*, analizada como una característica inherente a la modernidad líquida, para situar adecuadamente la función de Estado y de la democracia ante los flujos globales de datos. Para eso, explica como la palabra *surveillance* no puede traducirse directamente del inglés a otros idiomas sin pérdida semántica. Además, aborda los límites de los modelos del panóptico y del Big Brother para dilucidar la recolección de datos en masa en la era del *big data*. Aborda la ampliación de la *surveillance* en el siglo XXI, así como los efectos del *big data* y de los algoritmos predictivos en la construcción del tiempo y del espacio. Fundados en la guerra contra el terror, estos instrumentos intentan capturar el pasado y analizar el presente con el fin de predecir eventos futuros antes de que sucedan. Además, permiten la desterritorialización de las fronteras y su transformación en el espacio de control de flujos de personas consideradas indeseables. Demuestra que el Estado es un escenario frágil para la protección de los derechos humanos violados por la *surveillance*, lo que sugiere considerar marcos teóricos sistémicos - incluso la idea de constitucionalismo híbrido- como apropiados para proteger los derechos violados por las corporaciones transnacionales relacionadas con la tecnología de la información. Concluye que la protección de los derechos fundamentales violados por la *surveillance* no puede basarse únicamente en los medios de regulación legal asociados con el Estado, dada su incapacidad para hacer frente a los problemas que están más allá de la esfera de la política y del *container* territorial, lo que hace imprescindible la participación del sector privado en esta discusión.

Palabras clave: Surveillance. Vigilancia. Crisis del Estado. Derechos humanos. Internet.

LISTA DE TABELAS

Tabela 1 – Divisão dos teóricos da globalização em Held e McGrew	45
Tabela 2 – Diferenças entre a “traditional surveillance” e a “new surveillance”	99

LISTA DE FIGURAS

- Figura 1 – Mapa obtido dos documentos divulgados por Edward Snowden, indicando os pontos de coleta de dados da NSA e dos seus parceiros, bem como o tipo de acesso de cada ponto. 145
- Figura 2 – Mapa gerado pelo sistema *boundless informant*, indicando a abrangência da coleta de dados efetuada pela NSA..... 147

LISTA DE SIGLAS

AISE – Agenzia Informazioni e Sicurezza Esterna
AIVD – Algemene Inlichtingen en Veiligheidsdienst
API – *Advanced Passenger Information*
APL – Anteprojeto de Lei
ASD – Australian Signals Directorate
BND – Bundesnachrichtendienst
BvF – Bundesamt für Verfassungsschutz
CDC – Centers for Disease Control and Prevention
CFTV – Circuito Fechado de Televisão
CNE – Computer Network Exploitation
CNI – Centro Nacional de Inteligencia
CPI – Comissão Parlamentar de Inquérito
CPF – Cadastro de Pessoa Física
CSEC – Communications Security Establishment Canada
DARPA – Defense Advanced Research Projects Agency
DIMOF – Declaração de Movimentação Financeira
DGSE – Direction Générale de la Sécurité Extérieure
DHS – Department of Homeland Security
DTRA – Defense Threat Reduction Agency
FAQ – Frequently Asked Question(s)
FAST – Future Attribute Screening Technology
FBI – Federal Bureau of Investigation
FISA – Foreign Intelligence Surveillance Act
FORNSAT – Foreign Satellite Interception
FRA – Försvarets radioanstalt
GCHQ – Government Communications Headquarters
GPS – Global Positioning System
HIV – Human Immunodeficiency Virus
IATA – International Air Transport Association
ICANN – Internet Corporation for Assigned Names and Numbers
IMDB – Internet Movie Database

ISNU – Israeli SIGINT National Unit
MC – Ministério da Cultura
MCT – Ministério da Ciência e Tecnologia
MDP – Moderna, Dinâmica, Pluralista
NDB – Nachrichtendienst des Bundes
NIS – Norwegian Intelligence Service
NSA – National Security Agency
OCR – Optical Character Recognition
PET – Politiets Efterretningstjeneste
PNR – *Passenger Name Record*
POL – Patterns of Life
RFID – Radio Frequency Identification
SCS – Special Collection Service
SID – Security and Intelligence Division
SIGINT – Signal Intelligence
SIS – Schengen Information System
SPED – Sistema Público de Escrituração Digital
SSSS – Secondary Security Screening Selection
TAO – Tailored Access Operations
TAR – Territory, Authority, Rights
TIDE – Terrorist Identities Datamart Environment
TOR – The Onion Router
TSA – Transportation Security Administration

SUMÁRIO

INTRODUÇÃO	17
1 SOBERANIA DESTERRITORIALIZADA E AS TRANSFORMAÇÕES DO ESTADO	29
1.1 Os fundamentos do Estado e as crises dos seus fundamentos	33
1.1.1 O Estado Moderno	33
1.1.2 As crises do Estado.....	37
1.2 Globalização e forças centrífugas de poder.....	42
1.2.1 Notas introdutórias sobre a globalização	42
1.2.2 A modificação das capacidades do Estado.....	47
1.2.3 O Estado e a nova configuração da soberania	51
1.3 Transformações do Estado na modernidade líquida.....	58
1.3.1 A modernidade líquida	58
1.3.2 O Estado na modernidade líquida	61
1.4 O Estado na sociedade em rede.....	65
1.4.1 A sociedade em rede	65
1.4.2 O Estado na sociedade em rede.....	68
1.5 As limitações do Estado-nação para controlar os fluxos de dados.....	72
1.5.1 A incapacidade do Estado para controlar os fluxos de dados.....	72
1.5.2 Os limites do marco civil da Internet na proteção da privacidade	74
1.5.3 A CPI da espionagem	78
1.5.4 A rede Tor	82
2 SURVEILLANCE OU VIGILÂNCIA? ESTABELECENDO UM CONCEITO.....	85
2.1 Vigilância ou surveillance? Distinções para uma superação	88
2.1.1 Insuficiências semânticas.....	88
2.1.2 O papel da tecnologia na construção do conceito.....	94
2.2 Para além de um modelo panóptico da surveillance.....	103
2.2.1 O panóptico e o panoptismo	103
2.2.2 A insuficiência do modelo panóptico diante da surveillance.....	107
2.3 Do Big Brother às little sisters	113

2.4 As surveillance assemblages e a dataveillance.....	119
2.4.1 As surveillance assemblages	119
2.4.2 Dataveillance.....	121
2.4.3 Franz Kafka e a metáfora da dataveillance	125
2.5 O poder dos metadados e o anteprojeto de lei de proteção de dados pessoais	127
2.5.1 O que são metadados?	127
2.5.2 O anteprojeto de lei para a proteção de dados pessoais no Brasil e os (meta)dados “anônimos”	130
3 A EXPANSÃO DA SURVEILLANCE NO SÉCULO XXI: O <i>BIG DATA</i> E AS NOVAS RELAÇÕES TEMPO-ESPAÇO	136
3.1 Surveillance após Edward Snowden.....	141
3.1.1 A história envolvendo Edward Snowden	141
3.1.2 Uma tendência a ser seguida?.....	148
3.2 Surveillance como paradigma da sociedade contemporânea.....	151
3.2.1 Notas introdutórias: tendências da <i>surveillance</i> no mundo globalizado ..	151
3.2.2 Globalização, securitização, incerteza e risco.....	154
3.3 Análises probabilísticas e big data	160
3.3.1 Probabilidades e previsão de eventos futuros.....	160
3.3.2 O que é big data?	164
3.3.3 Alguns exemplos das potencialidades probabilísticas do big data.....	167
3.3.4 Sociedade dos sensores	170
3.4 Surveillance e modificações no tempo.....	173
3.4.1 Modelos preditivos e surveillance.....	173
3.4.2 Simulação e pós-panoptismo	180
3.4.3 Surveillance e o novo biopoder	183
3.5 Surveillance e modificação do espaço	187
3.5.1 A desterritorialização das fronteiras	187
3.5.2 As fronteiras como controle de fluxos: o banóptico	191
4 SURVEILLANCE PARA ALÉM DO ESTADO: DEMOCRACIA, DIREITOS HUMANOS E CONSTITUCIONALISMO	195

4.1 Surveillance e democracia.....	199
4.1.1 Democracia, accountability e visibilidade	199
4.1.2 Democracia e pluralismo político: o problema do filtro-bolha	205
4.1.3 Democracia e invólucro digital	213
4.2 Surveillance e direitos humanos.....	217
4.2.1 Notas introdutórias sobre o papel dos Estado na proteção dos direitos humanos violados pela <i>surveillance</i>	217
4.2.2 Surveillance como violadora dos direitos humanos.....	220
4.2.3 O Estado como palco fragilizado na proteção dos direitos humanos.....	228
4.3 Surveillance e constitucionalismo para além do Estado-nação.....	238
4.3.1 Constituição para além do Estado nacional: notas sobre o constitucionalismo societário.....	238
4.3.2 Constitucionalismo híbrido	250
4.3.3 Controle não estatal dos poderes selvagens	253
CONSIDERAÇÕES FINAIS	256
REFERÊNCIAS	272

INTRODUÇÃO

Imagine um sistema de computador que, automaticamente, libera a entrada de um viajante voltando para o seu país através da comparação entre a imagem do seu rosto e um banco de dados. Ou, talvez, outros sistemas similares que detectam eletronicamente placas de veículos roubados e identificam, pelo reconhecimento facial, se o usuário do transporte público é realmente beneficiário da gratuidade legal. Ou, ainda, uma máquina que sabe, mais do que os seus amigos, sobre o seu passado, presente, interesses, angústias e expectativas, ou, até mesmo, que consegue prever parte do seu futuro com grande precisão. Quiçá, um *drone* que, voando a 3.000 metros da superfície, identifica, de forma automática, rostos, comparando-os a uma base de dados para decidir se irá ou não lançar um ataque mortal.

Nada disso faz parte de um texto de ficção. O que, há alguns anos, seriam visões de uma clássica novela orwelliana, hoje são realidades em diversas partes do mundo, inclusive, bem aqui no Brasil. Neste exato momento, uma vasta quantidade de dados está sendo coletados por empresas e governos, cada um deles com o seu propósito, e não há nada as pessoas possam fazer quanto a isso.

A proposta deste trabalho não será explicar qual a solução para todos esses problemas. Muito pelo contrário, afinal, se cumprir com o seu propósito, este texto deixará, ao final, o leitor com mais dúvidas do que possui agora. Este é o objetivo do pesquisador, especialmente nas ciências sociais, que, antes de buscar soluções completas para os problemas, deve estar aberto para a possibilidade de reconhecimento do “novo enquanto novo”.

Assim, embora o problema levantado por esta tese seja respondido ao final, espera-se que ela abra caminhos para novas pesquisas sobre o tema. Não é, portanto, o intuito desta tese fornecer respostas prontas para situações específicas associadas à *surveillance*, uma vez que tais problemas só podem ser analisados em sua concretude espacial e temporal quando, efetivamente, ocorrerem. Ao invés disso, será elaborado o arcabouço teórico pelo qual esses problemas devem ser pensados.

Isso porque, antes de resolver qualquer problema, é necessário compreendê-lo. Qualquer tentativa de suplantar uma adversidade sem entendê-la adequadamente resultará em fracasso. Essa compreensão, contudo, só é possível através de um movimento de abertura em direção ao novo, que, nesse caso, é a tecnologia da

informação. Tema pouco afeito ao direito¹, a tecnologia move-se em uma velocidade distinta daquela a que estão acostumados os juristas. Ela não pode ser ignorada pela pesquisa jurídica em virtude de uma razão essencial: nos últimos tempos, a tecnologia da informação vem revelando aspectos antidemocráticos, além de estar sendo utilizada com o propósito de violar os direitos humanos.

Tendo isto em conta, o problema central desta tese é a necessidade de proteger os direitos afetados pela *surveillance*, considerando que isto não pode ocorrer, exclusivamente, através dos meios de regulação jurídica associados ao Estado, dada a sua impossibilidade de lidar com problemas que escapam à esfera da política e ao *container* territorial, o que torna imprescindível a participação da iniciativa privada nessa discussão.

Diante disso, parte-se da hipótese de que o desenvolvimento da tecnologia da informação e o seu uso para a coleta, transmissão, armazenamento e processamento de informações com impacto direto na vida humana cria uma nova situação de perigo para os direitos humanos. Essas tecnologias têm fomentado mudanças e debates em diversas áreas do conhecimento, o que deve incluir, também, o direito.

Em contrapartida, são muitas as abordagens repetitivas, que se mantêm atreladas à ideia de que a tecnologia da informação tem na violação da privacidade o seu principal efeito danoso e propõem que o recurso à lei é capaz de resolver todos os problemas². Em outras palavras, é possível afirmar que boa parte dessas pesquisas pensa a tecnologia *a partir* do Estado de direito, o que limita a compreensão das perplexidades que ultrapassam os limites do ente estatal. Apesar de ser um importante modelo para proteção de direitos humanos, o Estado-nação é extremamente limitado em determinadas situações ligadas à liquidez e à desterritorialidade³.

¹ Esta grafia com inicial minúscula tornou-se possível em virtude do Acordo Ortográfico de 1990 (Base XIX, art. 1º, alínea “g”).

² Com isso, não se está, por óbvio, criticando os trabalhos que buscam proteger a privacidade por meio da lei do Estado nacional. São trabalhos fundamentais para o universo jurídico e que contribuem muito para o debate. A crítica, aqui, é voltada para aqueles que consideram que esse recurso encerra as discussões sobre o problema.

³ Desterritorialização e desespacialização serão palavras utilizadas no decorrer do trabalho. Com elas, não se quer dar a entender que existem lugares sem território. Busca-se, somente, destacar que a tecnologia da informação possui a tendência de transpor espaços físicos com extrema facilidade, tornando secundária a análise territorial.

O ineditismo da pesquisa fica evidente através de uma busca pela expressão “*surveillance*” no banco de teses da CAPES, que não retorna nenhum resultado para dissertações ou teses das ciências humanas, tampouco nas ciências sociais aplicadas⁴. Essa ausência de resultados é o reflexo da escolha, pelo autor, da expressão no inglês/francês, em vez de utilizar o termo “vigilância”. Tal opção não é apenas uma escolha aleatória de palavras, pois traz uma série de consequências teóricas e denotam o foco de abordagem inédito no cenário jurídico nacional.

Ainda assim, uma busca pela palavra mais comum, “vigilância”, retorna apenas sete resultados dentro da área do direito. A grande maioria deles⁵ não dialogam com o tema desta tese e dizem respeito ao uso de monitoramento eletrônico de apenados. Nos outros dois casos⁶, tratam-se de pesquisas que reforçam a opção teórica pelo uso da palavra *surveillance* ao invés de vigilância. Isto porque são trabalhos que discutem apenas a necessidade de proteção da privacidade e dos dados pessoais, ignorando completamente o problema da democracia e de outros direitos humanos como a igualdade ou a liberdade.

Essa escolha deriva da matriz teórica adotada, qual seja, os *surveillance studies*⁷. Essa corrente das ciências sociais possui como principal expoente, na atualidade, é o sociólogo canadense David Lyon. Ela originou-se ainda nos anos 1980, nos EUA e no Canadá, e, desde então, vem ganhando cada vez mais importância na sociologia mundial. Uma linha de pensamento comum dessa corrente é a convicção de que a coleta, processamento e monitoramento dos fluxos de dados, por não

⁴ Isso não significa, contudo, que um segmento da sociologia nacional não tenha importante papel nesse estudo, pois há considerável produção de sociólogos brasileiros vinculados à matriz teórica dos *surveillance studies*.

⁵ HATA, F.Y.F. Monitoramento eletrônico: aplicação no ordenamento jurídico brasileiro. 01/10/2011. Mestrado. PUC-SP.

CORREA JUNIOR, A. Monitoramento eletrônico de penas e alternativas penais. 01/04/2012. Mestrado. USP.

PINTO, I. E. Monitoramento eletrônico. um caminho para a humanização da pena. 01/08/2012. Mestrado. Universidade Estácio De Sá.

OLIVEIRA, J. R. O monitoramento eletrônico na justiça criminal: um estudo sobre a implantação deste mecanismo de controle punitivo no Brasil. 01/03/2011. Mestrado. PUC-RS.

MIRANDA, R. E. O Estado de exceção cotidiana e a cultura do controle do crime. 01/06/2011. Mestrado. UFSC.

⁶ PINTO, A. E. M. Os efeitos da cidade digital: direito à privacidade e à liberdade de informação. Doutorado. UERJ.

ZANON, J. C. Direito à proteção dos dados pessoais. 01/10/2012. Mestrado. PUCSP.

⁷ Cumpre salientar que, com o intuito de possibilitar a fluidez na leitura, todas as citações em língua estrangeira – à exceção das tabelas – serão livremente traduzidas no corpo deste trabalho. Em tais casos, constará, como nota de rodapé, a transcrição do texto original no idioma da obra consultada. Além disso, sempre que a palavra *surveillance* for utilizada no original com o sentido que se pretende dar neste trabalho, o texto traduzido irá manter a grafia original entre colchetes.

estarem fundados em critérios democráticos de uso, são, frequentemente utilizados sem a necessária preocupação com a proteção dos direitos humanos.

Como resultado, essa linha de pesquisa entende que ocorre a perpetuação de situações de visibilidade assimétrica, as quais adquirem especial relevância em virtude do caráter fluido, descentralizado e desespacializado dos fluxos de dados globais. Por serem “descolados” das estruturas físicas do olhar (Michel Foucault), do capital (Karl Marx) e da burocracia (Max Weber), esses fluxos de dados ultrapassam os tradicionais modelos teóricos de análise do poder.

Explicitada a matriz teórica, passa-se à elucidação do objetivo geral desta tese, que é elaborar a categoria da *surveillance*, inédita no Brasil, e compreendê-la como uma característica típica da modernidade líquida. Com isso, será possível desenvolver o arcabouço teórico para proteger os direitos humanos e a democracia das violações patrocinadas pelos fluxos globais de dados. A desterritorialidade e a fluidez – características e, simultaneamente, efeitos das tecnologias da informação no século XX – exigem novos mecanismos de controle jurídico capazes de abstrair o elemento territorial e central do Estado-nação.

No que se refere aos objetivos específicos, é importante elencar os seguintes:

- a) Analisar a relação entre Estado, direito e fluxos de dados globais no contexto da modernidade líquida, especialmente as transformações sofridas pelo Estado e a crescente importância dos atores privados dentro da proposta da sociedade em rede.
- b) Demonstrar a insuficiência das soluções jurídicas pensadas na modernidade para lidar com os multifacetados e desterritoriais fluxos de dados, explicando a necessidade, mas também a insuficiência, da utilização das leis estatais na proteção dos direitos humanos violados pela *surveillance* em virtude da natureza rizomática do poder nas redes de dados.
- c) Construir um conceito de *surveillance* diferenciado da tradicional percepção da vigilância como forma de ultrapassar – ainda que sem ignorar – os limites teóricos comumente associados ao tema, especialmente as ideias de panopticismo, do *Big Brother* e de que se está diante de um cenário distópico, de algo inerentemente negativo cujo único objetivo é o controle.

- d) Investigar as tendências de expansão da *surveillance* no século XXI, sua relação com o desenvolvimento tecnológico e a criação de uma sociedade securitizada.
- e) Questionar como o espaço e o tempo são modificados pelos fluxos globais de dados, levando-se em conta os efeitos da globalização e as novas relações entre passado e futuro criadas por bancos de dados que nunca esquecem, bem como pela aplicação de técnicas estatísticas de previsão de comportamentos na criação de um futuro já pronto, no qual se busca concretização daquilo que será denominado “demônio de Laplace”.
- f) Analisar as relações assimétricas de visibilidade e os seus efeitos na democracia, em virtude da ausência de *accountability* das técnicas da *surveillance* e pela sua opacidade em relação aos indivíduos, cujos detalhes se movimentam livremente em uma rede descentralizada de dados.
- g) Demonstrar a relação entre a *surveillance* e a violação dos direitos humanos para além das perspectivas tradicionais, explicando como os fluxos globais de dados alteram, em razão do uso avançado dos metadados, o próprio conceito do que é informação privada. Além disso, será elucidada a insuficiência do debate sobre a privacidade, argumentando como, ironicamente, as legislações de proteção de dados pessoais acabam por normalizar a violação de outros direitos humanos.
- h) Buscar alternativas para o problema de violação da democracia e dos direitos humanos causadas pela *surveillance* dentro dos moldes da teoria sistêmica, especialmente através das lutas pela constitucionalização fora das estruturas tradicionais (territoriais) do Estado-nação e da inserção, nesse debate, de todos os atores capazes de violar direitos humanos, sejam eles públicos ou privados, nacionais ou transnacionais.

A estratégia metodológica a ser utilizada durante a abordagem do problema possui caráter fenomenológico-hermenêutico (HEIDEGGER, 1999; STRECK, 2014) e

transdisciplinar, tendo em vista a abrangência e complexidade dos conhecimentos relacionados ao tema estudado.

É necessário, ainda, deixar claro que não será realizada uma análise “externa”, como se o sujeito e objeto estivessem cindidos e dispersos no mundo. Muito pelo contrário, o pesquisador está necessariamente relacionado ao objeto de estudo, com ele interage e sofre os efeitos dos seus resultados.

Assim, não se trata de uma investigação alheia ao investigador, pois ele está no mundo onde a pesquisa será desenvolvida. Essa vinculação entre pesquisador e objeto de pesquisa, contudo, não significa a ausência de critérios para guiar o trabalho, o que impõe a adequação entre métodos e fases da pesquisa.

Uma forma de compreender esse mundo no qual a pesquisa está inserida é pela utilização da literatura. Por essa razão, o recurso a algumas obras literárias será realizado, de modo pontual, como forma de oferecer uma explicação alternativa para a realidade do pesquisador, ou seja, oferecendo a possibilidade de uso de metáforas capazes de explicar um fenômeno social fora dos tradicionais moldes do direito.

Ainda, necessidade de trabalhar-se com dados particulares para alcançar uma formulação geral, característica da fase de investigação, impõe uma abordagem eminentemente indutiva. A estruturação dos conhecimentos alcançados –e, portanto, a explicitação dos resultados da pesquisa– por sua própria natureza, exige uma abordagem de natureza principalmente dedutiva. Essa divisão, contudo, ao invés de limitar os rumos do trabalho, serve como orientadora no agir do pesquisador.

O método de procedimento a ser utilizado será o monográfico, no sentido de que a abordagem trata de um tema específico e bem delimitado, opondo-se a formas “manualescas” ou “enciclopédicas”. Muito embora a elaboração de uma tese monográfica não implique no abandono da perspectiva panorâmica, há que se reconhecer as diferenças entre usar um panorama como pano de fundo, o que se pretende, e elaborar um quadro panorâmico. A opção metodológica justifica-se pelo entendimento de que “quanto mais se restringe o campo, melhor e com mais segurança se trabalha” (ECO, 2007, p. 10). No que concerne à técnica de pesquisa, utilizar-se-á prioritariamente a consulta de documentação indireta, especialmente a pesquisa bibliográfica nacional e estrangeira.

Tendo sido analisados os pressupostos teóricos e metodológicos que permeiam esta tese, é imprescindível demonstrar a sua estrutura, o que facilitará a

compreensão do texto como um todo integrado e coeso. Dessarte, o primeiro capítulo demonstrará detalhes sobre as transformações do Estado em virtude da desterritorialização que marca a atual quadra da história. Para tanto, irá analisar os pressupostos que permitiram o surgimento do Estado-nação (1.1.1), bem como as crises que esse modelo de organização política vem enfrentando, nos moldes propostos por Jose Luis Bolzan de Moraes (1.1.2).

Ainda, analisará a globalização, um dos motivos para essa crise (1.2.1) como forma de compreender quais os seus efeitos sobre as capacidades do Estado no mundo globalizado, caracterizado pela natureza centrífuga do poder (1.2.2). Diante desse cenário global, que transforma o território em elemento secundário de análise, o Estado acaba sofrendo modificações, reconfigurando a sua própria soberania (1.2.3), visto que fundamentada, dentre outros, nos limites do território.

Essas transformações fazem parte de um contexto de extrema flexibilidade nos fluxos globais de conhecimento, capital, poder e, para fins deste trabalho, informações. Essa modernidade líquida será estudada (1.3.1), assim como os seus efeitos sobre o Estado (1.3.2). Da mesma forma, será vista como a ideia de que se vive hoje em uma sociedade em rede (1.4.1) que afeta o Estado (1.4.2), deixando de ser a principal força para ser apenas um dos nós na topologia da rede.

Diante desse contexto globalizado, líquido e caracterizado pela organização do poder em redes extremamente dinâmicas, será demonstrado como o Estado é incapaz de controlar os fluxos de dados globais (1.5.1). Como forma de ilustrar o problema, serão analisados três exemplos: o primeiro versará sobre os limites de uma legislação, como é o caso do marco civil da Internet, na proteção da privacidade (1.5.2); o segundo, sobre o caso da CPI da espionagem (1.5.3), que tentou, sem sucesso, investigar os eventos de coleta massiva de dados por parte das agências de segurança dos Estados Unidos e, o terceiro demonstrará que nem mesmo essa superpotência militar e tecnológica consegue responder, efetivamente, à liquidez das tecnologias da informação, como ficará claro com o exemplo da Rede Tor (1.5.4).

Para compreender o fenômeno da *surveillance*, será necessário, primeiro, demonstrar quais os motivos para a adoção da palavra em inglês na construção dessa categoria (2.1.1), o que possibilitará ver o seu estreito e inseparável vínculo com a tecnologia da informação (2.1.2). Como imagem mental mais comum quando o assunto é coleta de dados, será feita uma análise sobre o modelo panóptico e o

panoptismo (2.2.1), ainda que seja, logo em seguida, demonstrada a causa pela qual ele é insuficiente para compreender o fenômeno da *surveillance* (2.2.2), especialmente porque o que Foucault fez em “*Vigiar e punir*” foi uma análise historiográfica das relações de poder entre os séculos XVIII e XIX, não tendo sido seu objetivo analisar o século XX.

Outra imagem mental muito comum ao tema é a ideia do *Big Brother*, famosa após George Orwell desenhar o cenário de um futuro distópico, em que um Estado totalitário controla, por meio da coação, todos os aspectos da vida dos indivíduos. Por essa razão, será analisado esse modelo, verificando sua aplicabilidade ao século XXI, em um mundo onde a sedução do consumo substitui a ameaça constante, e o Estado totalitário orwelliano é suplantado por uma infinidade de empresas privadas, as *little sisters* (2.3).

Panóptico e Big Brother são as metáforas mais comuns quando o assunto é vigilância. No entanto, embora possibilitem destacar importantes aspectos desse fenômeno, os modelos são limitados no que diz respeito às modernas técnicas de coleta e processamento de dados. Em virtude disso, será trazido uma nova maneira de pensar a *surveillance* de modo adequado ao século XXI, ou seja, a partir da ideia de *assemblage*, como forma de analisar a convergência dos fluxos oriundos de sistemas de dados diversos (2.4.1).

Essas *assemblages* dependem de fluxos discretos de dados que, combinados, podem ser extremamente reveladores. Por isso, será analisado o conceito de *dataveillance* (2.4.2). Retomando a literatura, será demonstrado por quais motivos Franz Kafka – na sua obra “*O processo*” – é mais condizente com a realidade atual da *surveillance* (2.4.3) do que os modelos tradicionalmente utilizados.

Um dos pilares das *surveillance assemblages* e da *dataveillance* é a capacidade que sistemas eletrônicos possuem para gerar dados sobre todas as transações que ocorrem em meio digital, ou seja, metadados. Por isso, será explicado o que são metadados (2.5.1) e qual a importância da sua compreensão para entender os limites da ideia de “dados anônimos” do anteprojeto de lei para proteção de dados pessoais no Brasil (2.5.2).

Será demonstrado que a lei precisa estar minimamente adequada às tecnologias existentes, sob o risco de ser ainda mais prejudicial que a sua própria inexistência. Afinal, caso permaneça sem paralelo com a realidade tecnológica, a

legislação criará a falsa sensação de que um direito está protegido sem que ele realmente esteja.

Para tanto, é imprescindível que o direito compreenda, da melhor maneira possível, os detalhes do funcionamento da *surveillance* no século XXI, o que será feito no terceiro capítulo, que analisará a expansão da *surveillance* na atualidade e os efeitos que o *big data* possui nas relações do tempo e do espaço. Para alcançar tal objetivo, será necessário, inicialmente, fazer um retorno ao caso que ficou extremamente famoso em 2013, quando Edward Snowden, um analista da NSA, divulgou os detalhes de um sistema de análise massiva de dados usado pelo governo dos EUA (3.1.1).

Com base nas revelações de Snowden, serão analisados exemplos de outros países que seguiram a tendência imposta pelos EUA. Com a justificativa de segurança nacional e combate ao terrorismo, esses países tentam “apreender” os dados dentro das suas fronteiras, o que, como será visto, é extremamente problemático e incapaz de proteger direitos humanos (3.1.2).

Todos esses sistemas, contudo, revelam que a *surveillance* é um paradigma da sociedade contemporânea (3.2). Nesse sentido, serão explicitadas as tendências da *surveillance* no mundo globalizado (3.2.1) e a sua relação com o movimento de securitização (3.2.2), explicado a partir da ideia de manutenção do estado de exceção como ferramenta para combater o medo líquido, especialmente aquele ligado ao terrorismo.

Esse medo líquido gera uma busca incessante pela prevenção antes que os eventos aconteçam, o que é um dos principais “motores” da *surveillance* no século XXI. Como se trata de um trabalho jurídico, será necessário fazer esclarecimentos sobre alguns conceitos básicos de probabilidade antes de demonstrar como esses sistemas são usados para prever o futuro (3.3.1). Tais análises dependem, sempre, de uma quantidade elevada de dados, o que traz a necessidade de esclarecer o que é o *big data* (3.3.2) e como ele funciona em termos práticos (3.3.3).

Essa quantidade de dados torna-se possível em virtude da proliferação de sensores, ou seja, dispositivos capazes de analisar alterações no ambiente. Tais sensores não precisam ser dispositivos com essa única finalidade, já que elementos ordinários do cotidiano – telefones celulares, computadores, carros e até mesmo microchips implantados em animais – podem exercer a função de sensor, de modo

que será explicada a ideia de que se vive em uma sociedade dos sensores (3.3.4), capazes de gerar uma “onisciência diacrônica”.

As análises estatísticas baseadas no *big data* possuem o objetivo de apreender o passado, analisar o presente e prever o futuro, ou seja, alterar a percepção sobre o tempo. Os modelos preditivos permitem que, com base na análise do presente, preveja-se também o futuro (3.4.1). Se, como afirma Gilles Deleuze, estamos vivendo em uma época de crise generalizada de todos os meios de confinamento em que poderia ser aplicado o panóptico, os modelos preditivos permitem estabelecer que o novo paradigma pós-panóptico é baseado na ideia de simulação (3.4.2).

Além disso, será demonstrado que, se, por um lado, a análise de Foucault sobre o panóptico de Bentham não foi idealizada para o mundo contemporâneo, a sua teoria sobre o biopoder é extremamente útil, embora necessite de modificações para poder contribuir para a compreensão da *surveillance* na era do *big data* (3.4.3). O biopoder, agora híbrido, congrega uma diversidade enorme de tecnologias distintas, sempre com a finalidade de identificar e rastrear indivíduos e grupos, bem como criar modelos preditivos de comportamento e risco.

O tempo, porém, não é o único afetado pela *surveillance*. Por esse motivo, será demonstrado que o espaço também sofre os seus efeitos (3.5). Uma das formas de isso acontecer se dá através das mudanças que a desterritorialização das fronteiras (3.5.1), proporcionalizada pelos fluxos de dados, exerce sobre a liberdade. O “lugar” onde as portas de um país são abertas ou fechadas não corresponde, necessariamente, aos limites do território desse local. Logo, aqueles que se enquadram no “modelo” de viajante desejável acabam tendo a ideia de que a globalização está, realmente, acontecendo e o trânsito de pessoas está cada vez mais fácil. Por outro lado, as minorias e os indivíduos que não se enquadram naquele “modelo” encontram cada vez mais dificuldade para transitar livremente. Para essas pessoas, os “muros” das fronteiras estão cada vez mais altos e aparecem antes mesmo que saiam do seu país de origem, o que ficará claro com a ideia de banóptico (3.5.2).

O último capítulo irá tratar da natureza antidemocrática da Internet e da *surveillance*, bem como demonstrar que as violações dos direitos humanos não podem ser protegidas pelos modelos constitucionais centrados em um Estado. Para

tanto, será observada a relação entre a *surveillance* e as ideias de visibilidade e *accountability*, tão necessárias para a democracia (4.1.1). Com efeito, a principal característica dos regimes de visibilidade proporcionada pela *surveillance* nas sociedades contemporâneas é a incerteza gerada pelo desconhecimento sobre quais as regras a serem usadas para coletar os dados dos grupos e indivíduos e tratar deles. O risco para a democracia, nesse caso, está relacionado ao fato de que a *surveillance* torna visível uma quantidade maior de dados das pessoas e, ao mesmo tempo, não oferece *accountability* sobre o uso desses dados.

Outro risco para a democracia está associado à ideia de filtro-bolha e os seus efeitos deletérios para o pluralismo político e para o desenvolvimento de uma esfera pública livre e diversa (4.1.2). Isso em razão de a personalização viabilizada por algoritmos preditivos permitir que indivíduos vivam em universos paralelos, porém separados. A democracia, no entanto, só funciona quando os participantes conseguem pensar fora das suas esferas individuais, o que se torna extremamente difícil sem uma visão de mundo compartilhada, conhecendo o outro e as suas necessidades.

Similar ao filtro-bolha, a ideia dos invólucros digitais e os seus efeitos para a democracia serão trabalhadas (4.1.3) em virtude da colonização da Internet pelos detentores do poder, o que acontece por meio da apropriação, cada vez maior, dos espaços digitais por empresas de tecnologia. A assimetria nas relações de poder, a ausência de *accountability* e de transparência permitem que o ambiente virtual seja antidemocrático.

Sobre o tema dos direitos humanos violados pela *surveillance* (4.2), será feita uma introdução (4.2.1), explicando as razões por se acreditar que teorias sistêmicas sejam mais adequadas para a proteção daqueles direitos. Em seguida, será demonstrado como a *surveillance* viola direitos humanos, em especial a igualdade e a privacidade (4.2.2). Já que um dos temas mais interessantes – e menos explorados – dessa discussão é a capacidade que os sistemas de computadores, ao exercerem, com maestria, a tarefa de categorização de dados em grupos, permitem associar a *surveillance* à violação da igualdade. Os problemas para a privacidade, por outro lado, embora sejam, amplamente, discutidos em monografias especializadas, irão adquirir novos desenhos, o que permitirá realizar análises diferentes daquelas que já existem, especialmente através da ideia de mercantilização da privacidade.

Com base nessas violações, ficará evidente que o Estado agora é palco fragilizado na proteção dos direitos humanos (4.2.3), o que se deve, especialmente, aos seus limites de atuação ligados à territorialidade e ao sistema da política. Por essa razão, as tentativas de “subsumir” as novas tecnologias aos direitos elaborados através de Estados possuem sucesso limitado – ainda que sejam imprescindíveis.

Tudo isso culmina com um dos mais problemáticos pontos na relação entre *surveillance* e democracia: o papel fundamental do poder privado no desenvolvimento e utilização de mecanismos de gerenciamento de dados. Nesse sentido, será demonstrado que somente a ideia de uma constituição para além do Estado-nação poderá proteger, adequadamente, os direitos humanos violados pela *surveillance* (4.3.1), o que será feito com o suporte teórico da teoria sistêmica, em especial de Gunther Teubner.

Distanciar o vínculo existente entre o constitucionalismo e a política, contudo, não significa o fim do constitucionalismo político tradicional, tampouco do Estado, o que faz surgir a necessidade de discutir o constitucionalismo híbrido (4.3.2). Essa forma de organização política deve ser vista como condição de possibilidade para a inserção dos seres humanos na “esfera global”, de modo que não exista nenhuma contradição entre o desenvolvimento de estruturas globais não estatais e a permanência do Estado nacional.

Essa permanência do Estado, no entanto, não impede que sejam feitas críticas àquelas tentativas de controlar a natureza selvagem dos poderes sempre por intermédio do retorno ao ente estatal. Por isso, demonstrar-se-á como os poderes selvagens associados à *surveillance* precisam de controles não estatais (4.3.3), o que irá possibilitar que o direito constitucional tenha capacidade de controlar as tendências colonizadoras – selvagens – dos sistemas sociais.

Uma teoria do Estado democrático de direito que se queira comprometida com os direitos humanos deve possibilitar a compreensão dos novos poderes que colocam a democracia em perigo. Por isso, este trabalho irá demonstrar a necessidade de sair um pouco da zona de conforto dos juristas para, compreendendo adequadamente o fenômeno da *surveillance*, proteger a democracia e os direitos humanos.

1 SOBERANIA DESTERRITORIALIZADA E AS TRANSFORMAÇÕES DO ESTADO

*One world, it's a battleground
One world, and we will smash it down
One world ... One world
Invisible transfers, long distance calls
Hollow laughter in marble halls
Steps have been taken, a silent uproar
Has unleashed the dogs of war*

(Pink Floyd – The Dogs of War)

Em um mundo que se diz unificado, sem fronteiras, conectado por fluxos invisíveis, como ilustrado no trecho de música acima, a discussão sobre a crise do Estado⁸ torna-se um dos principais focos de estudo sobre essa modalidade de organização política surgida na Era Moderna.

No decorrer da história, o Estado se viu sujeito aos influxos dos diversos sistemas sociais. Isso exigiu mudanças na sua formatação, o que, por um lado, contribuiu para a sua consolidação e, por outro, demandou adaptações e transformações. É nesse contexto que ocorre o debate sobre as crises estatais. Por isso, a ideia de crise não está relacionada à extinção do Estado, mas ao conjunto de fenômenos que englobam as mudanças que ocorrem desde o seu surgimento.

Tendo em vista tal aspecto, este capítulo analisará os fundamentos do Estado, ou seja, aquilo que permitiu o seu surgimento na Idade Moderna. Fruto dos valores da modernidade, o Estado é, por excelência, o mecanismo político institucionalizador do poder. Isso porque, por meio da monopolização da força, se possibilitou a transferência das relações de dominação para um quadro geral e impessoal, cuja submissão exclusiva era imposta aos cidadãos.

Porém, essa mesma estrutura política vem sofrendo modificações, o que permite o questionamento a respeito das crises dos seus fundamentos. Por isso, será realizada, também, uma análise das crises do Estado a partir do marco teórico do modelo de crises desenvolvido por Jose Luis Bolzan de Moraes (2012).

Dentre tais fenômenos, o mais relevante está relacionado às mudanças na territorialidade proporcionadas pela globalização. Esse fenômeno acarreta a alteração do lugar de manifestação do poder e das fontes produtoras de direito. Isso tem, como

⁸ A crise do Estado é o principal tema de estudo da Rede de Pesquisa Estado & Constituição, composta por diversas universidades do mundo inteiro e coordenada pelo Prof. Dr. Jose Luis Bolzan de Moraes. Maiores detalhes sobre a rede e os seus eventos podem ser visualizados no seu *site*. Disponível em: < <http://www.repec.com.br> >. Acesso em: 26 mar. 2016.

consequência direta, a mudança na própria ideia de Estado, uma vez que, estritamente, vinculado a um território.

O problema é que a maior parte das análises sobre globalização tende a colocar o Estado no papel de vítima de um processo de desconstrução das suas estruturas, o que não é, necessariamente, verdade. Ainda, costumam dar ênfase aos movimentos obviamente globalizadores, sem atentar para as sutilezas dos microprocessos de construção e desconstrução do espaço nacional, estes muito mais sutis, caóticos e frequentemente multifacetados. O enfraquecimento do Estado não significa o seu fim, pois, conforme será constatado, não existe contradição entre a sua crise e a sua permanência. Isso porque, no contexto da multiplicação dos poderes selvagens (FERRAJOLI, 2011a), a existência de Estados fracos é interessante para a expansão dos poderes globais, que transpassam as estruturas estatais tradicionais.

Conforme será visto, a globalização é um fenômeno complexo, de múltiplas vias, ou seja, composto por microprocessos que, algumas vezes, resultam na desnacionalização das estruturas do Estado e, em outras, proporcionam o seu fortalecimento. É por essa razão que Saskia Sassen afirma que “a transformação que estamos vivenciando é uma arquitetura complexa com muitos elementos distintos, dos quais somente alguns podem ser facilmente codificados como globalização” (SASSEN, 2006, p. 1)⁹.

Diante desse contexto, será visto que Saskia Sassen (2006, 2007) critica os conceitos tradicionais de globalização, pois entende que esse fenômeno envolve, além do aumento da interdependência global, a produção de estruturas espaço-temporais diferentes daquelas comumente associadas ao Estado-nação. Sob tal aspecto, será possível falar na modificação das capacidades do Estado como decorrência da globalização.

Como resultado, será analisado o papel do Estado diante da nova reconfiguração mundial da soberania, decorrente tanto da modernidade líquida (Zygmunt Bauman) quanto da sociedade em rede (Manuel Castells). Nesse contexto, além da análise das referidas propostas teóricas, será analisado o papel do Estado nessas novas realidades que passam a valorizar, cada vez mais, a velocidade e a mutabilidade, elementos tradicionalmente contrários à ideia de Estado-nação, vez que

⁹ No original: “The transformation we are living through is a complex architecture with many distinct working elements, only some of which can easily be coded as globalization.”

este está vinculado à ideia da modernidade sólida, dependente de um território e de um espaço delimitado.

Sob essa ótica, o surgimento das novas tecnologias da informação, inquestionavelmente, coloca em xeque a ideia de efetividade do atual modelo de Estado, uma vez que tais tecnologias desestabilizam as tradicionais hierarquias associadas à modernidade sólida. Embora continuem existindo em diversos contextos da vida social – afinal, o surgimento de novos problemas não acaba com os antigos – , essas estruturas de poder da Era Moderna possuem baixa capacidade de controlar os fluxos globais de dados do mundo contemporâneo.

Por outro lado, é equivocado fazer afirmações no sentido de que as tecnologias da informação, especialmente a Internet, estão imunes a qualquer tipo de controle (SASSEN, 2006, p. 331), porque muitos Estados, especialmente os tecnologicamente mais desenvolvidos, participam, ativamente, no desenho da arquitetura de *hardware* e *software* da tecnologia. Além disso, uma grande fonte de regulamentação dos meios digitais são os interesses privados, especialmente os das grandes empresas de tecnologia, que modelam, conforme os seus interesses, os avanços e padrões técnicos.

Afinal, existem, sim, estruturas regulamentadoras da Internet. É o caso, por exemplo, da ICANN – sigla para “*Internet Corporation for Assigned Names and Numbers* –, responsável por gerenciar toda a estrutura de alocação de endereços IP e registro de domínios de Internet. No caso dos domínios terminados em “.br”, existe o Comitê Gestor da Internet no Brasil, criado pela Portaria Interministerial MC/MCT nº 147/95, alterada pelo Decreto nº 4.829/03.

Ainda assim, as categorias existentes na teoria do Estado – bem como do direito internacional – são incapazes de lidar com o surgimento de poderes não estatais com capacidade de ação transnacional. Por isso, este capítulo analisará como ocorrem tais transformações nos pressupostos do Estado, sobretudo, em virtude dos influxos da globalização e da desnacionalização de suas capacidades específicas, especialmente diante do contexto daquilo que se convencionou chamar de modernidade líquida (BAUMAN, 2001).

As limitações espaço-temporais do Estado não parecem ser capazes de lidar com os problemas que afetam o mundo, cada vez mais globalizado e “líquido”,

situação que já pode ser vista no direito ambiental¹⁰ e, para objetivos desta pesquisa, nos fluxos de informações pessoais oriundos dos avanços das técnicas da *surveillance*.

Essas limitações ficam claras quando, por exemplo, por meio de uma tecnologia relativamente simples, se consegue ignorar uma decisão judicial sobre o direito ao esquecimento¹¹ da mais alta Corte do maior bloco mundial. Para testar essas limitações, o desenvolvimento desta tese incluiu uma tarefa simples, porém reveladora. Utilizando um protocolo de segurança chamado VPN – *Virtual Private Network* –, foi possível realizar busca no *Google* como se um terminal estivesse localizado na União Europeia, mesmo estando ele no Brasil.

Posteriormente, foi feita uma pesquisa construída pelas palavras “Mario Costeja Gonzàlez hemeroteca lavanguardia”¹². Quando feita por um usuário brasileiro, o primeiro resultado é aquele que o Tribunal Europeu ordenou que fosse removido dos mecanismos de buscas. No entanto, quando o VPN “simula” que o usuário está dentro da União Europeia, o número de resultados diminui, o endereço proibido não é mostrado e obtém-se uma mensagem informando que o resultado foi modificado por decisão judicial¹³. Como o inverso também é possível – um usuário europeu passar como se estivesse no Brasil –, isso demonstra que, com alguns cliques, uma tecnologia relativamente simples consegue ultrapassar os limites do controle moldado na territorialidade do Estado-nação ou de uma estrutura dela derivada, como no caso do tribunal comunitário.

Não se trata de excluir o papel das estruturas públicas estatais na proteção dos direitos humanos, mas de ressaltar a necessidade de adição de novas respostas para problemas igualmente novos, que não podem ser pensados somente a partir do

¹⁰ A dificuldade do Estado-nação em lidar com fenômenos “descolados” do espaço não se restringe à tecnologia da informação. Nesse sentido, veja-se o exemplo da questão ambiental, analisada por Jose Luis Bolzan de Moraes (2011, p. 75), Leonel Severo Rocha (2009, p. 40) e Wilson Engelmann (2011, p. 315).

¹¹ Em 2014, um cidadão espanhol conseguiu que o Tribunal Europeu reconhecesse o que ficou conhecido como “direito ao esquecimento”. Conforme a decisão daquela Corte, os cidadãos da União Europeia têm direito de requisitar a remoção dos seus nomes dos resultados dos mecanismos de busca como o *Google* e o *Bing*. Sobre este evento, ver a matéria de Ashifa Kassam para o jornal *The Guardian*. Disponível em: < <http://surveillance.es/21> >. Acesso em: 27 mar. 2016.

¹² Trata-se do caso do direito ao esquecimento. Segundo a decisão do Tribunal Europeu, deveriam ser removidos do *Google* alguns resultados no site da hemeroteca do jornal “*La Vanguardia*”, relativos ao espanhol “Mario Costeja Gonzàlez”. O site proibido pode ser livremente acessado por quem dispõe do link, mesmo na União Europeia. Disponível em: < <http://surveillance.es/20> >. Acesso em: 27 mar. 2016.

¹³ “Es posible que algunos resultados se hayan eliminado de acuerdo con la ley de protección de datos europea”

direito estatal caso se deseje garantir a efetividade dos direitos humanos, em especial da privacidade e da igualdade. Para enfrentar o problema da falta de participação democrática no fenômeno representado pela *surveillance* e nos critérios de obtenção, utilização e classificação das informações coletadas, torna-se imprescindível sua invasão pela democracia.

Ao final, serão demonstradas as limitações do Estado-nação para controlar os fluxos de dados, trazendo três exemplos específicos. O primeiro envolverá as limitações do marco civil da Internet – lei nº 12.965/2014 –, com foco nas limitações de mecanismos territoriais como a lei estatal para proteger os direitos humanos violados por poderes selvagens globalizados. O segundo exemplo demonstrará os problemas relacionados à falta de compreensão do paradigma da *surveillance* pela CPI da espionagem e as consequências desse equívoco. O terceiro caso demonstrará a dificuldade que até mesmo os maiores Estados do mundo – como é o caso dos EUA – enfrentam ao se depararem com tecnologias descentralizadas e baseadas em criptografia forte, como é o caso da rede Tor.

1.1 OS FUNDAMENTOS DO ESTADO E AS CRISES DOS SEUS FUNDAMENTOS

1.1.1 O Estado Moderno

Antes de proceder a uma análise da crise do Estado, é imprescindível entender à qual entidade se está fazendo referência. Para tanto, deve-se situar no espaço e no tempo o surgimento dessa forma de organização do poder.

Um interessante conceito para “Estado” é dado por Anthony Giddens. Para ele, o Estado é

[...] um conjunto de formas institucionais de governança que mantêm o monopólio administrativo sobre um território com limites demarcados (fronteiras), seu domínio é sancionado pela lei e pelo controle direto dos meios de violência interna e externa (GIDDENS, 1985, p. 121)¹⁴.

Por sua vez, em outra obra, o mesmo autor informa que o Estado-nação é “a combinação de uma grande comunidade (nação) e uma forma territorial e política

¹⁴ No original: “[...] is a set of institutional forms of governance maintaining an administrative monopoly over a territory with demarcated boundaries (borders), its rule being sanctioned by law and direct control of the means of internal and external violence.”

(Estado), criando uma entidade cultural e política, agora a ‘unidade de sobrevivência’ mais difundida pelo mundo” (GIDDENS, 2014, p. 5045)¹⁵.

A capacidade de organização administrativa e poder bélico para governar, efetivamente, o território somente ganhou força na Idade Moderna. Por isso, dirão inúmeros livros de teoria do Estado, essa forma de organização política surgiu a partir da superação da fragilidade do modelo político da Idade Média e do desenvolvimento de três pressupostos: território, povo e governo. Tanto é que foi somente na Idade Moderna que a palavra “Estado” passou a ganhar popularidade no sentido de “[...] máxima organização de um grupo de indivíduos sobre um território em virtude de um poder de comando [...]” (BOBBIO, 2007, p. 64).

Ampliando o debate bobbiano sobre a continuidade ou a descontinuidade do Estado, Jose Luis Bolzan de Moraes e Lenio Streck adotam a tese da descontinuidade. Para eles,

o Estado Moderno como algo novo insere-se perfeitamente em uma descontinuidade histórica, isso porque um dos maiores argumentos a confirmar tal tese é de que é o processo inexorável da concentração do poder de comando sobre um determinado território bastante vasto, que acontece através da monopolização de alguns serviços essenciais para a manutenção das ordens interna e externa, tais como a produção do direito através da lei, que, à diferença do direito consuetudinário, é uma emanação da vontade do soberano, e do aparato coativo necessário à aplicação do direito contra renitentes, bem como através do reordenamento da imposição e do recolhimento fiscal, necessário para o efetivo exercício dos poderes aumentados (BOLZAN DE MORAIS e STRECK, 2007, p. 40).

Segundo os referidos autores, três características principais serviram para diferenciar o modelo político surgido na segunda metade do século XV. A primeira delas é a autonomia e a supremacia do poder estatal. A segunda é a diferenciação entre as esferas pública (Estado) e privada (sociedade civil)¹⁶. A terceira característica diferenciadora utilizada pelos citados autores é a mudança do fundamento do poder da propriedade para o monarca, representante da soberania estatal (BOLZAN DE MORAIS; STRECK, 2007, p. 39-40).

No mesmo sentido, Jacques Chevallier explica que o surgimento do Estado foi fruto dos valores da modernidade, em especial do culto da razão e do primado do

¹⁵ No original: “The combination of a large community (nation) and territorial, politica form (state), creating a cultural-political entity, now the most widespread ‘survival unit’ across thr world.”

¹⁶ Para uma análise percuciente da formação da esfera pública burguesa, ver (HABERMAS, 2003).

indivíduo. Assim, o Estado é o artefato político que institucionaliza o poder, pois transfere as relações de dominação para um quadro geral e impessoal, que exige submissão exclusiva dos cidadãos. Isso porque a cidadania excluiu, na época, outras espécies de relações de poder paralelas.

Ainda, o surgimento do Estado proporcionou a monopolização da força coercitiva e a consagração da unicidade da esfera pública distinta do resto da sociedade. “Por esses motivos”, diz Chevallier, “a construção do Estado aparece bastante indissociável de uma modernidade da qual ela é, por vezes, reflexo e vetor” (CHEVALLIER, 2009, p. 15).

Um dos principais resultados das mudanças no modo como se exerce o poder é a sua despersonalização. Com sua institucionalização, o poder deixa de ser titularidade de uma casta de indivíduos e passa para o Estado, ainda que este fosse identificado com a figura do monarca. Assim, desenvolveu-se o Estado absolutista, primeira expressão do Estado moderno. Ao concentrar todo o poder nas mãos do monarca, o Estado absolutista possibilitou a transição do feudalismo para o Estado moderno, uma vez que garantiu a unidade do território, elemento central do Estado.

Em sentido contrário ao defendido pelos autores até agora referidos, Saskia Sassen (2006, p. 27)¹⁷ discorda da interpretação de que existe uma descontinuidade entre o surgimento do Estado e o período medieval anterior. Ao partir da análise dos três elementos, que entende como essenciais para a sua obra (território, autoridade e direito), Sassen conclui que “[...] a noção complexa e abstrata de autoridade legítima da soberania nacional territorial não representa uma inovação radical da ordem pós-feudal” (2006, p. 28)¹⁸.

Segundo ela, o Estado moderno é apenas uma *assemblage* histórica que denota uma configuração específica de três elementos: território, autoridade e direito (TAR, na sigla em inglês). Essa *assemblage* evoluiu de tal modo que possibilitou a concentração pelo Estado da maior fatia possível dos TAR. Embora, em nenhum momento, frise-se, o Estado tenha agregado a totalidade desses três elementos, visto que sempre encontrou concorrência, os TAR acabaram por se tornar associados,

¹⁷ Segundo Bobbio (2007, p. 69), o debate sobre a continuidade ou descontinuidade depende de critérios de oportunidade, não de verdade.

¹⁸ No original: “[...] the complex and abstract notion of the legitimate authority of the national territorial sovereign does not represent a radical innovation of the postfeudal order.”

exclusivamente, ao Estado em um movimento centrípeto que fez com que ele concentrasse a maior parte daqueles elementos.

Desse modo, uma leitura da historiografia da Baixa Idade Média que leve em conta as “capacidades medievais”¹⁹ permite que se chegue à conclusão de que essas capacidades possibilitaram a formação do Estado nacional territorial e da sua noção de autoridade soberana.

A própria Sassen reconhece que parece paradoxal imaginar que o Estado nacional, uma entidade cuja autoridade está fundamentada na racionalidade e no território, possa ter evoluído das estruturas teológicas e desterritorializadas, que caracterizavam o medievo (a igreja, o feudalismo e o império). Todavia, argumenta que capacidades importantes criadas em um determinado período podem ser transportadas para dentro de uma lógica organizacional diametralmente oposta àquela em que elas foram criadas.

Isso ocorre porque as capacidades são multivalentes, ou seja, não são específicas de um determinado sistema, pois também se relacionam com outras capacidades. Por isso, Sassen explica que “[...] uma capacidade pode ser orientada para novas lógicas e ser alojada em novas estruturas. Eu vejo isso acontecendo na atual era global, quando as capacidades estatais historicamente construídas para a busca de objetivos nacionais são, nos dias de hoje, reorientadas para projetos globais” (SASSEN, 2006, p. 28)²⁰.

Ainda que, por exemplo, não existissem autoridades territorialmente exclusivas durante a Idade Média, já existiam autoridades que se pretendiam absolutas (embora não fixadas ao território), já que a igreja e o império não admitiam rivais nos respectivos âmbitos. Tal fato permite perceber que já existiam projetos de uma autoridade centralizada que foram reconfigurados para a construção de uma autoridade territorialmente centralizada.

A perspectiva de Sassen é importante não apenas para a compreensão da história do Estado-nação, mas, especialmente, como ferramenta de análise das atuais transformações que essa forma de organização política vem sofrendo. Recorrer à tese da continuidade (ou, pelo menos, de uma descontinuidade parcial) significa, também,

¹⁹ No original: “medieval capabilities”.

²⁰ No original: “[...] a capability can be regeared toward new logics and get lodged into novel path dependencies. I see this happening in the current global age when state capabilities historically constructed for the pursuit of national goals today get reoriented toward global projects.”

poder compreender as atuais mudanças como um processo que constitui o próprio Estado.

A ideia de crise do Estado, portanto, passa a ter um significado diferente, pois, se for considerado que a construção do moderno se deu a partir da mudança de objetivos de estruturas medievais, ficará mais evidente que a construção do global ocorre por meio da reorientação dos objetivos das estruturas estatais existentes. Sob tal aspecto, a própria crise é um instrumento de construção-desconstrução a partir das estruturas existentes do Estado.

1.1.2 As crises do Estado

A discussão sobre a crise do Estado foi iniciada, no cenário jurídico brasileiro, já na segunda metade da década de 1990, em texto publicado por Jose Luis Bolzan de Moraes (1996). Desde aquela época, o referido autor percebeu que, mais estudadas que o próprio Estado, as suas crises parecem ser um dos principais objetos da teoria do Estado. Além de coordenar a Rede de Pesquisa Estado & Constituição, o autor possui uma coluna quinzenal em que discute temas relacionados à crise do Estado a partir de eventos contemporâneos²¹.

Segundo Edgar Morin (MORIN, 2005, p. 13), a barbárie não é apenas um elemento do processo civilizatório, mas parte integrante dele. É possível expandir esse raciocínio para englobar o Estado nascido na modernidade. Na realidade, além de ter abrigado o desenvolvimento dos direitos fundamentais – faceta geralmente explorada na defesa da manutenção do modelo estatal –, o Estado também serviu de protagonista nas maiores violações de direitos perpetuadas na história da humanidade.

Por isso, Manuel Castells adverte: “Não nutro nenhuma simpatia especial pelos Estados-nações modernos, que tão avidamente mobilizaram seu povo para massacres em massa recíprocos no século mais sangrento da história humana: o século XXI” (CASTELLS, 2010a, p. 356)²². Dessarte, é necessário ressaltar, desde logo, que o Estado-nação está sujeito aos influxos da história e não existem motivos

²¹ A coluna “Scofinatto” é publicada, quinzenalmente, no *site* empório do direito. Disponível em: < <http://surveillance.es/1z> > . Acesso em: 26 mar. 2016.

²² No original: “I have no particular sympathy for modern nation-states that have eagerly mobilized their people for reciprocal mass slaughter in the bloodiest century of human history – the twentieth century.”

para um apego excessivo por algo que é, simplesmente, um modelo de civilização/barbárie.

Uma relevante abordagem no cenário nacional é aquela feita por Jose Luis Bolzan de Moraes (2012). Conforme o autor, a modernidade (e, em especial, sua grande invenção político-jurídica, o Estado) passa por uma fase de desconstrução de paradigmas decorrente do envelhecimento e da incompatibilidade das suas estruturas com os processos dominantes na sociedade contemporânea. Para correta compreensão deste trabalho, é imprescindível explicar um pouco sobre o modelo elaborado pelo autor, que divide em cinco os aspectos da crise do Estado contemporâneo: conceitual, estrutural, institucional, funcional e política.

A crise conceitual é caracterizada pelo esfacelamento da soberania como “[...] poder que é juridicamente incontestável, pelo qual se tem a capacidade de definir e decidir acerca do conteúdo e da aplicação das normas, impondo-as coercitivamente dentro de um determinado espaço geográfico [...]” (BOLZAN DE MORAIS, 2011, p. 27).

Não se trata de um problema novo: desde a sua criação, o Estado teve que lidar com os influxos de outras esferas de poder que, com ele, concorriam. Porém, a ênfase do autor se concentra nos processos mais recentes de interferências de poderes diversos, seja no âmbito exterior, seja no interior do próprio Estado.

A crise estrutural é caracterizada pelo enfraquecimento e flexibilização das estruturas públicas associadas aos direitos sociais. Isso ocorre em virtude **a)** das dificuldades para captar recursos públicos que sejam suficientes para cobrir os gastos (aspecto fiscal da crise); **b)** do questionamento sobre a forma de organização do Estado social e da burocratização da resposta estatal e **c)** da fragmentação do fundamento filosófico do modelo do Estado social.

A crise constitucional apresenta-se como o processo de desconstitucionalização patrocinado pelo neoliberalismo. Confunde-se, nesse sentido, com aquilo que Luigi Ferrajoli (2011a) denomina processo desconstituente. Este, nas palavras de Ferrajoli, é o fenômeno de desconstitucionalização do sistema jurídico-político, ou seja, do esvaziamento do núcleo fundamental de uma constituição. Essa situação se manifesta

[...] na construção de um regime antiliberal baseado no consenso ou, pelo menos, na aquiescência passiva de uma parte relevante da sociedade italiana a uma ampla série de violações da letra e do

espírito da constituição [...] e do próprio constitucionalismo, ou seja, dos limites e dos vínculos constitucionais impostos às instituições representativas [...] na progressiva transformação do nosso sistema político em uma forma de democracia plebiscitária ((FERRAJOLI, 2011a, p. 21)²³.

Esse processo é caracterizado pelo rebaixamento da esfera pública, da legalidade e da constitucionalidade, bem como pela desvalorização do Estado de direito como sistema de limites e vínculos impostos aos poderes. “Verticalização, concentração, confusão e vocação absolutista dos poderes públicos e privados equivalem, de fato, à hodierna versão do ‘governo dos homens’ em vez do ‘governo das leis’” (FERRAJOLI, 2005, p. 96)²⁴. Erode, assim, a esfera pública como conjunto de funções e instituições submetidas ao controle material dos direitos fundamentais, o que resulta na dilapidação, por meio da privatização e da confusão com os direitos patrimoniais, dos direitos fundamentais e, portanto, de toda a estrutura do Estado democrático de direito.

Conectada ao conceito de poderes selvagens de Luigi Ferrajoli está a crise funcional, o quarto viés da crise do Estado do modelo elaborado por Bolzan de Moraes. Essa crise diz respeito à multiplicidade dos *loci* de poder, o que resulta no enfraquecimento do Estado, como fonte central e exclusiva de poder.

Essa concorrência com outros poderes ocorre tanto na esfera interna, quanto na externa. Na interna, há a transformação da tradicional tripartição dos poderes, uma vez que cada poder assume atividades dos demais (o autor cita, como exemplo, as Comissões Parlamentares de Inquérito e a atividade legislativa do executivo via Medidas Provisórias). A manifestação externa da crise funcional fica evidente em virtude da concorrência do Estado com outras instituições globais para fazer valer a sua legislação.

Por fim, o último viés do modelo elaborado por Bolzan de Moraes é denominado crise política e de representação. Esta caracteriza-se pelo esvaziamento da política, especialmente em virtude do seu distanciamento com os problemas

²³ No original: “[...] en la construcción de un régimen antiliberal basado en el consenso o, cuando menos, en la aquiescencia pasiva de una parte relevante de la sociedad italiana a una amplia serie de violaciones de la letra y el espíritu de la Constitución [...] del propio constitucionalismo, es decir, de los límites y los vínculos constitucionales impuestos a las instituciones representativas [...] la progresiva transformación de hecho de nuestro sistema político en una forma de democracia plebiscitaria [...]”.

²⁴ No original: “Verticalizzazione, concentrazione, confusione e vocazione assolutistica dei poteri pubblici e privati equivalgono infatti all’odierna, nuova versione del ‘governo degli uomini’ in luogo del ‘governo delle leggi.’”

sociais, o que ocorre através da sua fantochização. O sistema político representativo, como resultado dessa crise, demonstra-se insuficiente para lidar com as complexas transformações da sociedade contemporânea, o que fragiliza a democracia, visto que esta acontece somente dentro do embate político.

Em perspectiva similar, Zygmunt Bauman (1999, p. 73) fala de uma nova expropriação, nos dias de hoje, cuja vítima é o Estado. No atual paradigma, nem mesmo deve ser esperado que os Estados exerçam a maior parte das funções que, em períodos mais distantes, foram consideradas a sua *raison d'être*. O maior impacto é a capacidade de o Estado regular a sua própria economia, vez que a volatilidade do mercado global passou a ser a dominante e fez incorporar as regras do sistema econômico global às economias internas dos Estados.

Esse enfraquecimento, entretanto, não significa o fim do Estado. Para Bauman, não há contradição alguma entre o desmantelamento e a manutenção do Estado, pois

a corrida para criar novas e cada vez mais fracas entidades territoriais “politicamente independentes” não vai contra a natureza das tendências econômicas globalizantes; a fragmentação política não é uma “trava na roda” da “sociedade mundial” emergente, unida pela livre circulação de informação. Ao contrário, parece haver uma íntima afinidade, mútuo condicionamento e reforço entre a “globalização” de todos os aspectos da economia e a renovada ênfase no “princípio territorial” [...] Pode-se dizer que todos têm interesses adquiridos nos “Estados fracos” – isto é, nos Estados que **são fracos**, mas mesmo assim **continuam sendo Estados** (1999, p. 75, grifos no original)

Conjugando Bauman e Ferrajoli, fica fácil perceber que a crise do Estado é útil aos poderes selvagens, porque garante que o Estado permaneça no controle, exercendo uma função que os poderes selvagens não querem assumir: a de polícia, ou seja, de garantir a ordem local. O Estado torna-se, assim, um fantoche dos poderes anônimos, que operam dentro das estruturas das redes criadas pela tecnologia da informação e que são imunes às fronteiras e aos limites territoriais.

Em virtude da sua própria natureza como construção humana e precária, o modelo estatal vive em crise desde a sua fundação. Entretanto, as análises mais recentes parecem ter o fenômeno da globalização como traço comum na discussão a respeito do destino do Estado-nação, especialmente levando-se em conta que o mundo atual é caracterizado pela expansão global da tecnologia da informação e da

riqueza, fenômenos que tendem a desintegrar a compreensão de fronteiras espaço-temporais.

Alguns autores apontam para a desintegração do Estado. Outros, com concepção completamente diferente, certamente mais otimistas, entendem que a expansão mundial e aplicação, em grande escala, do modelo estatal seria a forma mais adequada e viável de proteger os direitos (FERRAJOLI, 2011a). Um terceiro grupo, formado por teóricos como Manuel Castells (2010b), percebe que o mundo está passando por um processo de transformação diversificado – mudanças econômicas, políticas, tecnológicas, institucionais e culturais – e, por isso, acredita que se está presenciando o surgimento de uma ordem global multifacetada, cuja característica principal é a sua formatação em redes de cooperação entre Estados e instituições internacionais.

Sob essa ótica, Manuel Castells (CASTELLS, 2010a, p. xxxi) entende que,

para sobreviverem no novo contexto de governança global, os Estados-nações transformaram-se em diferentes formas. Não um governo global, como alguns profetizaram, mas em uma rede nacional e internacional de atores políticos que, conjuntamente, exercem a governança global.²⁵

Como resultado, ao invés de negar a importância do Estado ou de, pelo contrário, acreditar na possibilidade de sua aplicação em escala mundial, essa nova ordem multilateral de cogovernos requer a superação da noção de Estado da Idade Moderna, extremamente arraigada à indivisibilidade da soberania e à rigidez espaço-temporal.

Fazendo uma exposição sobre as teorias tradicionais do Estado, Bolzan de Moraes e Streck demonstram que, para aquelas matrizes teóricas, o território é entendido como um dos seus elementos centrais (BOLZAN DE MORAIS e STRECK, 2007, p. 164) ou, mais precisamente, que os teóricos tradicionais o consideram “[...] limite de validade espacial do direito do Estado, no sentido de que as normas jurídicas emanadas do poder soberano valem apenas dentro de determinadas fronteiras [...]” (BOBBIO, 2007, p. 94).

²⁵ No original: “in order to survive in the new context of global governance, the nation-states morphed into a different form. Not a global government, as some have prophesied, but a network of national and international political actors jointly exercising global governance.”

Essa centralidade do território, no entanto, é ignorada pelos fluxos de informações²⁶. Em razão disso, é possível afirmar que o Estado sofre os influxos da globalização, uma vez que o seu poder diminui em virtude da expansão de forças transnacionais capazes de reduzir a capacidade de controle dos governos em diversas áreas da vida de um povo.

Seguindo nessa direção, muitas áreas tradicionalmente associadas ao exercício da atividade estatal não podem mais ser pensadas sem a institucionalização de formas multilaterais de colaboração. As demandas proporcionadas pelos fluxos de dados, por exemplo, não podem ser resolvidas sem considerar a relação entre Estados e entidades privadas (HELD e MCGREW, 2003, p. 13).

Com efeito, a crise viabilizada pela globalização coloca o Estado, agora impossibilitado de gerenciar sozinho o seu próprio destino, em redes de atores públicos e privados dos mais variados tipos. Por esse motivo, é imprescindível compreender as relações entre a globalização e as forças que atuam na desconstrução do Estado.

1.2 GLOBALIZAÇÃO E FORÇAS CENTRÍFUGAS DE PODER

1.2.1 Notas introdutórias sobre a globalização

O conceito de globalização tem origens na literatura do final do século XIX e do início do século XX, com as produções de Karl Marx, Saint-Simon e Halford Mackinder, quando eles remetiam à ideia de uma integração do mundo. Contudo, somente nas últimas três décadas, tornou-se, extremamente comum, a referência, em artigos acadêmicos, à expressão “globalização”.

Embora alguns teóricos vejam a globalização como um fenômeno antigo, que vem acontecendo paulatinamente, é preciso concordar com Manuel Castells (2010a, p. 304-305). Para o mencionado autor, essas análises não levam em consideração a

²⁶ Zygmunt Bauman (1999) adota a tese de Paul Virílio sobre o “fim da geografia”, visto que considera que as distâncias físicas não importam mais. Para o autor, a geografia encontra-se em uma situação-limite em virtude da compressão do globo viabilizada pela globalização. Embora não seja possível concordar com a totalidade do argumento, há de se concordar com Bauman quando ele afirma que surgiram novas entidades extraterritoriais, ou seja, para as quais o espaço não constitui uma restrição, sendo elas independentes em relação às unidades territorialmente confinadas de poder político. Como resultado, o Estado acaba sendo enfraquecido nesse contexto da globalização em virtude do surgimento de poderes capazes de se mover dentro e através dos territórios.

dimensão das mudanças impactantes das novas tecnologias na economia, na organização da produção de bens e serviços, nas comunicações e na política

Por isso, é difícil aceitar a tese – razoavelmente difundida – segundo o qual se trata de uma repetição dos processos que ocorreram em séculos passados, já que as novas tecnologias da informação, ao permitirem o fluxo de informações e capital em tempo real, constituem uma mudança qualitativa nas relações sociais e econômicas.

É por tal razão que, somente após a rápida expansão proporcionada pela evolução das telecomunicações, a partir do final da década de 1960, floresceram os debates a respeito da impossibilidade de se compreender esse “admirável mundo novo”, utilizando os marcos teóricos dos períodos anteriores (HELD e MCGREW, 2003, p. 1).

Esclarecida a concepção temporal de globalização adotada nesta obra, é importante tentar tecer um conceito: afinal, o que é se quer dizer por “globalização”? Segundo David Held (1995, p. 21), ela deve ser entendida como, pelo menos, dois fenômenos distintos. Por um lado, globalização significa que muitos aspectos da atividade política, econômica e social estão adquirindo perspectivas globais. Por outro, caracteriza um novo contexto de intensificação dos níveis de interação e interconexão entre Estados e sociedades. A novidade reside no alcance das relações sociais, expandido em virtude da tecnologia da informação, o que intensifica aquelas interconexões.

A globalização, ao invés de um processo terminado, está acontecendo neste exato instante, através da intensificação das relações sociais globais que conectam locais distantes de modo que muitos acontecimentos locais são determinados por eventos que ocorrem em lugares remotos (HABERMAS, 2001, p. 84). Sob essa visão, “a transformação local é parte da globalização tanto quanto a extensão lateral das conexões sociais através do tempo e do espaço”²⁷ (GIDDENS, 2003, p. 60).

As teorias que versam sobre a globalização possuem três posicionamentos tradicionais: a primeira vê o Estado perdendo sua importância, ou seja, como vítima da globalização – teoria globalista; a segunda entende que pouca coisa mudou por causa da globalização e que o Estado continua atuando da mesma maneira de

²⁷ No original: “Local transformation is as much a part of globalization as the lateral extension of social connections across time and space.”

sempre – teoria cética; a terceira, uma posição intermediária dos posicionamentos anteriores, entende que o Estado se adapta à globalização, garantindo sua continuação como um dos principais atores nas relações de poder contemporâneas – ou seja, teoria transnacionalista (SASSEN, 2006, p. 45) (GIDDENS, 2009, p. 137). Este trabalho vincula-se, de certa forma, à corrente transnacionalista.

Simplificando, um pouco mais, essa compreensão, David Held e Anthony McGrew (2003) dividem os teóricos da globalização em dois grandes grupos: os “céticos” e os “globalistas”. As discordâncias entre eles dizem respeito, primariamente, ao conceito de globalização e aos seus efeitos em cinco pontos principais: distribuição do poder; cultura; efeitos na economia; modo de aumento da desigualdade e formas de governar o mundo globalizado. A seguinte tabela ilustra bem as diferenças entre os dois grupos:

Tabela 1 - Divisão dos teóricos da globalização em Held e McGrew

	<i>Sceptics</i>	<i>Globalists</i>
<i>1 Concepts</i>	<i>Internationalization not globalization</i> <i>Regionalization</i>	<i>One world, shaped by highly extensive, intensive and rapid flows, movements and networks across regions and continents.</i>
<i>2 Power</i>	<i>The nation-state rules</i> <i>Intergovernmentalism</i>	<i>Erosion of state sovereignty, autonomy and legitimacy</i> <i>Decline of nation state</i> <i>Rise of multilateralism</i>
<i>3 Culture</i>	<i>Resurgence of nationalism and national identity</i>	<i>Emergence of global popular culture</i> <i>Erosion of fixed political identities</i>
<i>4 Economy</i>	<i>Development of regional blocs</i> <i>Tradization</i> <i>New imperialism</i>	<i>Global informational capitalism</i> <i>The transnational economy</i> <i>A new global division of labour</i>
<i>5 Inequality</i>	<i>Growing North-South divide</i> <i>Irreconcilable conflicts of interest</i>	<i>Growing inequality within and across societies</i> <i>Erosion of old hierarchies</i>
<i>6 Order</i>	<i>International society of states</i> <i>Political conflict between states inevitably persists</i> <i>International governance and geopolitics</i>	<i>Multilayered global governance</i> <i>Global civil society</i> <i>Global polity</i> <i>Cosmopolitan orientations</i>

	<i>Primacy of ethically bounded community</i>	
--	---	--

(HELD e MCGREW, 2003, p. 38)

Embora divergentes, existem pontos que são comuns às duas correntes. Todas elas, por exemplo, entendem que o aumento da interconexão econômica, cultural e política das diferentes regiões do globo modifica as tradicionais hierarquias e gera novas desigualdades no que diz respeito à distribuição de poder, riqueza e conhecimento.

Além disso, todas concordam com o fato de que a proliferação de conflitos que ultrapassam as tradicionais fronteiras nacionais, como é o caso do fluxo global de dados, coloca em questão o problema de como o Estado pode atuar na proteção dos direitos. Tais problemas requerem novas formas de pensar a produção de um direito que seja capaz de, efetivamente, proteger os indivíduos e proporcionar a *accountability* típica dos regimes democráticos.

Tal contexto, ainda para David Held, coloca em risco o modelo de Estado que se conhece, ainda que não o aniquile. Isso porque entram, no jogo do poder, atores não sujeitos às tradicionais regras de democracia e *accountability*. Assim, sugere o autor, a globalização exige a ressignificação de conceitos como poder, legitimidade política e autoridade, separando-os das associações tradicionais com um território fixo. Isso, contudo, requer a criação de um suporte internacional capaz de lidar com o que Held denomina direito cosmopolita, que, para ele, é a pedra angular para a sobrevivência dos regimes nacionais democráticos no mundo contemporâneo²⁸.

De modo similar, Zygmunt Bauman (2001, p. 220) tem uma visão bastante sombria sobre os efeitos da globalização no Estado. Para ele, o interesse das multinacionais é a existência de um mundo sem Estados, ou, pelo menos, com Estados muito pequenos. Com isso, a soberania dos Estados seria desacreditada e removida do direito internacional, o que permite a substituição do “mundo de nações” por uma ordem supranacional.

O referido autor entende que a globalização e, especialmente, a anulação tecnológica das distâncias serviram para polarizar, ainda mais, os seres humanos, já

²⁸ Seguindo na mesma esteira, inclusive apoiado no conceito de globalização de David Held, Vicente de Paulo Barretto, com base na matriz teórica de cunho kantiano, faz uma percuciente análise das sociedade, cidadania e direito cosmopolitas (BARRETTO, 2013, p. 234 e ss.).

que esses fenômenos criaram duas categorias distintas de pessoas: de um lado, aqueles inseridos nas novas tecnologias, ou seja, emancipados dos territórios; de outro, os indivíduos excluídos que, incapazes de superar a “velocidade de escape”²⁹ da órbita do território, acabam sendo nele confinados.

A desvalorização do espaço físico, proporcionada pela globalização – e pela tecnologia da informação –, para Bauman,

[...] assegura para alguns a liberdade face à criação de significado, mas para outros pressagia a falta de significado. Alguns podem agora mover-se para fora da localidade – qualquer localidade – quando quiserem. Outros observam, impotentes, a única localidade que habitam movendo-se sob seus pés (BAUMAN, 1999, p. 25).

O viés positivo da globalização, nesse aspecto, só pode ser sentido por essa elite inserida no ciberespaço. Embora a materialidade do corpo seja irrelevante nesse ciberespaço, ele gera efeitos muito relevantes para os corpos. Por isso, Bauman acredita – corretamente – que a desterritorialização e a superterritorialização são dois lados da mesma moeda.

Embora sejam divididos, de modo geral, pelo nível de pessimismo ou otimismo, Bauman, Held e McGrew aproximam-se mais daquele grupo que, na tabela anterior, foi denominado “globalista”. Todos eles compartilham a ideia de um mundo unificado, o que resulta na erosão do Estado nacional, suplantado pelo multilateralismo na ordem global. O globalismo, para Held e McGrew,

[...] ilumina importantes transformações que estão acontecendo na organização espacial do poder – as mudanças da comunicação, a difusão e aceleração das mudanças técnicas, a proliferação do desenvolvimento econômico capitalista etc. – ainda que sua compreensão desses temas, às vezes, exagere sua magnitude e impacto (HELD e MCGREW, 2003, p. 39)³⁰.

No entanto, esse posicionamento não leva em conta um dado importante: a globalização e o Estado nacional não são mutuamente excludentes. O Estado não parece ser o grande ator do mundo globalizado, como querem os “céticos”; tampouco está caminhando para o seu fim, como querem os globalistas. O que parece ocorrer

²⁹ Na física, a velocidade de escape corresponde à energia necessária para um objeto escapar de um campo gravitacional.

³⁰ No original: “[...] does illuminate important transformations going on in the spatial organization of power – the changing nature of communication, the diffusion and speed-up of technical change, the spread of capitalist economic development, and so on – even if its understanding of these matters sometimes exaggerates their scale and impact.”

é uma reorganização, com a inserção de novos e poderosos players que concorrem com o Estado no mundo globalizado.

Por isso, a noção de “capacidades” trabalhada por Saskia Sassen (2006) é de vital importância para compreender como o Estado, apesar de ser modificado em virtude da globalização, continua sendo um importante ator na complexa rede de poderes mundiais, o que será visto no próximo item.

1.2.2 A modificação das capacidades do Estado

Ao criticar os conceitos mais comuns de globalização, Saskia Sassen (2007, p. 3) (2006, p. 23) afirma que esse fenômeno vai além da tradicional definição como aumento da interdependência, englobando também a produção de estruturas espaço-temporais que são distintas daquelas tradicionalmente erigidas pelo Estado-nação.

Por essa razão, a explicação de Held sobre o surgimento de instituições globais parece contar apenas metade da história. Isso porque a análise de Sassen pressupõe a existência de dois “níveis” de dinâmicas que regem a globalização. O primeiro diz respeito ao mesmo nível no qual trabalha Held, ou seja, na formação de instituições e processos explicitamente globais, como é o caso das organizações internacionais e do novo cosmopolitismo.

O segundo nível, no entanto, é mais profundo. Trata-se de processos que, embora não sejam aparentemente globais, são parte da globalização. De acordo com a autora,

esses processos ocorrem nas profundezas dos domínios territoriais e institucionais que foram largamente construídos em termos nacionais na maior parte do mundo. O que torna estes processos parte da globalização, embora eles estejam localizados na esfera nacional (ou subnacional), é o fato deles serem orientados em direção a propósitos e sistemas globais. Tais processos são redes e formações multilocalizadas e transfronteiriças, podendo incluir ordens normativas; elas conectam processos, instituições e atores subnacionais ou “nacionais”, mas não através do sistema formal interestatal. Exemplos disso são as redes transfronteiriças de ativistas engajados em lutas que, embora locais, possuem objetivos implícita ou explicitamente globais, como é o caso dos direitos humanos e das organizações ambientalistas; aspectos particulares do trabalho dos Estados como, por exemplo, certas políticas monetárias e fiscais essenciais para a constituição dos mercados globais e que estão sendo implementadas em um número de países cada vez maior; o uso dos instrumentos internacionais [de proteção dos] direitos humanos

em cortes nacionais; e as formas não cosmopolitas de política global que permanecem profundamente vinculadas ou concentradas com problemas e lutas localizadas (SASSEN, 2006, p. 3)³¹.

Assim, para a autora, os estudiosos, comumente, caem em uma espécie de “armadilha da endogenia” quando tentam estudar um objeto – a globalização –, centrando-se apenas nas qualidades deste objeto – as instituições e os processos globais. Não é por outra razão que a maior parte da literatura sobre globalização afirma somente que ela representa o aumento da interdependência entre nações e *players* globais, com o conseqüente declínio do Estado-nação (ou a necessidade de ele se modificar caso queira sobreviver, como afirma Held (1995, p. 22).

Sassen critica a ideia de que essa nova fase globalizadora elimina ou enfraquece aquilo que fez o Estado nacional forte. Trata-se, para a autora, de uma mudança de configuração das capacidades associadas ao Estado. Um claro exemplo dado por ela é o Estado de direito (*rule of law*), pois

[...] o “Estado de direito” é uma capacidade que foi essencial para o fortalecimento da autoridade estatal nacional na instituição do protecionismo econômico nacional. No entanto, hoje essa capacidade também é essencial para o desenvolvimento de uma economia global no intuito de abrir as economias nacionais. Ela é suficientemente desenvolvida a ponto de poder operar no contexto do protecionismo das economias nacionais e também tornar-se pedra angular para o sucesso da desregulamentação e da privatização neoliberal – que, em alguma medida, são opostas ao protecionismo. Mas isso só pode ocorrer através do realojamento [dessa capacidade] em uma nova lógica organizacional (SASSEN, 2006, p. 13-14).³²

³¹ No original: “These processes take place deep inside territories and institutional domains that have largely been constructed in national terms in much of the world. What makes these processes part of globalization even though they are localized in national, indeed subnational, settings is that they are oriented towards global agendas and systems. They are multisited, transboundary networks and formations which can include normative orders; they connect subnational or ‘national’ processes, institutions and actors, but not necessarily through the formal interstate system. Examples are cross-border networks of activists engaged in specific localized struggles with an explicit or implicit global agenda, for example, human rights and environmental organizations; particular aspects of the work of states, for example, certain monetary and fiscal policies critical for the constitution of global markets now being implemented in a growing number of countries; the use of international human rights instruments in national courts; and non cosmopolitan forms of global politics that remain deeply attached to or focused on localized issues and struggles.”

³² No original: “[...] the ‘rule of law’ is a capability that was critical to the strengthening of national state authority to institute national economic protectionism. But today it is also critical to the global economy in order to open national economies. It is sufficiently developed that it can operate in a context of national protected economies and also become a key building block for the success of neoliberal deregulation and privatization – to some extent features that are the opposite of protectionism. But it can do so only by getting relodged in a new organizing logic.”

A literatura, normalmente, chega a essa conclusão de eliminação do Estado porque estuda apenas a modificação óbvia da *assemblage* composta por território, autoridade e direito proporcionada pela globalização. No entanto, costuma-se esquecer que elementos importantes do “global” estão presentes dentro da estrutura do Estado nacional.

Em síntese, Sassen afirma que todas as “novidades” que aparecem na literatura sobre globalização têm alguma conexão e interdependência com as estruturas da modernidade associadas ao Estado-nação. Essas conexões do “novo” com o “antigo” tendem a ser tão profundamente enraizadas que, frequentemente, são ignoradas. Nas palavras de Sassen, “o novo é mais bagunçado, mais condicionado e com mais antigas linhagens do que sugerem as grandes instituições e capacidades globais”³³.

Seguindo esse raciocínio, o caso de Edward Snowden ³⁴ simboliza a reconfiguração de capacidades tradicionais. *Mutatis mutandis*, os instrumentos típicos da rigidez do Estado-nação (lei) e da sua relação com outros Estados (acordos internacionais) foram utilizados para permitir a coleta de dados em massa pelos EUA e seus parceiros, tarefa que incluiu, especialmente, grandes empresas de tecnologia.

Somente através do uso de estruturas estatais fortes, foi possível estabelecer um regime de coleta massiva de dados no mundo inteiro, fenômeno que é notoriamente desterritorializado. Nesse caso, o global (ou seja, o desenvolvimento da coleta massiva de dados por multinacionais e nações diversas) não poderia ter acontecido sem o uso do local (um aparato estatal incrivelmente desenvolvido e bem-estabelecido). Isso fica nítido em virtude de uma única potência mundial – os EUA – ser capaz de estabelecer os critérios de funcionamento da tecnologia utilizada em todo o globo.

Aqui, deve ser aplicada a mesma tese de Sassen sobre o debate continuidade/descontinuidade³⁵, ou seja, de que elementos específicos do território, da autoridade do direito estão sendo reorganizados em novas configurações globais. Sob esse aspecto, é possível afirmar que

[...] a realocação [dessas capacidades] nas lógicas organizacionais

³³ No original: “The new is messier, more conditioned, and with older lineages than the grand new global institutions and globalizing capabilities suggest.”

³⁴ Para detalhes do caso, ver item 3.1.1.

³⁵ Vide infra, item 1.1.1

desnacionalizadora e global não apenas reorienta essas capacidades para objetivos diferentes daqueles que elas eram orientadas, mas também reconstitui a construção do público e do privado, bem como dos limites entre esses domínios (SASSEN, 2006, p. 28)³⁶.

Ainda, sobre as análises tradicionais da globalização, é comum acreditar que o atual surgimento de múltiplos poderes não locais e privados guarda semelhança com o feudalismo. Não se trata de um retorno ao feudalismo, como querem alguns, pois a única semelhança entre a o período feudal e os dias de hoje, entretanto, diz respeito à mudança dos objetivos de algumas capacidades, ou seja, assim como a construção do moderno se deu a partir da reorientação (e não da destruição) das estruturas medievais.

Michael Mann (2003) possui uma visão um tanto similar à de Saskia Sassen no sentido de que a globalização não significa o fim do Estado. Embora reconheça que existe um processo de interconexão global, Mann entende que as instituições estatais continuam a ter importância no atual cenário mundial, especialmente na criação de condições de vida em sociedade e da regulação da vida social.

Existem cinco redes de interação social no mundo contemporâneo: local, nacional, internacional, transnacional e global. Dessas, as redes nacional e internacional são primariamente organizadas ao redor de Estados nacionais; por isso, para analisar a possibilidade de fim do Estado, deve-se verificar até que ponto as redes transnacional e global independem das redes protagonizadas pelo Estado.

Os entusiastas da globalização, dirá Mann (2003, p. 145), tendem a superestimar a força que o Estado nacional teve no passado e o seu atual declínio. Além disso, esquecem que a pluralidade de Estados inviabiliza falar em um processo unificado de extinção do Estado nacional, uma vez que é impossível afirmar que a fragilização do Estado ocorre da mesma forma, por exemplo, nos Estados Unidos da América e em Burquina Faso.

A globalização, portanto, não pode ser vista como um fenômeno de desconstrução do Estado-nação, como afirmam muitos teóricos. Não é a totalidade do Estado que está sendo desnacionalizado, mas apenas alguns dos seus elementos específicos. Além disso, a valência de uma capacidade determinada somente surge

³⁶ No original: "Getting relodged into denationalizing and global organizing logics not only reorients these capabilities toward objectives other than those to which they were oriented, it also reconstitutes the construction of the public and the private, and of the boundaries between these domains."

dentro da lógica na qual ela está inserida, de modo que é um equívoco colocar o global em rota de colisão com o local.

Sob essa ótica, a análise dos *tipping points*, feita por Sassen, permite concluir que o surgimento de uma nova ordem global não tem, como resultado automático ou óbvio, o fim da ordem anterior. Por outro lado, isso não quer dizer que o Estado permanece inalterado aos influxos da globalização, sem mudar suas estruturas.

Embora as redes global e transnacional estejam sendo fortalecidas pela globalização, isso não significa o fim das redes nacional e internacional. As interações humanas ocorrem de forma muito mais complexa que o possibilitado pelo raciocínio disjuntivo. Assim, é preferível falar de redes que se sobrepõem e, portanto, é incabível falar que a globalização leva ao fim do Estado.

1.2.3 O Estado e a nova configuração da soberania

A globalização da economia gera, sem dúvida, importantes mudanças na organização territorial da economia e do poder. Essa reorganização do poder modifica os pressupostos de exclusividade territorial do Estado-nação, ou seja, altera a compreensão acerca da soberania, que foi construída através da ideia de exclusividade territorial mutuamente excludente.

Nessa perspectiva, é a definição dada por Jose Luis Bolzan de Moraes. Para o autor, a soberania é

[...] um poder que é juridicamente incontestável, pelo qual se tem a capacidade de definir e decidir acerca do conteúdo e da aplicação das normas, impondo-as coercitivamente dentro de um determinado espaço geográfico, bem como fazer frente a eventuais injunções externas. Ela é, assim, tradicionalmente tida como una, indivisível, inalienável e imprescritível. Neste viés, pode-se dizer que a soberania moderna é aquela típica do Estado-Nação. Aquela caracterizada por uma estrutura de poder centralizado e que exerce o monopólio da força e da política – legislativa, executiva e jurisdicional – sobre um determinado território – como um espaço geográfico delimitado por suas fronteiras – e a população – como um conjunto de indivíduos que é reconhecido como cidadão/nacional – que o habita (BOLZAN DE MORAIS, 2011, p. 27).

Soberania e território continuam a ser importantes aspectos no mundo globalizado, embora eles estejam sendo deslocados para outras arenas institucionais fora dos moldes tradicionais do Estado-nação e do território nacional. Segundo Saskia

Sassen (1996), a soberania está sendo descentralizada, e o território, parcialmente desnacionalizado. A desnacionalização do território ocorre como efeito das práticas de empresas transnacionais e do surgimento de um regime jurídico paralelo, ainda que incipiente³⁷.

Para Sassen, ao invés de ser destruída, a soberania está sendo transformada pela globalização. Há uma proliferação dos *loci* onde ela é exercida, processo que ocorreu nos últimos anos através da reconfiguração da intersecção entre soberania e território. Assim, afirma a referida autora:

A atual fase da globalização consiste, pelo menos parcialmente, em sistemas globais evoluindo das capacidades que constituíram o Estado territorial soberano e o sistema interestatal. Em outras palavras, o Estado territorial soberano, com sua rigidez e exclusividade territorial, representa um conjunto de capacidades que, eventualmente, permitiram a formação ou evolução de sistemas globais particulares – eles próprios uma condição parcial – que não requerem territorialidade nem exclusividade (SASSEN, 2006, p. 21)³⁸.

Essa não é, contudo, a perspectiva mais amplamente difundida na literatura sobre o tema. Na maioria dos casos, entende-se que o Estado-nação está perdendo sua soberania, especialmente, porque esse conceito, desde Bodin, exige a exclusividade do poder de decisão. Nessa visão, Manuel Castells entende que a capacidade de reação do Estado está fatalmente comprometida, especialmente em virtude da globalização das atividades econômicas, do crime e das tecnologias da informação (CASTELLS, 2010a, p. 288).

A globalização, indiscutivelmente viabilizada pela tecnologia de informação, possibilita, na perspectiva visivelmente mais pessimista de Bauman (1999, p. 63), que o poder se mova em uma velocidade tal que ele esteja sempre a frente do – lento, porque territorial – Estado-nação. Movendo-se na velocidade da luz nas fibras ópticas e sinais de micro-ondas, o poder passa a se tornar livre das restrições relacionadas aos territórios.

³⁷ No item 4.3.1 será abordada a perspectiva de Gunther Teubner sobre o surgimento de um direito global desvinculado da ideia de Estado-nação.

³⁸ No original: “[...] the current phase of globalization consists at least partly of global systems evolving out of the capabilities that constituted territorial sovereign states and the interstate system. In other words, the territorial sovereign state, with its territorial fixity and exclusivity, represents a set of capabilities that eventually enable the formation or evolution of particular global systems—itsself a partial condition—that require neither territoriality nor exclusivity.”

É por isso que Bauman afirma que o Estado está sofrendo um processo de definhamento, rumo a um fim catastrófico, com o conseqüente surgimento de uma “nova desordem mundial”. Afinal, se “ordem”, para o referido autor, significa “estar no controle”, situação tradicionalmente associada à modernidade, a “desordem” resulta do inverso, ou seja, do completo caos de poderes ao qual está submetido o Estado.

Como parte desse caos, o Estado acabou perdendo o que, para Bauman, é uma das suas características mais importantes: a capacidade de transformar contingência em determinação, ou seja, diminuir a desordem. Isso significa que “os três pés do ‘tripé da soberania’ foram quebrados sem esperança de conserto. A autossuficiência militar, econômica e cultural do Estado – de qualquer Estado –, sua própria autossustentação, deixou de ser uma perspectiva viável” (BAUMAN, 1999, p. 73).

Esse fenômeno, para Bauman, ocorre como uma resposta do Estado. Em troca da manutenção da sua capacidade de policiar a lei e a ordem, o Estado passou a fazer alianças e entregar, voluntariamente, pedaços, cada vez maiores, da sua soberania. Aqui, embora não concordem no que diz respeito às conseqüências da perda da soberania, é aplicável também a perspectiva de Sassen a respeito da não vitimização do Estado, pois, segundo Bauman, os Estados não foram forçados a abrir mão da sua soberania, mas assim procederam de modo voluntário, já que eles

[...] imploravam que sua soberania lhes fosse tirada e dissolvida em formações supra-estatais. [...] A nova oportunidade representada pelo desprezo das duras e exigentes condições do Estado foi usada por dezenas de “novas nações” em uma corrida para instalar seus próprios escritórios no já superlotado edifício da ONU, não projetado para acomodar um número tão grande de “iguais”. [...] Paradoxalmente, foi a *morte* da soberania do Estado, não o seu triunfo, que tornou tão popular a idéia da condição estatal (BAUMAN, 1999, p. 72, grifo no original).

De maneira similar à de Bauman, Manuel Castells (2010a, p. 304) entende que a soberania do Estado-nação é decisivamente minada pela globalização de diversos processos e atividades na sociedade contemporânea, como ocorre com o fluxo de capitais, produção econômica, crime etc.

Por isso, é possível afirmar que a globalização é, em parte, endógena do próprio Estado-nação, tendo evoluído a partir das suas capacidades. Porém, é difícil, para a teoria do Estado tradicional, afirmar, como pretende Sassen, que o Estado

ainda retém soberania (moderna) quando esta é compartilhada. Para uma teoria mais conservadora, essa nova distribuição de poder pode ser considerada outra coisa: uma nova configuração mundial, com uma nova forma desterritorializada do exercício do poder, mas não soberania no sentido tradicional. A soberania, tradicionalmente, tem um sentido sólido, indivisível, uno, típico da modernidade do *hardware* (BAUMAN, 2001); as novas configurações desterritorializadas de poder possuem fluidez típicas da modernidade do *software*.

Para escapar, um pouco, dessa ideia de soberania tradicional, Michael Hardt e Antonio Negri (2003, p. 116) entendem que ocorreu o declínio da soberania do Estado-nação, mas não da soberania em si. Para os referidos autores, a globalização continua sustentando a existência de atores capazes de exercer o controle político, as funções estatais e os mecanismos regulatórios, ainda que esses papéis não sejam atribuídos ao Estado.

No entanto, os autores não afirmam que os Estados compartilham a soberania com outras instituições. De acordo com eles, a própria soberania tomou uma nova configuração ao ser composta de forma global, exercida por Estados e instituições supranacionais, regidos por uma única regra. Essa soberania globalizada recebe um novo nome: “Império”.

A passagem para o Império, por sua própria natureza, somente ocorre com o declínio da soberania da modernidade. Ao contrário do modelo anterior, o Império não necessita de um centro territorial que emana poder, tampouco depende de estruturas territorializadas. Assim, o Império

é um aparato de governo descentralizado e desterritorializador que progressivamente incorpora todo o domínio global com as suas fronteiras abertas e expansíveis. O Império gerencia identidades híbridas, hierarquias flexíveis e trocas plurais através de redes de comando moduladas (HARDT e NEGRI, 2003, p. 117)³⁹.

Por tal razão, a proposta de Sassen é interessante para compreender que o aparato do Estado-nação, ao invés de ser destruído pela globalização, torna-se ele próprio o suporte para o desenvolvimento da nova ordem, afinal, “uma nova ordem não é uma invenção ab novo, e ela não necessariamente se anuncia como nova, como

³⁹ No original: “It is a decentered and deterritorializing apparatus of rule that progressively incorporates the entire global realm within its open, expanding frontiers. Empire manages hybrid identities, flexible hierarchies and plural exchanges through modulating networks of command.”

uma estranheza radical – como ficção científica ou relato futurista” (SASSEN, 2006, p. 11)⁴⁰.

De modo absolutamente diverso, Georg Sørensen (2010) entende que o núcleo da soberania permanece intacto mesmo diante das mudanças proporcionadas pela globalização. Segundo ele, existem três aspectos que justificam a sua hipótese e que devem ser analisados: **1)** o núcleo jurídico da soberania, que ele entende ser a independência constitucional; **2)** as normas que regulam essa soberania, ou seja, a reciprocidade e a não intervenção e **3)** a realidade material do Estado, ou seja, sua capacidade real para agir e controlar sua economia e instituições político-administrativas.

O autor apresenta o contraponto no que chama “debate sobre o fim da soberania”, contestando aqueles que, para ele, assumem uma postura “apocalíptica” do fim do Estado e aqueles que entendem que a soberania e o Estado estão mais fortalecidos do que nunca. Aponta cinco fatores principais que impulsionam o debate:

1. As transmissões de dados informatizados, as emissões de rádio, a detecção remota por satélite e as chamadas por telefones celulares não se restringem nos controles de fronteira. Ademais, essas comunicações ocorrem: (a) a velocidades que fazem difícil que a vigilância dos Estados as detecte de antemão; e (b) em quantidades que nenhum Estado pode perseguir, ainda que aumente as suas capacidades.
2. Os meios eletrônicos de massas também supõem uma perda do domínio do Estado sobre a construção da língua e da educação.
3. Um estado não pode exercer autoridade plena sobre associações transfronteiriças e empresas globais.
4. Um Estado não pode assegurar com êxito o domínio supremo e exclusivo sobre os fluxos financeiros globais que atravessam a sua jurisdição.
5. As condições ecológicas mundiais, como a diminuição da camada de ozônio e da diversidade biológica também minaram os requisitos materiais da soberania (SORENSEN, 2010, p. 129)⁴¹.

⁴⁰ No original: “A novel order is not an invention ab novo, and it does not necessarily announce itself as new, as radical strangeness – like science fiction or a futuristic account.”

⁴¹ No original: “1. Las transmisiones de datos informatizados, las emisiones de radio, la detección remota por satélite y las llamadas por teléfonos celulares no se detienen en los puestos aduaneros. Además dichas comunicaciones suceden: (a) a velocidades que hacen difícil que la vigilancia de los Estados las detecte de antemano; y (b) en cantidades que ningún Estado puede seguir, incluso aunque aumente sus capacidades. 2. Los medios electrónicos de masas también suponen una merma del dominio del Estado sobre la construcción de la lengua y la educación. 3. Un Estado no puede ejercer autoridad plena sobre asociaciones transfronterizas y empresas globales. 4. Un Estado no puede asegurar con éxito el dominio supremo y exclusivo sobre los flujos, financieros globales que atraviesan su jurisdicción. 5. Las condiciones ecológicas mundiales, como la disminución de la capa de ozono y de la diversidad biológica también han mermado los requisitos materiales de la soberanía.”

Sørensen, ao negar que esses fatores são capazes de remover a soberania do Estado, aponta que as propostas a respeito do “fim da soberania” estariam fundamentadas em um erro de categoria. De acordo com ele, a soberania deve ser entendida como uma instituição jurídica que compreende a independência constitucional e das suas normas reguladoras.

Logo, por entender que tais características permanecem impávidas aos cinco problemas que elenca, Sørensen acredita que os defensores do esvaziamento da soberania em virtude da diminuição das oportunidades de controle por parte do Estado estão, na realidade, confundindo a realidade material do Estado – que o autor entende sofrer mudanças – com a instituição jurídica da soberania – que, para Sørensen, permanece inalterada.

A fim de defender seu ponto de vista, Sørensen afirma que a história do modelo estatal é mal-interpretada, uma vez que as interferências sempre existiram nos assuntos do Estado, que nunca foi capaz de regular, completamente, os fluxos nas suas fronteiras.

Além disso, argumenta que a força do Estado-nação resta evidente em virtude da multiplicação do número de Estados soberanos a partir dos anos de 1945, sem competidores que coloquem, na opinião dele, essa primazia estatal em risco⁴². Esse, contudo, não é argumento suficiente, pois, conforme explicitado anteriormente, o enfraquecimento do Estado e a proliferação de Estados débeis não são eventos excludentes.

Por conseguinte, ainda que o “jogo moderno” e o “novo jogo” sejam diferentes, Sørensen acredita que a independência constitucional do Estado permanece intacta. Esse posicionamento, contudo, demonstra-se descabido, especialmente se for considerado a partir do problema da globalização e dos fluxos globais de dados. Ao contrário do que afirma Sørensen, quando fala da liberdade dos países europeus de simplesmente saírem da União Europeia, os Estados não estão nada livres para decidir se participam ou não dos fluxos globais de dados. Veja-se, por exemplo, o

⁴² Em sentido contrário, veja-se a notícia sobre o formulário do sistema de busca *Bing*, da *Microsoft*, para solicitação de retirada dos resultados das pesquisas, obedecendo à sentença do Tribunal Europeu relativa ao direito ao esquecimento. Embora a ordem tenha partido do Tribunal, quem, no final das contas, decide sobre essa “ponderação” de direitos humanos é a equipe da *Microsoft*. Segundo o formulário, “ces informations nous aideront à évaluer l'équilibre entre votre intérêt individuel à la protection de votre vie privée, et l'intérêt public consistant à protéger la libre expression et le libre accès à l'information [...] Microsoft ne garantit pas qu'un résultat de recherche spécifique sera bloqué”. Ver a matéria no jornal *Le Monde*. Disponível em: < <http://surveillance.es/20> >. Acesso em: 27 mar. 2016.

caso brasileiro que, vulnerável à interferência da coleta de dados por parte da NSA, não foi capaz de tomar nenhuma medida para alterar a situação⁴³.

Parte dessa falta de compreensão talvez esteja relacionada ao fato de que Sørensen utiliza bibliografia da década de 60 e 80 do século passado para tentar capturar as mudanças propiciadas pela tecnologia da informação, que iniciou seu crescimento exponencial somente a partir do final da década de 1980.

As limitações da territorialidade, as transformações da soberania e a desnacionalização são características essenciais da globalização. Tais transformações são tão importantes que Jose Luis Bolzan de Moraes (BOLZAN DE MORAIS, 2012, p. 28) afirma que “falar em soberania, nos dias atuais, como um poder irrestrito, muito embora seus limites jurídicos, parece mais um saudosismo do que uma avaliação lúcida dos vínculos que a circunscrevem”.

Muitos dos processos globais, porém, ainda dependem, frequentemente, da entrada no âmbito do Estado-nação para serem operacionalizados. Trata-se de um fenômeno complexo, que resiste à simplicidade das explicações duais e que requer que sejam decifradas as “[...] profundas mudanças estruturais que subjazem às continuidades superficiais e, alternativamente, às profundas continuidades estruturais que subjazem às descontinuidades superficiais” (SASSEN, 2006, p. 12)⁴⁴.

Em síntese: o Estado-nação é muito pequeno para lidar com os problemas globais relacionados aos fluxos globais de dados, mas muito grande para resolver os problemas dos indivíduos. Apesar da contradição simbolizada pelo poder militar dos EUA, a liquidez, cada vez maior, do mundo aponta para um processo de diminuição sistemática da soberania e do poder do Estado-nação como forma de manter sua longevidade.

Ficou claro que, ao contrário do que afirma Sørensen, é desconstruída a ideia de soberania como algo absoluto. Até mesmo na Era Moderna, a soberania dos Estados “no papel” era muito maior que a realidade. A história dos últimos séculos, para Anthony Giddens (2003, p. 61), não foi uma história de gradual perda de soberania do Estado, mas um processo desigual de perda para alguns e ganho para outros.

⁴³ Sobre o caso, ver item 1.5.3.

⁴⁴ No original: “[...] deep structural shifts underlying surface continuities and, alternatively, deep structural continuities underlying surface discontinuities.”

Logo, a teia de poder soberano não pode ter sido formada antes das relações entre Estados, pois a própria soberania sempre envolveu uma interdependência, vez que sempre se tratou do reconhecimento da soberania de um Estado por outro. O que se pretendeu, com essa análise da soberania, foi modificar a tendência das ciências sociais (especialmente do direito) de pensar os fenômenos sociais, políticos e econômicos somente dentro das estruturas do Estado-nação.

1.3 TRANSFORMAÇÕES DO ESTADO NA MODERNIDADE LÍQUIDA

1.3.1 A modernidade líquida

Sobre a “modernidade líquida”, Zygmunt Bauman (BAUMAN, 2001, p. 8) justifica a metáfora da fluidez como a mais adequada para o mundo atual, pois, distintamente da rigidez dos sólidos, a fluidez dos líquidos confere-lhes habilidade para suprimir o tempo e ignorar, com facilidade, o espaço. Esse é um traço fundamental que permeia aquilo que Bauman chama de “modernidade líquida”. Para as perspectivas deste trabalho, a tecnologia da informação, muito além de mera ferramenta facilitadora dessa liquidez, é uma das suas pedras angulares.

Na metáfora de Bauman, a modernidade “tradicional” (com começo após a Idade Média e fim nos dias atuais) pode ser chamada de modernidade “pesada”, “era do *hardware*” ou, em termos weberianos, a era da racionalidade instrumental. Trata-se de uma modernidade cujo valor fundamental era o maior tamanho/volume, ou seja, a lógica do “quanto maior, melhor”. Foi a era das máquinas grandes e potentes, dos muros divisores e da busca incessante pela conquista do território. “A modernidade pesada”, diz Bauman, “foi a era da conquista territorial. A riqueza e o poder estavam firmemente enraizados ou depositados dentro da terra – volumosos, fortes e inamovíveis como os leitos de minério de ferro e de carvão” (2001, p. 132).

O ponto elementar nessa compreensão é a nova percepção do espaço e do tempo. Um corpo líquido não se fixa no espaço nem mantém sua forma com o passar do tempo. Os líquidos ocupam espaços com mais facilidade (são deformáveis), mas essa ocupação dura tão somente o tempo necessário até que haja uma modificação das forças que atuam sobre aquele objeto. Nas palavras de Bauman,

enquanto os sólidos têm dimensões espaciais claras, mas neutralizam o impacto e, portanto, diminuem a significação do tempo (resistem efetivamente a seu fluxo ou o tornam irrelevante), os fluidos não se

atêm muito a qualquer forma e estão constantemente prontos (e propensos) a mudá-la; assim, para eles, o que conta é o tempo, mais do que o espaço que lhes toca ocupar; espaço que, afinal, preenchem apenas “por um momento”. [...] Ao descrever os sólidos, podemos ignorar inteiramente o tempo; ao descrever os fluidos, deixar o tempo de fora seria um grave erro (BAUMAN, 2001, p. 8)

Como resultado, maior e mais forte deixam de ser os traços mais desejados no mundo atual. Se, no passado, as relações de dominação ocorriam entre o “maior” e o “menor”, hoje, vemos essa relação entre o mais rápido e o mais lento. “Dominam os que são capazes de acelerar além da velocidade de seus opositores”, diz Bauman (BAUMAN, 2001, p. 215).

O poder, na modernidade sólida, estava associado ao tamanho do *hardware* e, como tal, tendia a ser lento e de baixa mobilidade. O seu crescimento não estava associado à capacidade de mudar de lugar, mas de aumentar o seu tamanho, o que retroalimentava esse ciclo de lentidão e expansão. A centralização em uma estrutura física era importante em todos os contextos: na fábrica, no hospital, nas prisões. Nesses locais, “ a lógica do poder e a lógica do controle estavam fundadas na estrita separação entre o “dentro” e o “fora” e em uma vigilante defesa da fronteira entre eles” (BAUMAN, 2001, p. 133).

O tempo, na modernidade sólida, devia ser métrico. Já na modernidade líquida, devia ser, simultaneamente, flexível e rígido. Flexível na busca de conquistar cada vez mais espaços no menor intervalo de tempo. Rígido para, uma vez conquistado o espaço, o tempo ser dividido uniformemente, “domado”, neutralizando o seu dinamismo.

Assim, o tempo “domesticado” passava a ser essencial para a colonização do espaço. Basta lembrar, por exemplo, do modelo fordista de produção: uma grande fábrica onde ocorre toda a montagem do veículo, com atividades laborativas específicas, bem-segmentadas e inflexíveis. Uma linha de montagem exclusiva para produção de um determinado item, sem flexibilidade sequer para a mudança de cor do produto final – daqui a clássica afirmação de Henry Ford de que “os clientes podem ter o carro pintado de qualquer cor que eles quiserem, desde que seja preta” (FORD e CROWTHER, 1923, p. 72)⁴⁵.

Diametralmente oposto é o que ocorre na modernidade leve, líquida ou, no contraste com a nomenclatura do período anterior, na era do *software*. Nesse

⁴⁵ No original: “Any customer can have a car painted any colour that he wants so long as it is black.”

contexto, modifica-se a percepção do mundo, que passa a ser apreendido como ambivalente, mutável e rápido, ou seja, onde não há lugar para a rigidez das estruturas sólidas e duráveis. Assim,

a mudança em questão é a nova irrelevância do espaço, disfarçada de aniquilação do tempo. No universo de *software* da viagem à velocidade da luz, o espaço pode ser atravessado, literalmente, em “tempo nenhum”; cancela-se a diferença entre “longe” e “aqui”. O espaço não impõe mais limites à ação e seus efeitos, e conta pouco, ou nem conta. Perdeu seu “valor estratégico”, diriam os especialistas militares (BAUMAN, 2001, p. 136).

A capacidade de alcançar qualquer espaço instantaneamente acaba por destituir de valor o lugar físico e tornar irrelevantes as referências ao tempo. Ao contrário do que ocorria na era do *hardware*, o tempo não necessita ser dividido para aumentar a eficácia na busca de um determinado objetivo: o tempo tende ao infinito.

Além da relação espaço-tempo, a relação entre espaços também passa a ser severamente modificada, visto que qualquer espaço pode ser alcançado em tempo desprezível. Deixa de fazer sentido pensar na relação centro-periferia, afinal, nenhuma parte do espaço é privilegiada pelo rápido acesso – todas são acessíveis instantaneamente. Portanto, torna-se irrelevante a busca pela conservação e controle dos espaços, devendo ser os recursos existentes gastos no controle dos fluxos, independentemente dos espaços onde ocorram. O tempo tende a tornar-se, ao contrário da sua unidade física no sistema métrico, adimensional.

O acesso à instantaneidade passa a ser o grande diferenciador entre quem detém poder e quem é desprovido dele. Enquanto, na modernidade sólida, os poderosos e os servos permaneciam juntos dentro da mesma prisão, na modernidade líquida, somente os mais fracos encontram dificuldade na mobilidade. Para fins desta pesquisa, como será visto, essa mudança tem efeitos até mesmo na concepção de “vigilância”, uma vez que a modernidade líquida torna desnecessária a existência de estruturas como o panóptico. Isso porque o controle dos lugares deixa de ser o objetivo do poder, agora concentrado no controle dos fluxos.

Da mesma forma, o poder na modernidade líquida passa a ser desvinculado de um território, além de extremamente flexível e mutável. Não mais preso às tradicionais estruturas do seu exercício, o poder passa a fluir junto com os fluxos que ele mesmo controla. Sem um local que o emana, o poder busca atingir a onipresença e a onisciência, típica das divindades.

O Estado, como instituição criada pelo homem, não passou incólume por essas mudanças nas estruturas da humanidade. Os efeitos da modernidade líquida sobre o Estado são tratados por Bauman (2001, p. 212) como um romance entre Estado e nação. Para ele, esse antigo romance está chegando a um fim, que não é um “divórcio”, mas uma opção por uma forma de “relacionamento aberto”, onde o “viver juntos” não requer a lealdade incondicional.

Nessa nova fase do romance, Estado e nação estão livres para buscarem novas alianças, já que a relação entre eles não é mais o padrão obrigatório e exclusivo. Por isso, mostra-se essencial estudar o papel desempenhado pelo Estado no contexto dessa modernidade líquida.

1.3.2 O Estado na modernidade líquida

Considerando que a modernidade líquida passa a valorizar mais o mutável e o veloz em detrimento do estático e lento, as estruturas tradicionais do Estado, obrigatoriamente vinculadas a um território, tornam-se uma desvantagem. Por essa razão, na modernidade líquida, o Estado perde a função de provedor de certezas, seguranças e garantias, especialmente diante do surgimento dos novos poderes globais. Esses poderes são capazes de retribuir, rápida e impiedosamente, a violação do “novo estatuto global” (BAUMAN, 2001, p. 212), uma vez que dotados de extraterritorialidade e extrema velocidade de resposta caso sejam contrariados.

O Estado, nesse sentido, não pode se abster de participar do jogo das novas regras globais, sob pena de ser penalizado por esses novos poderes. As punições geralmente vêm na forma de restrições econômicas – como ocorre, por exemplo, com o rebaixamento de nota dada pelas empresas internacionais de classificação de risco soberano de crédito – ou de acesso aos padrões de tecnologia – é o caso dos padrões de uso e acesso à tecnologia, bem como protocolos de comunicações e especificações técnicas impostos por grandes organizações (como a IEEE-SA⁴⁶) ou pelos Estados Unidos da América .

⁴⁶ Sigla para o “Institute of Electrical and Electronics Engineers Standards Association”, entidade responsável pela elaboração de padrões mundiais para uma ampla gama de indústrias, em especial nas áreas de geração de energia, saúde, tecnologia da informação, robótica, telecomunicação, transporte, nanotecnologia, dentre outros. Ao contrário de outros grupos elaboradores de padrões, (como ISO, IEC, ITU), o IEEE-SA não está ligado (oficialmente) a nenhum Estado-nação.

Como já indicado no trecho dedicado à globalização, merece atenção a análise de Saskia Sassen (2006) a respeito das “*assemblages*” na era global digital, protagonizada pelos reflexos das tecnologias da informação no Estado. Embora reconheça as transformações de paradigma que envolvem as novas dinâmicas institucionais da globalização, Sassen não trabalha com a perspectiva comum de “vitimização” do Estado, uma vez que ele continua sendo o lugar privilegiado de formação jurídico-institucional.

Essa fase atual da modernidade líquida não significa o fim do Estado, mas demonstra a importante imbricação entre a pluralidade de instituições globais desnacionalizadas e o próprio Estado, já que aquelas instituições, geralmente, são operacionalizadas quando adentram na estrutura estatal. Nesse sentido, é possível afirmar que

[...] as maiores transições que iniciam os novos arranjos [...] podem depender das múltiplas capacidades da ordem anterior. Essa ‘dependência’ não é necessariamente fácil de reconhecer, uma vez que as novas lógicas organizacionais podem e irão tender a alterar a valência de uma determinada capacidade. [...] algumas das antigas capacidades são essenciais para a constituição crítica da nova ordem, mas isso não significa que suas valências sejam as mesmas; os sistemas relacionais ou as lógicas organizacionais dentro das quais elas adquirem funcionalidade podem ser radicalmente diferentes. O ponto crítico é a intermediação que as capacidades produzem entre a nova ordem e a antiga; enquanto elas mudam de caminho, tornam-se partes constitutivas e, simultaneamente, podem disfarçar essa mudança vestindo as mesmas roupas de sempre (SASSEN, 2006, p. 8).⁴⁷

De certa forma, Bauman também trabalha com a ideia de não incompatibilidade entre Estado e modernidade líquida, já que seria contra o interesse das forças globalizadoras. Assim, ao invés de serem opostos, “[...] a fragmentação política e a globalização econômica são aliados íntimos e conspiradores afinados. A integração e a divisão, a globalização e a territorialização são processos mutuamente complementares” (BAUMAN, 1999, p. 77).

⁴⁷ No original: [...] major transitions ushering novel arrangements [...] might depend on multiple capabilities of the older order. This “dependence” is not necessarily easy to recognize, as the new organizing logic can and will tend to alter the valence of a given capability [...] some of the old capabilities are critical in the constituting of the new order, but that does not mean that their valence is the same; the relational systems or organizing logics within which they then come to function may be radically different. The critical issue is the intermediation that capabilities produce between the old and the new orders: as they jump tracks they are in part constitutive and at the same time can veil the switch by wearing some of the same old clothes.”

Quando se fala das tecnologias da informação e do seu impacto nas estruturas estatais, um dos pontos centrais é o questionamento a respeito da capacidade regulatória que os modelos de Estado e democracia vigentes possuem sobre essas tecnologias. Elas desestabilizam as estruturas hierárquicas formais, pois estas passam a ser substituídas por novas estruturas ainda não formalizadas, frequentemente, apropriadas por poderes privados e imunes aos influxos democráticos.

Do ponto de vista da *surveillance*, isso significa que, embora essas práticas escapem, frequentemente, da regulação estatal – especialmente quando envolvem a iniciativa privada ou os segredos de Estado –, elas não estão imunes ao controle, mas, muito pelo contrário, submetem-se à regulamentação dos detentores das tecnologias – ainda que sejam Estados, como no caso dos EUA. Tal situação é problemática, pois impossibilita a análise pública da *surveillance* até mesmo quando ela é utilizada pelo Estado, como ficou claro com as notícias envolvendo Edward Snowden.

Por isso, ao analisar as transformações do Estado na modernidade líquida, é equivocado utilizar as categorias que foram desenvolvidas em outros contextos espaço-temporais, ou seja, é preciso “olhar o novo como novo”. Isso reforça a necessidade de entender a capacidade que as novas tecnologias da informação têm para liquefazer aquilo que, comumente, não era líquido, ou seja, de atribuir “hipermobilidade” àquilo que é físico.

A perda de diversos componentes da autoridade formal do Estado não significa o desaparecimento das antigas estruturas de poder, mas o seu rearranjo. É por esse motivo que Saskia Sassen afirma que

as teorias existentes não são suficientes para mapear a atual multiplicação de atores não estatais e formas transfronteiriças de cooperação e conflito, como no caso das redes globais de negócios, ONGs, cidades globais, esferas públicas transfronteiriças e os novos cosmopolitismos (2006, p. 346).⁴⁸

Como consequência, é possível afirmar que o direito internacional – comumente mencionado como possível solução para os problemas

⁴⁸ No original: “existing theory is not enough to map today’s multiplication of nonstate actors and forms of cross-border cooperation and conflict, such as global business networks, NGOs, diasporas, global cities, transboundary public spheres, and the new cosmopolitanisms.”

desterritorializados das novas tecnologias da informação – também é insuficiente. A causa disso é que suas categorias foram pensadas para relações interestatais (cujos sujeitos são exclusivamente Estados nacionais) e ignora o fato de que, atualmente, os atores globais de grande relevância não são necessariamente Estados e, portanto, não obedecem à lógica do *jus cogens*.

A soberania estatal – entendida como a capacidade, dentro de um determinado território, para centralizar e legitimar o poder e o direito – torna-se instável, já que as manifestações de poder nos territórios deixam de ser mutuamente excludentes. Por essa razão, ainda que o Estado permaneça sendo importante no cenário interno e externo, diversos poderes – associados a determinados territórios ou não – passam a ganhar cada vez mais espaço no cenário atual.

De maneira similar, Jose Lus Bolzan de Moraes (2012) ressalta que o modelo estatal atual não consegue lidar com as perplexidades oriundas da multipolarização do mundo globalizado. As categorias tradicionais da teoria do Estado, associadas às estruturas de poder modernas, também são fragilizadas pela descentralização e concorrência de poderes diversos, tornando-se insuficientes para caracterizar o fenômeno estatal do mundo globalizado.

Isso requer a superação do modelo “fechado” do Estado, reconhecendo as inevitáveis transformações associadas à pulverização do poder. Essa pulverização, embora possibilite o deslocamento do poder em direção a outros *loci*, não exclui o poder público, uma vez que “embora fragmentado e fragilizado [...] este foi redefinido, mas não abolido” (BOLZAN DE MORAIS, 2012, p. 35).

Desse modo, é possível, através de um raciocínio similar ao que Bolzan de Moraes usa para tratar do problema ambiental, afirmar que a compreensão jurídica do fenômeno dos fluxos globais de dados não pode ignorar as transformações do Estado no mundo globalizado, visto que elas ultrapassam a lógica do modelo de direito da modernidade sólida, submetido à territorialidade estatal.

Para além de estarem meramente relacionadas, as novas tecnologias da informação reestruturam a visibilidade, a territorialidade e a temporalidade. Se isso tem consequências, como será visto no item 2.1, para a diferenciação aqui proposta entre “vigilância” e “*surveillance*”, é provável que também tenha para o que se entende como Estado.

Parece claro que não se está presenciando o fim do Estado. Ele ainda é importante. As legislações sobre proteção de dados, exemplos do direito desse Estado, ainda são importantes. Todavia, existem problemas que não podem ser resolvidos por essas vias tradicionais. O papel do jurista é reconhecer esses problemas, deslocando-se do discurso fetichizado da lei que, seguindo a etimologia da palavra, enfeitiça o profissional do direito, fazendo-o acreditar que o direito vinculado à territorialidade estatal é a solução para todos os problemas do homem.

O que o direito precisa reconhecer é que o mundo da modernidade líquida é demasiado complexo e caótico para caber no espaço rígido e seguro da lei derivada do Estado-nação. Nesse caos, globalização e regionalização são dois processos simultâneos que criam redes interseccionais de poder que ignoram os limites do território geográfico. Dessa forma, conforme salientado por David Held e Anthony McGrew (2003, p. 39), esses processos desgastam a noção de mundo westfaliana, ou seja, do princípio da exclusiva soberania sob um determinado território.

Na modernidade líquida, o poder político – e, portanto, o direito – deixa de ser exercido somente pelo Estado, uma vez que diversas forças – públicas, privadas, nacionais, internacionais – passam a contestá-lo. Os direitos, nessa perspectiva, passam a ser determinados por forças que estão fora das amarras da legislação nacional e que, portanto, escapam dos tradicionais controles democráticos. É precisamente essa estrutura de poderes em rede que será examinada no próximo item.

1.4 O ESTADO NA SOCIEDADE EM REDE

1.4.1 A sociedade em rede

As estruturas sociais que surgiram nos últimos anos – especialmente aquelas vinculadas à globalização e ao fluxo de dados e comunicações globais – remodelam a forma de organização da sociedade. Essa nova morfologia social, típica da “Era da Informação”, organiza-se na forma de redes, cuja principal característica é a extinção de centros e periferias.

Ainda que essa modalidade de organização não seja exatamente nova, tendo ocorrido em outras fases da história, o surgimento da tecnologia da informação permite a expansão da morfologia da rede de uma forma inédita tanto na sua

velocidade, quanto no seu alcance. É por isso que Habermas afirma que, no mundo atual,

“rede” [Netzwerk] tornou-se uma palavra-chave, e tanto faz se se trata das vias de transporte para bens e pessoas, de correntes de mercadorias, capital e dinheiro, de transmissão e processamento eletrônicos de informações ou de circulações de pessoas, técnica e natureza (HABERMAS, 2001, p. 84).

A própria estruturação em forma de rede é mais significativa do que os fluxos de poder que compõem a rede, de modo que a sua simples existência retroalimenta sua expansão. Parafraseando Marshall McLuhan (1969), a rede é a mensagem. É por isso que Manuel Castells afirma que “[...] essa lógica de rede induz a uma determinação social de nível mais alto que aquele dos interesses sociais específicos expressos através das redes: o poder dos fluxos prevalece em relação aos fluxos do poder” (CASTELLS, 2010b, p. 500)⁴⁹. Essa sociedade, cuja forma em rede prevalece sobre o conteúdo, é chamada por Castells de “sociedade em rede”.

Uma rede, segundo Castells, é um conjunto interconectado de nós, que, por sua vez, são um ponto no qual uma curva se intersecciona. O que concretamente constitui um nó depende do tipo de rede ao qual se refere. No caso específico deste trabalho, os nós da rede da *surveillance*, por exemplo, são as empresas de tecnologia – *Google, Facebook, Microsoft, Apple* etc. –, bem como as agências de inteligência – *NSA, GCHQ, BND, DGS* etc. –, indivíduos, governos, empresas e todos aqueles sujeitos à coleta massiva de dados.

A forma como a rede é organizada – sua topologia – determina a intensidade da interação entre os seus nós. A distância entre dois pontos – e, conseqüentemente, a interação entre eles – depende do fato de estarem ou não na mesma rede (ou em redes conectadas): caso estejam, a distância é sempre zero (não há centro, todos os nós são acessíveis de qualquer posição); caso negativo, a distância tende ao infinito, o que resulta em possibilidades de interação extremamente limitadas.

A natureza dinâmica da estrutura em rede permite a rápida inserção e exclusão, o que viabiliza sua expansão ilimitada. O único pré-requisito é que seja possível a comunicação entre os nós ou redes. Assim, “a estrutura social baseada em

⁴⁹ No original: “this networking logic induces a social determination of a higher level than that of the specific social interests expressed through the networks: the power of flows takes precedence over the flows of power.”

rede é um sistema altamente dinâmico e aberto, suscetível à inovação sem que o seu equilíbrio seja ameaçado” (CASTELLS, 2010b, p. 501-502)⁵⁰. Isso possibilita que essa forma de organização seja incrivelmente compatível com os processos descentralizadores da globalização e também com as ideias de mutabilidade, flexibilidade e supressão do espaço-tempo, típicas da modernidade líquida.

A sociedade em rede proporciona mudanças significativas nas estruturas tradicionais de poder, como pôde ser visto nos itens anteriores relativos à globalização e à crise do Estado na Era da Informação. O poder, embora comparativamente mais difuso do que na modernidade sólida, ainda se concentra. A diferença é que, nesse contexto de sociedade em rede, o poder tende a concentrar-se mais nos elementos conectores, ou seja, nos pontos que viabilizam a conexão entre redes distintas – *switchers*. Como resultado,

[...] os códigos interoperacionais e os conectores entre redes tornam-se as principais fontes de ordenação, orientação e desorientação das sociedades. A convergência entre a evolução social e a tecnologia da informação criou uma nova estrutura material para a realização de atividades através da estrutura social. Essa estrutura material, elaborada nas redes, determina os processos sociais dominantes e, portanto, ordenam a própria estrutura social (CASTELLS, 2010b, p. 502)⁵¹.

As redes não interrompem a sua expansão e o seu fluxo em virtude das fronteiras do Estado nacional, cujas instituições e capacidades foram geradas na era da modernidade sólida. Espaço, tempo e sociedade são transformados em virtude da organização das funções sociais dominantes em uma estrutura de rede de geometria variável.

Como resultado, o Estado perde sua capacidade de controlar e regular o fluxo global de riqueza e informação, ocorrendo, pois, uma mudança qualitativa da experiência estatal em relação àquela construída na Idade Moderna (CASTELLS, 2010b, p. xviii). Imprescindível, portanto, analisar como o Estado se comporta dentro desse novo contexto da sociedade em rede.

⁵⁰ No original: “A network-based social structure is a highly dynamic, open system, susceptible to innovating without threatening its balance.”

⁵¹ No original: “the inter-operating codes and switches between networks become the fundamental sources in shaping, guiding, and misguiding societies. The convergence of social evolution and information technologies has created a new material basis for the performance of activities throughout the social structure. This material basis, built in networks, earmarks dominant social processes, thus shaping social structure itself.”

1.4.2 O Estado na sociedade em rede

O Estado da modernidade sólida teve, como principal característica, a habilidade de domesticar o espaço – através da colonização do território – e o tempo – através da neutralização do seu dinamismo⁵² (BAUMAN, 2001). No entanto, os fluxos globais de dados tendem a ignorar esse tradicional papel do Estado como organizador de espaço e tempo. Isso ocorre em virtude de tais fluxos possuírem tempo e espaço próprios: o tempo instantâneo e o espaço comprimido. Por isso, “o deslocamento dos valores, de ‘senhor do território’ para ‘mestre da velocidade’, parece enfraquecer o Estado nacional” (HABERMAS, 2001, p. 86).

A resposta do Estado é a sua descentralização em blocos regionais e, em sentido aparentemente inverso, em estruturas locais de administração e poder. Como resultado, ocorre o crescente esvaziamento da soberania estatal, cujas causas estão relacionadas à inabilidade do Estado-nação “[...] para navegar nas águas inexploradas e turbulentas entre o poder das redes globais e os desafios das identidades singulares” (CASTELLS, 2010a, p. 304)⁵³.

Isso não significa, como visto, a completa desestruturação estatal, porque suas instituições políticas, frequentemente, resistem à perda do poder. Contemporaneamente, tal situação fica evidente, uma vez que, além da crise do Estado, verifica-se uma simultânea reformulação das suas instituições como forma de viabilizar a sua permanência no século XXI.

Se, no passado, o maior desafio dos Estados autoritários era controlar os meios de comunicação de massas – algo que podia ser feito de maneira relativamente fácil através do controle legal da sua propriedade –, os fluxos de dados, atravessando o globo terrestre, não podem ser domesticados da mesma maneira.

Apesar de existirem diversas tentativas por parte do direito para controlar, de alguma maneira, a tecnologia da informação, o imaginário teórico dos juristas está inescapavelmente associado à territorialidade estatal, de modo que suas tentativas de controle têm pouca ou nenhuma significância. Nesse sentido, Castells entende que

⁵² Vide item 1.3.1 supra.

⁵³ No original: “[...] to navigate the uncharted, stormy waters between the power of global networks and the challenge of singular identities.”

[...] nos próximos anos, os Estados-nações lutarão para controlar a informação circulando nas redes de comunicação globalmente interconectadas. Eu aposto que é uma batalha perdida. E, com sua eventual derrota, cairá a pedra angular do poder estatal. De modo geral, a globalização/localização das mídias e das comunicações eletrônicas equivale à desnacionalização e desestatização da informação, duas tendências por enquanto inseparáveis (CASTELLS, 2010a, p. 320-321).⁵⁴

A desnacionalização e a desestatização da informação colocam em cheque o ideal de soberania indivisível. Isso não implica, contudo, a impossibilidade de que determinados Estados tenham acesso ao fluxo mundial de informações, como ficou bem claro em virtude das recentes declarações do analista da NSA, Edward Snowden.

Naquele caso específico, tratou-se de um retorno tardio ao Estado-nação motivado pelo medo criado pela “guerra contra o terror” e que, no atual contexto, só pode ser patrocinado pelo “último dos Estados soberanos”, na expressão de Castells, cujo domínio da tecnologia da informação garante uma temporária resistência à tendência descentralizadora dos fluxos globais de dados.

Esse retorno ao monopólio da violência do Estado-nação – alimentado pela ideia de união em uma situação de exceção contra um inimigo indefinido – contraria as tendências de criação de uma rede global. Assim, “[...] ao invés de um Estado em rede aprendendo a promulgar uma governança global, estamos presenciando a manifesta contradição entre o último hurra imperial e o primeiro mundo realmente interdependente” (CASTELLS, 2010a, p. 355)⁵⁵.

Apesar dessa contradição contingencial, a dissolução da soberania na rede de poder é uma consequência do surgimento de novas estruturas não estatais de autoridade e poder. Agora, vulnerável aos ataques cada vez menos específicos – e, por isso mesmo, mais inevitáveis – das diversas fontes de poder do mundo contemporâneo, o Estado sofre a reformulação das suas funções, passando a agir não mais como centro, mas como “nó” de uma rede descentralizada de poder.

Por essa razão, Saskia Sassen (1996) entende que a soberania e o território permanecerão como características fundamentais do sistema da sociedade em rede.

⁵⁴ No original: “[...] for the years to come, nation-states will be struggling to control information circulating in globally interconnected telecommunication networks. I bet it is a lost battle. And with this eventual defeat will come the loss of a cornerstone of state power. Altogether, the globalization/localization of media and electronic communication is tantamount to the de-nationalization and de-statization of information, the two trends being inseparable for the time being.”

⁵⁵ No original: “[...] instead of a network state learning to enact global governance, we are witnessing the unfolding contradiction between the last imperial hurrah and the first truly interdependent world.”

No entanto, eles foram parcialmente desviados em direção a outras arenas institucionais fora do Estado e do modelo de território nacionalizado. Dado que a exclusividade da soberania e a do território, do ponto de vista histórico, são essenciais para o atual modelo de Estado-nação, essa mudança representa uma reconfiguração do Estado.

Dentro da proposta do Estado em rede, o poder se manifesta nas relações entre os diferentes “nós” que integram essa rede. Considerando que cada um desses nós é diferente, sua capacidade de influenciar os outros depende de uma série de fatores extremamente dinâmicos. Por isso, Manuel Castells explica que

nem todos os nós da rede são iguais e os seus interesses divergem, aglutinam ou entram em conflito, dependendo das questões e contextos. Ademais, sob certas circunstâncias, um dos componentes da rede (por exemplo, o Estado americano no início do século XXI) pode decidir por impor os seus interesses para toda a rede utilizando-se da sua capacidade organizacional superior. Ainda que seja uma situação dificilmente sustentável (caso fosse, a rede seria substituída por uma cadeia de comando global), sua lógica unilateral desestabiliza o delicado equilíbrio de cooperação e competição no qual se baseia o Estado em rede. Em última análise, o unilateralismo quebra o Estado em rede em diferentes redes e introduz uma lógica de confronto entre essas redes (CASTELLS, 2010a, p. 365).⁵⁶

Assim, o Estado-nação, com sua soberania e autoridade, é antagonizado pelos influxos dos diversos poderes que também são nós da rede, como acontece, por exemplo, quando informações sobre as atividades dos indivíduos nas suas vidas cotidianas circulam livremente entre as empresas que monetizam esses dados, sem a possibilidade de controle pelo direito estatal.

Logo, no contexto da sociedade em rede, continua a ser necessária uma teoria do Estado, visto que as relações de poder, embora não confinadas exclusivamente à esfera estatal, permanecem sendo parte de toda atividade do Estado. No entanto, passa a ser cada vez mais importante relacionar o Estado à

⁵⁶ No original: “Not all the nodes of the network are equal, and their interests diverge, coalesce, or conflict, depending on issues and contexts. Moreover, under some circumstances, one of the components of the network (e. g. the American state in the early twenty-first century) may decide to impose its interests on the whole network, using its superior organizational capacity. While it is unlikely that it can prevail systematically (if it does the network would be replaced by a global chain of command), its unilateral logic destabilizes the delicate balance of cooperation and competition on which the network state is based. Ultimately, unilateralism breaks the network state into different networks and introduces a confrontational logic between these networks.”

sociedade em uma estrutura de geometria variável de poder. Isso porque, conforme Manuel Castells,

[...] ainda que os Estados-nacionais continuem a existir, e eles continuarão no futuro previsível, eles são, e continuarão a ser cada vez mais, nós de uma ampla rede de poder. Eles serão confrontados por outros fluxos de poder na rede que diretamente contradizem o exercício da sua autoridade [...] Os Estados-nacionais podem reter a capacidade de tomada de decisões, mas, tendo se tornado parte de uma rede de poderes e contra-poderes, eles dependem de um sistema mais amplo de exercício de autoridade e influência oriundos de múltiplas fontes (CASTELLS, 2010a, p. 358)

Todavia, é um traço comum de toda a teoria do Estado a pressuposição de que este só existe dentro de uma nação. O problema passa a ser, então, como pensar uma teoria do Estado que não seja baseada na unidade da nação, mas na pluralidade de perspectivas e interesses. Por isso, continua Castells, é necessário repensar a teoria do Estado – e, acrescente-se, do direito – de modo a inserir novas categorias capazes de lidar com as novas relações de poder, especialmente, as viabilizadas pela tecnologia da informação.

Considerando a perda de poder do Estado e o fato de que, na sociedade em rede, ele é apenas mais um dos nós da rede global de exercício de controle e poder, deve-se pensar, junto à teoria do Estado, uma teoria do poder capaz de reconhecer que, embora todas as questões de Estado sejam questões de poder, nem todas as questões de poder são questões de Estado (CASTELLS, 2010a, p. 359).

Com efeito, o Estado deve ser sempre colocado em relação à sociedade de modo que seja possível distinguir as dimensões do território ao qual se refere: local, nacional e regional. Em cada um desses níveis, diversos atores – através dos seus representantes – articulam seus interesses na formação de blocos de poder. Esses níveis não são necessariamente equivalentes, ou seja, o bloco de poder na esfera local não corresponde ao da esfera nacional.

Extrapolando esse conceito, é possível determinar a existência do Estado em rede dentro de uma outra dimensão territorial – a global. No entanto, diante da inexistência de uma autoridade global legítima, a definição de objetivos globais – como a proteção dos direitos – depende da dinâmica das relações de poder expressas na rede da qual o Estado faz parte. Nessa rede, dificilmente, um Estado conseguirá fazer valer seus interesses com base na legitimidade da sociedade que representa, pois dependerá sempre das relações de poder com os demais nós da rede – o que não

impossibilita, contudo, a coordenação de interesses entre os nós para a consecução de uma vontade comum.

Essa composição do Estado em rede é incrivelmente frágil, como se pode imaginar. Sua estabilidade depende da perda de soberania de todos os nós da rede, inclusive daqueles econômica, tecnológica e militarmente mais poderosos. Assim, quando um dos nós dessa rede se recusa a perder soberania – através de atos unilaterais –, gera-se uma reação em cadeia com os demais nós agindo de igual maneira e rompendo o frágil equilíbrio da rede, num retorno tardio à modernidade sólida (CASTELLS, 2010a, p. 360).

Portanto, pode-se concluir que, dentro dessa rede múltipla de poderes nacionais, supranacionais, públicos e privados, o Estado nacional encontra dificuldades para agir unilateralmente, sobretudo, em problemas que transcendem o seu território. Sob esse aspecto, Jose Luis Bolzan de Moraes (2012, p. 35) aponta que, “em vez da unidade estatal própria dos últimos cinco séculos, tem-se uma multipolarização das estruturas, ou da falta delas [...]” nos mais diversos níveis – local ou global, público ou privado.

Um desses casos de dificuldade de ação unilateral do Estado ocorre quando ele tenta conter os fluxos de dados, objeto central deste trabalho. Conforme será explanado, a seguir, o controle desses fluxos através dos tradicionais mecanismos territorialmente vinculados – leis – demonstra as limitações de um modelo de controle do poder que desconsidera a estrutura em rede da qual o Estado é apenas um dos nós.

1.5 AS LIMITAÇÕES DO ESTADO-NAÇÃO PARA CONTROLAR OS FLUXOS DE DADOS

1.5.1 A incapacidade do Estado para controlar os fluxos de dados

A informação, já se afirmou anteriormente, é a pedra angular da sociedade contemporânea. Desde a revolução industrial, a fábrica, mais que um espaço para acúmulo do capital, já era um lugar de dominação social através da acumulação do saber (BOLZAN DE MORAIS, 1998, p. 32). A relação entre saber e poder não é novidade, mas, atualmente, está sendo completamente redesenhada ou mais precisamente, elevada a pontos inimagináveis.

O acúmulo de informações é um dos traços caracterizadores desse redesenho. No entanto, de pouco adiantaria o livre fluxo e acumulação de dados sem que existissem instrumentos capazes de analisá-los. Figurativamente, seria como possuir uma enorme biblioteca e não saber ler. É por tal razão que o surgimento de microprocessadores cada vez mais poderosos vai ao encontro do desenvolvimento dos canais para fluxo de dados.

Com efeito, a capacidade virtualmente ilimitada de coletar e, especialmente, analisar informações torna-se uma das características mais marcantes do mundo atual, de maneira que pode ser considerada o aspecto de maior relevância, tanto política quanto social, da tecnologia da informação (LYON, 2007, p. vi).

As práticas da *surveillance*, auxiliadas pela tecnologia de informação, tornam visíveis mais dados ao pequeno grupo que dispõe de recursos econômicos e técnicos para processá-los. Contudo, os critérios de coleta, análise e classificação das informações são opacos, especialmente em razão de serem conhecimentos eminentemente técnicos e, portanto, de difícil compreensão por leigos.

É por isso que a análise jurídica desses critérios, embora difícil, demonstra-se indispensável; afinal, “[...] o modo como o direito realmente funciona – ou não funciona – na prática é, também, uma consideração vital nos estudos sobre a [surveillance]” (LYON, 2007, p. 21)⁵⁷. Sob essa perspectiva, observa-se que a prática da *surveillance* deve ser submetida ao controle democrático antes de se transformar em códigos de computador, ou seja, o respeito aos direitos deve anteceder todos os mecanismos de *surveillance*.

O Estado e o direito dele originado, como visto, demonstram-se incapazes de resolver, exclusivamente, os problemas oriundos da violação de direitos pelos fluxos de dados. Essa situação fica nítida com os problemas tipicamente enfrentados pela nova cultura jurídica das sociedades complexas sendo, portanto, “[...] imperioso que se pense em provocar irritações dentro do sistema do Direito de maneira que a lógica estrutural seja uma lógica que não se confine somente na organização estatal e na Constituição” (ROCHA, KING e SCHWARTZ, 2009, p. 40).

A tentativa, por parte do “juridismo universal” (FOUCAULT, 1999), de fixar limites ao exercício dos poderes ignora o fato de que a *surveillance* está difundida em

⁵⁷ No original: “[...] how law actually works – or does not work – in practice is also a vital consideration in surveillance studies.”

todos os lugares. Como resultado, “[...] faz funcionar, ao arripio do direito, uma maquinaria ao mesmo tempo imensa e minúscula que sustenta, reforça, multiplica a assimetria dos poderes e torna vãos os limites que lhe foram traçados” (FOUCAULT, 1999, p. 184).

Por isso, o apelo exclusivo ao direito estatal pode resultar em violação dos direitos humanos, especialmente em virtude do “[...] deslocamento/ocupação dos *loci* de poder onde mesmo a democracia como procedimento ainda não chegou [...]” (BOLZAN DE MORAIS, 2012, p. 71).

Assim, é possível afirmar que o modelo estatal moderno já não é capaz de dar conta da complexidade dos movimentos estruturantes/desestruturantes da sociedade em rede, o que cria um “vácuo” a ser preenchido por formas incontroladas de poder. A formação desse “vácuo” é especialmente perigosa quando as respostas jurídicas tradicionais se pretendem aptas a solucionar completamente os problemas, criando uma falsa sensação de segurança, como será visto nos exemplos abaixo: o marco civil da Internet no Brasil, o relatório final da CPI da espionagem e a tentativa de bloqueio da rede Tor pela França.

1.5.2 Os limites do marco civil da Internet na proteção da privacidade

O marco civil brasileiro da Internet tem sido festejado por diversos setores da sociedade, sendo comumente considerado uma “constituição da Internet”. O objetivo da Lei 12.965/2014 é disciplinar o uso da Internet no Brasil, assegurando a proteção de diversos direitos fundamentais, inclusive da proteção contra violação dos fluxos de dados e das comunicações privadas armazenadas (art. 7º, incisos II e III). Dessa maneira, pretende garantir a preservação da intimidade e da privacidade, uma vez que esse conteúdo somente poderá ser acessado por ordem judicial. Será mesmo?!

Será mesmo que, como intenta o Estado brasileiro através do marco civil da Internet e da CPI da espionagem, o recurso à lei regulamentadora – instrumento tipicamente vinculado à ideia de territorialidade – é capaz de controlar os fluxos globais de dados? Qual o impacto do marco civil brasileiro no acesso indiscriminado de comunicações privadas por parte de empresas transnacionais e entidades de inteligência em servidores localizados do outro lado do planeta?

Essas perguntas são puramente retóricas. O marco civil brasileiro, por óbvio, trouxe diversos avanços – veja-se, por exemplo, a ideia de neutralidade da rede. Todavia, conforme será ressaltado, é ingênuo acreditar que as comunicações pessoais armazenadas passaram a estar protegidas em virtude da promulgação de uma lei no Brasil.

Igualmente ingênuo é acreditar – como quer o relatório da CPI da espionagem – que a elaboração de uma nova lei seria capaz de evitar a interferência nos fluxos de dados mundiais⁵⁸. As legislações de proteção de dados são essenciais para proteger os direitos humanos, mas, sem entender corretamente o fenômeno da *surveillance*, nada estará protegido. É como se o direito tentasse obter respostas sem sequer saber fazer as perguntas corretas.

Considerando todos os elementos que compõem o quadro de mudanças da privacidade na era digital, é possível afirmar que o marco civil da Internet fracassou. O artigo 7º, no conjunto dos seus incisos, é um exemplo claro do que será demonstrado nesta tese. Isso porque dá início ao capítulo que, justamente, trata dos direitos e garantias dos usuários, mas restringe esses direitos à privacidade.

O marco civil da Internet, ao proteger a vida privada (inciso I), o sigilo do fluxo das comunicações (II) e, especialmente, o sigilo das comunicações privadas armazenadas (III) não entendeu que existem outros direitos muito mais afetados pela *surveillance*.

Isso não significa dizer que a proteção da privacidade não seja importante. Entretanto, a partir dos estudos que serão aprofundados nesta obra, objetiva-se deixar claro, fundamentalmente, dois aspectos: primeiro, que é insuficiente a forma reducionista como vem sendo tratada a questão da privacidade, apenas como sinônimo de vida particular, ou seja, de intromissão nas comunicações privadas armazenadas (vide inciso III); segundo, que os problemas oriundos da “modernidade

⁵⁸ O relatório da CPI dos Crimes Cibernéticos, votado no dia 27/04/2016, sofre dos mesmos problemas de base teórica – ou seja, o retorno ao Estado como ferramenta para resolução de problemas. Em que pese discutir temas extremamente relevantes – como a imprescindível legislação criminal tipificando condutas associadas aos crimes virtuais –, a possibilidade de bloqueio de *sites* e aplicações de Internet (itens 1.5 e 1.7 do relatório) sofrem dos mesmos limites técnicos já mencionados quando se comentou sobre o direito ao esquecimento na União Europeia. Nesse sentido, o simples uso de um VPN “derrubaria” a ordem judicial que determinasse a indisponibilidade de um *site*, situação que reforça a fragilidade do uso de mecanismos territoriais para controlar fenômenos desterritorializados. Disponível em: < <http://surveillance.es/2u> >. Acesso em: 04 maio 2016.

líquida” não podem ser resolvidos a partir de soluções dependentes da territorialidade, como é o caso do marco civil.

Sob a perspectiva da fluidez e da desterritorialização dos fluxos de dados e dos servidores que guardam as comunicações privadas, o marco civil da Internet, embora seja um avanço em outros aspectos, pouco pode fazer⁵⁹. Certamente, alguma proteção é melhor que nenhuma, de maneira que há possibilidade de (pouca) efetividade dos trechos da legislação em questão⁶⁰. Porém, seria ingênuo acreditar que esse tipo de solução sólida (dispositivo legal) tem condições para lidar com a liquidez dos fluxos de dados – embora essa espécie de pensamento seja extremamente comum no imaginário jurídico do Brasil e do mundo.

Veja-se, por exemplo, o caso emblemático do *Google* em relação ao marco civil brasileiro. Seus termos de serviço garantem o seu acesso a todas as mensagens e conversas dos usuários dos seus serviços de e-mail e bate-papo⁶¹. Assim, é de se perguntar: se até mesmo os termos de serviço do *Google* – uma empresa com representação no Brasil que provê serviços a milhões de brasileiros, empresas e órgãos da administração pública e que, portanto, está totalmente enquadrada nos critérios do marco civil – “valem mais” do que o disposto no art. 7º, inciso III da lei 12.965/2014⁶², por qual motivo deveríamos acreditar que essa legislação será respeitada por outras empresas com muito menos vínculos no Brasil ou por agências de inteligência?

Ainda, como será visto em tópico específico sobre o tema dos metadados, sua utilização causou uma mudança importante no conceito daquilo que é “informação

⁵⁹ Vale lembrar que, mesmo se tivesse sido aprovada a proposta, que constava no projeto inicial, de obrigar que as empresas possuíssem servidores em território nacional, de nada adiantaria. Afinal, é próprio da computação na nuvem a existência de múltiplos níveis de redundância. Logo, não existe, por exemplo, somente “um servidor da empresa X, localizado no endereço Y”, mas uma infinidade de equipamentos espalhados em diversos pontos do globo. Mesmo com um servidor do *Google* no Brasil, ainda existiriam outras centenas deles em lugares completamente diversos do globo terrestre. Fica difícil, portanto, determinar “onde” está a informação: ela é ubíqua.

⁶⁰ Veja-se, por exemplo, a importância que a neutralidade da rede possui na proteção da liberdade de informação dos usuários da Internet. Em virtude dessa neutralidade, as empresas de telecomunicações ficam impedidas de discriminar o tráfego que circula da sua rede, impedindo que elas controlem quais conteúdos serão acessados pelo usuário.

⁶¹ “Nossos sistemas automatizados analisam o seu conteúdo (incluindo e-mails) para fornecer recursos de produtos pessoalmente relevantes para você, como resultados de pesquisa customizados, propagandas personalizadas e detecção de spam e malware. Essa análise ocorre à medida que o conteúdo é enviado e recebido, e quando ele é armazenado.” O Termo de Serviço do *Google* está disponível em: < <http://surveillance.es/7> >. Acesso em: 29 jan. 2016.

⁶² Observe-se que, nos termos dessa mesma lei (art. 8º, inciso I), a referida cláusula do termo de serviço utilizado como exemplo deveria ser nula de pleno direito. E, mesmo assim, o *Google* continua (e, fatalmente, continuará) a analisar e-mails, bate-papos e muitas outras informações.

privada” para muito além das simples “comunicações privadas armazenadas” do marco civil. No mundo atual, as pessoas são identificadas por processos técnicos de alta complexidade e que são, em grande parte, de baixa visibilidade e *accountability* (BENNET, HAGGERTY, *et al.*, 2014, p. 74).

Os metadados, embora escapem do conceito de “comunicação privada” trabalhado no marco civil, podem dizer muito mais sobre a vida privada de um indivíduo do que o conteúdo de e-mails, por exemplo. A coleta, armazenamento, análise e processamento de metadados permite identificar e fazer inferências sobre os mais íntimos segredos do ser humano.

Alguns exemplos desse tipo especial de informação são: endereços IP (*Internet protocol*); números MAC (*media access control*); ESN (*electronic serial number*); SPIN (*service provider identification number*), IMEI (*international mobile equipment identity*), EMSI (*international mobile subscriber identity*); *cookies* com dados de pesquisas em mecanismos de busca e sites visitados; informações de posicionamento por satélite transmitidas para fabricantes de *smartphones* ou *tablets* e inseridas automaticamente como metadados nas fotografias feitas nesses dispositivos⁶³; informações de localização das torres de transmissão próximas de terminais móveis de telefone e Internet; origem, destinatário e hora de telefonemas, envio de mensagens e e-mails etc.

Essa lista – incompleta – é apenas um indicativo da quantidade de informações não protegidas pelo conceito de “comunicações pessoais” que podem ser utilizadas para associar qualquer indivíduo a um ponto específico no espaço e no tempo. Além disso, permitem estabelecer sua rede de contatos e relacionamentos. Nesse sentido, Bennet *et al* afirmam que, “se você sabe e combina um número suficiente de informações *online* e *offline*, você talvez tenha dados suficientes para fazer um palpite muito provável (às vezes quase perfeito) sobre quem estava fazendo o que, quando e onde” (BENNET, HAGGERTY, *et al.*, 2014, p. 74)⁶⁴.

⁶³ Recentemente, o exército russo encontrou-se em uma situação delicada depois que um soldado postou uma foto durante operação militar na rede social *Instagram* e os dados gravados pelo GPS do seu telefone celular mostraram que ele estava em território ucraniano controlado por rebeldes russos. A matéria completa de Laurie Segall para a CNN está disponível em: < <http://surveillance.es/2i> >. Acesso em: 28 abr. 2016.

⁶⁴ No original: “If you knew and combined enough online and offline information, you might have enough data to make a highly probable (sometimes almost perfect) guess about who was doing what, when, and where.”

Além disso, os hábitos de navegação e interação dos usuários, por exemplo, são utilizados pelas grandes empresas de publicidade *online* – como o *Google* e o *Facebook* – para direcionar anúncios “relevantes”. Atualmente, grande parte da vida real (lazer, trabalho, educação) dialoga com elementos do ambiente virtual – basta imaginar, por exemplo, sobre a impossibilidade de fazer uma viagem ao exterior sem uma consulta no *Google* ou *Bing*. O uso de redes sociais aumenta, ainda mais, esse vínculo entre “real” e “virtual”. Nenhuma dessas informações, aparentemente, está enquadrada no conceito de privacidade, o que significa que são menos protegidas, ainda que sejam tão ou mais reveladoras do que o tipo de informação protegida pelas legislações de proteção de dados e pelo marco civil brasileiro.

Se a finalidade desse tipo de legislação é proteger a privacidade dos indivíduos, é possível afirmar, desde logo, que elas falham em seu objetivo, como também será visto oportunamente no exemplo do anteprojeto de lei de proteção de dados. Assim, deve ser feita uma pergunta: como é possível proteger a privacidade em pleno século XXI se a confiança é atribuída somente a instrumentos feitos para lidar com problemas inaugurados no século XVI? É possível afirmar, *mutatis mutandis*, que o imaginário equivocado sobre os limites e possibilidades do marco civil da Internet sofre da mesma miopia da CPI da espionagem realizada pelo Senado Federal, conforme ilustrado a seguir.

1.5.3 A CPI da espionagem

O mesmo tipo de raciocínio equivocado sobre os efeitos dos fluxos de dados e a capacidade de regulamentação do Estado – já vistos no caso do marco civil da Internet – permeia o relatório final da CPI da espionagem realizada pelo Senado.

Como resposta aos eventos envolvendo Edward Snowden⁶⁵, o Senado liberou o relatório final da “CPI da espionagem” (BRASIL, 2014b). O próprio nome da CPI expressa a posição adotada em relação às informações divulgadas por Snowden. Apesar dos eventuais avanços – toda pesquisa sobre o uso da *SIGINT* (*signals intelligence*) parece ser válida, especialmente se for considerado que pouco se fala sobre o assunto –, o relatório da CPI é extremamente míope em relação à

⁶⁵ Ver item 3.1.1.

compreensão do fenômeno que quer discutir e às soluções elencadas para os problemas.

O relatório faz amplo uso da palavra “espionagem” para se referir ao seu objeto de estudo. Todavia, o problema deixou de ser mera “espionagem” ou “vigilância”, ou seja, um evento específico e dirigido contra determinados sujeitos, passando a constituir uma das características inevitáveis das sociedades contemporâneas. Não apenas grandes potências militares, como os EUA, mas, especialmente, grandes grupos privados dedicam cada vez mais esforços no desenvolvimento de tecnologia para coleta, análise e processamento de informações.

Existe, no relatório, uma mistura entre eventos pontuais de espionagem – como, por exemplo, a invasão de servidores da Petrobrás ou da Presidência da República – e eventos generalizados que, de maneira alguma, podem ser considerados “espionagem”.

A coleta massiva de metadados por entidades públicas e privadas para a elaboração de perfis (de uso, risco, preferências pessoais, compras etc.) não pode ser considerada espionagem por dois motivos principais: a) a coleta de dados não é individualizada, mas feita no atacado (salvo casos pontuais – esses, sim, de espionagem) e b) tais dados fazem parte da própria existência do ser humano nas sociedades contemporâneas.

No mundo atual, ocorre um deslocamento da ideia de “espionagem” para um conceito mais amplo de coleta e análise generalizada de quaisquer tipos de dados. Deixou-se de coletar informações específicas e passou-se a armazenar todos os tipos de informações que, individualmente, podem parecer irrelevantes, mas que, conjuntamente, são capazes de dizer muito sobre um determinado indivíduo ou grupo.

Logo, uma das características centrais dessa mudança é a prática da *data mining*⁶⁶ pela iniciativa privada. Através desse mecanismo, o *Google* pode cruzar todas as pesquisas feitas no seu sistema de busca com os dados oficiais sobre surtos de gripe e dengue (GINSBERG, MOHEBB, *et al.*, 2009). Como resultado, a empresa de *Mountain View* é capaz de prever surtos daquelas doenças com precisão e antecedência muito maior que os órgãos oficiais de controle de doenças.

⁶⁶ Detalhes sobre essa temática serão abordados no item 2.4.2.

Desfaz-se, assim, a imagem segundo a qual o problema é apenas a existência de um “grande irmão” estadunidense que deseja espionar a vida de todos⁶⁷. Muito além disso, todos os movimentos dos indivíduos nas sociedades contemporâneas podem ser coletados, processados e analisados com a finalidade de extrair um sentido daquele conjunto aparentemente caótico de dados – transações eletrônicas, detalhes de chamadas telefônicas realizadas, e-mails enviados, interações em redes sociais, posicionamento no espaço-tempo (através de tecnologias como GPS, *iBeacon* e RFID), dentre outros.

Em resumo: a tecnologia da informação destrói não apenas os muros do panóptico, mas todas as tradicionais categorias que buscam contê-la. Ela não é pública, não é privada, não está aqui, não está ali: ela está em todos os lugares como parte inerente da vida em sociedade.

Assim, falha a CPI ao considerar equivalentes eventos intrinsecamente distintos – espionagem de autoridades pela *NSA* e coleta massiva de dados de todos os indivíduos pela iniciativa pública e privada. A espionagem, conforme o próprio relatório, é a segunda profissão mais antiga da humanidade e, agora, encontra-se “turbinada” pela assimetria no poder tecnológico de países como os EUA. A *surveillance*, muito mais ampla, é uma novidade viabilizada por uma conjunção de fatores extremamente complexos e que escapam explicações simplistas da ideia de espionagem.

Como consequência, o relatório da CPI torna-se extremamente míope para a violação de direitos que não sejam a privacidade, como, por exemplo, a igualdade. Afinal, será que existe realmente igualdade se todos os passos – aparentemente aleatórios – dos indivíduos são analisados e, através de sistemas com critérios dos quais escapa qualquer ideia de democracia, eles são classificados em categorias que irão ter efeitos reais nas suas vidas (como “autorizado”, “não autorizado”, “de interesse comercial ou para segurança”, “liberal”, “democrata”, “judeu”, “católico”, “ateu” etc.)?

O problema é muito mais amplo e complexo do que a ocorrência de algumas “espionagens”. Fossem a mesma coisa, não haveria necessidade de tanto debate – tampouco de uma CPI –, porque, afinal, a espionagem é tão antiga quanto a própria humanidade. Não haveria novidade exceto do meio utilizado para espionar. Esse, obviamente, não é o caso, o que pode ser confirmado pela simples existência da CPI.

⁶⁷ Detalhes sobre essa temática serão abordados no item 2.3.

No que diz respeito às soluções propostas pelo relatório da CPI, ele busca – em uma espécie de “corrida científica do século XXI” – aumentar a capacidade do Estado brasileiro para coletar e processar dados. *Mutatis mutandis*, é como se a solução para o problema das armas fosse comprar mais armas. Em seu item VI. 1.2, o relatório reconhece que,

se existe uma afirmação que pode ser feita sobre a espionagem internacional é que esta continuará e, de fato, mostrar-se-á mais intensa com o desenvolvimento de recursos tecnológicos que permitam a operação no ambiente virtual. Essa espionagem, feita por governos, empresas e organizações não pode ser objeto de qualquer regulamentação internacional, pois é atividade típica do sistema internacional anárquico. Assim, iniciativas de se propor um regime internacional para regular o recurso à espionagem por parte de governos é, na melhor das hipóteses, utópica e ingênua. O direito internacional dificilmente alcançará o ofício dos espões. Diante dessa realidade, o que o Estado brasileiro deve fazer é investir em contrainteligência. Isso envolve mais recursos para os serviços secretos, aquisição e desenvolvimento de equipamentos, capacitação de recursos humanos e, ainda, estabelecimento de legislação que dê amparo ao setor de inteligência e permita a seu pessoal atuar em defesa do Estado e da sociedade.

Há que se concordar com a afirmação de que “o direito internacional dificilmente alcançará o ofício dos espões”. O problema, no entanto, é que o reconhecimento da *surveillance* como fenômeno impede que se fale de mera espionagem, como já se pretendeu deixar claro anteriormente. Por isso, é necessário insistir na ideia de que a compreensão equivocada do problema gera respostas igualmente erradas.

Dentre as soluções propostas pelo relatório, estão “investimento em contrainteligência”; “maior dotação orçamentária para a comunidade de inteligência”; “criação de agência brasileira de inteligência de sinais”; “criação de comissão temporária, no âmbito do Senado Federal, para propor reformas na legislação brasileira de inteligência”; “aprovação da PEC 67/2012”; “aprofundamento dos mecanismos de controle externo da atividade de inteligência”. Todas elas têm, em comum, o objetivo de fortalecer algo que deveria ser enfraquecido. Como o caso estadunidense mostra, o principal alvo desses serviços é a população. A consequência final desse desenvolvimento terá pouco a ver com uma segurança maior das “informações brasileiras” e estará muito mais direcionada contra os próprios brasileiros.

Obviamente, devem ser buscados mecanismos para proteger empresas nacionais estratégicas – como a Petrobras – ou as informações trocadas pelo alto escalão do poder público. Contudo, sem a capacidade técnica para auditar sistemas e equipamentos, é nula qualquer tentativa de proteger essas informações. Isso porque a inserção deliberada de fragilidades em sistemas essenciais é uma conhecida tática utilizada pela NSA.

É de se questionar, no entanto, se o Brasil possui alguma chance de combater esse tipo de ataque, uma vez que, por mais desenvolvida que seja a tecnologia nacional, ainda dependerá de processadores, memórias, equipamentos de rede etc., todos eles produzidos com tecnologia estrangeira.

O último – e mais importante – problema diz respeito ao pano de fundo no qual se movem as soluções apontadas tanto pelo relatório da CPI, quanto pela crença na capacidade do marco civil da Internet para regulamentar o fluxo de dados. A tecnologia da informação dissolve as fronteiras de espaço e de tempo. Perde qualquer sentido, pois, sustentar que o mecanismo “lei” – associado ao Estado vinculado a um território – possa ser capaz de conter um fenômeno marcado pela desterritorialidade.

A mudança espacial da infraestrutura defendida tanto pela CPI da espionagem, como pelos debates no anteprojeto do marco civil – através da concentração de servidores e rotas de dados em território nacional – também é de baixa relevância. Pouco importa a localização física de um determinado servidor: os fluxos de dados não conhecem as fronteiras do Estado-nação. Fica claro, assim, que não adianta pensar os fluxos de dados através de proposições baseadas na ideia de territorialidade.

Não se trata, no entanto, de um erro exclusivo do Estado brasileiro. Como será visto a seguir, a França comete o mesmo equívoco elementar em relação à rede Tor.

1.5.4 A rede Tor

O Tor – anteriormente, sigla para *The Onion Router* – é uma rede de túneis criptografados onde os roteadores da rede são os próprios computadores dos seus usuários. Foi desenvolvido pelo departamento naval da marinha dos Estados Unidos como uma forma segura de comunicação com múltiplas camadas de criptografia – daí

o nome “onion”, no inglês, cebola, fazendo referência às várias camadas que compõem aquele vegetal. É por meio do Tor que usuários do mundo inteiro conseguem acessar a chamada Internet profunda (*deep web*), uma estrutura de rede não acessível a partir de navegadores comuns de Internet.

Na rede Tor, os dados são roteados múltiplas vezes, garantindo que seja extremamente difícil⁶⁸ rastrear a sua origem. Em virtude de assegurar um maior grau de anonimato aos usuários, é amplamente utilizada para finalidades diversas, algumas benéficas – divulgação de informações por *whistleblowers* como Julian Assange e Edward Snowden⁶⁹ ou pesquisadores, jornalistas e ativistas que desejam fugir da censura imposta por um país –, outras nem tanto – comércio internacional de drogas, armas e serviços ilegais, comunicação de terroristas etc. (PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY, 2015).

Um dos famosos exemplos de finalidades ilegais da rede Tor é o seu uso para criação de mercados de venda de drogas na *deep web*. Embora tenham ocorrido sucessivos ataques por parte dos órgãos policiais ao redor do mundo, somente o *FBI* – em conjunto com a *NSA* – conseguiu desarmar um dos maiores sites de venda de drogas na *deep web*. Naquele site, chamado *Silk Road*, os usuários podiam comprar livremente narcóticos utilizando criptomoedas – sendo a mais conhecida delas o *Bitcoin*.

Embora tenha conseguido derrubar um site dentro da *deep web*, algo que só poderia ser feito com muito esforço, tempo e, especialmente, com o uso dos avançados sistemas da *NSA*, no dia seguinte, já existiam diversos outros sites similares, no que pode ser denominado “efeito hidra”⁷⁰.

Logo, até mesmo o mais potente Estado-nação, detentor do maior aparato tecnológico e militar existente, os EUA, tem dificuldades para agir dentro da rede Tor – afinal, aquele país levou mais de dois anos para conseguir localizar o servidor do *Silk Road*. Isso demonstra a diferença no tempo do Estado e no tempo da tecnologia,

⁶⁸ Embora seja muito difícil rastrear servidores dentro da rede Tor, as revelações de Edward Snowden demonstraram que a *NSA* possui ferramentas capazes de identificar nós naquela rede.

⁶⁹ A rede Tor foi indispensável para a divulgação dos eventos envolvendo Edward Snowden, conforme será analisado no item 3.1.1.

⁷⁰ A hidra é um animal da mitologia grega. Era um monstro, filho de Tifão e Equidna, que habitava um pântano no lago de Lerna, na Argólida. Possuía corpo de dragão e sete cabeças de serpente. Ao tentar cortar uma das suas cabeças, outras duas surgiam no lugar, tornando o animal quase imortal.

além de, obviamente, ser irônico⁷¹ o fato de que um *software* criado por um departamento do governo estadunidense não possa por ele ser controlado.

Após os eventos envolvendo o atentado terrorista na França nos dias 07 e 09 de janeiro de 2015 o governo francês, dentre outras medidas que serão vistas posteriormente neste trabalho⁷², está tentando elaborar uma regulamentação que impeça o uso da rede Tor no território francês, uma vez que há indícios de que os responsáveis pelo ataque utilizaram essa rede para troca de mensagens⁷³. Outros países que seguiram o mesmo caminho – como é o caso do Irã e da China – não alcançaram sucesso completo em virtude das medidas evasivas dos usuários interessados em entrar na rede.

Esse exemplo, assim como os anteriores, possuem um liame comum: demonstram como o Estado, pelo menos nos moldes como é conhecido, é uma das primeiras instituições a sentir o distanciamento, típico da “modernidade líquida”, entre política – entendida como a capacidade de escolher as ações a serem tomadas – e poder – entendido como a capacidade de agir (BAUMAN e LYON, 2013), especialmente diante daquilo que aqui se denomina *surveillance*, conceito que será construído no capítulo a seguir.

⁷¹ No caso, para ser mais preciso, não se trata, exatamente, de uma ironia, mas de uma demonstração clara da vantagem na adoção de um modelo de código-fonte aberto, para programas de computador.

⁷² Ver item 3.1.2.

⁷³ O governo francês propôs a proibição dos pontos de Internet *Wi-Fi* compartilhados, visto que eles garantem a navegação potencialmente anônima dos usuários. Pelo mesmo motivo, busca, assim como muitos governos em países totalitários, banir o uso da rede Tor. A matéria completa de Andrew Griffin para o jornal *Independent* está disponível em: < <http://surveillance.es/2n> >. Acesso em: 01 maio 2016.

2 SURVEILLANCE OU VIGILÂNCIA? ESTABELECENDO UM CONCEITO

*Welcome my son, welcome to the machine
Where have you been? It's alright we know where you've been
What did you dream? It's alright we told you what to dream
So welcome to the machine*

(Pink Floyd – Welcome to the machine)

No 24º filme da série 007, *Spectre*, James Bond luta contra a formação de uma organização mundial de cooperação entre múltiplos países e empresas cuja finalidade é coletar dados em massa com a suposta finalidade de desenvolver atividades de inteligência dos Estados envolvidos.

Trata-se, por motivos óbvios, de um tema bastante atual. Afinal, desde as declarações de Edward Snowden – que, inclusive, valeram à Laura Poitras o Oscar de melhor documentário de 2014 – há informação de que agências de inteligência – em especial a NSA e o GCHQ – realizam a coleta massiva de dados dos indivíduos no mundo inteiro.

No entanto, e daí surgiu a necessidade desta pesquisa, o cenário nacional não incorporou muito bem esses fenômenos. Boa parte disso se deve à ideia de que o que existe é uma “vigilância”, ou seja, de que há alguém – geralmente um governo – espionando tudo o que se faz. Afinal, se alguém está sob vigilância, existe sempre outra pessoa vigiando, correto? Errado.

Para evitar equívocos como esse, o presente capítulo será dedicado à construção de um conceito que seja capaz de superar a ideia de “mera” vigilância. Nesse sentido, será exposto que o conceito de *surveillance*, importado diretamente do inglês, deve ser utilizado para se evitarem algumas confusões teóricas sobre o fenômeno que está sendo analisado.

Para tanto, é indispensável, inicialmente, demonstrar a insuficiência semântica da utilização do vocábulo “vigilância”, uma vez que está associada a um paradigma em crise, especialmente em virtude do surgimento dos meios eletrônicos de tratamento⁷⁴ de informação. O papel das máquinas – ou seja, da tecnologia de

⁷⁴ Adota-se, neste trabalho, uma concepção ampliada de tratamento de dados que é baseada no anteprojeto de lei de proteção de dados – analisada no item 2.5.2 infra. Nesse sentido, tratamento de dados é toda operação realizada com quaisquer tipos de dados e metadados, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

informação – na superação do conceito de “vigilância” é fundamental, pois não se trata apenas de uma modificação quantitativa – mais informação –, mas qualitativa – quais os tipos de informação e quais conhecimentos podem ser extraídos dela.

Dessa forma, o que se busca é diferenciar a vigilância no sentido tradicional – ou seja, como espionagem, controle e investigação sigilosa de atividades individuais – das técnicas viabilizadas pela tecnologia da informação que, por sua natureza, são endêmicas nas sociedades contemporâneas. Tais técnicas têm como objetivo a sistemática coleta, armazenamento, processamento, individualização e classificação das informações sobre as pessoas em determinados grupos.

Veja-se, por exemplo, o caso do *site* “*Apply Magic Sauce*”⁷⁵, utilizado pelo centro de psicometria da universidade de Cambridge para aplicação do estudo de Kosinski, Stilwell e Graepel (2013). Através de informações publicamente disponíveis, é possível fazer inferências, com precisão de até 93% de acertos, sobre aspectos íntimos dos usuários da Internet⁷⁶. No caso específico do *site*, são utilizadas as informações sobre as “curtidas” do usuário no *Facebook* – embora, afirmem os autores, possam ser usados quaisquer tipos de dados para alimentar o mesmo mecanismo preditivo – para chegar a conclusões sobre traços de personalidade, sexo, opção sexual, inteligência, satisfação com a própria vida, idade, área de concentração profissional, opinião política e religiosa.

Isso não significa, contudo, que o aspecto tecnológico seja o único na análise do fenômeno. Ele não está “descolado” das realidades social, econômica e política, ainda que a tecnologia seja o instrumento necessário para coletar, armazenar, processar, classificar e transmitir informações. Ao invés de ser um aspecto externo – como remete a ideia de “vigilância” –, a tecnologia é parte da textura que compõe a vida nas sociedades contemporâneas.

Como forma de superar o tradicional conceito de vigilância, serão expostas as duas principais metáforas utilizadas para explicar esse fenômeno: a ideia de *Big Brother*, derivada do romance de George Orwell e o modelo panóptico, de Jeremy

⁷⁵ Pode-se fazer o teste do próprio perfil do *Facebook*. Para usuários acadêmicos e empresas, é possível inserir um grupo de indivíduos e obter a análise pronta. Disponível em: < <http://surveillance.es/q> >. Acesso em: 15 fev. 2016.

⁷⁶ A maior precisão das análises (93%) refere-se à identificação de uma pessoa como mulher. A orientação sexual tem precisão de 88% para homens e 75% para mulheres. Para uma lista completa, consultar a documentação com as informações sobre a precisão das análises. Disponível em: < <http://surveillance.es/r> >. Acesso em: 15 fev. 2016.

Bentham e Michel Foucault. A superação dessas metáforas é primordial, pois, conforme o alerta de Daniel Solove (2004), as metáforas não são apenas um acessório intelectual, mas parte dos sistemas conceituais, ou seja, elas afetam a nossa forma de compreender o mundo.

Por isso, a constante referência a esses modelos na literatura tradicional limita a compreensão da realidade. Isso porque será explicado que, ao contrário do ideal do panóptico, que era uma máquina de poder cuja função era manter os indivíduos controlados dentro de um determinado espaço por meio da repressão constante, o mundo de hoje é caracterizado pela supressão das tradicionais barreiras físicas e pela sedução. Afinal, para que haja consumo no contexto da globalização, é primordial que os indivíduos sejam seduzidos e controlados fora das estruturas físicas do panóptico. Ainda, em defesa de Foucault, será demonstrado que o problema não é o modelo panóptico – afinal, o estudioso francês apenas fez uma historiografia das relações de poder do final do século XVIII até o século XIX. O equívoco, do ponto de vista da *surveillance*, consiste na utilização de um modelo que foi pensado para outra época e que, portanto, é incompatível com as relações de poder do século XXI.

A outra metáfora geralmente associada ao paradigma da vigilância, o Big Brother de George Orwell, também é analisada neste capítulo. Embora a genialidade de Orwell não deixe de surpreender – como é o caso das teletelas presentes no romance e o recente escândalo envolvendo as *SmartTVs* da fabricante *Samsung*⁷⁷ –, sua aplicação ao mundo contemporâneo é bastante limitada. Isso se deve ao fato de a tarefa de monitoramento, como será visto, ter sido expandida, tornando-se parte fundamental das estratégias de *marketing* da iniciativa privada. Como resultado, o mundo atual parece mais compatível com conjunto de *little sisters* do que com um único *Big Brother*.

Para superação dessas metáforas, é apresentado um modelo diferenciado chamado “*surveillance assemblages*”, proposto por Richard Ericson e Kevin Haggerty

⁷⁷ As *Smart TVs* da *Samsung* que utilizam reconhecimento de voz e são conectadas à Internet transmitem todas as informações que chegam ao microfone da televisão, inclusive quando ela está desligada, tanto para a *Samsung* quanto para uma terceira empresa especializada no reconhecimento de voz. Em síntese: a TV escuta tudo que é falado no ambiente e envia, para a fabricante e suas parceiras, o que se assemelha muito à teletela prevista por Orwell. Para leitura detalhada sobre o tema, remete-se à política de privacidade para *Smart TVs* da *Samsung*. Disponível em: < <http://surveillance.es/12> >. Acesso em: 16 fev. 2016.

(2000). Esse modelo dá ênfase aos fluxos discretos⁷⁸ de dados, ou seja, ao aspecto da *surveillance* que se convencionou chamar de *dataveillance*. Como alternativa de metáfora para se pensar esse modelo e como fundamento para os próximos capítulos deste trabalho, propõe-se o uso da obra “O processo”, de Franz Kafka (1999).

Por fim, à semelhança do que aconteceu no capítulo anterior, será abordada a relação do tema com as insuficiências presentes no cenário jurídico nacional. No caso, será analisado o problema dos fluxos de dados – e metadados – e como a ausência de compreensão da *surveillance* gera consequências nefastas para o anteprojeto de lei de proteção de dados e o que nele é classificado como “dados anônimos”.

Concluir-se-á que, sem a correta compreensão daquilo que é tratado neste capítulo, será impossível proteger adequadamente os direitos humanos no referido anteprojeto, o que é extremamente perigoso. A existência de uma lei essencialmente equivocada pode gerar a falsa sensação de que os direitos estão protegidos, o que é tão – ou mais – perigoso que a inexistência da lei.

2.1 VIGILÂNCIA OU SURVEILLANCE? DISTINÇÕES PARA UMA SUPERAÇÃO

2.1.1 Insuficiências semânticas

Os estudiosos, diz Saskia Sassen (1996), encontram enormes dificuldades para analisar mudanças significativas que lhes sejam contemporâneas. Os câmbios paradigmáticos, frequentemente, não podem ser “capturados” por eles, uma vez que estão tanto imersos no paradigma antigo, quanto confrontados com o ineditismo do novo.

Logo, os vocabulários, categorias e modelos disponíveis nessa situação-limite são incapazes de responder, suficiente e eficazmente, às mudanças fundamentais que causam perplexidade ao pesquisador. Nesse mesmo sentido, Wilson Engelmann, embora dissertando sobre as nanotecnologias, afirma que “vivencia-se um momento da história do conhecimento, pois está sendo gerada uma verdadeira inflexão revolucionária. São descobrimentos que não permitem a acomodação dos conceitos até então aceitos [...]” (ENGELMANN, p. 307-308).

⁷⁸ A palavra, aqui, é utilizada na acepção matemática que, conforme o dicionário Michaelis, “diz-se da quantidade que exprime seres ou objetos semelhantes, porém distintos”.

É possível traçar um paralelo entre os estudos da *surveillance* e a noção de paradigma inserida na obra “Estrutura das revoluções científicas” de Thomas Kuhn (1998). Nos períodos da ciência normal, os cientistas utilizam vocábulos próprios do paradigma compartilhados, os quais são suficientes para dar conta dos problemas existentes.

Com o progresso da ciência normal, as anomalias, inevitavelmente, aparecem. Elas passam a ser analisadas através do paradigma vigente até o momento em que suas discrepâncias se tornam grandes demais para serem ignoradas ou explicadas, o que resulta na crise de paradigma. Diante dessa situação, os pesquisadores passam a especular a respeito de novas possibilidades que ajudem a explicar essas anomalias e, quando um novo conjunto de ferramentas de análise desses fenômenos é aceito, ocorre a mudança de paradigmas. Nas palavras de Kuhn,

[...] as revoluções científicas iniciam-se com um sentimento crescente, também seguidamente restrito a uma pequena subdivisão da comunidade científica, de que o paradigma existente deixou de funcionar adequadamente na exploração de um aspecto da natureza, cuja exploração fora anteriormente dirigida pelo paradigma (KUHN, 1998, p. 126).

É neste contexto de crise paradigmática que se encontra este trabalho. Isso porque, nos últimos anos, o panóptico foi o modelo padrão nos estudos sobre a vigilância. Ainda que as práticas de vigilância sejam tão antigas quanto a própria civilização ocidental, elas adquiriram maior força na modernidade em virtude da necessidade de organização burocrática do Estado moderno. Todavia, um aumento exponencial no estudo sobre a *surveillance* somente ocorreu com o surgimento de novas tecnologias e suas nítidas consequências nos âmbitos do armazenamento e processamento de dados.

Com o tempo, passaram a surgir cada vez mais situações que não podiam ser explicadas através do panóptico. Isso porque, como demonstrado no capítulo anterior, as características inerentes às novas tecnologias e formas de organização social – especialmente a fluidez, a descentralização e a desterritorialização – possibilitaram a superação da ideia de mera vigilância – que, não se deve deixar-se enganar, continua a existir. Por isso, é possível “importar” a expressão *surveillance* para a língua portuguesa. Além de diferenciar o problema objeto deste estudo, a adoção dessa nomenclatura evita as armadilhas que uma simples tradução poderia resultar.

É exatamente o caso que se enfrenta aqui. Por esse motivo, mostra-se essencial explicar a opção pela palavra “*surveillance*”⁷⁹ para conceituar um fenômeno que, cotidianamente, tem sido simplesmente traduzido como “vigilância”, muito provavelmente na esteira da versão para o português do livro de Michel Foucault – “Vigiar e Punir”.

Sob essa ótica, é claro o alerta de Schopenhauer (2009, p. 148). Para o filósofo alemão, não é possível encontrar para cada palavra um equivalente exato em outros idiomas, de modo que, nem sempre, os conceitos designados por palavras em uma língua correspondem aos sentidos atribuídos por outra. As diversas palavras do outro idioma seriam sempre aproximações da ideia trazida pelo conceito original, mas nunca a mesma ideia. Para ele,

às vezes ocorre também que uma língua estrangeira expresse um conceito com uma sutileza que a nossa própria língua não lhe dá, de modo que o pensamos apenas naquela língua com tal sutileza. Com isso, cada pessoa que busca uma expressão exata de seu pensamento usará a palavra estrangeira, sem se importar com a algazarra dos puristas pedantes. Em todos esses casos, não é exatamente o mesmo conceito que determinada palavra de uma língua designa, em comparação com outra língua, e o dicionário oferece diversas expressões aparentadas que se aproximam do significado, só que não de modo concêntrico, mas em várias direções como na figura precedente, estabelecendo assim as fronteiras entre as quais esse significado se encontra (SCHOPENHAUER, 2009, p. 149-150).

Por isso, continua o filósofo, poemas não podem ser traduzidos, mas recriados, o que gera, frequentemente, resultados de qualidade duvidosa. Logo, ele acredita que toda tradução já nasce morta, visto que, caso se apegue à tradução literal, ela será rígida e forçada. Por outro lado, caso seja uma tradução livre, será falsa, uma vez que se tratará apenas de uma tentativa de aproximação na expressão do sentido da palavra traduzida.

Assim, embora a tradução literal – vigilância – seja linguisticamente adequada, a palavra em língua inglesa – bem como na francesa – possui uma polissemia que não é alcançada pelo termo em português. Logo, será sempre uma

⁷⁹ Para além dos motivos teóricos que serão expostos, a utilização da palavra *surveillance* terá uma vantagem prática durante a pesquisa, que é a de facilitar a compreensão de expressões que serão amplamente utilizadas, como, por exemplo, *dataveillance* e *sousveillance*.

aproximação de um conceito, não o próprio conceito⁸⁰. Ao utilizar o conceito em inglês, forma-se um novo sentido para a palavra *surveillance*, incapaz de ser abarcado pela sua tradução literal. Com situação similar, por exemplo, deparou-se Luigi Ferrajoli, quando do enfrentamento do tema da *privacy*, para quem “observou-se que o termo ‘*privacy*’ não é adequadamente traduzível para o italiano, pois inclui uma multiplicidade de direitos e aspectos não imediatamente reduzível à nossa ‘*riservatezza*’” (FERRAJOLI, 2007)⁸¹.

Sob essa perspectiva, Schopenhauer, mais uma vez, é preciso na sua avaliação. Para ele, o aprendizado de uma nova língua expande os horizontes conceituais do indivíduo, pois permite a formação de novos conceitos para designar novos signos. Sobre a passagem da ideia de vigilância para *surveillance*, é possível aplicar a disposição de Schopenhauer de que, com a utilização da palavra em inglês,

distinguem-se certos conceitos que antes constituíam juntos um conceito mais amplo, portanto mais indeterminado, exatamente porque só havia uma palavra para eles; relações que não eram conhecidas até então são descobertas, porque a língua estrangeira designa o conceito por meio de um tropus ou metáfora que lhe é peculiar. Assim, mediante a língua apreendida, toma-se consciência de uma quantidade infinita de sutilezas, semelhanças, diferenças, relações entre as coisas (SCHOPENHAUER, 2009, p. 153).

Esse problema fica evidente quando, por exemplo, tenta-se traduzir as palavras *surveillance* e *vigilance* para o português. No inglês, essas palavras não são equivalentes, de modo que não podem ser intercambiadas sem prejuízo ao sentido de um texto. Quando da sua tradução para o português, ambas costumam ser convertidas em “vigilância”, sem distinção. Até mesmo na língua inglesa, é possível verificar o limite semântico da palavra quando alguns teóricos estrangeiros fazem a distinção entre “*surveillance*” e “*new surveillance*”, respectivamente associadas à modernidade tradicional e à modernidade líquida. No entanto, a maturidade do debate no exterior permite que os autores anglófonos ressignifiquem a palavra em inglês.

Ao contrário da ideia segundo a qual o debate sobre a descontinuidade ou a continuidade do Estado depende de critérios de oportunidade, não de verdade

⁸⁰ O uso da expressão *surveillance*, inclusive, gera o efeito em cascata de facilitar o uso de expressões extremamente relevantes para esta pesquisa, mas que são de tradução igualmente difícil, como é o caso, por exemplo, de *sousveillance* ou *dataveillance*.

⁸¹ No original: “È stato osservato che il termine ‘*privacy*’ non è adeguatamente traducibile in italiano, includendo molteplici diritti ed aspetti non immediatamente riducibili alla nostra ‘*riservatezza*’.”

(BOBBIO, 2007, p. 69), a percepção sobre a existência de diferenças quantitativas ou qualitativas capazes de diferenciar vigilância de *surveillance* depende do nível de abstração adotado na análise. Isso em razão de que quanto mais abstrata a análise, menos perceptível será a diferença, ou seja, “[...] quanto mais detalhada a análise, mais fácil será ver as diferenças ou, neste caso, as mudanças” (MARX, 2002, p. 16)⁸².

As sociedades humanas sempre irão possuir determinados graus de continuidade em relação aos períodos anteriores. A coleta e uso de informações é uma atividade tão antiga quanto o próprio ser humano; no entanto, essa afirmação pueril não possibilita a adequada compreensão do fenômeno que se quer explicar. Isso se deve ao fato de que os meios que viabilizam a coleta de informações são de extrema relevância. Retomando a paráfrase de Marshall McLuhan (1969) já feita no capítulo anterior, o meio é a mensagem. Nesse sentido, Marx argumenta que

os meios importam e não são simplesmente reativos. Função ou necessidade não são a mesma coisa que estrutura ou meios. Certo que existem algumas necessidades comuns, no entanto, elas podem ser cumpridas de formas diferentes, com diferentes consequências. Eu não acredito que ganhem nada ao afirmar que os julgamentos por ordália, a tortura, o polígrafo e a análise de DNA são todos meios de coletar informações e de avaliar alegações sobre a verdade. Nem que nos ajuda muito considerar, em um certo nível, que interceptar uma mensagem de texto de um celular equivale à leitura dos sinais de fumaça de um grupo por outro (MARX, 2002, p. 17)⁸³.

A carga semântica do vocábulo “vigilância” é demasiadamente forte no Brasil, ou seja, é uma palavra que sofre de algo comparável àquilo que Lenio Streck (STRECK, 2011, p. 501) chama de “poluição semântica”. Isso que faz com que seu significado seja fragilizado, ou, ainda retomando à metáfora de Streck, sofra de “anemia significativa”. Tal fenômeno ocorre por vários motivos, inclusive por estar muito mais ligada à palavra “*vigilance*” (inglês e francês). Como resultado, na ausência de tradução que compartilhe o mesmo sentido, opta-se, neste trabalho, por utilizar o termo diretamente do inglês.

⁸² No original: “[...] the more fine-grained the analysis, the easier it is to see differences, or in this case, changes.”

⁸³ No original: “Means matter and are not simply reactive. Function or need is not the same thing as structure or means. Granted there are some common needs, yet these can be met in very different ways with different consequences. I don’t think we gain a great deal by noting that trial by ordeal, torture, the polygraph, and DNA analysis are all means of gathering information and assessing truth claims. Nor are we helped much by seeing that at some level intercepting a cellular telephone message is equivalent to one group reading another’s smoke signals.”

A distinção entre o conceito de *surveillance* e a mera vigilância é fundamental para captar todas as nuances do fenômeno que se pretende explicar neste trabalho. Contudo, isso não significa que vigilância e *surveillance* estejam completamente dissociadas, mas que a *surveillance* expressa um fenômeno muito mais complexo, que pode ou não ter componentes de vigilância.

No mesmo sentido, com o objetivo de diferenciar esta “*new surveillance*”, Gary T. Marx (2002) critica a definição do dicionário como “uma observação próxima, especialmente de um indivíduo suspeito”, crítica esta, inclusive, que pode ser aplicada ao conceito de “vigilância”.

Tradicionalmente, os estudiosos da vigilância focaram-se em quatro vertentes principais de relação, todas elas conectadas à noção de modernidade sólida: ao Estado-nação; à burocracia; à lógica tecnológica e à economia política. Em todos os casos, as propostas evidenciam um aumento do interesse das organizações nas vidas dos indivíduos (LYON, 2001, p. 109).

Embora o que se pretenda aqui, justamente, superar a ideia de vigilância –, o que importa é notar que todas as perspectivas que trabalham com essa noção estão vinculadas à ideia de modernidade sólida. Ainda assim, elas têm em comum a referência à tecnologia como uma forma de aumentar a capacidade de vigilância e “[...] frequentemente produzem novos medos a respeito do controle centralizado ou da violação da vida pessoal” (LYON, 2001, p. 113)⁸⁴.

O problema é que, ao contrário daquilo que pode ser percebido nessas análises da vigilância, a tecnologia não é simplesmente uma terceira coisa separada da vida, mas constitui o próprio tecido que possibilita as relações sociais no cotidiano do século XXI. A todo instante, as interações dos indivíduos com o mundo acontecem através da tecnologia – seja na escrita deste trabalho, no uso de dispositivos móveis de comunicação ou no pagamento de um simples café.

As deficiências das análises tradicionais na compreensão do papel das novas tecnologias da informação são sintetizadas de forma percuciente por David Lyon. Para ele, o foco dessas perspectivas nas estruturas institucionais físicas pode ser considerado

[...] uma fraqueza quando se fala das novas tecnologias, que

⁸⁴ No original: “[...] often producing some fresh fears about centralized control, or de violability of personal life.”

frequentemente têm o efeito de produzir convergência. Funções gerenciais de supervisão e monitoramento, por exemplo, são ofuscadas com a adoção das tecnologias eletrônicas. [...] A tecnologia frequentemente aparece como um fator 'externo' nas concepções anteriores, ao invés de aparecer como um modo de mediar a vida cotidiana (LYON, 2001, p. 119)⁸⁵.

Assim, o conceito de *surveillance* ultrapassa os limites da concepção tradicional de vigilância, uma vez que permite trazer a tecnologia para dentro das relações sociais. Ao invés de ser uma terceira coisa que aumenta as capacidades de vigilância, a tecnologia da informação passa a ser condição de possibilidade das interações humanas. Essa sutileza só pode ser conseguida superando-se o conceito de vigilância.

2.1.2 O papel da tecnologia na construção do conceito

Em sua obra "*Empire and Communications*", cuja primeira versão foi publicada em 1950, Harold Innis analisou diversos impérios da Antiguidade e relacionou sua ascensão à tecnologia de comunicação que possuíam. Além disso, demonstrou o conceito de *bias* – que, aqui, pode ser traduzido como "tendência" – e argumentou que as diferentes tecnologias de comunicação seriam capazes de moldar a forma de construção e organização do poder político a partir da sua "tendência" de privilegiar certas características em detrimento de outras.

Em determinados meios, pode ser que prevaleça o tempo – como nos casos da escrita entalhada em pedras –, traço característico das pequenas e pouco mutáveis sociedades da Antiguidade; em outros, como no exemplo do "*the bias of the paper*" (INNIS, 1986, p. 136) (INNIS, 2008, p. 1843), pode ser que se privilegie a expansão do espaço físico, situação ocorrida no Império Romano, que, ao utilizar a portabilidade e a efemeridade do conteúdo do papiro, se caracterizou tanto por sua vasta expansão territorial, quanto pela sua maior instabilidade social (INNIS, 1986, p. 87) (INNIS, 2008, p. 469).

Dessa forma, é possível verificar que a tecnologia de uma época é capaz de facilitar algumas manifestações de poder e dificultar outras. Por isso, ela é

⁸⁵ No original: "[...] a weakness when it comes to new technologies, which often have the effect of producing convergence. Management functions of supervision and monitoring, for example, become blurred when electronic technologies are adopted. [...] Technology often appears as an 'external' factor in earlier accounts rather than as a mode of mediating daily life."

imprescindível na elaboração do conceito de *surveillance* adequado à modernidade líquida e às revoluções tecnológicas características desse período. Isso se deve ao fato de que as tecnologias da informação desse período tenderem a privilegiar o fluxo do poder em estruturas descentralizadas e extremamente flexíveis.

Para que a ideia permaneça ecoando na mente do leitor já de antemão, é importante adiantar, com destaque, a concisa e precisa definição de David Lyon. Para ele, a *surveillance* é

[...] qualquer coleta e processamento de dados pessoais, identificáveis ou não, com o propósito de influenciar ou gerenciar aqueles que tiveram os dados coletados. [...] A [surveillance] discutida aqui não envolve geralmente pessoas monitorando outras. Ao invés disso, ela busca fragmentos factuais abstraídos dos indivíduos. Hoje, um dos meios mais importante da [surveillance] reside no poder de computação, que permite que os dados coletados sejam armazenados, combinados, recuperados, processados, comercializados e circulados (LYON, 2001, p. 2).⁸⁶

Existem três perspectivas principais quando se fala no poder que as novas tecnologias telemáticas possuem para modificar as relações sociais em relação à *surveillance*. A primeira delas é aquela segundo a qual nada mudou em relação ao passado. Para aqueles que seguem essa corrente de pensamento, as sociedades sempre necessitaram de formas de coleta de informações para fins de organização, controle e proteção. Sob essa perspectiva, seria adequado referir-se à vigilância, já que essa corrente entende que as as novas tecnologias proporcionam apenas uma mudança quantitativa, e não modificam qualitativamente o tradicional fenômeno de vigilância (MARX, 2002).

Por outro lado, as duas outras perspectivas possuem em comum o fato de compreenderem que as mudanças viabilizadas pela tecnologia da informação, muito além de modificarem quantitativamente a vigilância, alteram a sua essência de forma importante. Embora concordem nesse ponto, discordam no que se refere aos potenciais efeitos dessas novas tecnologias – ou seja, se elas são benéficas ou não.

⁸⁶ No original: “[...] any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered. [...] The surveillance discussed here does not usually involve embodied persons watching each other. Rather, it seeks out factual fragments abstracted from individuals. Today, the most important means of surveillance reside in computer power, which allows collected data to be stored, matched, retrieved, processed, market and circulated.”

De toda forma, para aqueles que concordam com ambas as abordagens, não deve parecer estranha a utilização da terminologia *surveillance* para se referir ao conjunto de fenômenos estudados neste trabalho. Afinal, as novas tecnologias de informação e comunicação alteram qualitativamente o fenômeno da vigilância, transformando-o em algo distinto, não mais explicável pelo uso da mesma palavra.

Esse desgaste do uso da palavra vigilância pode ser observado tanto no uso cotidiano – como foi visto no segmento anterior sobre a CPI da espionagem⁸⁷ –, quanto na própria definição do dicionário. Segundo o dicionário Houaiss eletrônico, “vigiar” significa “observar com atenção; estar atento; observar secretamente ou ocultamente; espreitar; espionar”.

Essa definição, assim como na crítica de Gary Marx à definição tradicional em inglês (2002, p. 10), obrigatoriamente, remete à distinção entre sujeito e objeto do ato de vigiar: uma pessoa vigia outra, o que faz absoluto sentido se o pensamento se inserir no contexto da modernidade sólida: um policial vigia um suspeito; um agente secreto vigia um alvo de interesse etc., sempre utilizando um elemento de observação atenta, especialmente visual.

De acordo com Marx, o uso de novas tecnologias da informação transforma a *surveillance*, uma vez que tais tecnologias não necessitam da proximidade física, tampouco envolvem apenas indivíduos suspeitos de terem praticado algum ato ilícito. Além disso, uma definição tradicional de “vigilância” exige polos definidos de função, visto que divide os indivíduos em “observador” e “observado”, delimitação bem mais difícil quando se trata de bancos de dados difusos, análises de padrões de dados, uso de redes sociais etc.

O fenômeno que se pretende classificar como *surveillance* não requer o uso da visão e, quando envolve, utiliza avançadas ferramentas que decompõem as informações visuais em dados quantificáveis com o intuito de extrair conclusões específicas desses dados. Por esse motivo, “o uso de múltiplos sentidos e fontes de dados é uma importante característica que engloba muito da nova vigilância”.⁸⁸ Como será visto no item relativo ao uso de *dataveillance*⁸⁹, milhares de informações são, a todo instante, coletadas e analisadas na busca de determinados padrões. Não se

⁸⁷ Item 1.5.3.

⁸⁸ No original: “The use of multiple senses and sources of data is an important characteristic of much of the new surveillance.”

⁸⁹ Item 2.4.2.

trata, portanto, de um olhar atento, mas de uma coleta generalizada de dados que são analisados sem que, necessariamente, possuam um foco específico.

Esse é o caso, por exemplo, do sistema *FAST – Future Attribute Screening Technology* –, desenvolvido pelo *DHS – Department of Homeland Security* – dos EUA, que, como será relatado posteriormente, coleta informações, inclusive visuais, para determinar se um suspeito está ou não mentindo.

Portanto, esse novo conceito de *surveillance* pode ser caracterizado, especialmente, pelo uso dos “sentidos estendidos”, ou seja, pela utilização de meios técnicos capazes de extrair ou criar informações pessoais. Tais informações não são apenas “sobre indivíduos”, visto que também levam em conta o contexto da sua coleta. Isso permite afirmar que boa parte da *surveillance* está ligada ao reconhecimento de padrões relacionais do indivíduo com os outros, com o espaço e com o tempo.

Dessa maneira, “o significado pode residir na classificação cruzada de distintas fontes de dados (como ocorre com combinação e análise de perfis) que, neles mesmos, podem não ser reveladores. Os sistemas, assim como as pessoas, são de interesse” (MARX, 2002, p. 12)⁹⁰.

A seguinte tabela serve bem para diferenciar a “*traditional surveillance*” (cuja compreensão equivale, no Brasil, à vigilância) da “*new surveillance*” (que, nesta pesquisa, é identificada apenas como “*surveillance*”). A partir dela, é possível verificar algumas dimensões utilizadas como critério para distinguir esses fenômenos.

Tabela 2 - Diferenças entre a "traditional surveillance" e a "new surveillance"

DIMENSON	A. Traditional Surveillance	B. The New Surveillance
<i>Senses</i>	<i>Unaided senses</i>	<i>Extends senses</i>
<i>Visibility (of the actual collection, who does it, where, on whose behalf)</i>	<i>Visible</i>	<i>Less visible or invisible</i>
<i>Consent</i>	<i>Lower proportion involuntary</i>	<i>Higher proportion involuntary</i>
<i>Cost (per unit of data)</i>	<i>Expensive</i>	<i>Inexpensive</i>

⁹⁰ No original: “Meaning may reside in cross classifying discrete sources of data (as with computer matching and profiling) that in and of themselves are not of revealing. Systems as well as persons are of interest.”

<i>Location of data collectors / analyzers</i>	<i>On scene</i>	<i>Remote</i>
<i>Ethos</i>	<i>Harder (more coercive)</i>	<i>Softer (less coercive)</i>
<i>Integration</i>	<i>Data collection as separate activity</i>	<i>Data collection folded into routine activity</i>
<i>Data collector</i>	<i>Human, animal</i>	<i>Machine (wholly or partly automated)</i>
<i>Data resides</i>	<i>With the collector, stays local</i>	<i>With 3rd parties, often migrates</i>
<i>Timing period</i>	<i>Single point or intermittent</i>	<i>Continuous (omnipresent)</i>
<i>Time period</i>	<i>Present</i>	<i>Past, present, future</i>
<i>Data availability</i>	<i>Frequent time lags</i>	<i>Real time availability</i>
<i>Availability of technology</i>	<i>Disproportionately available to elites</i>	<i>More democratized, some forms widely available</i>
<i>Object of data collection</i>	<i>Individual</i>	<i>Individual, categories of interest</i>
<i>Comprehensiveness</i>	<i>Single measure</i>	<i>Multiple measures</i>
<i>Context</i>	<i>Contextual</i>	<i>Acontextual</i>
<i>Depth</i>	<i>Less intensive</i>	<i>More intensive</i>
<i>Breadth</i>	<i>Less extensive</i>	<i>More extensive</i>
<i>Ratio of self to surveillant knowledge</i>	<i>Higher (what the surveillant knows, the subject probably knows as well).</i>	<i>Lower (surveillant knows things the subject doesn't)</i>
<i>Identifiability of object of surveillance</i>	<i>Emphasis on known individuals</i>	<i>Emphasis also on anonymous individuals, masses</i>
<i>Emphasis on</i>	<i>Individuals</i>	<i>Individual, networks systems</i>
<i>Form</i>	<i>Single media (likely or narrative or numerical)</i>	<i>Multiple media (including video and/or audio)</i>
<i>Who collects data</i>	<i>Specialists</i>	<i>Specialists, role dispersal, self-monitoring</i>
<i>Data analysis</i>	<i>More difficult to organize store, retrieve, analyze</i>	<i>Easier to organize, store, retrieve, analyze</i>
<i>Data merging</i>	<i>Discrete non-combinable data (whether because of different format or location)</i>	<i>Easy to combine visual, auditory, text, numerical data</i>
<i>Data communication</i>	<i>More difficult to send, receive</i>	<i>Easier to send, receive</i>

As diferenças propostas neste trabalho entre “vigilância” e “*surveillance*” podem ser vistas, com grande precisão, na tabela acima, embora não excluam a possibilidade de existirem outros elementos diferenciadores. Com a sistematização de Marx, é possível perceber que a *surveillance* ocorre de modo involuntário para aqueles cujos dados são coletados. Isso se torna possível pela utilização de dispositivos eletrônicos, em vez de pessoas, o que faz com que a obtenção de informações seja proporcionalmente mais barata que com os meios tradicionais.

A tabela deixa claro, também, que a coleta e o processamento de dados, como fenômeno da modernidade líquida, podem ser remotos, transcendendo, pois, o espaço. Por sua vez, a *surveillance* ultrapassa também a barreira do tempo⁹¹, uma vez que a disponibilização de dados ocorre em tempo real (presente), além de utilizar dados coletados no passado para inferir a possibilidade de um evento no futuro.

Em síntese, é possível afirmar que os pontos fundamentais da divisão de Marx são: 1) o uso de sentidos estendidos, ou seja, de ferramentas técnicas que expandem a capacidade de coletar informações; 2) a baixa visibilidade de como ocorrem, ou seja, sem que os sujeitos percebam que estão sendo submetidos à coleta de dados; 3) a sua natureza involuntária, uma vez que a *surveillance* está inserida nos aspectos mais triviais da vida humana nas sociedades contemporâneas; 4) a desnecessidade de compartilhamento do mesmo espaço físico, pois a análise de informações pode ocorrer em qualquer lugar com uma conexão de dados e 5) o menor custo associado à obtenção e processamento de informações se comparado às tradicionais técnicas de vigilância.

De maneira similar, David Lyon (1994, p. 40) fala do surgimento de uma “*new dimension of surveillance*” em virtude do uso da capacidade de processamento dos computadores agregada às telecomunicações. Essas tecnologias, para Lyon, servem como elementos que modificam qualitativamente a vigilância, transformando-a em algo diverso, pois agregam capacidades novas à coleta e análise de informações, especialmente no que diz respeito a quatro pontos: 1) a capacidade de armazenamento do sistema; 2) a capacidade de descentralização das informações armazenadas; 3) a velocidade dos fluxos de informações em uma rede ou sistema e

⁹¹ Essa relação entre a *surveillance* e o tempo será vista com, maior detalhamento, no item 3.4.

4) a quantidade de pontos de contato – ou seja, de coleta de informações – entre os sistemas e os indivíduos (LYON, 1994, p. 51-52).

Sobre esses pontos, é possível afirmar que, no mundo contemporâneo, o baixo custo das unidades de armazenamento de dados aliado à redução de tamanho dos dispositivos eletrônicos permite a guarda ilimitada de informações – expansão de escopo –, o que também viabiliza que elas sejam coletadas em um nível de detalhamento também ilimitado – expansão de profundidade.

No que se refere à capacidade de descentralização, esta deve ser considerada como uma característica intrínseca aos sistemas. Isso em razão de a estrutura das redes de comunicação permitir a distribuição dos servidores de dados em locais distintos. Importante lembrar, contudo, que descentralização não significa dificuldade de recuperação dos dados, tendo em vista que a estrutura de rede faz com que todos os nós sejam equidistantes. Como resultado, as informações descentralizadas são facilmente centralizáveis caso seja necessário reavê-las. Sob tal aspecto, “o que parece estar acontecendo em vários países é tanto a maior centralização quanto a maior descentralização” (LYON, 1994, p. 51)⁹².

O terceiro ponto, o aumento da velocidade nas comunicações, afeta a capacidade de resposta de um determinado sistema às mudanças das variáveis, ou seja, torna extremamente dinâmica a reação independentemente da distância física entre os locais de análise de dados e os locais onde ocorreram as modificações nas circunstâncias. É o caso, por exemplo, do *e-Gate*, portais automatizados de controle de fronteira que já são utilizados no Brasil⁹³.

O quarto ponto caracterizador dessa mudança qualitativa que caracteriza a *surveillance* é a quantidade de pontos de contato dos indivíduos com os sistemas de coleta de dados. Como é discorrido durante este trabalho, a quase totalidade dos momentos da vida das pessoas nas sociedades contemporâneas gera, de alguma forma, informações: telefones celulares, computadores, GPS, câmeras de segurança conectadas a bancos de dados automatizados, *tokens* de acesso, enfim, o ser

⁹² No original: “What seems to be happening in many countries is that both greater centralization and increased decentralization is occurring.”

⁹³ Esse sistema verifica a integridade do *chip* RFID do passaporte do viajante, faz uma busca por antecedentes criminais e mandados de prisão em aberto e compara, através de biometria, o rosto do viajante com aquele no banco de dados da polícia federal, tudo isso instantaneamente. A matéria completa da Secretaria de Aviação Civil para o Portal Brasil está disponível em: <<http://surveillance.es/3>>. Acesso em: 04 fev. 2016.

humano está quase sempre em contato com dispositivos eletrônicos que coletam informações diversas sobre o usuário e o ambiente ao seu redor. Essa quantidade de pontos de contato torna o indivíduo completamente visível, dificultando que ele opere fora dessa rede. “Logo, conscientemente ou não, continuamos a interagir com sistemas de [surveillance], que tecem sua teia de modo cada vez mais fino”⁹⁴.

Por isso, é possível afirmar que um dos processos-chave para caracterizar a *surveillance* é o atual uso, para finalidades diversas, de bancos de dados indexáveis no processamento de informações. As novas infraestruturas da tecnologia da informação, ao permitirem o processamento em tempo real e o armazenamento ilimitado de dados, não apenas “qualificam” a vigilância, mas introduzem mudanças qualitativas que permitem o salto aqui proposto em direção ao conceito de *surveillance*⁹⁵. Assim, “os computadores, em conjunto com as técnicas avançadas de estatística, ajudam a inaugurar uma nova dimensão da vigilância”⁹⁶ (LYON, 1994, p. 40).

De maneira similar às propostas de Gary T. Marx e de David Lyon, Colin Bennet *et al.* afirmam que “[...] devemos rotular como ‘*surveillance*’ muitas outras práticas além das escutas telefônicas ou da busca por suspeitos da polícia” (2014, p. 183)⁹⁷. Para eles, a ideia de vigilância traz à mente a imagem de agentes secretos andando por becos estreitos, espionando indivíduos, colocando escutas em ambientes, tirando fotos dos alvos, ou seja, sempre envolvendo a ideia de “vigiar”, de ver através dos olhos. No mundo atual, contudo, mais do que com os olhos, as pessoas são vistas através dos dados que elas produzem.

Dessarte, reforça-se a tese de que a *surveillance*, muito além de uma “vigilância”, é uma das grandes marcas das sociedades contemporâneas e depende intrinsecamente do uso dos bancos de dados, sistemas de informação e programas de computador. Necessita-se dessas tecnologias para se mover pelo mundo cotidiano, uma vez que é impossível escapar da ubiquidade desses sistemas de coleta

⁹⁴ No original: “Thus, consciously or not, we continue to interact with surveillance systems, which weave their web ever more finely.”

⁹⁵ De maneira similar, ver a justificativa de Manuel Castells (2010a, p. 304) para considerar a globalização atual como um fenômeno novo, distinto dos eventos associados à expansão do capitalismo no final do século XIX.

⁹⁶ No original: “[...] computers in tandem with advanced statistical techniques help inaugurate a new dimension of surveillance.”

⁹⁷ No original: “[...] we must label as ‘surveillance’ many more practices than just wiretapping or the trailing of suspects by police.”

e processamento de informações. Esse fato permite demonstrar algumas características da *surveillance* capazes de diferenciá-la das formas tradicionais de controle social. Trata-se não apenas de uma “versão eletrônica da vigilância”, mas de um fenômeno qualitativamente novo e que possui os seguintes diferenciais:

Ela transcende a distância, a escuridão e as barreiras físicas. Transcende o tempo, o que pode ser visto, especificamente, na capacidade de armazenamento e recuperação que possuem os computadores; informações pessoais podem ser ‘congeladas’, para usar a expressão de Goodwin e Humphey. Ela é de baixa visibilidade ou invisível; os indivíduos cujos dados são coletados possuem cada vez menos ciência disso. Ela é frequentemente involuntária, como notamos anteriormente. A prevenção é a sua maior preocupação; pense nas bibliotecas com livros com código de barras ou nos shopping centers com câmeras de segurança que estão lá para prevenir a perda, não para ensinar que roubar é imoral. Ela [a *surveillance*] faz uso intensivo de capital, não do trabalho, o que a torna economicamente mais atrativa. Ela envolve políticas descentralizadas de autocontrole; mais uma vez, notamos como participamos no nosso próprio monitoramento. Isso leva a uma mudança da identificação específica de indivíduos em direção a uma suspeita categórica. Ela é, simultaneamente, mais intensiva e mais extensiva. Utilizando a metáfora de Stanley Cohen, a rede é mais fina, mais maleável e mais ampla (LYON, 1994, p. 53)⁹⁸.

Por isso, é possível afirmar que o elemento “líquido” (BAUMAN e LYON, 2013) é o traço essencial do que se pretende, aqui, denominar *surveillance*. Inseridos no contexto da modernidade líquida, os fluxos de dados por sistemas de computadores tornam difícil o controle pelas estruturas tradicionais associadas à modernidade sólida, já que operam, como visto anteriormente, com noções de tempo e espaço muito diferentes.

Mostra-se claro, assim, que *surveillance* significa muito mais do que vigiar a vida de alguém ou grampear telefones. Trata-se de uma prática organizacional que possui, como resultado, a categorização de pessoas em grupos diferentes com o intuito de tratá-los diferentemente (BENNET, HAGGERTY, *et al.*, 2014, p. 6). Da

⁹⁸ No original: “It transcends distance, darkness and physical barriers. It transcends time, and this can be seen especially in the storage and retrieval capacity of computers; personal information can be ‘freeze-dried’, to use Goodwin and Humphreys’ term. It is of low visibility or invisible; data-subjects are decreasingly aware of it [...]. It is frequently involuntary, as we noted above. Prevention is a major concern; think of bar-coded library books or shopping mall video cameras, which are there to prevent loss, not to teach the immorality, of theft. It is capital – rather than labour – intensive, which makes it more and more economically attractive. It involves decentralized self-policing; again, we noted above how we participate in our own monitoring. It triggers a shift from identifying specific suspects to categorical suspicion. It is both more intensive and more extensive. In Stanley Cohen’s metaphor, the net is finer, more pliable, and wider.”

Receita Federal brasileira até o *Google*, passando pela *NSA*, *Amazon*, dentre outras, a classificação de pessoas em categorias é uma das características essenciais da *surveillance*.

Dessa forma, muito além da privacidade, a questão fundamental da *surveillance* é “como – e com base em quais critérios – somos categorizados?”. Embora nenhum instrumento jurídico estatal existente possa fornecer respostas para essa pergunta, a ausência de qualquer tentativa de proteger, por exemplo, a igualdade, como ocorre no marco civil brasileiro da Internet⁹⁹, é o símbolo do atraso do direito em relação à emergência de problemas reais que violam os direitos humanos.

Como resultado, devem ser superadas as tradicionais noções associadas à “vigilância” –, especialmente sua relação com elementos da modernidade sólida, com a ideia de panóptico ou com os modelos centralizadores, como é o caso do *Big Brother*, presente no romance 1984, de George Orwell. Com base nessa superação, que será feita a seguir, busca-se fortalecer a ideia de que a *surveillance* representa um novo paradigma nas relações de poder e demanda respostas jurídicas que levem em consideração as suas peculiaridades.

2.2 PARA ALÉM DE UM MODELO PANÓPTICO DA SURVEILLANCE

2.2.1 O panóptico e o panoptismo

Jeremy Bentham, um jurista inglês do século XVIII, publicou uma série de cartas que havia trocado com o seu irmão, um arquiteto que morava na Rússia. A publicação tinha um título grande e bastante sugestivo: “*Panopticon; or, The Inspection-House: Containing the Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in Which Persons of Any Description Are to be Kept under Inspection; and Particular to Penitentiary-Houses, Prisons, Poor-Houses, Lazarettos, Houses of Industry, Manufactories, Hospitals, Work-Houses, Mad-Houses and Schools with a Plan of Management Adapted to the Principle*” (STAPLES, 2014, pos. 798)¹⁰⁰.

⁹⁹ Como visto no item 1.5.2.

¹⁰⁰ A abreviatura “pos.” servirá, durante o trabalho, para referenciar determinados tipos de obras digitais que não trabalham com páginas, mas com “posições”.

Nessa publicação, Bentham propôs uma penitenciária panóptica como estrutura capaz de resolver diversas mazelas sociais. Essa construção possuía uma arquitetura distinta, cujo objetivo era maximizar a visibilidade que se tinha dos detentos. Na prisão panóptica, os detentos ficariam isolados em celas individuais, retroiluminadas e dispostas ao redor de uma torre de observação. Nela, guardas gozariam de uma visibilidade unidirecional: embora pudessem ver os detentos, estes não poderiam vê-los. Como resultado, os vigiados tinham plena consciência de que a qualquer momento poderiam estar sendo observados. Essa incerteza gerada nos prisioneiros era o principal objetivo do projeto arquitetônico proposto por Bentham, cujo desejo era transformar o comportamento dos presidiários através das contínuas reflexões que deveriam ter sobre as próprias atitudes.

Trata-se de um modelo que Michel Foucault propôs como paradigma do exercício do poder disciplinar exercido através da vigilância hierárquica. Nesse modelo, o poder disciplinar se dá através de “[...] um dispositivo que obrigue pelo jogo do olhar; um aparelho onde as técnicas que permitem ver induzam a efeitos de poder, e onde, em troca, os meios de coerção tornem claramente visíveis aqueles sobre quem se aplicam” (FOUCAULT, 1999, p. 143).

É através do exame que se combina a hierarquia de vigilância com o poder de sanção. Uma das consequências imediatas do panóptico é a inversão da relação de visibilidade do poder. Esse fenômeno ocorre porque, até então, o mais comum era a opulência das demonstrações de poder, porque este guardava uma relação diretamente proporcional com a visibilidade. Assim, “aqueles sobre o qual ele é exercido podem ficar esquecidos; só recebem luz daquela parte do poder que lhes é concedida, ou do reflexo que mostram em algum instante”. O poder disciplinar, por outro lado, inverte essa lógica, uma vez que o seu exercício depende da maior visibilidade dos súditos e invisibilidade de quem exerce o poder, ou seja, “é o fato de ser visto sem cessar, de sempre poder ser visto, que mantém o sujeito o indivíduo disciplinar” (FOUCAULT, 1999, p. 156).

Foucault utiliza a cerimônia política para ilustrar essa mudança proporcionada pelo exame. Na tradição anterior, esse tipo de cerimônia era extremamente suntuosa como forma de demonstrar publicamente o brilho do poder monárquico e garantir o efeito daquele poder nos súditos.

A disciplina, por sua vez, tem outro tipo de ritual: a revista ou a parada. Nesses casos, os súditos são oferecidos como objeto de observação do poder, cuja única tarefa é fiscalizar a partir de um ponto mais elevado. É o caso típico dos desfiles para autoridades ou das revistas das forças armadas pelos seus comandantes, cerimônias extremamente comuns até os dias de hoje.

Além disso, o exame busca registrar os detalhes do corpo no espaço e no tempo, pois, quando “[...] coloca os indivíduos num campo de vigilância, situa-os igualmente em uma rede de anotações escritas; compromete-os em toda uma quantidade de documentos que os captam e os fixam” (FOUCAULT, 1999, p. 157). Como resultado, a escrita aparece como elemento indispensável do poder disciplinar, especialmente quando concatenada com a lógica organizacional da criação de códigos específicos para separar categorias: códigos de doenças, de qualificação, de identificação etc.

O registro escrito possibilita a “transformação” do indivíduo em dados analisáveis, viabilizando a manutenção do saber permanente sobre as variações das suas características no decorrer do tempo. Além disso, a organização desses registros viabiliza a quantificação dessas características, tornando-as comparáveis com outros indivíduos e permitindo o agrupamento destes em virtude da semelhança daquelas. Como resultado, os indivíduos submetidos a alguma relação de subordinação – Foucault fala em crianças, doentes, loucos e condenados – tornam-se “casos”, sempre passíveis de descrição e análise.

Segundo Foucault, o panopticismo suprime dois fundamentos do “princípio da masmorra”: privar de luz e esconder. Somente se conserva o poder de trancar, já que o Panóptico é uma estrutura física com paredes. A função mais importante desse modelo é

[...] induzir no detendo um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder. Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos em uma situação de poder que eles mesmos são os portadores (FOUCAULT, 1999, p. 166).

Dessa maneira, a arquitetura panóptica permite a economia de recursos de vigilância, visto que o vigiado não precisa estar sendo visto a toda hora, mas somente

deve internalizar essa sensação. Ao permitir a ruptura da dualidade do binômio “ser e ser visto”, o panóptico automatiza e despersonaliza o poder, que deixa de ser exercido por uma pessoa e passa a ser parte de uma estrutura – a torre central de vigilância.

Ao transferir a imagem do poder para uma máquina, o panóptico torna inútil as cerimônias de demonstração do poder, visto que a sua própria estrutura garante a assimetria entre os poderosos e os subjugados. Como resultado, deixa de ter relevância quem está dentro da torre de vigilância ou qual o motivo para o exercício do seu poder, sendo possível afirmar que “o panóptico é uma máquina maravilhosa que, a partir dos desejos mais diversos, fabrica efeitos homogêneos de poder” (FOUCAULT, 1999, p. 167).

Ainda que esse esquema remeta, imediatamente, à ideia da prisão, deve ficar claro que Foucault pensou o panóptico como uma forma de organização do poder, especialmente relevante para quando existir uma multiplicidade de indivíduos que precisam ter o comportamento gerenciado com menor emprego de recursos humanos. Ou seja,

o esquema panóptico é um intensificador para qualquer aparelho de poder: assegura sua economia (em material, em pessoal, em tempo); assegura sua eficácia por seu caráter preventivo, seu funcionamento contínuo e seus mecanismos automáticos (FOUCAULT, 1999, p. 170).

Essa estrutura pode ser transferida para o exercício do poder político através da sua inserção em qualquer função, permitindo uma reconfiguração das relações entre poder e saber, sendo, para os seus defensores, uma verdadeira panaceia. Essa transposição do panóptico para os demais aspectos da vida se deu em virtude da expansão dos dispositivos de disciplina nos séculos XVII e XVIII.

Tal expansão permitiu que o Estado pudesse, através da estatização dos mecanismos e disciplina, utilizar a polícia para exercer a vigilância permanente e onipresente do panóptico por meio de uma rede hierarquizada de agentes que, além de observar tudo e todos, elaborem registros dessas observações.

Para Foucault, o poder exercido por intermédio do panóptico torna-se leve, incorpóreo. Obviamente, essa afirmação deve ser considerada com parcimônia. Isso se deve à leveza do poder do panóptico, que só pode existir por comparação, ou seja, se for contrastada com outras formas de controle de indivíduos. Essa leveza se aplica especialmente no âmbito das prisões e demais estruturas totais, que envolvam masmorras, grilhões, correntes, enfim, uma estrutura quase medieval. Como será

visto no próximo item, o panóptico ainda exige uma estrutura pesada, inclusive com paredes físicas – afinal, trata-se de celas de prisão, que nada têm a ver com as atuais estruturas da *surveillance* – esta, sim, extremamente leve e verdadeiramente incorpórea.

2.2.2 A insuficiência do modelo panóptico diante da *surveillance*

Para o bem e para o mal, é comum, especialmente para o público não especializado no estudo da *surveillance*, visualizar, no modelo panóptico (FOUCAULT, 1999), uma ideia brilhante, pois, além de ser um exemplo “prático” de vigilância, é um arquétipo da estrutura do poder nas sociedades da modernidade.

No entanto, também é comum que, na literatura especializada da *surveillance*, “[...] a simples menção do panóptico provoque suspiros exasperados. Para eles [os teóricos da *surveillance*], muitos esperaram demais do panóptico e, como resultado, esse diagrama é utilizado em cada oportunidade concebível para, bem, explicar a [surveillance]” (BAUMAN e LYON, 2013, p. 52)¹⁰¹.

No modelo panóptico, o domínio do tempo e do espaço era a forma de exercer o poder. Pela sua estrutura, o panóptico é um modelo caro, vez que requer a conquista e a manutenção de um espaço, a construção de estruturas e a administração dos internos. Nas palavras de Bauman, “havia edifícios a erigir e manter em bom estado, os vigias profissionais a contratar e remunerar, a sobrevivência e a capacidade de trabalho dos internos a ser preservada e cultivada” (2001, p. 17).

É necessário questionar os limites do modelo de Bentham e Foucault para lidar com a dissolução dos muros das diversas “prisões” no mundo contemporâneo, em razão de Foucault perguntar se “devemos ainda nos admirar que a prisão se pareça com as fábricas, com as escolas, com os quartéis, com os hospitais, e todos se pareçam com as prisões?” (1999, p. 187). Como é possível perceber, todos os exemplos dados pelo filósofo referem-se aos espaços físicos que envolvem muros, grades e estruturas bem palpáveis.

Questionar, contudo, não significa negar, mas apenas reconhecer a incapacidade do modelo para lidar com a complexidade da *surveillance*

¹⁰¹ No original: “[...] mere mention of the panopticon elicits exasperated groans. For them, too much has been expected by too many of the panopticon with the result that the diagram is wheeled out at every conceivable opportunity to, well, explain surveillance.”

contemporânea. O panóptico continua a existir, inclusive fortalecido pela tecnologia da informação. No entanto, ele não é mais a estratégia de dominação universal que Bentham ou Foucault imaginavam, tendo em vista que

o panóptico tem sido deslocado e confinado às partes da sociedade 'intratáveis', como as prisões, assentamentos, clínicas psiquiátricas e outras 'instituições totais', no sentido dado por Erving Goffman. [...] Em outras palavras: práticas no estilo do panóptico estão limitadas aos lugares onde os seres humanos estão no lado do débito, declarados inúteis e completamente e realmente 'excluídos' – e onde a incapacitação dos corpos, ao invés do seu aproveitamento para o trabalho útil, é o único propósito por trás da lógica organizacional (BAUMAN e LYON, 2013, p. 56)¹⁰².

Muito além de estruturas físicas de disciplina, típicas da modernidade sólida, a *surveillance* trabalha em um outro contexto: o da modernidade líquida. As paredes não existem para os fluxos de dados, fato não abordado por Foucault. Afinal, em nenhum momento das suas reflexões, ele fez alusão à tecnologia da informação, embora elas datem de períodos em que essa análise já seria possível. Nesse sentido, David Lyon afirma que “é irônico que Foucault, que não tinha quase nada para dizer sobre computadores, tenha inspirado algumas abordagens novas e radicais sobre a [surveillance] digital” (2001, p. 114)¹⁰³.

O poder, na modernidade líquida, move-se na velocidade do sinal eletrônico, o que faz com que ele se torne extraterritorial, não mais sofrendo interferência do espaço. “Isso dá aos detentores do poder uma oportunidade verdadeiramente sem precedentes: eles podem se livrar dos aspectos irritantes e atrasados da técnica de poder do Panóptico” (BAUMAN, 2001, p. 18).

Como resultado dessa análise, será demonstrada a necessidade de ultrapassar a ideia do panóptico para compreender o mundo dos dias atuais, ou seja, para além da mera vigilância, a *surveillance*. Por essa razão, David Lyon (2006, p. 4) ressalta um problema central que faz com que o modelo panóptico não seja compatível com o atual momento histórico: quanto mais rigoroso e visível é o controle – como ocorre no panóptico –, mais ele gera resistência por parte dos indivíduos que estão submetidos.

¹⁰² No original: “The panopticon has been shifted and confined to the ‘unmanageable’ parts of society, such as prisons, camps, psychiatric clinics and other ‘total institutions’, in Erving Goffman’s sense. [...] In other words, panopticon-like practices are limited to sites for humans booked to the debit side, declared useless and fully and truly ‘excluded’ – and where the incapacitation of bodies, rather than their harnessing to useful work, is the sole purpose behind the setting’s logic.”

¹⁰³ No original: “[...] It is ironic that Foucault, who had almost nothing to say about computers, should inspire some radically new approaches to digitized surveillance.”

Inversamente, quanto mais sutil e imperceptível, ou seja, líquido, mais tende a criar os tão desejados corpos dóceis. A modernidade líquida, dirá Bauman, é pós-panóptica, pois

o que importava no Panóptico era que os encarregados ‘estivessem lá’, próximos, na torre de controle. O que importa, nas relações de poder pós-panópticas é que as pessoas que operam as alavancas do poder de que depende o destino dos parceiros menos voláteis na relação podem fugir do alcance a qualquer momento – para a pura inacessibilidade. O fim do Panóptico é o arauto do fim da era do engajamento mútuo: entre supervisores e supervisados, capital e trabalho, líderes e seguidores, exércitos em guerra. As principais técnicas do poder são agora a fuga, a astúcia, o desvio e a evitação, a efetiva rejeição de qualquer confinamento territorial, com os complicados corolários da construção e manutenção da ordem, e com a responsabilidade pelas consequências de tudo, bem como com a necessidade de arcar com os custos (BAUMAN, 2001, p. 18).

Ainda que Foucault fale da leveza do panóptico, o seu caráter opressivo continua, muito além das prisões, no campo dos estudos sobre a *surveillance*. Obviamente, não pelos motivos originais do projeto de Jeremy Bentham, mas por ter deixado de ser apenas um edifício prisional e ter se transformado em uma metáfora para analisar as manifestações do poder e da *surveillance* em um mundo com características imprevisíveis por Bentham e negligenciadas por Foucault (HAGGERTY, 2006).

Até mesmo pela sua importância histórica e aplicabilidade – ainda que restrita –, os estudos sobre o tema não podem ignorar o panóptico, mas, certamente, devem ir além dele. Logo, é possível afirmar que a proposta de Foucault possui uma vinculação com um determinado período da história, a saber, a segunda metade do século XIX, o que não significa que se deva abandonar a metodologia proposta por Foucault, mas somente evitar a aplicação do modelo panóptico no mundo contemporâneo. É, justamente, nesse sentido que David Murakami Wood afirma que

parece muito estranho, portanto, para aqueles estudando a [surveillance] quase dois séculos depois de 1840, tomar o panoptismo como fundamento teórico para qualquer novo desenvolvimento sociotecnológico, como se nada tivesse mudado em termos de poder/conhecimento, ao invés de seguir Foucault em seu método e rastrear a inextricavelmente interligada evolução histórica das tecnologias punitivas e das relações de poder e objeto (MURAKAMI WOOD, 2007, p. 251)¹⁰⁴.

¹⁰⁴ No original: “It seems very strange, therefore, for those studying surveillance almost two centuries after 1840, to take panopticism as a theoretical base for any new sociotechnological development, as if

Um pouco mais radical é a proposta de Kevin Haggerty (2006). Para ele, o paradigma do panóptico e sua pretensão de totalidade devem ser abandonados. O excessivo apego a esse modelo pode resultar na imobilização dos estudos da *surveillance*, uma vez que essa escolha limita o campo de conhecimento do pesquisador. Isso ocorre porque o panóptico pré-determina quais as análises que devem ser priorizadas e, pior, negligenciadas, ainda mais por serem tão comuns as tentativas de extrapolação da aplicação do modelo panóptico na busca por explicar fenômenos que, dificilmente, podem ser abarcados pela proposta de Foucault.

Como consequência dessa predileção pelo modelo panóptico, é possível verificar a ampla remissão da literatura aos diversos “-ópticos”. Para citar alguns:

[...] ‘omnicon’, ‘ban-opticon’, ‘global panopticon’, ‘panspectron’, ‘myoptic panopticon’, ‘fractal panopticon’, ‘industrial panopticon’, ‘urban panopticon’, ‘pedagopticon’, ‘polyopticon’, ‘synopticon’, ‘panoptic discourse’, ‘social panopticism’, ‘cybernetic panopticon’, ‘neo-panopticon’ [...] (HAGGERTY, 2006, p. 26)¹⁰⁵.

Cada um deles representa uma expansão/adaptação do modelo de Foucault, com distinções para superar as limitações do original. Isso demonstra, além da óbvia popularidade da ideia, a incapacidade do panóptico para lidar com os aspectos dessa nova *surveillance*, já que cada novo “óptico” aponta para uma limitação do modelo de Foucault no mundo contemporâneo.

Por isso, contra a permanência da metáfora do panóptico, Kevin Haggerty é bem radical. Segundo ele,

[...] mudanças nos processos e práticas da [surveillance] estão diminuindo progressivamente a relevância do modelo panóptico na compreensão da [surveillance] contemporânea. Foucault continua a reinar de modo supremo nos estudos da [surveillance], mas talvez seja hora de cortar a cabeça do rei. O modelo panóptico esconde tanto quanto revela, dando ênfase a processos de relevância cada vez menor enquanto ignora ou despreza as dinâmicas que estão fora dos seus limites teóricos (HAGGERTY, 2006, p. 27)¹⁰⁶.

nothing had changed in terms of power/knowledge, rather than to follow Foucault in his method, and trace the inextricably interlinked historical evolution of punitive technologies, and power and object relations.”

¹⁰⁵ Haggerty faz a associação entre cada uma das expressões e os respectivos autores. Para detalhes, remete-se o leitor à página indicada na citação.

¹⁰⁶ No original: “[...] changes in surveillance processes and practices are progressively undermining the relevance of the panoptic model for understanding contemporary surveillance. Foucault continues to reign supreme in surveillance studies and it is perhaps time to cut off the head of the king. The

A perspectiva panóptica, para Foucault, tem, como objetivo principal, induzir um estado consciente de visibilidade capaz de assegurar a automaticidade do poder. Esse estado de autoconsciência induzido na relação entre observador-observado não ocorre na maioria das situações encontradas no paradigma da *surveillance*. Muito pelo contrário, existem diversos motivos – geralmente comerciais ou políticos – para ocultar tanto os detalhes sobre quais informações são coletadas, quanto o modo como elas são processadas. Como defendido neste trabalho, esse é um dos principais traços que permitem o surgimento de novas relações de invisibilidade: a ausência de transparência sobre como a *surveillance* opera é uma das suas mais importante característica na sociedade pós-panóptica.

A proposta de Bentham, certamente, ultrapassou a prisão para a qual foi originalmente pensada, mas um traço comum entre todas as suas posteriores aplicações é a aposta na racionalização como ferramenta para economizar recursos e aumentar a eficiência das manifestações de poder. No mundo contemporâneo, contudo, a *surveillance* está envolvida em uma infinidade de projetos que vão desde a suposta “guerra contra o terror” até o incentivo ao consumo – por exemplo, através da compilação de bancos de dados com preferências de compras dos clientes de determinadas empresas. Sob esse aspecto, é possível afirmar que

[...] a [surveillance] sai dos recintos enclausurados e passa a permear toda a vida. A [surveillance] é universal uma vez que ninguém está imune ao seu olhar. A [surveillance] também é universal uma vez que onde quer que novos sistemas sejam adotados, eles tendem a ter uma característica tecnológica similar (LYON, 2007, p. 56)¹⁰⁷.

Assim, é cada vez mais difícil identificar a *surveillance* simplesmente como uma forma de controle social, como sugere a ideia do panóptico, porque os sistemas e práticas evoluem de modo imprevisível e incorporam características, inicialmente, não imaginadas na sua criação.

A crescente capacidade de armazenar uma enorme quantidade de informações para só depois analisá-las de infinitos modos possíveis – fenômeno

panoptic model masks as much as it reveals, foregrounding processes which are of decreasing relevance, while ignoring or slighting dynamics that fall outside of its framework.”

¹⁰⁷ No original: “[...] surveillance comes out of specific enclosures to permeate all of life. Surveillance is universal in the sense that no one is immune from the gaze. Surveillance is also universal in the sense that wherever new systems are adopted they tend to have a similar technological character.”

conhecido como *big data*¹⁰⁸ – deixa claro o fato de que não existe uma finalidade predeterminada para a *surveillance*. Pelo contrário: assim como a tecnologia que ela utiliza, a *surveillance* é um fenômeno incapaz de ser reduzido a uma série de conceitos estáticos e, atualmente, só encontra dois limites: a capacidade técnica dos seus instrumentos e a criatividade dos indivíduos para criar novos sistemas de categorização e análise de dados.

Outra distinção é que os tipos de visibilidade relacionadas ao modelo panóptico envolvem o monitoramento de pessoas que, de alguma forma, são consideradas socialmente inferiores ou dependentes. Nesse sentido, “[...] é reminescente do funcionamento do microscópio, onde específicos grupos marginalizados ou perigosos são situados sob o olhar unidirecional dos poderosos, que podem ver sem ser vistos” (HAGGERTY, 2006, p. 29)¹⁰⁹.

A proliferação de “pontos de contato” (LYON, 1994, p. 51-52) entre tecnologia de coleta de dados e seres humanos destrói o caráter unilateral do olhar panóptico. Embora seja verdade que diversas instituições utilizam a tecnologia da informação com a finalidade de monitorar grupos considerados inferiores, o exclusivo apelo ao modelo panóptico ignora o fato de que as tradicionais hierarquias de visibilidade estão sendo completamente reconfiguradas, pois a *surveillance* ocorre de maneira onipresente nos mais diversos âmbitos da sociedade contemporânea, não sendo direcionada exclusivamente contra grupos desfavorecidos.

Haggerty (2006, p. 32) também reitera a crítica de que Foucault desconsiderou as mudanças viabilizadas pela tecnologia da informação, um dos traços diferenciadores entre *surveillance* e vigilância. O panóptico falha ao não incorporar os avanços tecnológicos da sua época. Como resultado, aqueles que adotam esse modelo de análise acabam por ter de fazer modificações tão fundamentais que melhor seria se não o utilizassem.

Ainda que possa ser feita a tradicional defesa de que Foucault pensou nas estruturas do século XIX, como já mencionado anteriormente neste trabalho, Haggerty não aceita essa linha de argumentação. De acordo ele,

[...] a negligência de Foucault com as tecnologias contemporâneas

¹⁰⁸ Sobre o tema do big data, ver item 3.3.2.

¹⁰⁹ No original: “[...] it is reminiscent of the functioning of a microscope, where specific marginalized or dangerous groups are situated under the unidirectional gaze of the powerful who can watch while remaining unseen by their charges.”

não deve ser rejeitada tão facilmente. Foucault não era um historiador exclusivamente interessado em compreender os desenvolvimentos característicos de um período de tempo específico. Suas preocupações históricas eram parte de um projeto para escrever a história do presente como um meio de detalhar as relações de poder contemporâneas. A esse respeito, ele não pode recorrer à justificativa do historiador de que os recentes desenvolvimentos pré-datam a sua época e, portanto, não são sua preocupação (HAGGERTY, 2006, p. 32-33)¹¹⁰.

Ainda, o modelo panóptico falha ao explicar a dinâmica da relação de visibilidade, pois pressupõe que os indivíduos permaneçam submissos ao olhar da torre central, o que ocorre em virtude de eles saberem que, a qualquer momento, podem estar sendo observados. Embora, em muitos casos atuais, isso seja aplicável, a *surveillance* trabalha com uma ideia de invisibilidade que não cabe nos moldes do panóptico. Tal fato ocorre porque, como será visto posteriormente no tópico sobre a *dataveillance*¹¹¹, muitas vezes, é interessante que aqueles cujos dados são coletados não tenham consciência de que isso é feito e, mais importante, desconheçam completamente sob quais critérios aqueles dados serão analisados.

Como não poderia ser diferente em assuntos com essa complexidade, aos diversos fenômenos da *surveillance* misturam-se, no mundo real, traços panópticos – ou, para seguir a linha de raciocínio desenvolvida por David Lyon (2007) “modernos” – e pós-panópticos – também, para o mesmo autor, “pós-modernos”. Entretanto, reconhecer que o modelo panóptico é incapaz de explicar todo o fenômeno da *surveillance* já permite observar melhor os complexos traços pós-panópticos que inundam o cotidiano e ameaçam os direitos humanos.

2.3 DO BIG BROTHER ÀS LITTLE SISTERS

Um outro modelo de análise da *surveillance* ficou bastante popular no imaginário comum. Talvez mais ainda que o panóptico: a distopia do *Big Brother*, presente na obra “1984”, de George Orwell, é uma imagem muito difundida da

¹¹⁰ No original: “[...] Foucault’s neglect of contemporary technology cannot be dismissed so lightly. Foucault was not a historian exclusively interested in understanding developments characteristic of a particular time period. His historical preoccupations were part of a project to write the history of the present as a means to detail contemporary power relations. In that respect, he does not have recourse to the historian’s justification that recent developments antedate his time period, and are therefore not his concern.”

¹¹¹ Item 2.4.2.

surveillance. No romance, um governo totalitário utilizava um enorme aparato burocrático e tecnológico para controlar todos os aspectos das vidas dos habitantes de Oceania. Partindo do pressuposto de que a tecnologia atual é infinitamente superior àquela pensada por Orwell – a *dataveillance*, por exemplo, é muito mais avançada e barata que a “teletela” –, é de se questionar por qual motivo não se vê o *Big Brother* nos dias atuais.

Como bem nota Kevin D. Haggerty (2006, p. 33), George Orwell se aproximou muito mais que Foucault da tecnologia existente nos dias de hoje, mesmo tendo escrito décadas antes dele. Enquanto o romancista britânico conseguiu imaginar a teletela e o falaescreve – dois dispositivos bastante interessantes, especialmente considerando que foram pensados no ano de 1949¹¹² –, Foucault, mesmo em 1975, considerava que as grandes invenções da humanidade eram os óculos e as lentes de aumento, conforme é possível notar a partir da seguinte passagem de *Vigiar e Punir*: “Ao lado da grande tecnologia dos óculos, das lentes, dos feixes luminosos, unida à fundação da física e da cosmologia novas [...]” (FOUCAULT, 1999, p. 144).

A visão de Orwell demonstra a genialidade da obra e sua pertinência para o mundo contemporâneo. A importância dos bancos de dados governamentais, manipulados pela tecnologia da informação, são visíveis no romance distópico. Da mesma maneira, o olhar do *Big Brother* era onipresente e indeterminado, situação que, de maneira semelhante ao panóptico, inibia qualquer desejo de fuga do indivíduo, uma vez que ele poderia estar sendo vigiado a qualquer momento.

Também, lembrando, assustadoramente, aspectos da atualidade, questões sobre direitos humanos, como igualdade e dignidade, são tocadas pela obra de Orwell. A dignidade, em 1984, está associada à impossibilidade de construir uma identidade própria, distinta das massas e da ideologia do partido (Ingsoc).

¹¹² Não é difícil imaginar os equivalentes da teletela e do falaescreve no mundo atual. O primeiro pode ser comparado, por exemplo, ao sensor *Kinect*, presente no Xbox, console de videogames da *Microsoft*, que possui uma câmera capaz de detectar detalhes surpreendentes do ambiente onde está instalada, inclusive fazendo reconhecimento biométrico facial dos usuários, bem como monitorando o humor – através de leitura de microexpressões faciais – e até mesmo os batimentos cardíacos dos jogadores. Já o segundo, o falaescreve, é bastante comum nas tecnologias de reconhecimento de voz amplamente disponíveis no mercado. A aplicação mais conhecida dessa tecnologia é a *Siri* – *Speech Interpretation and Recognition Interface* –, assistente pessoal desenvolvida para dispositivos da *Apple*. Para detalhes sobre a habilidade do Kinect para medir a frequência cardíaca do jogador, ver a notícia publicada pela própria fabricante do dispositivo no blog da empresa. Disponível em < <http://surveillance.es/w> >. Acesso em: 15 fev. 2016.

Para detalhes sobre o surgimento da Siri, ver a matéria de Bianca Bosker para o jornal *The Huffington Post*. Disponível em: < <http://surveillance.es/x> >. Acesso em: 15 fev. 2015.

A desigualdade é mostrada, claramente, por Orwell através dos distintos modos de exercício de controle de acordo com cada grupo social. Os membros externos do partido e a classe média eram aqueles cujo controle era exercido com maior cuidado; os proles¹¹³ – que correspondiam a cerca de 85% da população – eram mantidos nos guetos e, dada sua insignificância política para o partido, não necessitavam de maior controle. A importância, para este trabalho, está no caráter desigual e excludente que o controle social exerce na obra de Orwell.

É fundamental lembrar que a manutenção da ordem social em Oceania ocorria através do elemento centralizador do Estado, sempre no controle de toda informação. Contudo, ainda que governos centralizem uma enorme capacidade de coletar e processar dados – basta lembrar o “efeito Snowden” –, os dois traços mais importantes da *surveillance* são a descentralização e a mudança das suas finalidades – antes, para otimizar a produção, hoje, para aumentar o consumo. O grau de refino e de imbricação – novamente, como pode ser visto nas parcerias reveladas por Snowden – entre público, privado, nacional e internacional impõem o questionamento sobre os limites desse tipo de pensamento dicotômico presente na obra de Orwell.

Todavia, é certo que Orwell “[...] nunca poderia ter adivinhado o quão importante para o controle social pode ser o consumismo descentralizado” (LYON, 1994)¹¹⁴. De modo diferente do cenário excludente desenhado por Orwell, o consumo massificado, ao invés de excluir, busca incluir um número cada vez maior de pessoas no incessante círculo da economia. A *surveillance* encanta; logo, ao contrário de um Estado totalitário que, pela força, obtém determinado comportamento, o que se vê, no mundo contemporâneo, é a presença “amiga” e personalizada das empresas privadas.

Tais empresas, com o intuito de proporcionar, cada vez mais, uma experiência de consumo individualizada e interativa, utilizam mecanismos sutis da *surveillance* dentro daquilo que Mark Andrejevic (2007, p. 2) chama de invólucro digital – *digital enclosure*¹¹⁵. Nesse invólucro, protagonizado pelas grandes empresas de varejo e

¹¹³ Esses seres não humanizados, segundo a obra, “nasciam, cresciam nas sarjetas, iam para o trabalho aos doze, atravessavam um breve período de floração da beleza e do desejo sexual, casavam-se aos vinte, atingiam a maturidade aos trinta, e em geral morriam aos sessenta” (Cap. 7) (ORWELL, 2009).

¹¹⁴ No original: “[...] never guessed just how significant a decentralized consumerism might become for social control.”

¹¹⁵ Sobre o tema, ver item 4.1.3.

tecnologia – por exemplo, *Google, Facebook, Amazon, Apple, Microsoft, Yahoo, Walmart*, dentre outros – cada movimento gera uma informação sobre ele mesmo¹¹⁶. Essas informações são utilizadas com a finalidade de aumentar o consumo de produtos e serviços, retroalimentando, sem limites, o sistema.

A apropriação privada dos mecanismos da *surveillance* – que deixaram de ser uma ferramenta de controle da produção na fábrica para se tornarem uma forma de aumento do consumo – tem importância talvez, ainda maior, para a sua análise no mundo contemporâneo. Essa é a reviravolta que Orwell não conseguiu prever e que, em parte, demonstra a incapacidade dos discursos que se focam na perda de privacidade como resultado da ação estatal. É por isso que, talvez, Aldous Huxley, na obra “Admirável mundo novo”, ou Franz Kafka, na obra “O processo”, consigam se aproximar, com mais precisão, das formas como a *surveillance* opera no mundo atual.

Uma das características centrais dessa mudança é a prática da *data mining*¹¹⁷ pela iniciativa privada. Essa expressão, em língua inglesa, está relacionada ao armazenamento indiscriminado de todo tipo de informação não processada – *raw data* – com a finalidade de, posteriormente, aplicar algoritmos computacionais para extrair quaisquer informações que sejam relevantes. Assim funcionam, por exemplo, os mecanismos publicitários utilizados em sistemas de e-mails ou redes sociais: ao armazenarem todo o conteúdo das mensagens trocadas ou das interações realizadas, possibilitam a classificação das preferências dos usuários, tornando a publicidade cada vez mais direcionada e precisa.

Os exemplos da utilização das técnicas da *surveillance* pela iniciativa privada para incentivar o consumo são inúmeros, mas demonstrá-los, exaustivamente, não é o objetivo deste fragmento do trabalho. Tais exemplos servem apenas para ilustrar como a *surveillance* é parte da vida de cada indivíduo, especialmente, quando no papel de consumidor.

Pesquisas na internet, compras, listas de amigos, atividades praticadas: todas essas informações alimentam bancos de dados que são explorados com a finalidade de identificar a melhor maneira de aumentar o consumo de determinado indivíduo – sim, a especificidade da coleta de dados permite, inclusive, a individualização dos consumidores. Por esses motivos, Zygmunt Bauman e David Lyon acreditam que

¹¹⁶ Esses “dados que geram dados” são, na realidade, metadados, tipo de informação que será analisada no item 2.5.1.

¹¹⁷ O *data mining* será melhor analisado junto com *big data* no item 3.3.2.

[...] os departamentos de pesquisa e desenvolvimento das grandes empresas estão no processo de assumirem a liderança do atual cenário de desenvolvimento de equipamentos e estratégias da [surveillance], deixando para trás os laboratórios militares ultrassecretos (BAUMAN e LYON, 2013, p. 129)¹¹⁸.

Com efeito, é possível argumentar, com Manuel Castells, que se desfaz a imagem do *Big Brother*, dado que o estatismo orwelliano perdeu força com a pluralidade dos *loci* da *surveillance*. De acordo com ele,

a tecnologia seguiu uma trajetória diferente durante esta última metade de século, algo que, certamente, era possível. No entanto, o estatismo desintegrou-se em contato com as novas tecnologias da informação, ao invés de tornar-se capaz de controlá-las; e as novas tecnologias da informação liberaram o poder da estrutura em rede e da descentralização, o que, na realidade, minou a lógica centralizadora das instruções unidirecionais, verticais da burocracia. Nossas sociedades não são prisões ordenadas, mas selvas desordenadas (CASTELLS, 2010a, p. 341).¹¹⁹

Logo, o referido autor também concorda com a ideia de que o problema real da *surveillance* no mundo contemporâneo envolve, especialmente, a coleta de dados por parte da iniciativa privada. Ou seja, ao invés de ser a ferramenta de um *Big Brother* opressor, a *surveillance* é utilizada por uma infinidade de “*little sisters*”, cujo objetivo principal é conhecer melhor o indivíduo-consumidor através da invasão de todas as esferas da sua vida. A *surveillance* deixa de ser uma característica de um Estado burocrático vigilante e passa a ser um traço da sociedade contemporânea.

Paradoxalmente, os recentes eventos envolvendo Edward Snowden parecem fortalecer as teorias amparadas no *Big Brother* orwelliano, porque, pelo menos, de maneira superficial, demonstram a capacidade de um Estado em coletar informações e controlar diversos aspectos da vida humana. Ocorre que o próprio Snowden, que possuía uma autorização de acesso em nível “*top secret*”, era funcionário de empresas privadas contratadas pela NSA – Dell e, posteriormente, Booz Allen

¹¹⁸ No original: “[...] R&D departments of big commercial companies are in the process of taking over the lead in the present-day development of surveillance gadgets and strategies from the top-secret military laboratories.”

¹¹⁹ No original: “technology had followed a different trajectory in the past half-century, something that was certainly within the realm of possibility. But statism disintegrated in contact with new information technologies, instead of being capable of mastering them; and new information technologies unleashed the power of networking and decentralization, actually undermining the centralizing logic of one-way instructions and vertical, bureaucratic surveillance. Our societies are not orderly prisons, but disorderly jungles.”

Hamilton. Na atualidade, do total de autorizações de nível “*top secret*”, – 1.406.890 – , cerca de 32% – 456.700 – foram dadas a funcionários de empresas privadas contratadas pelo governo dos EUA (OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, 2015, p. 5).

A troca de informações entre entidades públicas e privadas não é exclusividade dos Estados Unidos. No Brasil, a Receita Federal, como será visto logo adiante, utiliza as instituições financeiras privadas como fonte de informação para auxiliar no combate à sonegação fiscal. Em outra situação, o Tribunal Superior Eleitoral estava prestes a fazer um acordo com a empresa *Serasa Experian*, cujo conteúdo previa, além do fornecimento de dados públicos, a validação de informações do cadastro da Serasa com o cadastro eleitoral em troca de certificados digitais que seriam fornecidos pela empresa.

O acordo inicial foi cancelado¹²⁰, mas, em virtude de novo acordo, o TSE repassará à *Serasa Experian*, durante cinco anos, informações de CPF, número do título de eleitor, nome completo e dados relativos aos óbitos de todos os eleitores nacionais, tudo em troca de 5.000 certificados digitais que, no varejo, custam aproximadamente R\$127,00 cada.

Tais eventos deixaram claro que, talvez, além daquilo que até mesmo as mais criativas teorias da conspiração poderiam imaginar, o *Big Brother* e as *little sisters* não se excluem, mas formam uma “família grande e feliz”. Isso ficou evidente com a participação essencial das empresas privadas no repasse de dados que alimentam os sistemas da NSA. “O Estado ainda depende da violência e da [surveillance], mas não possui mais o seu monopólio, nem pode exercê-las dentro do seu invólucro nacional” (CASTELLS, 2010a, p. 344)¹²¹.

Obviamente, as abordagens que partem do *Big Brother* devem ser atualizadas, o que não significa que sejam irrelevantes. Muito do que Orwell escreveu pode ser aplicado à sociedade contemporânea, embora não seja capaz de descrever todo o problema. Com o surgimento das *little sisters*, é questionável a possibilidade de proteção dos direitos humanos quando violados pela iniciativa privada, ou seja, naquelas esferas em que, conforme alertou Norberto Bobbio (1997), a democracia não chegou nem mesmo como procedimento.

¹²⁰ Conforme notícia oficial. Disponível em: < <http://surveillance.es/13> >. Acesso em: 16 fev. 2016.

¹²¹ No original: “The state still relies on violence and surveillance, but it does not hold the monopoly on them any longer; nor can it exercise them from its national enclosure.”

2.4 AS SURVEILLANCE ASSEMBLAGES E A DATAVEILLANCE

2.4.1 As *surveillance assemblages*

Nos itens anteriores, foram demonstrados os dois modelos mais comuns de abordagem da *surveillance*: o panóptico (Foucault) e o Big Brother (George Orwell). Ainda que o autor britânico tenha ressaltado o papel importante da tecnologia no controle social, a sociedade prevista por Orwell estava fundamentada na violência e na opressão, características incompatíveis com a sedução que orienta o consumo, um dos grandes fundamentos da *surveillance* no mundo contemporâneo.

Por outro lado, o panóptico oferece uma base sociológica de análise das relações de poder, apostando na manifestação do poder como consequência da constante incerteza do monitoramento. No entanto, esse modelo envolve um meio de exclusão dos mais fracos, o que é um problema se for considerado o caráter incluyente da *surveillance* no mundo contemporâneo.

Panóptico e Big Brother são as metáforas mais comuns quando o assunto é vigilância. Contudo, embora possibilitem destacar importantes aspectos da vigilância, os modelos são limitados no que diz respeito às modernas técnicas de coleta e processamento de dados.

Um outro modo de pensar a *surveillance* é trazido por Kevin D. Haggerty e Richard V. Ericson (2000). Com base nos trabalhos de Gilles Deleuze e Félix Guattari (1997) e na ideia de agenciamento, Haggerty e Ericson estabelecem o conceito de “*surveillant assemblage*” como forma de analisar a convergência de fluxos oriundos de sistemas individuais de coleta de dados. A multiplicidade desses sistemas permite abstrair o corpo humano do seu contexto territorial, separando-o em vários fluxos distintos que podem ser recombinados em locais e modos diferentes, formando os *data doubles*, ou seja, os alteregos digitais.

Esse conceito de “*assemblage*” (agenciamento) consiste na multiplicidade de objetos distintos cuja unidade provém do fato de que eles funcionam em conjunto como uma entidade funcional. Os agenciamentos são constituídos por

[...] fluxos distintos de uma gama essencialmente ilimitada de outros fenômenos, como pessoas, signos, químicos, conhecimento e instituições. Ao escavar através da estabilidade superficial de qualquer entidade encontra-se uma série de diferentes fenômenos e processos

operando em conjunto (ERICSON e HAGGERTY, 2000, p. 608)¹²².

Os fluxos de dados, portanto, são anteriores à própria *assemblage* e, somente através dele, se fixam no espaço, ainda que temporariamente. Por isso, não é possível atribuir um caráter estável à ideia de *surveillant assemblage*. Muito pelo contrário, os fluxos convergem e desorganizam-se com incrível facilidade de acordo com o propósito que possuem em um dado momento.

É comum que as análises sobre a *surveillance* se foquem em determinadas capacidades dos sistemas tecnológicos ou práticas sociais. A ideia de *assemblage*, por outro lado, identifica a tendência de convergência dos diversos sistemas e prática. Nesse prisma, ao invés de, por exemplo, associar a *surveillance* com o modelo do estado totalitário pensado por Orwell, a ideia de *assemblage* opera com elementos que pertencem tanto ao Estado, quanto ao poder privado (ERICSON e HAGGERTY, 2000, p. 610).

A metáfora do rizoma (DELEUZE e GUATTARI, 1997) é utilizada pelos autores da ideia da *surveillant assemblage* para demonstrar a expansão da *surveillance* no mundo contemporâneo. Isso porque, para os filósofos franceses, os rizomas são estruturas de algumas plantas cujos brotos têm a capacidade de ramificar-se em qualquer ponto e funcionar como outras partes – raiz, talo ou ramo – independentemente da sua localização na estrutura da planta

Por definição, os rizomas são não lineares, não unitários e não binários. Ao contrário do modelo da árvore, com sua tendência centralizadora, típica dos sistemas hierárquicos de decisão e controle, os rizomas são descentralizadores, já que eles podem ser entendidos como uma série de nós interconectados que crescem nas mais distintas direções, e não são afetados caso um determinado ponto dessa estrutura seja danificado. É justamente essa característica dos rizomas que Ericson e Haggerty entendem ser caracterizadora da *surveillant assemblage*. A expansão de pontos de contato (LYON, 1994, p. 51-52) entre seres e tecnologia só aumenta o número de fluxos discretos de coleta de dados.

Tanto as propostas de Foucault, quanto as de Orwell estabelecem uma situação em que os mais fracos são observados pelos (poucos) mais poderosos. A

¹²² No original: “[...] discrete flows of an essentially limitless range of other phenomena such as people, signs, chemicals, knowledge and institutions. To dig beneath the surface stability of any entity is to encounter a host of different phenomena and processes working in concert.”

ideia de rizoma modifica essa estrutura, visto que também inclui os mais poderosos nos esquemas de coleta de fluxos de dados, em razão de ser muito difícil, para qualquer grupo, por mais poderoso que seja, colocar-se de fora dos fluxos que convergem na *surveillant assemblage*. Ressalte-se que tal visibilidade dos mais poderosos não extingue a sua capacidade de controle, mas apenas modifica a forma como esse controle é exercido. A partir da estrutura do rizoma, pode-se abandonar a verticalidade do controle panóptico em decorrência daquilo que William Bogard (2006, p. 102) chama de “nivelamento rizomático”.

Com efeito, é possível estabelecer que a ideia de *surveillant assemblages* decompõe o indivíduo em diversos fragmentos que, posteriormente, poderão ser analisados com o intuito de gerenciar pessoas, gerar lucro e entreter. Diante da natureza complexa dos diversos fluxos que compõem a *assemblage*, é impossível ficar de fora dela, razão pela qual Ericsson e Haggerty falam do “desaparecimento do desaparecimento” (2000, p. 630). Uma das características primordiais dessa *assemblage* é aquilo que pode ser chamado de *dataveillance* e que será analisado no item a seguir.

2.4.2 Dataveillance

Dataveillance é uma daquelas palavras que seriam impossíveis de traduzir caso se estivesse tratando do fenômeno da *surveillance* como mera vigilância. A tradução mais simples seria “vigilância de dados”, mas isso não traria a real dimensão desse fenômeno. Dentro da ideia das *assemblages*, os fluxos discretos de dados dizem respeito à *dataveillance*, ou seja, traços de informações que, embora fluam de modo separado, podem ser rematerializados na construção de um conjunto de dados coerente.

O surgimento da expressão é atribuído ao cientista da computação Roger Clarke em textos dos anos de 1980 (CLARKE, 1988, 2003; MITROU, 2010)¹²³. Trata-se da aglutinação das palavras *data* e *surveillance* e pode ser definida como o uso

¹²³ Por outro lado, um dos projetos de big data do Google, o “Google Books Ngram Viewer” informa que a primeira vez que a palavra *dataveillance* surgiu em uma publicação no idioma inglês foi em 1973, no título do volume 4, edição nº 1 da Columbia Law Review: “Surveillance, Dataveillance, and Personal Freedoms: Use and Abuse of Information Technology”. O serviço Ngram Viewer pode ser consultado em < <http://surveillance.es/b> >. Acesso em: 12 fev. 2016.

sistemático de sistemas de dados pessoais na investigação e monitoramento de ações e comunicações de um ou mais indivíduos.

Esse deslocamento em direção aos dados ocorreu porque monitorar pessoas ou grupos sempre foi uma tarefa dispendiosa do ponto de vista de recursos humanos e econômicos, mesmo quando existe o suporte tecnológico, como é o caso dos CFTVs, que necessitam de uma enorme quantidade de agentes para monitorar as imagens.

A percepção das pessoas sobre a *dataveillance* ainda tende a ser incrivelmente baixa, especialmente em virtude da hegemonia de modelos como o panóptico e o Big Brother, em que predomina o aspecto visual, mais relacionado à vigilância do que à proposta da *surveillance*. Embora a vigilância ainda seja um problema em determinados contextos, conforme já salientado, a coleta massiva de dados faz parte de um outro patamar de complexidade.

Sistemas eletrônicos produzem, constantemente, uma enorme quantidade de dados¹²⁴. Com o crescente número de pontos de contato entre o mundo físico e o virtual, praticamente toda atividade humana gera um fluxo discreto de dados que pode ser reconstruído posteriormente conforme a demanda. A criação de metadados ocorre em todos os momentos do dia normal da vida em sociedade: nas relações sociais mediadas eletronicamente, nas transações comerciais ou, até mesmo, no simples ato de andar pela rua – afinal, um *smartphone* típico, constantemente, envia os dados de geolocalização do usuário para o fabricante e outras empresas.

A utilização de fluxos de dados discretos oferece um amplo leque de vantagens na análise de pessoas e grupos, já que esse tipo de análise é mais barata; pode ser feita simultaneamente em um número maior de pessoas; é “transparente” ao cotidiano dos indivíduos, ou seja, não é invasiva; ocorre de forma automática e é ubíqua (SCHNEIER, 2015). Cada um desses aspectos será analisado doravante.

Historicamente, as empresas coletavam poucas informações sobre os seus clientes, geralmente, apenas o necessário para alcançar algum objetivo imediato, como a venda de um produto. Até mesmo sistemas de busca, como o Google,

¹²⁴ Em 2013, a *Incapsula*, uma empresa de segurança cibernética, concluiu que os dados gerados automaticamente – sem nenhuma intervenção humana – já somavam mais de 61% do tráfego da internet. A matéria completa de Leo Kelion para o jornal *BBC* está disponível em: < <http://surveillance.es/e> >. Acesso em: 12 fev. 2016.

coletavam – comparando-se aos dias de hoje – poucas informações dos seus usuários.

Com a massificação do acesso aos computadores nos últimos anos, o custo da tecnologia de armazenamento e processamento diminuiu drasticamente, o que tornou economicamente viável o maior armazenamento de dados por empresas e governos. Além disso, com a atual expansão do *big data*¹²⁵, é cada vez mais vantajoso guardar o máximo de informações possíveis; afinal, sempre podem ser descobertos novos significados a partir de um conjunto de dados aparentemente irrelevante.

O barateamento da tecnologia necessária para a coleta e o armazenamento de dados permitiu um salto também em relação à identificação dos indivíduos que tinham seus dados coletados. Se, anteriormente, o custo desses sistemas permitia o foco apenas em determinados indivíduos, hoje há uma tendência de ampliação para englobar todas as pessoas.

Essas tecnologias tornaram-se baratas a ponto de serem implementados serviços de reconhecimento biométrico facial dos usuários de transporte público de cidades como Porto Alegre¹²⁶ e Manaus¹²⁷ com o intuito de verificar se o portador do cartão de gratuidade é realmente o titular daquele direito. Ou, ainda, de serem instaladas câmeras de altíssima definição na cidade de Novo Hamburgo/RS¹²⁸, região metropolitana de Porto Alegre, capazes de fazer a leitura automática das placas dos veículos que transitam nas ruas da cidade e verificar se eles possuem alguma espécie de restrição.

Similarmente, a Receita Federal brasileira passou a utilizar diversos mecanismos de análise de transações eletrônicas financeiras com a finalidade de

¹²⁵ O tema do big data será abordado no item 3.3.2.

¹²⁶ Em Porto Alegre, 1.550 ônibus já analisam, diariamente, os rostos de 240 mil usuários do transporte público. Caso o rosto do passageiro não seja o mesmo daquele armazenado pela empresa, é gerada uma notificação que pode resultar na suspensão ou até mesmo no cancelamento do benefício da gratuidade. A matéria de Vanessa Kanneberg para o jornal Zero Hora está disponível em < <http://surveillance.es/f> >. Acesso em: 13 fev. 2016.

¹²⁷ Assim como em Porto Alegre, os ônibus da cidade de Manaus utilizam biometria facial para fiscalizar o uso do benefício da gratuidade do transporte público. Com essa medida, a Secretaria Municipal de Transportes Urbanos conseguiu impedir gastos equivalentes a R\$230.000,00 mensais com fraudes. A matéria de Adneison Severiano para o portal G1 está disponível em < <http://surveillance.es/g> >. Acesso em: 13 fev. 2016.

¹²⁸ As câmeras de vídeo monitoramento da Guarda Municipal do município de Novo Hamburgo/RS possuem tecnologia de reconhecimento óptico de caracteres (OCR). Interligados ao sistema do DETRAN, esse sistema permite a detecção automática das placas dos veículos e a comparação com a base de dados de veículos com restrições de roubo ou mandados judiciais pendentes. A matéria de Tatiana Hentz para o jornal NH está disponível em < <http://surveillance.es/h> >. Acesso em: 13 fev. 2016.

evitar a sonegação fiscal. Desde dezembro de 2015, o fisco passou a receber os dados das movimentações financeiras de todos os brasileiros cujo valor total mensal supere dois mil reais¹²⁹. Esses dados serão compartilhados com os Estados Unidos da América e com outros 100 países em virtude de acordos estabelecidos com a finalidade de evitar evasão de dívidas.

Se, antes, a Receita Federal tinha que se dedicar a determinados grupos de indivíduos para fazer uma investigação minuciosa das suas fontes de receitas, hoje, ela pode coletar informações sobre a renda de grande parte da população economicamente ativa, especialmente, se for levado em consideração que a renda média do brasileiro é de cerca de R\$ 2.117,10 (LISBOA, 2015), ou seja, acima do limite estabelecido pela Receita Federal.

A transparência – não do tipo desejável – e a automaticidade no modo como ocorre a coleta de fluxos de dados discretos é um outro ponto fundamental para a compreensão da *dataveillance* dentro da ideia de *assemblage*. Com a multiplicação de pontos de contato entre a tecnologia e o mundo, quase tudo o que se faz gera um fluxo de dados sem que sequer se tenha conhecimento. Hábitos de navegação na internet; movimentação de telefones celulares no espaço-tempo; informações sobre uso de meios eletrônicos de pagamento. Tudo isso gera fluxos de informações sobre os indivíduos sem que eles percebam.

Ocorre que, quanto mais transparente for a criação desses fluxos de dados, mais fácil é ignorá-los e considerá-los parte normal do cotidiano. Existem dois exemplos claros para ilustrar isso: a maioria das pessoas iria se sentir desconfortável com a ideia de colocar uma tornozeleira eletrônica com monitoramento por GPS durante 24 horas ao dia ou de fazer perguntas extremamente íntimas aos seus amigos. No entanto, dificilmente pensam duas vezes antes de sair de casa com um

¹²⁹ Sob as acusações de que o sistema e-Financiera viola a privacidade dos usuários, a Receita Federal elaborou uma nota de esclarecimento em sua defesa. No referido documento, argumenta que os mecanismos que compõem aquele sistema (DIMOF – Declaração de Movimentação Financeira e o SPED – Sistema Público de Escrituração Digital) possuem fundamento na Lei Complementar nº 105/2001, bem como nas Instruções Normativas RFB nº 811 e 1.571. Obviamente, trata-se de uma análise rasa, pois o debate sobre direitos humanos não pode ser justificado com instruções normativas do próprio órgão que se beneficia com a coleta de dados. Nesse sentido, as sábias palavras de Lenio Streck, para quem “A dramaticidade da ausência de uma teoria das fontes aparece mais fortemente no plano da legislação de ‘quarta divisão’, como é o caso das portarias, resoluções, etc. Os juristas brasileiros parecem ter uma paixão pela legislação “baixo clero”, como portarias, resoluções e instruções normativas” (STRECK, 2012, sem paginação). Os detalhes sobre a referida nota da RFB estão disponíveis em < <http://surveillance.es/> >. Acesso em: 13 fev. 2016.

telefone celular ou de transformar os seus mais ocultos segredos em pesquisas do *Google*.

Como resultado da incorporação, cada vez maior, da tecnologia à vida humana, a coleta de dados torna-se ubíqua, especialmente quando for considerado o constante fluxo de metadados. Estes, como será visto posteriormente, podem dizer muito mais do que os dados aos quais se referem e têm consequências sérias na proteção dos direitos humanos.

2.4.3 Franz Kafka e a metáfora da *dataveillance*

Diante do que foi exposto anteriormente nesta pesquisa, diversos aspectos da *surveillance* não foram capturados nem por Foucault nem por Orwell, especialmente no que diz respeito à constante análise dos dados dos indivíduos e a falta de transparência sobre como essas informações são processadas. Por isso, uma metáfora interessante para a análise da *dataveillance* é a obra “O processo”, de Franz Kafka (1999).

A obra começa com o protagonista (Joseph K.) acordando em uma manhã com a presença de um grupo de policiais no seu apartamento, informando-lhe que ele estava preso. Nem K. nem os policiais faziam a menor ideia de quais as acusações que eram imputadas ao protagonista, que, também, não se lembrava de ter cometido qualquer ofensa à lei. Além disso, K. não fazia nenhuma ideia de quem poderia ser o autor da denúncia. Mesmo preso, ao invés de ser levado para a delegacia ou presídio, os oficiais simplesmente foram embora, deixando K. onde ele estava.

Durante o restante da história, Joseph K. busca, incessantemente, saber por qual motivo ele foi preso e como o processo será resolvido. Uma grande burocracia parece ter elaborado um dossiê sobre ele através de um tribunal clandestino e misterioso cujos arquivos são inacessíveis ao público e ao acusado. Em um esforço para descobrir o funcionamento do tribunal, K. sai pela cidade colhendo informações com quem quer que possua algum conhecimento sobre o *modus operandi* do tribunal, até que um pintor esclarece que os autos

continuam, como o ininterrupto movimento das repartições da justiça o exige, a levá-lo aos tribunais superiores, volta aos tribunais inferiores e fica, assim, a oscilar com grandes e pequenas amplitudes, com grandes e pequenas interrupções. Estes percursos são imprevisíveis

[...] Um dia, para completa surpresa de todos, um Juiz qualquer pega com mais atenção no auto [...]

— E o processo começa de novo? — perguntou K., quase incrédulo.
— Com certeza — respondeu o pintor — o processo começa de novo, mas volta a existir a possibilidade, tal como antes, de se conseguir uma absolvição aparente. Torna-se de novo necessário concentrar todas as forças e lutar sem desfalecimento (KAFKA, 1999, p. 112-113).

Ironicamente, após a sua prisão, é o próprio Joseph K. quem busca o tribunal. Ele é informado que o interrogatório ocorrerá no domingo, mas somente se ele não tiver nenhuma objeção. No domingo, ele correu para chegar ao local marcado às nove horas, embora ninguém tivesse especificado o horário em que deveria estar lá. Depois do interrogatório, o tribunal pareceu ter perdido o interesse nele que, por sua vez, ficou obcecado em ser notado e ter o seu caso resolvido. Na realidade, ser ignorado pela justiça foi pior do que ser preso.

Conforme continua a sua saga, o protagonista é, cada vez mais, surpreendido pelo funcionamento estranho do tribunal, cujo ar de segredo é a única constante. Ainda assim, Joseph K. busca a absolvição por um crime – que ele sequer sabe qual – perante uma autoridade acusadora que ele não consegue encontrar. Ao final, Joseph K. é apreendido no meio da noite e executado com uma facada no coração.

Essa obra consegue captar uma descrição mais condizente com a realidade da *dataveillance*. Através dos traços exagerados do mundo desenhado por Kafka, que beiram o cômico e o absurdo, é possível ver a indiferença da burocracia, na qual o indivíduo é apenas mais uma peça em uma engrenagem secreta, sem possibilidades de interferir no resultado do processo.

Joseph K. sente o desamparo e a vulnerabilidade de alguém que tem a vida completamente esmiuçada por grandes organizações, que tomam decisões, com base nesses dados, capazes de afetá-lo, mas sem que ele tenha conhecimento sobre o procedimento adotado ou qualquer possibilidade de reação.

É possível, pois, argumentar que Kafka (1999) apresenta uma metáfora da *dataveillance* sobre a incapacidade que os indivíduos têm para controlar os dados que são coletados sobre eles, o segredo absoluto que rege o funcionamento dessas instituições e a forma como elas utilizam os dados dos indivíduos sem que estes tenham a possibilidade de intervir no resultado final, ainda que disso resultem consequências drásticas nas suas vidas.

É dessa desigualdade nas relações de poder que ocorrem as violações dos direitos humanos. Assim como a burocracia de Kafka, a coleta de dados retira do indivíduo o seu controle sobre as próprias informações. Tal qual a *surveillance*, não é possível falar na existência de um motivo diabólico ou um grande plano de dominação global por trás das ações da burocracia kafkiana. O que ocorre é a dissolução do ser humano em uma rede composta por práticas padronizadas, procedimentos secretos e a incapacidade de interação com aqueles que definem os critérios de processamento das informações. Assim como em Kafka, as consequências são sempre atribuídas a um sistema – que funciona quase como uma entidade abstrata, pois inacessível –, cujo modo de funcionamento é desconhecido, embora gere consequências diretas para as vidas das pessoas.

2.5 O PODER DOS METADADOS E O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS

2.5.1 O que são metadados?

O metadado é a “[...] informação estruturada que descreve, explica, localiza ou que, de algum modo, facilita a recuperação, uso ou gerenciamento de uma fonte de informação. O metadado é comumente denominado dado sobre dado ou informação sobre informação” (NATIONAL INFORMATION STANDARDS ORGANIZATION, 2004, p. 1)¹³⁰.

De modo simplificado, é possível utilizar a metáfora de uma carta ordinária¹³¹. Assim, enquanto os dados seriam o conteúdo da correspondência, os metadados seriam informações sobre aquela carta: o tipo do papel utilizado, o tamanho do envelope, os dados do remetente e destinatário, a data e o local de postagem, os traços de DNA e impressões digitais encontrados na carta, o tipo e a cor da tinta utilizada para escrever a carta, o tamanho e o peso da correspondência, o número de

¹³⁰ No original: “[...] is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information.”

¹³¹ A metáfora da carta talvez não seja tão metafórica assim. O United States Postal Service (USPS, os correios nos Estados Unidos) possui um programa denominado “Mail Isolation Control and Tracking”. Em síntese, esse sistema tira fotos de alta resolução de todas as correspondências enviadas ou recebidas nos EUA e monitora todo o seu trajeto. Os dados do exterior dos envelopes são, então, processados por um sistema de reconhecimento ótico de caracteres – OCR – e, por não serem confidenciais, não necessitam de ordem judicial para serem acessados pela polícia. Com base somente nessas informações, é possível criar uma rede detalhada sobre todas as trocas de correspondências entre indivíduos ou empresas. A matéria de Ron Nixon para o jornal *The New York Times* está disponível em < <http://surveillance.es/m> >. Acesso em: 14 fev. 2016

letras e palavras, os traços de substâncias impregnadas no papel, as informações sobre quaisquer outras correspondências similares no sistema postal, nome do carteiro que fez a entrega etc.

Os metadados não são uma novidade da era digital – afinal, fichas catalográficas dos livros em uma biblioteca também são metadados –, mas a quantidade, tipo e capacidade de análise deles só adquiriram a relevância atual em virtude dos avanços na tecnologia da informação. E, com essa maior quantidade e poder de análise, os metadados tornaram-se capazes de informar mais que os dados propriamente ditos.

Com o escândalo envolvendo Edward Snowden¹³², o discurso dominante na defesa da coleta em massa de dados foi a de que apenas metadados eram analisados pelas agências de inteligência, de modo que não estaria ocorrendo nenhuma violação da privacidade. No entanto, ainda que somente metadados fossem coletados – o que não era verdade –, isso já seria suficiente para extrair informações extremamente pessoais das vidas das pessoas, já que metadados não são inocentes pedaços de informação descontextualizada. Eles são o próprio contexto. Em documentário produzido pela *John Hopkins University*, um antigo diretor da NSA, General Michael Hayden, declarou, explicitamente, que o governo dos EUA comete assassinatos com base em conhecimento obtido através de metadados¹³³. Por esse motivo, Stefano Rodotà tem razão ao afirmar que

Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações (RODOTÀ, 2008, p. 37)

Existe um experimento em andamento cujo intuito é demonstrar para as pessoas a relevância dos metadados. Intitulado *MetaPhone* (MAYER; MUTCHER, 2014), o estudo realizado pelo *Center for Internet and Society*, vinculado à escola de direito da Universidade de *Stanford*, funciona da seguinte forma: usuários que desejassem participar e que possuíssem *smartphones* com a plataforma *Android* instalaram, voluntariamente, um aplicativo em seus celulares. O programa envia para

¹³² Mais detalhes no item 3.1.1.

¹³³ O vídeo completo está disponível no canal da referida universidade no YouTube. Disponível em: < <http://surveillance.es/1r> >. Acesso em: 10 mar. 2016.

os pesquisadores as seguintes informações: número de destino da chamada, duração da ligação e data e hora em que ela foi feita. Os números de destino eram comparados com bases de dados públicas de telefones; assim, em vez de, simplesmente, terem um número, os pesquisadores poderiam ter o nome do destinatário da chamada telefônica.

Dentre os diversos padrões de uso que foram encontrados pelos pesquisadores do projeto *MetaPhone*, cinco são bem relevantes no que diz respeito à importância dos metadados: o “participante A” comunicou-se, várias vezes, com diversos neurologistas locais, com uma farmácia especializada em produtos neurológicos, com um serviço de apoio a portadores de doenças raras e com o serviço de atendimento ao consumidor de um laboratório farmacêutico especializado em esclerose múltipla.

O “participante B” fez ligações longas para cardiologistas de um grande centro médico, fez uma ligação curta para um laboratório de análises clínicas, recebeu ligações de uma farmácia e fez várias ligações curtas para um serviço de acompanhamento automático de um dispositivo médico utilizado para monitorar arritmias cardíacas.

O “participante C” fez ligações para uma loja de armas de fogo especializada em rifles semiautomáticos e fez chamadas longas para o serviço de atendimento ao consumidor de uma fabricante do mesmo tipo de rifle.

O “participante D” fez contato, dentro de um período de três semanas, com uma loja de utensílios para jardinagem, com chaveiros, lojas de hidroponia e com lojas especializadas na venda de artigos relacionados à maconha.

A “participante E” fez uma longa ligação, muito cedo da manhã, para a sua irmã. Dois dias depois, ela ligou várias vezes para uma clínica de aborto. Um mês depois, ela fez a última ligação para a clínica.

Os pesquisadores puderam telefonar para os envolvidos e confirmar que o “participante B” possui um problema cardíaco e que o “participante C” possui armas de fogo semiautomáticas. No entanto, preferiram não ligar para os participantes A, D e E em virtude da sensibilidade das informações coletadas. Ainda assim, fica evidente que os metadados são informações de extrema relevância para identificar quem são os indivíduos.

Somente com metadados de ligações telefônicas, foi possível chegar a conclusões tão pessoais sobre a vida dos participantes – reitere-se, o *MetaPhone* não envia a gravação das chamadas. Imagine-se, então, o que seria possível inferir caso se adicionassem os metadados de *e-mails* trocados, mensagens instantâneas ou até mesmo buscas no *Google* – sim, por fazerem parte da URL, os termos pesquisados nos serviços de busca são considerados metadados.

Extrapolando um pouco esses projetos, imagine que um determinado sistema coleta, durante alguns meses, informações sobre todos os contatos realizados – não o conteúdo das comunicações – por um indivíduo – frequência, duração, destinatário, horário –, além de todas as suas movimentações no espaço – com rotas percorridas, velocidade, etc. Qualquer pessoa poderia extrair conclusões interessantes desses dados: quem são as pessoas importantes para esse indivíduo? Quais os meios de transporte que ele utiliza? Qual a sua profissão provável? Afinal, se todos os dias, às 03 horas da madrugada, ele está no hospital, possivelmente, é um profissional da saúde. Se isso ocorre apenas excepcionalmente, provavelmente está doente.

Obviamente, um sistema pode tirar conclusões muito mais avançadas com esses dados no atacado: esse indivíduo chama-se Fulano, é médico, número de CPF tal, possui uma esposa e quatro filhos, dirige um veículo de marca tal e, por isso, tem 85% de probabilidade de votar no partido X, possui determinados traços de personalidade e, portanto, tem um risco 75% maior de desenvolver demência na velhice. A concatenação de dados é quase infinita e pode parecer absurda, mas é utilizada, diariamente, no mundo do *big data*¹³⁴ para determinar riscos, preferências e hábitos das pessoas. A sofisticação desses sistemas – vide, por todos, Kosinski Stillwell e Graepel (2013) e do *site* da aplicação da pesquisa – informado na introdução deste capítulo – parece retirada de filmes de ficção científica.

2.5.2 O anteprojeto de lei para a proteção de dados pessoais no Brasil e os (meta)dados “anônimos”

Após a aprovação do marco civil da internet, instaurou-se um novo debate sobre o anteprojeto de lei (APL) para a proteção de dados pessoais. No dia 19 de outubro de 2015, o Ministério da Justiça finalizou uma nova versão do anteprojeto, o

¹³⁴ Sobre o *big data*, vide item 3.3.2.

que ocorreu depois de mais de 1300 colaborações no *site* da consulta pública (PEDRUZZI, 2015).

Como ficou claro nos itens anteriores, o recurso às legislações nacionais é insuficiente para garantir a proteção dos direitos humanos violados pela *surveillance*. Em que pese essa limitação da discussão no âmbito do Estado-nação, não se pode desconsiderar a importância, ainda que simbólica, dessas legislações.

Mesmo que se tenham sempre em vista os limites e as possibilidades da lei para tratar de problemas eminentemente desterritorializados, o referido anteprojeto é de imensa importância para inaugurar o debate sobre a *surveillance* no cenário legislativo brasileiro. Quando aprovada, essa lei irá servir como um dos fundamentos para a formação do imaginário dos juristas, especialmente para a compreensão sobre a relação entre violação dos direitos humanos e os fluxos de dados.

No entanto, o referido anteprojeto (BRASIL, 2015) sofre de um problema fundamental, pois considera que ainda se está lidando apenas com dados pessoais. Isso torna-se evidente já no artigo 1º, onde é estabelecido que “*esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.*”

Com uma definição desse tipo, o APL esquece um dos direitos humanos mais importantes e que é colocado em risco pelos fluxos globais de dados: a igualdade. O senso comum presente no APL tende a associar o problema da *surveillance* à privacidade e à liberdade. Obviamente, não se trata de um erro, pois, realmente, existe uma ligação óbvia e forte entre *surveillance* e privacidade.

No entanto, trata-se de uma abordagem limitada, porque, embora esses problemas continuem a ser relevantes, é cada vez mais claro que eles não contam a história completa sobre a *surveillance*, porque ela, nos dias de hoje, classifica pessoas em categorias de interesse ou risco com consequências reais nas suas vidas. Logo, a *surveillance* torna-se um instrumento de estratificação da discriminação, o que faz com que deixe de ser apenas um problema de privacidade individual, mas, especialmente, de justiça social.

Ainda que a omissão do artigo 1º do APL fosse considerada um mero “esquecimento”, suas consequências para a proteção dos direitos humanos seriam igualmente prejudiciais, especialmente quando se percebe que a coleta massiva de dados é capaz de categorizar pessoas em grupos de risco ou de (des)interesse

econômico e social. No entanto, o APL vai mais fundo ao ignorar a igualdade e fazer a equivocada distinção entre três categorias de dados: pessoais, sensíveis e anônimos.

O dado pessoal, conforme art. 5º, inciso I, é aquele “[...] relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa” (BRASIL, 2015).

Os dados sensíveis, de acordo com o inciso III do mesmo artigo, são um tipo especial de dados pessoais, ou seja, são

[...] dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos (BRASIL, 2015).

Por fim, os dados anônimos, conforme inciso IV do artigo 5º do APL, seriam aqueles “[...] dados relativos a um titular que não possa ser identificado” (BRASIL, 2015).

Trata-se de uma classificação que cria três níveis de proteção distintos: os dados sensíveis gozarão da maior proteção dentre todos, seguidos pelos dados pessoais e, por fim, pelos dados anônimos. Estes últimos gozam de menor privilégio, uma vez que, supostamente, não seriam capazes de identificar os indivíduos aos quais se referem.

Contudo, esta é uma classificação fantasiosa, especialmente dentro do contexto dos avançados algoritmos de extração – *data mining* – e análise massiva de dados e, especialmente, de metadados – *big data*. Esses metadados – que, dependendo do contexto, podem ser classificados pelo APL como dados pessoais ou, até mesmo, como dados anônimos – são de grande importância para a compreensão da falha dessa classificação. Como visto no exemplo anterior do *MetaPhone*, com uma abordagem estatística adequada, informações como remetente, destinatário, assunto, horário de envio e endereço IP podem ser tão ou mais valiosas que o conteúdo dos e-mails.

Assim, os dados não são, como quer a lei, “essencialmente” pessoais, sensíveis ou anônimos. São apenas dados, cujo sentido é atribuído no momento da aplicação do algoritmo. Como resultado, dados que foram “anonimizados” podem

sofrer o processo inverso e tornarem-se identificáveis, revelando informações sensíveis sobre um indivíduo ou grupo de indivíduos.

Quanto mais fontes anônimas de dados forem concatenadas, menos anônimos esses dados serão. Assim, a classificação proposta pelo APL permite que seja dada baixa proteção ao conjunto de informações que podem ser utilizadas para afetar diretamente a vida das pessoas, violando uma série de direitos humanos. Desse estado da arte, a classificação equivocada entre dados pessoais, sensíveis e anônimos coloca em risco os direitos humanos, em especial a igualdade, uma vez que possibilitará a proteção deficiente de dados potencialmente sensíveis e de extrema relevância para a vida das pessoas.

É possível apontar alguns exemplos emblemáticos de como não existem dados – e metadados – anônimos¹³⁵. No ano de 2014, um grupo de cientistas da *Carnegie Mellon* conseguiu uma façanha interessante. Com simples imagens de pessoas obtidas na rua, os pesquisadores conseguiam descobrir o nome, perfil de rede social, número do seguro social (o equivalente ao CPF nos EUA) e, através de consultas de bases de dados de acesso público, inferir informações como orientação sexual e traços de personalidade (ACQUISTI, GROSS e STUTZMAN, 2014).

Em outro exemplo, pesquisadores da universidade do Texas, em Austin, desenvolveram um programa de computador capaz de “desanonimizar” um conjunto grande de dados, a saber, a base de notas dadas aos filmes pelos usuários do serviço Netflix (NARAYANAN e SHMATIKOV, 2008). Como isso ocorreu?

Em 2006, o *Netflix* – o maior serviço de *streaming* de vídeo pago do mundo – fez um concurso público para que fosse desenvolvido um algoritmo mais refinado de sugestões de filmes para os seus usuários. Para tanto, liberou um banco de dados parcial, contendo 100.408.507 avaliações criadas por 490.189 usuários do *Netflix*, dos quais foram removidos todos os dados identificadores dos clientes, ficando disponível apenas a nota atribuída pelo usuário e a data em que a avaliação foi feita. O *Netflix* tinha tanta confiança de que os dados continuariam anônimos que, na seção de dúvidas frequentes (FAQ) do desafio, inseriu as seguintes pergunta e resposta:

¹³⁵ Existe um projeto de pesquisa de Arvind Narayan, cientista da computação da universidade de *Princeton* e pesquisador afiliado do “*Center for Internet and Society*” da escola de direito da universidade de Stanford. O projeto, denominado “*33 bits of Entropy*” analisa a impossibilidade de existirem dados anônimos na sociedade contemporânea. Disponível em: < <http://surveillance.es/v> >. Acesso em: 15 fev. 2016.

Existe alguma informação dos clientes no conjunto de dados que deve ser mantida em segredo?

Não, toda a informação de identificação dos clientes foi removida; tudo o que resta são as avaliações e as datas. Isso segue a nossa política de privacidade, que você pode revisar aqui. Ainda que, por exemplo, você conhecesse todas as suas próprias avaliações e as datas em que foram feitas, você provavelmente não poderia identificá-las de maneira confiável nos dados disponibilizados, pois somente uma pequena amostra foi incluída (menor que um décimo do nosso conjunto de dados completo) e esses dados estão sujeitos a variações. É claro que, já que vocês todos conhecem as suas próprias avaliações, isso não seria realmente um problema de privacidade, seria? (NETFLIX, 2006)¹³⁶.

Os pesquisadores, então, desenvolveram um programa que comparou aquela base de dados a uma outra de acesso público, o IMDB – *Internet Movie Database* –, *site* que também reúne *reviews* cinematográficos postados voluntariamente por internautas. Como resultado, eles conseguiram identificar quais usuários eram responsáveis pelos *reviews* da base de dados do Netflix, ou seja, “desanonimizaram” o conteúdo.

Com base nos resultados dessa pesquisa, foi possível pegar um conjunto de dados completamente anônimos e cruzar com outro banco de dados (público) para saber quem viu qual filme e qual foi a sua avaliação. Com isso, seria possível fazer a concatenação com os outros exemplos dados no decorrer do trabalho, inclusive identificação pessoal com número do “CPF”, traços de personalidade, orientação religiosa, política e sexual etc¹³⁷.

É preciso, portanto, cautela na hora de utilizar mecanismos rígidos para tentar controlar eventos extremamente fluidos. Embora se tenha plena consciência de que a lei não é capaz de proteger integralmente os direitos humanos violados pela *surveillance*, deve-se reconhecer que ela pode ser um instrumento benéfico, especialmente do ponto de vista simbólico.

A lei precisa estar minimamente adequada às tecnologias existentes, sob o risco de ser ainda mais prejudicial que a sua própria inexistência, visto que a sua mera

¹³⁶ No original: “Is there any customer information in the dataset that should be kept private? No, all customer identifying information has been removed; all that remains are ratings and dates. This follows our privacy policy, which you can review here. Even if, for example, you knew all your own ratings and their dates you probably couldn’t identify them reliably in the data because only a small sample was included (less than one-tenth of our complete dataset) and that data was subject to perturbation. Of course, since you know all your own ratings that really isn’t a privacy problem is it?”

¹³⁷ A concatenação de múltiplas bases de dados na busca pela extração de conhecimento útil será objeto da análise sobre *big data* e *data mining* do item 3.3.2.

existência, sem paralelo com a realidade tecnológica, cria a falsa sensação de que um direito está protegido sem que ele realmente esteja. Esse é o desafio de uma legislação brasileira de proteção de dados pessoais, especialmente no que diz respeito ao que considera “dados anônimos”.

Para tanto, é imprescindível que o direito compreenda da melhor maneira possível, os detalhes do funcionamento da *surveillance* no século XXI, o que será feito no próximo capítulo.

3 A EXPANSÃO DA SURVEILLANCE NO SÉCULO XXI: O *BIG DATA* E AS NOVAS RELAÇÕES TEMPO-ESPAÇO

*All that you touch
All that you see
All that you taste
All you feel
All that you give
All that you deal
All that you buy, beg, borrow or steal
All that is now
All that is gone
All that's to come
And everything under the sun is in tune
But the sun is eclipsed by the moon*

(Pink Floyd – Eclipse)

Assim como o trecho da música que inicia este capítulo, a *surveillance* busca transformar a totalidade dos eventos e tempos da vida em informações analisáveis por computador. Afinal, além de as interações humanas serem, em sua maioria, mediadas por meios digitais, a multiplicação de sensores e dispositivos conectados em redes permite a captura automatizada de dados em níveis inacreditáveis.

Um dos casos mais recentes nos meios de comunicação sobre o tema diz respeito ao vazamento de informações da NSA por Edward Snowden. Por esse motivo, os eventos relacionados ao evento relativo a Snowden serão analisados neste capítulo, o que só poderá ser feito de maneira muito resumida, tendo em vista que o foco desta pesquisa não é relatar todos os projetos (secretos) do governo estadunidense, mas analisar o fenômeno que eles representam.

A música que inicia este capítulo faz parte de um álbum cuja capa possui a ilustração de um prisma, mesmo objeto que dá nome a um dos sistemas mais populares da NSA – *Prism*. Assim como outros sistemas que serão vistos neste capítulo, o *Prism* depende dessa tendência atual de armazenar grandes conjuntos de dados, fenômeno conhecido como *big data*.

As revelações de Snowden, no entanto, são apenas a ponta do *iceberg*. Como será visto, a difusão da tecnologia de informação para cada vez mais lugares do mundo é um traço característico da atual fase da globalização. Seguindo essa esteira, serão apontadas nove tendências da *surveillance* no mundo globalizado. Por trás de todas elas, está a ideia de modernidade líquida e a sua associação com o desaparecimento das instituições totais e que guardam relação com os modelos

derivados da modernidade sólida, como é o caso do panóptico. Ao contrário desses modelos, todos baseados na criação de restrições físicas ao movimento, a *surveillance* funciona sob a égide da modulação, facilitando ou dificultando fluxos, o que é essencial para a globalização.

No mundo globalizado, existe a necessidade de facilitar, cada vez mais, os fluxos e, simultaneamente, restringi-los. A *surveillance* como tendência da globalização não é uma conspiração global, mas uma consequência da importância, no mundo globalizado, dos fluxos de pessoas e capitais. Todavia, esses mesmos fluxos possibilitam o surgimento de um “lado negro” da globalização, caracterizado pela expansão daquilo que Zygmunt Bauman chama de medo líquido e que, como será visto, deriva justamente das incertezas criadas pela interconexão viabilizada pela globalização.

Essas incertezas geram demandas por novos mecanismos prontos para neutralizá-las. Aposta-se, então, na criação de modelos de computador preditivos, capazes de antecipar o futuro através de análise matemática de eventos do passado. Por não ser um ramo de amplo conhecimento no mundo jurídico, será feita uma pequena digressão para introduzir o leitor no universo da estatística. O objetivo desse segmento do texto será familiarizar o leitor com a ideia de que, em análises estatísticas e probabilísticas, uma única nova informação é capaz de modificar radicalmente o resultado da análise¹³⁸.

Se isso é verdade para uma única informação, não fica difícil imaginar quais seriam as possibilidades de análises com um volume de dados tão grande que nem mesmo os sistemas tradicionais de computação conseguem dar conta, como é o caso do *big data*. Como resultado do barateamento das estruturas de coleta e armazenamento de dados, passaram a surgir novas possibilidades para análises e identificação de padrões em eventos aparentemente aleatórios.

Isto ocorre porque, fora dos limites humanos, o *big data* trabalha com conjuntos tão grandes de dados que permitem a identificação de correlações que, para um ser humano, parecem desconexas. Como visto anteriormente, é possível utilizar, por exemplo, as “curtidas” na rede social *Facebook* para inferir traços de personalidade e, até mesmo, orientação sexual do usuário. As correlações, no mundo

¹³⁸ Para uma outra digressão, com outros exemplos, mas com objetivo similar, consultar o debate sobre “The (Occasional) Power of Numbers”, realizado pelo jurista estadunidense Cass R. Sunstein (2006).

do *big data*, são infinitas, pois um mesmo conjunto de dados pode ser analisado por algoritmos distintos na busca por novos padrões. Os resultados dessas análises parecem completamente aleatórios em virtude de esses sistemas serem capazes de associar informações em uma escala sem precedentes na história humana.

Como modo de aproximar o leitor desse universo, serão demonstradas algumas potencialidades das análises probabilísticas derivadas do *big data*. Desde previsão de doenças através da análise das buscas realizadas por usuários do *Google*, passando pelo uso de metadados de celulares para inferir indicadores econômicos e de emprego, até a previsão, com 100% de precisão, dos resultados de uma eleição presidencial de um país como os EUA, esses mecanismos de análise utilizam uma enorme quantidade de dados para aumentar a confiabilidade das previsões matemáticas.

O *big data*, contudo, depende da coleta massiva de informações. A regra é sempre “quanto mais, melhor”. Os dados sequer precisam ser relevantes no momento da sua coleta, pois a importância surgirá somente depois, com o processamento através do algoritmo adequado. Como resultado da multiplicação desses dispositivos de coleta de dados, será possível falar no surgimento de uma sociedade dos sensores, onde todos os aspectos da vida humana e do meio ambiente tendem a ser mensurados, automaticamente, por dispositivos eletrônicos.

É inquestionável a onipresença de dispositivos capazes de coletar dados sobre o usuário e o ambiente onde estão instalados, especialmente se for considerado que a maioria dos equipamentos eletrônicos, embora não possam ser conceituados como sensores exclusivos, desdobram-se como tal. Afinal, a grande maioria dos dispositivos eletrônicos possuem sensores diversos que melhoram a experiência do usuário e agregam novas funções ao equipamento, como é o caso dos giroscópios e sensores de proximidade, de movimento, de luz, de umidade e de campo magnético presentes na maioria dos *smartphones* atuais.

Mesmo no caso de eventos que não sejam imediatamente mensuráveis por um sensor, a utilização do algoritmo certo transforma padrões de uso em informações derivadas mensuráveis. Como exemplo, é possível transformar um telefone celular em um sensor capaz de inferir o humor do usuário. Esse é o caso do *software* “*MoodScope*”, desenvolvido por um time da Universidade de Houston e o laboratório de pesquisas da *Microsoft* (LANE, LIKAMWA, *et al.*, 2013).

Os dados coletados por esses sensores são imprescindíveis para a compreensão dos modelos preditivos utilizados pela *surveillance*. Por isso, serão explicadas técnicas como *data mining*, *machine learning* e *predictive analytics*, essenciais para a compreensão de como os sistemas de computador criam modelos preditivos de futuro. Esses mecanismos são utilizados, cotidianamente, para realizar análises diversas que geram consequências concretas na vida das pessoas, inclusive com a possibilidade de violação de direitos humanos.

Isso fica claro, por exemplo, com a construção de modelos preditivos de risco, seja pela iniciativa privada – como é o caso das análises de risco na concessão de crédito por instituições financeiras, por exemplo –, seja pelo Estado – por exemplo, através da análise do risco de que um determinado viajante seja um terrorista. Isso se torna mais grave se for analisado o fato de que, embora extremamente sofisticados, esses modelos preditivos geram resultados falsos. Escondidos sob um manto de suposta neutralidade, tais mecanismos preditivos incorporam os preconceitos dos seus desenvolvedores, o que resulta em erros com consequências drásticas para os direitos humanos.

Esses mecanismos preditivos serão, portanto, analisados sob duas matrizes teóricas. A primeira diz respeito à ideia de simulação e sua vinculação com um modelo pós-panóptico de *surveillance*, em virtude da passagem das sociedades disciplinares para as sociedades do controle, o que é viabilizado pelo surgimento das novas tecnologias de informação, que garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos.

A segunda perspectiva de análise irá retornar a Michel Foucault, através do conceito de biopoder que, por sua vez, está vinculado à ideia de um Estado que viabiliza o desenvolvimento do capitalismo, através do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos. Ao contrário da proposta panóptica, o biopoder é exercido de um modo diferente, visto que precisa ser, cada vez mais, dócil. Por isso, deve garantir a sua manutenção do modo mais assimilável possível, sem causar perturbações ou dificuldades na vida cotidiana, o que torna o biopoder extremamente compatível com o caráter sedutor da *surveillance* na sociedade do consumo.

Além de modificar o tempo, as tecnologias de informação e comunicação alteram também as perspectivas de espaço. Nesse sentido, será demonstrado que a

reconfiguração horizontal rizomática da *surveillance* viabiliza o exercício do poder independentemente da vinculação a um território específico e das fronteiras do Estado-nação. Para tanto, irá explicar como as fronteiras deixam de ser associadas a um local e passam a “acontecer” dentro das redes de computadores, antes mesmo que o indivíduo tenha contato com o território estrangeiro.

O que significa dizer que fronteiras “acontecem”? Diante do paradigma da *surveillance*, as fronteiras deixam de ser territoriais, um lugar rígido de controle de fluxos de bens e pessoas. Elas passam a ser uma concatenação de uma quantidade absurda de dados, oriundos de entidades públicas e privadas em diversos lugares do mundo e que servem como fundamento para que um sistema de computador garanta ou impeça a mobilidade das pessoas.

Essas “barreiras” virtuais têm efeitos bem reais na vida das pessoas. Para qualquer brasileiro que já solicitou um visto para visitar os EUA, por exemplo, fica bem claro que a fronteira estadunidense está bem aqui, no Brasil, no ponto de entrevista no consulado onde um sistema informa ao agente de imigração se o candidato é uma pessoa aceitável ou não.

Indo mais longe: até pouco tempo atrás, os turistas brasileiros precisavam de um visto prévio para ir ao Canadá. Se o brasileiro solicitasse um visto para passear no Canadá, existiam duas possibilidades de desfecho – aqueles que não possuem um visto estadunidense deveriam ir até o consulado canadense coletar informações biométricas e prestar mais esclarecimentos. Por outro lado, aqueles que já possuíam o visto norte-americano estavam dispensados de realizar coleta de informações biométricas pelo consulado canadense. Isso porque eles já possuem os dados biométricos da rede do departamento de imigração dos EUA que, por força de acordo entre aqueles países, é compartilhado com o governo canadense.

Aqui, a história fica mais confusa ainda: a “fronteira” real – ou seja, o ponto de controle que autoriza a entrada do brasileiro no Canadá – não é a fronteira física do Canadá. Tampouco é a fronteira física do consulado canadense. A fronteira canadense, nesse caso, “aconteceu” naquele mesmo momento quando também “aconteceu” a fronteira estadunidense: como resultado do sistema que orientou o oficial do consulado americano a fornecer ou negar o visto dos EUA.

A partir dessa ideia segundo a qual as fronteiras “acontecem”, será possível vislumbrar a sua transformação em membranas semipermeáveis que, por um lado,

têm como finalidade facilitar os fluxos de pessoas e capitais e, por outro, dificultar os mesmos fluxos quando os indivíduos forem considerados “indesejáveis”. Com isso, pretende-se associar a *surveillance* à discriminação de pessoas em categorias de indesejáveis, o que será essencial para a compreensão do capítulo posterior.

3.1 SURVEILLANCE APÓS EDWARD SNOWDEN

3.1.1 A história envolvendo Edward Snowden

Em 20 de maio de 2013, um analista de sistemas contratado pela Booz Allen Hamilton – uma empresa de tecnologia que presta serviços à NSA – embarca em um voo para Hong Kong imediatamente após sair do seu local de trabalho, um prédio da NSA no Havaí. Pouco tempo depois, em 03 junho de 2013, aquele analista, até então conhecido apenas pelo codinome *Citizenfour*, encontra-se com dois jornalistas do periódico britânico *The Guardian* – Glenn Greenwald e Ewen MacAskill – e com a documentarista Laura Poitras com a finalidade de divulgar uma informação que causaria impacto no mundo inteiro. Segundo ele,

[...] existe uma infraestrutura instalada nos Estados Unidos e no resto do mundo que a NSA construiu, em cooperação com outros governos, para interceptar basicamente toda comunicação digital, toda comunicação de rádio, toda comunicação analógica que tenha sensores instalados para detectá-la. Com essas capacidades, basicamente a vasta maioria das comunicações humanas e entre computadores, ou seja, comunicações entre dispositivos que viabilizam as relações entre humanos, são automaticamente coletadas sem diferenciação. Isso permite que indivíduos possam pesquisar de modo retroativo todas as suas comunicações com base em auto-certificações. [...] Meu nome é Edward Snowden. As pessoas me chamam de Ed. Edward Joseph Snowden é o meu nome completo.¹³⁹

¹³⁹ No original: [...] there is an infrastructure in place in the United States and worldwide that NSA has built in cooperation with other governments as well that intercepts basically every digital communication, every radio communication, every analogue communication that it has sensors in place to detect and with these capabilities basically the vast majority of human and computer to computer communications and device based communications which sort of form a relationship with humans are automatically ingested without targeting. And, uh, with these capabilities, basically, the vast majority of human and computer-to- computer communications, device-based communications, which sort of inform relationships between humans, are automatically ingested without targeting. And that allows individuals to retroactively search your communications based on self- certifications. [...] my name is Edward Snowden. I go by Ed. Edward Joseph Snowden is the full name.”. Esse trecho da fala de Snowden está no documentário *Citizenfour*, de Laura Poitras, e acontece, especificamente, no 28º minuto do filme.

Especialmente após os eventos do 11 de setembro de 2001, ganhou popularidade a utilização do lema da “guerra contra o terror” para criar diversas ferramentas de análise e compartilhamento internacional de dados pessoais, biométricos e genéticos. Esse tipo de iniciativa, apoiada em legislação de constitucionalidade questionável¹⁴⁰, não se restringiu aos EUA, incluindo, dentre outros, Suíça¹⁴¹, Suécia¹⁴², União Europeia¹⁴³ e, em certa medida, até mesmo o Brasil¹⁴⁴.

No passado, um dos casos mais famosos de coleta massiva de dados dizia respeito à rede de interceptação e monitoramento global de dados denominada ECHELON, anterior, até mesmo, ao *motto* da “guerra contra o terror”. Apesar de ter sido negada durante muitos anos pelos países envolvidos – EUA, Reino Unido, Canadá, Austrália e Nova Zelândia –, sua existência restou confirmada pela

¹⁴⁰ Em 09 de outubro de 2012, a “*petition for a writ of certiorari*” do caso *Hepting v. AT&T* foi negada pela Suprema Corte dos Estados Unidos da América, o que garantiu a imunidade civil e penal às empresas de telecomunicações que viabilizam interceptações sem ordem judicial, apenas a requerimento do poder executivo. Em 10 de fevereiro de 2015, no caso *Jewel v. NSA* – que buscava impedir que a NSA realizasse interceptações sem ordem judicial com base na *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* – foi negado o questionamento da constitucionalidade do sistema UPSTREAM sob a alegação de que isso poderia tornar públicas informações que constituem segredo de Estado. O tribunal não decidiu a respeito da constitucionalidade da coleta, por parte da NSA, de dados de Internet e telefone.

¹⁴¹ Veja-se o “Rapport de la Délégation des commissions de gestion des Chambres fédérales du 10 novembre 2003” sobre o “Système d’interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx»)”.

¹⁴² Em 18 de junho de 2008, o parlamento sueco aprovou a denominada “*FRA-lagen*”, um pacote de leis que permite que sua agência de inteligência intercepte todas as comunicações de voz e dados naquele país.

¹⁴³ A União Europeia possui um projeto de pesquisa denominado “INDECT” (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*), cuja finalidade é elaborar sistemas automatizados de detecção de ameaças terroristas, violência e comportamentos criminosos. Outro aspecto problemático no bloco é a “Directiva 2006/24/CE do Parlamento Europeu e do conselho de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE”. Em síntese, essa medida obriga os Estados-membros a manterem registros detalhados das telecomunicações de dados e voz de todos os indivíduos por um período de até 24 meses.

¹⁴⁴ O Brasil não faz parte do tradicional grupo de países com grandes investimentos nos setores de coleta e processamento de dados de inteligência. Contudo, desde 2006, a Receita Federal utiliza supercomputadores para análise de informações sobre os contribuintes. O software Harpia, desenvolvido pelo Instituto Tecnológico da Aeronáutica e pela Universidade de Campinas, é “alimentado” por dados de diversas fontes (secretarias fazendárias estaduais, Poder Judiciário, Banco Central, instituições financeiras etc) para elaborar bancos de dados individualizados e analisar as atividades financeiras e fiscais de cada contribuinte brasileiro. Sobre o assunto, ver a notícia no portal do Serviço Federal de Processamento de Dados. Disponível em: < <http://surveillance.es/1o> >. Acesso em: 10 mar. 2016.

“Comissão Temporária sobre o Sistema de Intercepção ECHELON”, vinculada ao Parlamento Europeu¹⁴⁵.

As revelações de Snowden¹⁴⁶ provaram a existência de uma estrutura mundial capaz de coletar e tratar informações em escala vista somente em filmes de ficção. Ficou claro que quinze grandes agências de inteligência – NSA, dos Estados Unidos; ASD, da Austrália; GCHQ, do Reino Unido; FRA, da Suécia; BND e BfV, da Alemanha; CSEC, do Canadá; AISE, da Itália; PET, da Dinamarca; DGSE, da França; AIVD, da Holanda; NIS, da Noruega; CNI, da Espanha; NDB, da Suíça, SID, de Singapura e ISNU, de Israel – possuem acordos de cooperação de SIGINT – inteligência de sinais. Além disso, ficou evidente que grandes empresas de tecnologia contribuem para esses sistemas, seja permitindo o acesso aos seus servidores – como é o caso do *Google*, *Microsoft*¹⁴⁷, *Apple*¹⁴⁸, *Yahoo*, *Facebook* e *LinkedIn* –, seja recebendo dinheiro para inserir falhas deliberadas em sistemas e padrões de criptografia – como é o caso da RSA¹⁴⁹.

Nesse último caso, uma das grandes prioridades da NSA e seus parceiros é aumentar a sua capacidade de acessar comunicações criptografadas de indivíduos,

¹⁴⁵ Em síntese, foi constatado que se tratava de uma rede capaz de interceptar, em todo o globo, comunicações de dados e voz transmitidas através de cabos, fibra ótica, satélites, rádio e micro-ondas. Isto ficou reconhecido no documento de sessão do Parlamento Europeu PE 305.391, de 11 de julho de 2001, intitulado “relatório sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção ‘ECHELON’)”. O relatório completo está disponível em < <http://surveillance.es/1y> >. Acesso em: 25 mar. 2016.

¹⁴⁶ Um arquivo completo com todo o material que Edward Snowden vazou foi disponibilizado e catalogado pela *Canadian journalists for free expression*. Disponível em: < <http://surveillance.es/1l> >. Acesso em: 10 mar. 2016.

¹⁴⁷ Sobre o caso específico da *Microsoft*, os documentos vazados por Snowden demonstram que a empresa ajudou a NSA e outras agências dos EUA a burlar a criptografia dos sites *outlook.com* e *hotmail.com*, permitindo que tivessem acesso aos e-mails e conversas entre usuários. Além disso, permite que a NSA acesse diretamente os arquivos armazenados pelos 250 milhões de usuários do serviço de armazenamento na nuvem *SkyDrive*. A matéria de Glenn Greenwald para o jornal *The Guardian* está disponível em: < <http://surveillance.es/1p> >. Acesso em: 10 mar. 2016.

¹⁴⁸ Recentemente, um debate tomou conta dos meios de comunicação nos EUA. O *FBI* está brigando judicialmente para que a *Apple* desbloqueie um iPhone utilizado por um dos atiradores do ataque que resultou na morte de 14 pessoas na cidade de San Bernardino, na Califórnia. A *Apple* estaria se recusando desbloquear o dispositivo. Segundo Edward Snowden, trata-se de um golpe publicitário, visto que o *FBI* conta com o apoio da *Apple* no fornecimento de ferramentas necessárias para quebrar a segurança dos equipamentos produzidos por ela. Segundo Snowden: “The FBI says Apple has the ‘exclusive technical means’ to unlock the phone. Respectfully, that’s bullshit.” A matéria de Samuel Gibbs para o jornal *The Guardian* está disponível em < <http://surveillance.es/1q> >. Acesso em: 10 mar. 2016.

¹⁴⁹ Veja-se, por exemplo, o caso da falha do Dual_EC_DRBG: de acordo com Snowden, a NSA investiu 10 milhões de dólares para a RSA criar um backdoor em uma tecnologia de criptografia amplamente utilizado, tornando vulnerável a ataques grande parte dos sistemas criptográficos existentes até então. A matéria de Josep Menn para a agência *Reuters* está disponível em < <http://surveillance.es/1t> >. Acesso em: 10 mar. 2016.

empresas e Estados estrangeiros. Segundo o material divulgado por Edward Snowden, o orçamento anual do governo dos EUA para subornar empresas e inserir vulnerabilidades em padrões criptográficos é de 250 milhões de dólares por ano (GREENWALD, 2013). Com esse dinheiro, a NSA, através de alianças comerciais secretas, espera inserir vulnerabilidades nos sistemas de criptografia utilizados no mundo inteiro (NATIONAL SECURITY AGENCY, 2012, p. 4).

Existe uma infinidade de programas secretos de coleta e análise massiva e dados. O escopo deste trabalho não é revisar cada um dos que se teve notícia¹⁵⁰, mas deixar o leitor ciente da existência dos mais importantes, tendo uma noção básica da sua função. Por isso, serão mencionados, muito brevemente, dez sistemas: *STORMBREW*, *Fairview*, *Dishfire*, *Tempora*, *Bullrun*, *Edgehill*, *PRISM*, *MUSCULAR*, *Boundless Informant* e *XKeyscore*.

Os quatro primeiros – *STORMBREW*, *Fairview*, *Dishfire* e *Tempora* – são sistemas de interceptação massiva de voz e dados através da inserção de “grampos” em grandes *backbones* – geralmente, pontos de entrada e saída de cabos de fibra óptica submarinos que ligam os continentes. Eles fazem parte de uma categoria que a NSA denomina *Upstream collection* e, em geral, ocorrem com o apoio técnico das grandes empresas de telecomunicações, como é o caso da parceria entre a NSA e a AT&T no programa *Fairview*. O alcance desse tipo de sistema pode ser visto na imagem abaixo, retirada dos arquivos tornados públicos por Edward Snowden.

¹⁵⁰ Como tese de doutoramento, este trabalho necessita de um recorte teórico limitado. Por óbvio, seu escopo não é descrever cada um dos sistemas de coleta de dados que se teve notícia – isso poderia ficar a cargo de uma tese na área de computação ou ciência política –, mas fazer com que o leitor compreenda as várias dimensões dos fenômenos que envolvem a *surveillance*. De modo similar ao que foi feito outras partes desta pesquisa, a utilização de exemplos do cotidiano tem o objetivo de tornar acessível o conhecimento sobre os fenômenos que explicam a *surveillance*, não fazer análises minuciosas de sistemas secretos, cuja única fonte de conhecimento se restringe a um único homem.

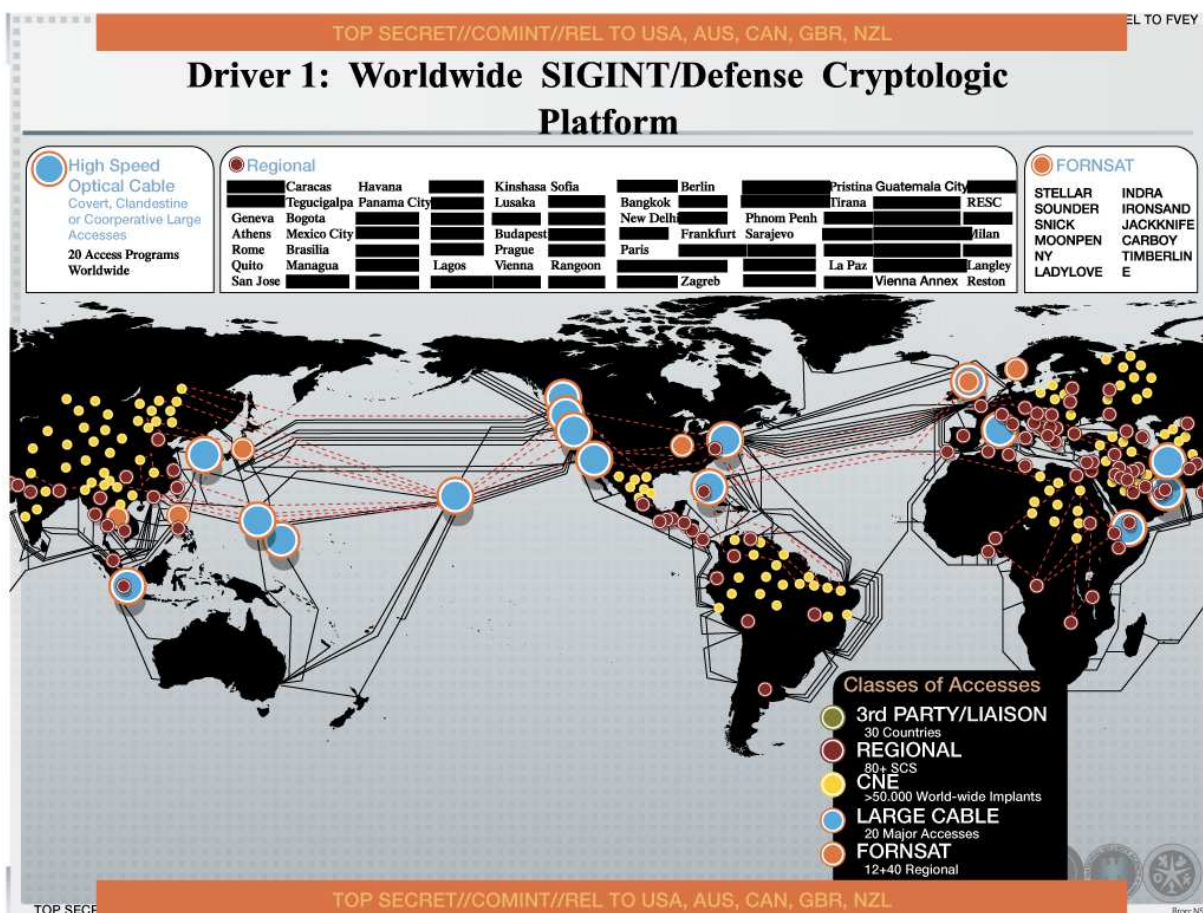


Figura 1 – Mapa obtido dos documentos divulgados por Edward Snowden, indicando os pontos de coleta de dados da NSA e dos seus parceiros, bem como o tipo de acesso de cada ponto. Disponível em: < <http://surveillance.es/1v> >. Acesso em: 11 mar. 2016.

No mapa, pode ser vista a presença global desses sistemas de coleta de dados. As linhas pretas cruzando os oceanos são os cabos de fibra óptica submarinos e cada cor na legenda representa um tipo de acesso. A cor verde (*3rd party / liaison*) indica os trinta serviços de inteligência ao redor do mundo que fornecem dados para a NSA.

A cor bordô (*regional*) refere-se aos oitenta pontos de *Special Collection Services* (SCS). Trata-se de um programa secreto cujo objetivo é inserir “grampos” de voz e dados em equipamentos de difícil acesso, como aqueles em embaixadas, grandes empresas e organizações governamentais. Como pode ser visto no mapa, há pontos SCS no Brasil.

A cor amarela (CNE) é uma sigla para *Computer Network Exploitation* e indica a existência de mais de cinquenta mil sistemas comprometidos por uma divisão da NSA chamada *Tailored Access Operations* – TAO. Essa divisão é especializada em

invadir sistemas de computadores de governos e de grandes corporações – vide o caso da Petrobras – com o propósito de inserir vulnerabilidades que garantam à NSA o acesso aos dados daquela máquina e de outras interligadas na mesma rede.

A cor azul (*large cable*) refere-se aos vinte maiores pontos de interceptação dos cabos ópticos submarinos. Por fim, a cor laranja (*FORNSAT*) é sigla para *Foreign Satellite Collection* e indica os locais onde existem sistemas de interceptação de comunicações globais via satélite.

Já *Bullrun* (NSA) e *Edgehill* (GCHQ)¹⁵¹ são sistemas cujo principal objetivo é minar os padrões de segurança e criptografia, o que frequentemente ocorre, como já mencionado, através da inserção deliberada de falhas em sistemas. Isso é viabilizado de diversas formas: suborno, agentes infiltrados no quadro de programadores das empresas e apropriação de entidades que estabelecem padrões de tecnologia.

Os quatro últimos sistemas – *PRISM*, *MUSCULAR*, *Boundless Informant* e *XKeyscore* – são mais recentes que os demais e possuem, como traço característico, o aproveitamento da expansão do *big data*¹⁵² para obtenção e tratamento de *SIGINT*. *PRISM* e do *MUSCULAR*; são ambos projetos da parceria entre NSA e GCHQ e compartilham o mesmo objetivo: acessar os servidores das grandes empresas de tecnologia – *Google*, *Yahoo*, *Microsoft*, *Apple*, *Dropbox* etc. A diferença é que, por estar localizado fisicamente no Reino Unido, o *MUSCULAR*, ao contrário do *PRISM*, permite que a NSA acesse tais dados sem ordem judicial do tribunal *FISA*¹⁵³ dos EUA.

Todas essas informações coletadas pelos oito programas já expostos precisam ser processadas, exploradas e disponibilizadas para os analistas da NSA, função desenvolvida por Edward Snowden antes de sua fuga. Para isso servem os sistemas *XKeyscore* e *Boundless Informant*, que, em síntese, são mecanismos de *big data* para análise de quantidade massiva de dados na busca por *POL's* – sigla em inglês para *Patterns of Life* –, que busca, exatamente, analisar padrões de

¹⁵¹ Apenas a título de curiosidade, *Bullrun* e *Edgehill* são os nomes dos locais onde ocorreram as primeiras batalhas da guerra civil dos EUA (1861-1865) e da primeira guerra civil da Inglaterra (1642-1646).

¹⁵² Sobre o *big data*, ver item 3.3.2.

¹⁵³ O tribunal *FISA* leva esse nome por ter sido criado pela Foreign Intelligence Surveillance Act of 1978. Trata-se de um tribunal federal secreto, composto por onze juízes, especializado em causas que envolvem espões estrangeiros dentro dos Estados Unidos. Detalhes aprofundados sobre os processos que tramitam no tribunal são, por óbvio, inacessíveis ao público. No site do tribunal constam dados públicos sobre os procedimentos que foram publicizados ou detalhes a respeito da composição do tribunal remete-se ao site oficial do tribunal. Disponível em: < <http://surveillance.es/2y> >. Acesso em: 20 maio 2016.

comportamento, comunicação e deslocamento que são únicos a cada indivíduo. Através deles, é possível vincular os dados que circulam pela Internet às pessoas a quem eles se referem, facilitando a integração dos diversos tipos de dados sobre os indivíduos. A quantidade de informações coletadas em cada parte do globo varia conforme os interesses do governo estadunidense na região, conforme ilustra o mapa abaixo.

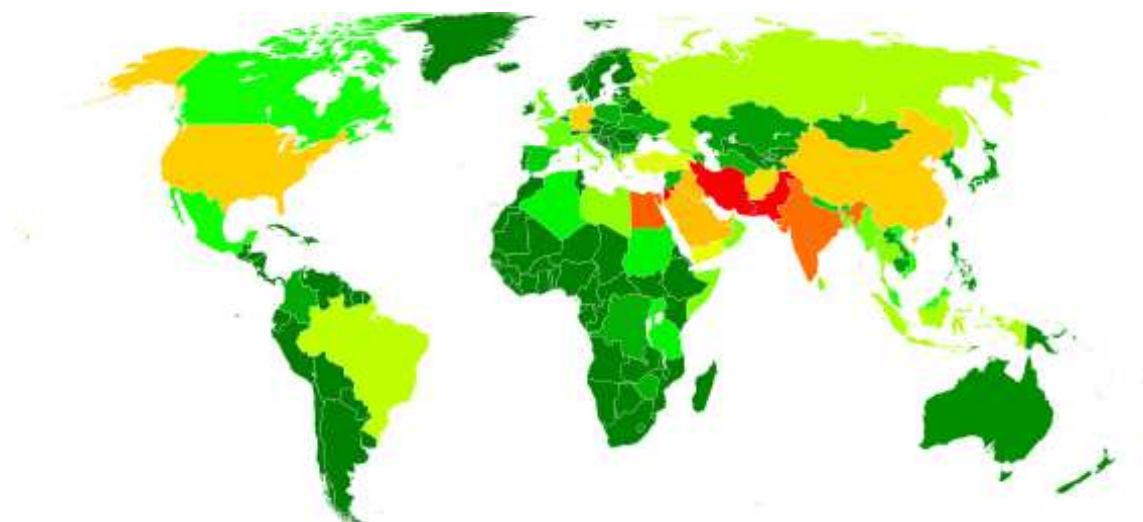


Figura 2 – Mapa gerado pelo sistema *boundless informant* indicando a abrangência da coleta de dados efetuada pela NSA. Quanto mais próximo da cor vermelha, maior a quantidade de dados coletados. Disponível em: < <http://surveillance.es/1m> >. Acesso em: 10 mar. 2016.

As denúncias de Edward Snowden indicam, portanto, que o *big data* é cada vez mais importante para a *surveillance*, o que reforça a transferência do poder para os nós na rede que são capazes de agregar e processar quantidades absurdas de dados. Um fato curioso, no entanto, é que todas as falas de Snowden se restringem à violação da privacidade. Como será visto no próximo capítulo, a privacidade é apenas a ponta do *iceberg* da *surveillance*, pois existem outros direitos humanos violados, como a igualdade e a liberdade. Ainda assim, é útil o questionamento feito por ele durante suas falas: será que as pessoas querem viver em uma sociedade onde elas são cada vez mais transparentes, e as estruturas de coleta de dados, inversamente, cada vez mais opacas?

Entretanto, antes de seguir para o referido capítulo, é importante fazer uma análise das consequências das revelações de Snowden em outras legislações nacionais. Isso será feito no próximo tópico.

3.1.2 Uma tendência a ser seguida?

Por óbvio, as revelações de Snowden surtiram efeitos no modo como o restante do mundo elabora legislações de segurança nacional. Por um lado, o estado de exceção instalado pelo medo líquido relacionado ao terrorismo cria o ambiente político propício para inserção de leis capazes de violar os direitos humanos em nome da segurança nacional. Por outro, cria um movimento de nacionalização dos servidores – nos mesmos moldes daquele inicialmente proposto quando o marco civil brasileiro da Internet ainda era um anteprojeto – em virtude da crença de que, colocando os servidores das empresas de tecnologia no território do Estado, este será capaz de proteger direitos dos seus cidadãos.

Obviamente, essa linha de raciocínio é absurda. Não é necessário profundo conhecimento da topografia das redes de grandes empresas como *Facebook*, *Google*, *Apple*, *Dropbox* e *Amazon*, por exemplo, para saber que elas contam com múltiplos servidores em diversos locais do mundo. Isso garante que, em caso de falha catastrófica do sistema em um determinado lugar, a integridade dos dados possa ser mantida.

Em outras palavras: um conjunto de dados armazenados em um servidor no Brasil, por exemplo, está também armazenado na Islândia, Austrália, EUA etc. Assim, pouco importa, para fins de proteção de dados dos cidadãos, se existe um servidor dessas empresas no seu território. Disso, é possível inferir que o motivo para “nacionalizar” servidores não pode ser jamais o de “proteção dos dados”.

No mesmo sentido, a Rússia aprovou, em julho de 2014, a lei federal nº 242-FZ, que alterou, dentre outras, a lei federal nº 152-FZ, exigindo que os operadores de Internet mantivessem, exclusivamente, em território russo, a gravação, sistematização, acumulação, guarda, atualização e acesso aos bancos de dados dos cidadãos russos¹⁵⁴. Aplica-se aqui a mesma crítica à ideia de nacionalização dos

¹⁵⁴ No original: “5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети “Интернет”, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных

servidores no Brasil, pois, em virtude da impossibilidade de se controlar esses fluxos de dados, é difícil acreditar que o intuito da Rússia é proteger direitos dos cidadãos russos.

Talvez, seja mais razoável supor que se trate de uma expansão do SORM (sigla para Sistema para atividades de investigativas operacionais – Система Оперативно-Розыскных Мероприятий), o “primo” russo do PRISM. Ocorre que, ao contrário do PRISM, o SORM tem abrangência limitada aos servidores que, por lei, são obrigados a instalar “*backdoors*”, ou seja, aqueles fisicamente localizados na Rússia. Com a lei federal nº 242-FZ, ampliaram-se, incrivelmente, as capacidades de intervenção estatal nos dados das grandes empresas da Internet, uma vez que serão obrigadas a cumprir os requisitos técnicos que possibilitam a interceptação de dados pelo governo russo, ou seja, a instalação de “blackboxes”.

No caso mais recente, havia sido apresentado à Assembleia Nacional da França, em nome do Chefe de Governo, o projeto de lei nº 2669/15, agora convertido na lei nº 2015-912, de 24 de julho de 2015. Dentre outras mudanças, estabelece que, “*dans la partie législative du code de la sécurité intérieure, il est ajouté un livre VIII intitulé: «Du renseignement»*”. Na exposição de motivos da lei, consta que a sua finalidade é, através da coleta de informações, conhecer os desafios e prevenir os riscos a que estão submetidos os franceses, visto que, de acordo com a lei, a garantia dos direitos dos franceses depende da manutenção da ordem pública e que, no atual contexto das políticas nacional e internacional, é imprescindível reforçar as políticas de inteligência de dados¹⁵⁵.

A legislação permite que os órgãos de inteligência franceses grampeiem telefones, interceptem comunicações eletrônicas e forcem empresas de Internet a viabilizar maneiras para que a autoridade estatal intercepte todas as informações dos seus usuários (franceses ou estrangeiros, dentro ou fora da França), assim como ocorre na Rússia. Além disso, a lei francesa também permite a coleta e o uso massivo

граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.”

¹⁵⁵ No original: “Le renseignement permet de connaître et de prévenir les risques et les menaces pesant sur notre pays et sa population, ainsi que de mieux appréhender les grands enjeux auxquels ils sont confrontés. Par là-même, il participe de la garantie des droits des citoyens, qui dépend notamment de l’ordre public pour être pleinement assurée. Dans le contexte actuel, international aussi bien qu’intérieur, le renforcement de la politique du renseignement, dans le strict respect des libertés individuelles, est nécessaire.”

de metadados – nos mesmos moldes da NSA –, a instalação de microfones escondidos em objetos, veículos e residências e o uso de dispositivos capazes de interceptar comunicações de celulares e mensagens de texto.

O que se vê, nos casos mencionados, é que as situações de emergência estão “contaminando” as legislações de controle de coleta e uso de dados por parte dos Estados. O recurso amplo e indiscriminado à “guerra contra o terror” possibilita um campo fértil para a multiplicação desse tipo de legislação. Afinal, em virtude da indeterminação do terrorismo, todos são potencialmente suspeitos e a única forma de “filtrar” essa ameaça é através da análise de todos, independentemente da existência de uma suspeita prévia. A análise de todos os dados, sob essa perspectiva, é a forma de antecipar os resultados desastrosos e impedir ameaças terroristas.

Ao que parece, os escândalos envolvendo Edward Snowden inauguraram uma nova era de recurso à legislação nacional que aumenta os poderes do Estado na coleta e processamento de informações. Essa tendência demonstra que a *surveillance*, entendida como fenômeno que permeia o mundo atual, não tem, como consequência, a implosão do Estado. Trata-se de uma novidade muito mais imbricada às tradicionais instituições do que geralmente se supõe.

O que ocorrerá, quando as diversas legislações nacionais tentarem impor às grandes empresas de tecnologia de informação limitações que sejam mutuamente excludentes, ninguém sabe. Menos ainda, tem-se conhecimento sobre a real disposição desses poderosos *global players* em colaborar com os diversos Estados, especialmente, quando tiverem seus interesses contrariados.

Os Estados Unidos parecem ter criado um novo padrão absurdo de legislação relativa à coleta e processamento de dados em massa. Os demais países, incapazes de tomar alguma atitude para diminuir o poder estadunidense, estão “seguindo a corrente” da exceção justificada na prevenção ao terrorismo. “Se não puder vencê-los, junte-se a eles”. O problema é que, na frágil estrutura da sociedade em rede, para lembrar de Manuel Castells, essa situação é insustentável.

Contudo, somente uma descrição de sistemas e leis isoladas não permite avançar adequadamente sobre o tema. É preciso, portanto, compreender como a *surveillance* e o *big data* tornaram-se tendências globais em todas as esferas da vida. Não se trata apenas de coletar dados, mas de transformá-los em conhecimento, em

ação. É por isso que o restante deste capítulo irá aprofundar o impacto da *surveillance* no mundo globalizado e os efeitos do *big data* na ideia de tempo e espaço.

3.2 SURVEILLANCE COMO PARADIGMA DA SOCIEDADE CONTEMPORÂNEA

3.2.1 Notas introdutórias: tendências da *surveillance* no mundo globalizado

Como foi possível apreender dos dois capítulos anteriores, a modernidade líquida, a globalização e a *surveillance* são fenômenos extremamente sinérgicos, já que as práticas da *surveillance* têm, como foco, a mobilidade, o movimento e os diversos tipos de fluxos no planeta – capital, pessoas, conhecimento etc.

Como uma forma de introduzir as principais características da *surveillance* no mundo contemporâneo, é possível falar sobre nove tendências principais da *surveillance* no século XXI (BENNET, HAGGERTY, *et al.*, 2014, p. viii-ix). A primeira tendência é a sua expansão, o que ocorre em virtude da difusão da tecnologia da informação para um número cada vez maior de pessoas nos mais diversos lugares do mundo. O que, no passado, era considerado uma prática excepcional passa a ser aceito como normal na sociedade contemporânea – veja-se, por exemplo, que a coleta de informações biométricas deixou de ser uma exclusividade de quem era preso e passou a ser a regra para os eleitores do Brasil.

Uma segunda tendência da *surveillance* é que sua demanda aumenta em virtude da busca por maior segurança, o que pode ser visto comumente no fato de que os atentados terroristas geram um frenesi por mais coleta e análise de dados de fontes diversas¹⁵⁶. No entanto, a tendência parece ser a de incluir a ideia de risco em cada vez mais áreas da vida e a solução é sempre algum dispositivo eletrônico de coleta e processamento de dados. Se o problema são os assaltos, utilizam-se rastreadores veiculares por satélite. Fraudes? Biometria nas transações financeiras. Doenças imprevisíveis? Sequenciamento genético. Enfim, para cada incerteza da vida, a tendência é que haja uma tecnologia cujo objetivo seja “anular” os riscos. Tudo passa a ser monitorado na busca por mais segurança. Nas palavras de Edward Snowden para Laura Poitras,

por enquanto, saiba que cada fronteira que você cruza, cada compra

¹⁵⁶ A eficácia dessas medidas é questionável, ainda mais levando-se em conta os relatos de Edward Snowden, conforme visto no item 3.1.1.

que você faz, cada torre de celular que você passa, [cada] amigo que você mantém, [cada] *site* que você visita e [cada] assunto que você digita está nas mãos de um sistema cujo alcance é ilimitado, mas cujas garantias não o são (GREENBERG, 2014)¹⁵⁷.

A terceira tendência é a confusão entre as esferas pública e privada. Se, na modernidade sólida, a vigilância era uma prática associada, quase que exclusivamente, ao Estado – através das agências de inteligência, da polícia, das prisões etc –, o mesmo não pode ser visto na *surveillance* – associada à modernidade líquida. A coleta de informação torna-se uma prática tanto da iniciativa pública quanto de entidades privadas, como foi demonstrado anteriormente na análise do *Big Brother* e das *little sisters*. O fato de a informação ser monetizada faz com que a coleta, processamento e troca de dados sejam um negócio incrivelmente lucrativo para a iniciativa privada – o *Facebook*, por exemplo, fechou o ano de 2015 com faturamento de 17.92 bilhões de dólares¹⁵⁸.

A quarta tendência é o fato de que, no mundo da *surveillance*, é mais difícil estabelecer os limites entre quais informações são privadas e quais não o são¹⁵⁹. Existe uma enorme quantidade de dados e metadados que podem ser usados para identificar indivíduos e tirar conclusões sobre diversos aspectos das suas vidas. Conforme analisado anteriormente – e será aprofundado no tópico sobre o *big data* –, é virtualmente impossível desidentificar uma informação, especialmente, caso se esteja lidando com um grande conjunto de dados.

A quinta tendência é o crescimento do interesse no espaço/tempo, o que ocorre em decorrência da necessidade que a globalização tem de facilitar a mobilidade sem perder a capacidade de intervir. Assim, não basta identificar o indivíduo e suas atividades. Torna-se necessário colocá-lo em um contexto espaço-temporal, o que é viabilizado, em especial, pelo uso de telefones celulares e demais dispositivos portáteis com conectividade sem fio, capazes de enviar, automaticamente, relatórios sobre a localização do usuário.

¹⁵⁷ No original: “From now, know that every border you cross, every purchase you make, every call you dial, every cell phone tower you pass, friend you keep, article you write, site you visit, subject line you type, and packet you route, is in the hands of a system whose reach is unlimited but whose safeguards are not.”

¹⁵⁸ Disponível em: < <http://surveillance.es/14> >. Acesso em: 18 fev. 2016.

¹⁵⁹ Essa é, inclusive, uma das falhas do marco civil de proteção de dados pessoais, analisado no item 1.5.2.

A sexta tendência é a expansão do caráter global da *surveillance*, ou seja, o modo como o fluxo de dados permite a supressão das tradicionais fronteiras associadas ao Estado-nação. Exemplos disso são sistemas como os API e PNR – sigla em inglês para *Advanced Passenger Information / Passenger Name Record* –¹⁶⁰, que enviam os dados das reservas de bilhetes aéreos e dos *check-ins* no aeroporto antes mesmo que o viajante chegue ao país de destino.

A sétima tendência é a inserção da *surveillance* no cotidiano, o que ocorre em virtude da proliferação de computadores na vida humana. E, aqui, a palavra “computadores” deve ser entendida em sentido amplo: telefones, carros e até mesmo animais – como aqueles que possuem chip RFID ou coleiras com GPS – possuem computadores embutidos. Um exemplo disso é a “Internet das coisas”¹⁶¹, que viabiliza a expansão de uma nova camada de computadores e sensores capazes de coletar e transmitir informações sobre o ambiente. Com essa ubiquidade, a *surveillance* torna-se mais disseminada e menos perceptível.

A oitava tendência é a transformação do corpo em fonte de dados analisáveis. Isso inclui o uso de biometria – dados extraídos dos corpos, geralmente com a finalidade de confirmação de identidade – ou bancos de dados de perfis genéticos – sejam eles públicos ou privados – cujas finalidades são diversas: desde persecução penal¹⁶² até a criação de redes sociais de pessoas geneticamente relacionadas, como é o caso da empresa *23andme*¹⁶³, que, até junho de 2015, já tinha sequenciado amostras de DNA de 1.000.000 usuários (RAMSEY, 2015).

¹⁶⁰ O API/PNR é utilizado por diversos países que fazem parte da IATA, o que inclui o Brasil. Aqui, a regulamentação do tema é feita pela resolução 255/2012 da ANAC e estabelece que “a disponibilização de API e do PNR tem como finalidade a prevenção e a repressão a atos de interferência ilícita e a facilitação do desembarço junto às autoridades de controle migratório, aduaneiro, sanitário e agropecuário”.

¹⁶¹ A Internet das coisas (IoT, na sigla em inglês) é uma rede de objetos cotidianos – livros, chaveiros, carteiras, carros, roupas – equipados com sensores e conectividade com a Internet, o que possibilita que coletem e transmitam informações entre eles. Isso permite que objetos interajam uns com os outros, bem como sejam controlados a distância, o que permite uma interação maior entre o mundo físico e o mundo digital.

¹⁶² Sobre o tema, remete-se ao artigo de Taysa Schiocchet (2013) e às pesquisas do grupo BioTechJus: <http://www.biotechjus.com.br>.

¹⁶³ O *23andme* é uma empresa cuja fundadora é nada menos que Anne Wojcicki, esposa do fundador do Google, Sergey Bin. Muito além de criar “redes sociais de parentes”, o grande propósito da empresa é a aplicação de técnicas de *big data* com dados genéticos e de doenças (fornecido pelos usuários). Como o negócio do *Google* é informação e, certamente, ele não entra nesse jogo para acumular prejuízos, é de se imaginar como serão utilizados esses perfis genéticos. Os termos de uso do serviço deixam claro que “23andMe may also include your information in Aggregated Genetic and Self-Reported Information disclosed to third-party non-profit and/or commercial research partners who will not publish that information in a peer-reviewed scientific journal. [...] You understand that the technical processing and transmission of the Services, including your Personal Information, may involve (a) transmissions

Paradoxalmente, apesar de utilizar informações oriundas do corpo, ou seja, individualizadas, a automatização da análise de dados substitui o ser humano pelos dados compilados sobre ele e que, nem sempre, são fiéis à realidade. Sob essa perspectiva, é fácil perceber que quanto mais informação é acumulada, menos são vistas as pessoas a quem aqueles dados se referem (ANDREJEVIC, 2007, p. 241).

Por fim, a nona tendência é o crescimento do aspecto social da *surveillance*, consequência da expansão do uso de redes sociais. Como resultado do incentivo para que as pessoas divulguem a própria vida, normaliza-se a ideia de que se está sempre sendo analisado. Por trás dessas nove tendências, está a ideia de modernidade líquida, detalhada anteriormente neste trabalho. A tese de que a *surveillance* é líquida já era trabalhada por David Lyon (2010) antes mesmo de ter escrito a obra em conjunto com Bauman (BAUMAN e LYON, 2013)¹⁶⁴. Isso porque a metáfora da liquidez descreve, com precisão, as relações estabelecidas pelos fluxos de dados e a transformação de informações, inclusive retiradas do próprio corpo, em conjuntos de dados analisáveis.

Essa liquidez faz desaparecer as antigas instituições totais relacionadas, por exemplo, ao modelo panóptico. Se, por um lado, a metáfora panóptica tinha a finalidade de criar restrições de entrada e saída através da construção de muros, a *surveillance* no século XXI trabalha com a ideia de modulação. Afinal, ela é utilizada para facilitar alguns fluxos e dificultar outros, o que, como será visto a seguir, é imprescindível para a globalização.

3.2.2 Globalização, securitização, incerteza e risco

O que significa, então, dizer que a *surveillance* segue os efeitos da globalização? Dizer que algo está sendo globalizado implica afirmar que ocorre um redimensionamento de um processo que, anteriormente, ocorria em escala local (MURAKAMI WOOD, 2012, p. 333). Como resultado dessa interconexão do mundo, os fenômenos de coleta e processamento de dados não podem mais ocorrer somente dentro de estruturas pré-determinadas, como era o caso do panóptico. A globalização

over various networks; and (b) changes to conform and adapt to technical requirements of connecting networks, or devices.”. Disponível em: < <http://surveillance.es/1n>>. Acesso em: 10 mar. 2016.

¹⁶⁴ Como já era de se esperar, o livro foi lançado no Brasil em 2014 e traduzido para o português como “vigilância líquida”, o que não contribui muito para a discussão do fenômeno.

demanda a facilitação de fluxos, de modo que qualquer modelo que dependa do confinamento é inadequado para explicar a *surveillance* no mundo globalizado. Por isso, é extremamente difícil para o Estado-nação controlar os fluxos de dados globais, em razão de que um simples e-mail pode dar uma volta ao globo antes de chegar ao destinatário, ainda que ele e o remetente estejam sentados a cinco metros de distância.

Entre as principais mudanças viabilizada pela *surveillance*, no mundo globalizado, está a superação da sociedade disciplinar pensada por Foucault (DELEUZE, 1992). Passa-se do confinamento para a modulação, cuja distinção, conforme Deleuze, é a seguinte:

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 (DELEUZE, 1992, p. 221)

Isso porque o modelo disciplinar demonstrou ser incapaz de se adaptar às demandas de modulação da globalização, o que reclama uma nova forma de moldagem capaz de se modificar instantaneamente junto com a necessidade dos fluxos. Isso é viabilizado pela ideia de invólucro digital, trabalhada por Mark Andrejevic (2007, 2012), que se baseia no fato de que a *surveillance* é ubíqua, o que permite a coleta constante de dados em um espaço que é constantemente monitorado.

Todavia, essa ideia de monitoramento constante não deve induzir à falsa conclusão de que existe uma autoridade central, sempre monitorando todos os espaços. Embora, para bem da verdade, os eventos envolvendo Edward Snowden tenham demonstrado a assustadora capacidade de uma única entidade para coletar grande parte dos dados mundiais, a NSA não é responsável pelas diversas redes – especialmente privadas – como *Google*, *Yahoo*, *Facebook* –, que possuem seus próprios objetivos. No atual contexto, é possível afirmar que a NSA está mais próxima de um parasita do que de uma autoridade central, visto que consegue utilizar os recursos dos “hospedeiros” – ou seja, as empresas de tecnologia – sem sua concordância.

Tal fato ocorre, tendo em mente que, como visto no debate anterior sobre a inadequação da metáfora do *Big Brother* para explicar a *surveillance*, o mundo atual é composto por uma série de diferentes redes, controladas por entidades diversas,

cada uma com capacidade distinta para coletar dados. No mesmo sentido, Mark Andrejevic explica que essa descentralização

não exclui a possibilidade de que dados possam ser agregados em um controle centralizado sob certas circunstâncias. A habilidade que autoridades em algumas jurisdições possuem para acessar bancos de dados comerciais, por exemplo, pode tornar possível a coleta, por uma única instituição, de uma ampla série de dados originalmente capturados por diferentes entidades com propósitos variados. Ainda, na medida em que certas plataformas desenvolvidas por empresas privadas como Google ou Facebook podem servir de base para uma série de atividades, entidades comerciais possuem a capacidade de agregar grandes quantidades de dados sob o seu controle (ANDREJEVIC, 2012, p. 93)¹⁶⁵.

Esse traço fluido da *surveillance* na sociedade contemporânea viabiliza a “concentração” e “desconcentração” instantânea dos diversos fluxos de dados. Justamente pela sua natureza líquida, o alcance desse tipo de sistema é ilimitado, o que só é possível em virtude da ideia do aumento constante de trocas viabilizado pela globalização.

Entretanto, existe um “lado negro” da globalização, que é o surgimento do medo líquido (BAUMAN, 2008), um medo que, assim como os fluxos de dados, ultrapassa as fronteiras e ignora a soberania estatal. Isso acontece porque,

em um planeta globalizado, habitado por sociedades forçosamente ‘abertas’, a segurança não pode ser obtida, muito menos garantida de maneira confiável, em um único país ou grupo de países: não por seus meios próprios e não independentemente do estado das coisas do mundo (BAUMAN, 2008, p. 127).

Essa interconexão cria uma rede de incertezas; afinal, atitudes tomadas de um lado do globo podem gerar consequências danosas para os habitantes do outro lado. Para alguns, como Ulrich Beck (1998), os riscos foram multiplicados em virtude da globalização, constituindo um dos principais problemas a serem resolvidos pelas sociedades. Contudo, a perspectiva de Beck sofre críticas em virtude de o autor entender que o risco é um fenômeno objetivo. Além disso, outros autores consideram que Beck não leva em consideração o fato de que o risco é construído de acordo com

¹⁶⁵ No original: “This is not to rule out the possibility that data might be aggregated under centralized control under certain circumstances. The ability of authorities in some jurisdictions to access commercial databases, for example, would make it possible to collect under one umbrella a range of data originally captured by different entities for varying purposes. Also, to the extent that certain platforms devised by companies like Google or Facebook might serve as the basis for a range of different activities, commercial entities have the ability to aggregate large swathes of data under their control.”

interesses políticos e comerciais, o que ficou claramente visto após os atentados nos Estados Unidos, no dia 11 de setembro de 2001.

Sob essa perspectiva, Zygmunt Bauman (2008, p. 129) critica a ideia de que se vive em uma sociedade de risco. Para ele, o risco só existe se for considerado que o mundo funciona de modo regular, sob parâmetros roteirizados, o que é exatamente o contrário daquilo possibilitado pela multiplicação das incertezas.

A razão disso é que os riscos podem ser estatisticamente calculados diante de um cenário de razoável homogeneidade, o que, para Bauman, não acontece no mundo atual. Como resultado, o referido autor entende que o conceito de risco não é compatível com o mundo contemporâneo, “negativamente globalizado. Para ele, o que torna o mundo atual perigoso é, justamente, a natureza incalculável¹⁶⁶ dos perigos, o que gera um dos grandes paradoxos contemporâneos: por um lado, vive-se em um mundo com ferramentas tecnológicas incríveis e com enormes potenciais para resolver diversos problemas que poderiam gerar incertezas e medo no homem; por outro, nunca os seres humanos se sentiram tão inseguros.

Embora não seja possível concordar integralmente com Bauman – afinal, o risco existe e o seu cálculo em meio à heterogeneidade é o principal propósito das técnicas de *big data* e *predictive analytics* –, pode-se afirmar que a incerteza, mais do que o risco, é uma das características da modernidade líquida.

Como consequência, também, é possível dizer que riscos são, simultaneamente, reais e construídos, ou seja, são, em parte, fato; em parte, ficção (MCCULLOCH e WILSON, 2016). São reais porque fazem parte da vida cotidiana, sejam em escala individual ou coletiva, micro ou macro, mas também são construídos, uma vez que a sua percepção pode ser amplificada ou diminuída. Em outras palavras,

de um oceano de possíveis riscos, o poder constrói o conhecimento que destaca, esconde ou nega certos riscos e transforma riscos reconhecidos em aceitáveis ou inaceitáveis. O risco é politizado e o medo coletivo é apropriado como uma forma de estruturar tolerância ou intolerância (MCCULLOCH e WILSON, 2016, p. 38)¹⁶⁷.

¹⁶⁶ Um contraponto sobre a natureza incalculável dos riscos será trazido no capítulo sobre as análises preditivas de risco, item 3.4.1.

¹⁶⁷ No original: “From an ocean of possible risk, power builds knowledge that highlights hides or denies certain risks and constructs acknowledged risks as either acceptable or unacceptable. Risks are politicized and public fears appropriated as a way of structuring tolerance and intolerance.”

Um dos exemplos clássicos dos medos vividos pelas sociedades contemporâneas é o terrorismo que, seguindo a tendência de liquefação da modernidade líquida, descentraliza a guerra e a violência, que deixam de ser coordenadas e associadas a um determinado espaço físico.

Logo, a própria ideia de “guerra ao terror” é extremamente contraditória, pois o sentido tradicional de guerra está ligado à modernidade sólida¹⁶⁸. Os pesados armamentos das grandes guerras mundiais, por exemplo, foram desenhados para localizar e destruir alvos específicos, não as células terroristas, estas caracterizadas pela desvinculação a um território específico, descentralização e mobilidade.

Nesse contexto antiterrorista, a aplicação de ferramentas de *big data* que caracterizaram a *surveillance*, apostam em técnicas preditivas como forma de neutralizar os riscos, o que acaba por diminuir o limiar entre risco tolerável e intolerável. Como resultado, desvia-se do foco em fatos e passa-se a agir mediante especulações¹⁶⁹, construindo a ideia de uma constante iminência de ataques terroristas, o que reforça, ainda mais, o desenvolvimento de técnicas preventivas de risco, retroalimentando esse ciclo.

Os ataques terroristas, por sua natureza, constituem um tipo de ameaça que não pode ser prevista ou calculada através dos métodos tradicionais – e, portanto, não constituem um “risco”, mas uma incerteza na perspectiva de Bauman (2008, p. 129). Em uma análise mais sóbria, McCulloch e Wilson compreendem a ameaça do terrorismo, simultaneamente, como incerteza e risco. Segundo os autores,

o risco e a incerteza têm muito em comum e não são conceitos separados ou binários [...] O risco é inerentemente incerteza, e tanto risco quanto incerteza estão ambos ligados à dúvida e à insegurança. O risco, contudo, sugere um conceito mais aberto ao cálculo ou ou estimação baseada em evidência, enquanto a incerteza é mais próxima ao desconhecido e incalculável (MCCULLOCH e WILSON,

¹⁶⁸ Sobre a modernidade sólida, remete-se ao item 1.3.1.

¹⁶⁹ Aqui, a “especulação” pode ir longe demais. Em 2001, o DARPA desenvolveu um “mercado futuro do oriente médio” – chamado *Policy Analysis Market*, vinculado ao projeto *FutureMAP* – que funcionava como uma bolsa de valores, permitindo que contratos futuros fossem negociados com base nas possibilidades de desfechos para eventos em países do Oriente Médio – o que levava em conta, inclusive, a tomada de poder por grupos considerados terroristas. A teoria por trás desse mercado é a de que o valor monetário de um contrato futuro reflete a probabilidade de acontecimento de um evento a ele relacionado, vez que os investidores negociam contratos com base em informações privilegiadas. Em tese, aqueles com informações sobre mudanças políticas no Oriente Médio forneceriam indiretamente informações aos EUA através do aumento ou diminuição do valor de mercado dos contratos futuros no Oriente Médio.

2016, p. 41)¹⁷⁰

Logo, os instrumentos preditivos associados à *surveillance* no mundo contemporâneo encontram lugar, justamente, nas incertezas, pois envolvem uma substituição do cálculo do risco pela especulação de modelos computacionais de futuros prováveis. Como consequência da utilização desses modelos, transfere-se cada vez mais poder para os atores públicos e privados, que detêm a tecnologia capaz de realizar essa análise preventiva.

Esse movimento faz parte de uma mudança de paradigma da defesa em direção ao da segurança. Essa “securitização”, que caracteriza a “guerra contra o terror”, significa

[...] o movimento de uma atitude reativa e conservativa em direção a outra ativa e construtiva, tanto dentro quanto fora das fronteiras nacionais: da preservação da atual ordem social e política interna para a sua transformação e, similarmente, de uma atitude de guerra reativa, que responde aos ataques externos, para uma atitude ativa, que busca antecipar o ataque (HARDT e NEGRI, 2004, p. 20)¹⁷¹.

Como óbvia consequência, a securitização enfraquece a soberania moderna em virtude da sua capacidade para normalizar uma situação de guerra constante, que deveria ser excepcional. Desestabiliza-se, assim, o poder em direção aos atores públicos – das grandes potências – e privados –, detentores da tecnologia da informação.

Tais atores passam a coletar a maior quantidade possível de dados sob a alegação de que, se, devidamente analisadas, tais informações podem ajudar a diminuir as inseguranças da sociedade contemporânea. Para esse discurso, a superação das técnicas estatísticas tradicionais em direção aos modelos preditivos permite encontrar sentido no meio do caos, transformando o incalculável em probabilidade e a dúvida em ação política. Esse é o tema do item que segue.

¹⁷⁰ No original: “Risk and uncertainty have much in common and are not discrete or binary concepts [...] Risk is inherently uncertain, and both risk and uncertainty are closely related to doubt and insecurity. Risk, however, suggests a concept more open to calculation or estimation based on evidence, while uncertainty is more closely aligned to the unknowable and incalculable.”

¹⁷¹ No original: “[...] the movement from a reactive and conservative attitude to an active and constructive one, both within and outside the national boundaries: from the preservation of the present domestic social and political order to its transformation, and similarly from a reactive war attitude, which responds to external attacks, to an active attitude that aims to preempt attack.”

3.3 ANÁLISES PROBABILÍSTICAS E BIG DATA

3.3.1 Probabilidades e previsão de eventos futuros

Em 1814, o matemático e físico Pierre Simon Laplace referiu-se, em um ensaio sobre as probabilidades, a uma ideia – depois denominada “demônio de Laplace” – que se tornaria o ponto de partida para todos os debates posteriores sobre o caos, o acaso e o determinismo. Consoante seu pensamento,

devidos, portanto, considerar o presente estado do universo como o efeito de seu estado anterior e, como a causa do que ocorre depois. Uma inteligência que, em um dado instante, conheça todas as forças que animam a natureza e a situação respectiva dos seres que a compõem, se fosse grande o suficiente para enviar esses dados para análise, compreenderia com a mesma fórmula os movimentos dos maiores corpos do universo e aqueles do átomo mais leve; nada seria incerto para ela, e o futuro, como o passado, estaria presente diante dos seus olhos (LAPLACE, 1840, p. 2).¹⁷²

Como visto anteriormente, a tecnologia da informação possui a capacidade de alterar a percepção do tempo e do espaço, porque a estrutura rizomórfica das redes de comunicações e a velocidade dos fluxos de dados que nela transitam permitem o acesso instantâneo às informações independentemente da sua localização.

Esse efeito de compressão do tempo, contudo, não é o único associado à *surveillance*. Em virtude do constante e difuso medo em que vive a sociedade contemporânea, um dos principais objetivos do tratamento de dados é a utilização de dados do passado e do presente para a construção de modelos preditivos do futuro. Assim como o demônio de Laplace, a ideia principal é a de que, dispondo de informações suficientes sobre o passado e o presente, será possível prever as consequências de futuras.

Uma imagem clara dessa construção do tempo futuro é aquela presente no filme *Minority Report* (2002), dirigido por Steven Spielberg e protagonizado por Tom Cruise. O desenrolar da trama ocorre ao redor do que é denominado “sistema de pré-crime”. Este, por sua vez, consiste na junção de tecnologia de ponta com os poderes

¹⁷² No original: “Nous devons donc envisager l'état présent de l'univers, comme l'effet de son état antérieur, et comme la cause de celui qui va suivre. Une intelligence qui, à un instant donné, connaîtrait toutes les forces dont la nature est animée et la situation respectiva des êtres qui la composent, si d'ailleurs elle était suffisamment vaste pour soumettre ces données à l'analyse, embrasserait dans la même formule les mouvements des plus grands corps de l'univers et ceux du plus léger atome; rien ne serait incertain pour elle, et l'avenir, comme le passé, serait présent à ses yeux.”

psíquicos de três indivíduos capazes de ver fragmentos do futuro – *precogs*. Ao juntar esses fragmentos, forma-se uma previsão de um futuro aparentemente inescapável, de modo que os potenciais crimes violentos são interrompidos antes mesmo do seu acontecimento, com a prisão do “criminoso” sem que tenha ocorrido o crime propriamente dito.

Na vida real, embora não existam os *precogs* no sentido dado pelo filme, a tecnologia da informação tenta fazer as suas vezes. Uma das formas de se conseguir isso é através das análises estatística e probabilística. No dia a dia, todos fazem alguma análise que envolve probabilidades, seja verificando a previsão do tempo antes de sair de casa, escolhendo qual a fila no supermercado, consultando, no GPS, a rota com menos trânsito etc. A busca por padrões passados para inferir comportamentos futuros faz parte da forma como o ser humano se movimenta no mundo.

Por esse motivo, o tema merece um pouco de atenção, ainda mais, por ser razoavelmente alienígena para os juristas, público-alvo deste trabalho. Os juristas – e a grande maioria das pessoas – manejam, com dificuldades, as análises probabilísticas do cotidiano, sem considerar vários dos seus aspectos mais importantes. Por isso, embora com as limitações oriundas da escrita de um jurista, este item do trabalho pretende demonstrar: a) como são equivocados os raciocínios intuitivos sobre estatística e b) como esse tipo de análise pode ser utilizada para aperfeiçoar as habilidades de pensar o futuro.

Um dos equívocos mencionados é a aplicação daquilo que Daniel Kahneman e Amos Tversky chamam de “lei dos pequenos números” (KAHNEMAN e TVERSKY, 1971). Apesar do nome, não se trata de uma lei propriamente dita, mas de um erro comum que leva as pessoas a acreditarem que uma pequena amostra é suficiente para que possam calcular a probabilidade de acontecimento de um evento no futuro. Os indivíduos agem como se cada segmento de uma sequência aleatória tivesse que manter a proporção esperada.

Uma outra versão do mesmo erro é explicada, com clareza, por Leonard Mlodinow (2008) e chama-se falácia do jogador. Segundo o físico, é comum pensar que a probabilidade de um evento futuro acontecer aumenta caso ele não tenha (ou tenha) acontecido recentemente. Por exemplo: em uma série de 100 lançamentos de moeda, caso os 44 primeiros tenham sido “cara”, a tendência é a de que as pessoas

imaginem que o próximo resultado tem maior chance de ser “coroa”, como se o universo conspirasse para compensar a ausência de coroas e chegar aos 50% de coroas nos 100 lançamentos.

Em ambos os casos, trata-se de um erro de compreensão daquilo que é chamado processo de Bernoulli. Em estatística, um processo de Bernoulli é uma sequência finita ou infinita de eventos independentes entre si e cujo resultado possível é binário – exatamente como o lançamento de uma moeda. O problema desse tipo de série é que o índice de confiança de que um determinado resultado ocorrerá depende do número de eventos na série.

Assim, embora seja de conhecimento notório que existe 50% de chances de uma moeda lançada ser cara ou coroa caso o seu peso seja perfeitamente balanceado, é necessário um número extremamente grande de lançamentos para garantir que uma série obedecerá a essa proporção em 99,9% das vezes. Mais precisamente, seriam necessários 2.775 lançamentos¹⁷³ para garantir, com 99,9% de confiança, que uma moeda obedece à proporção de 50% cara e 50% coroa.

Ocorre que, no mundo real, dificilmente, as chances de um evento ocorrer independem da ocorrência de outros eventos. Aplica-se, nesses casos, a chamada probabilidade condicional, desenvolvida por Thomas Bayes no século XVIII, como modo de adequar os resultados caso novos dados apareçam.

Trata-se de um tipo de análise extremamente comum no cotidiano: desde pessoas – que fazem análises bayesianas com frequência – até avançados mecanismos preditivos, como é o caso dos sistemas de filtro de e-mails indesejados – *spam*. Ao receber novas variáveis, os sistemas de computador ajustam as probabilidades da ocorrência de um evento futuro. É assim, por exemplo, que as seguradoras de veículos conferem descontos no prêmio pago pelo segurado que não sofreu acidentes; afinal, o lapso do tempo sem a ocorrência de sinistros – ao contrário do lançamento de moedas – influencia na probabilidade de sinistros futuros.

Um exemplo interessante de como o ajuste de variáveis interfere no resultado é o caso do teste de HIV que ocorreu com o próprio Mlodinow (2008, p. 115). Os exames atuais para detecção do HIV são 99,9% sensíveis e 99,999% específicos, ou seja, produzem resultados falso positivo 1 em cada 1.000 vezes e falso negativo 1 vez

¹⁷³ A fórmula é $n = \frac{Z^2}{4E^2}$, onde n é o número de jogadas, Z é o intervalo de confiança e E é o erro máximo.

a cada 100.000 vezes. A princípio, então, parece ser extremamente improvável que uma pessoa receba um diagnóstico positivo sem que tenha o vírus do HIV.

Mlodinow, que foi testado positivo para HIV, conta que o médico lhe informou o resultado do exame de HIV como uma sentença de morte. Segundo o médico, somente 1 em cada 1.000 testes é falso positivo, de modo que as suas probabilidades de possuir HIV seriam, ainda para o médico, de 999 em 1.000.

O raciocínio feito pelo médico – e pela maioria das pessoas na mesma situação – é, no entanto, fruto do equívoco na compreensão da teoria bayesiana. Nesse tipo de análise, as chances de um evento “A” acontecer se o evento “B” acontecer diferem das chances de “B” acontecer se “A” acontecer. Como resultado, o médico confundiu a probabilidade de que o exame desse positivo se Mlodinow não fosse HIV-positivo com a probabilidade de que Mlodinow não fosse HIV-positivo se o exame desse positivo.

Para realizar uma análise bayesiana desse exemplo, é necessário, primeiro, delimitar o espaço amostral, ou seja, o conjunto de todos os resultados possíveis: pessoas infectadas com exame positivo; pessoas não infectadas com exame positivo; pessoas não infectadas com exame negativo e pessoas infectadas com exame positivo.

Para saber o primeiro elemento do conjunto, ou seja, pessoas infectadas com exame positivo, Mlodinow utilizou-se dos dados epidemiológicos do centro de controle de doenças dos Estados Unidos – CDC – e observou que indivíduos com o seu perfil – caucasiano, heterossexual, não usuário de drogas injetáveis – possuíam a incidência de HIV de 1 em cada 10.000 pessoas.

O número de pessoas não infectadas com exame positivo já foi estabelecido pela sensibilidade do exame (99,9%), ou seja, 1 em cada 1.000. Como resultado, em um conjunto de 10.000 pessoas, 1 terá realmente a doença; 10 terão o teste positivo, mas não terão a doença, nenhum terá o teste falso negativo e o restante, 9.989, não são portadores do vírus e têm o teste negativo.

A conclusão, então, é a de que a cada 10 mil pessoas, 11 terão o exame positivo. Destas, apenas 1 será portadora do HIV, de modo que as chances de Mlodinow realmente ser HIV-positivo diminuíram de 99,9% – como havia dito o médico – para 1 em 11, ou seja, 9,09%. Isso demonstra como é possível alterar, radicalmente,

a análise da probabilidade de um resultado com a inserção de uma única informação – os dados epidemiológicos do CDC.

Os problemas no mundo da *surveillance* são, extremamente, mais complexos que a análise acima. No entanto, os sistemas que realizam esse tipo de análise são muito mais avançados, eficientes e dispõem de um número de informação cada vez maior.

Tome-se, por exemplo, o já mencionado *site* de aplicação do estudo sobre determinação de traços psicológicos a partir das “curtidas” do *Facebook* (KOSINSKI, STILLWELL e GRAEPEL, 2013). A cada nova “curtida”, o usuário insere uma nova informação no sistema e aumenta a precisão do resultado. Além disso, os pesquisadores continuam aprimorando o mecanismo de análise dos dados, de modo que eles são capazes de alterar os parâmetros do sistema e, igualmente, aumentar a precisão do algoritmo.

Para deixar a situação ainda mais interessante, em fevereiro de 2016, o *Facebook* implementou a função “*reactions*” ao botão de curtir. Agora, os usuários podem expressar outros cinco sentimentos, além do “curtir”: amor, risadas, espanto, tristeza e raiva. Com isso, o *Facebook* irá coletar seis vezes mais dados que o tradicional “curtir”, o que transforma as novas opções em uma ferramenta extremamente poderosa de coleta de dados, capaz de aumentar, ainda mais, a precisão do algoritmo classificador do *Facebook*.

O resultado de uma análise probabilística, portanto, depende, em muito, da forma como se analisam os fenômenos estatísticos e da quantidade de dados disponíveis para realizar essa análise. Por esse motivo, um dos traços que marcam a *surveillance* é a busca pela aquisição da maior quantidade de dados possíveis para que sejam desenvolvidas ferramentas que permitam a sua análise, possibilitando, dentre outros, a previsão de comportamentos futuros. São esses os temas dos próximos itens.

3.3.2 O que é big data?

Em um mundo hiperconectado, a vida humana ocorre através de estruturas digitais. Desde o nascimento até a morte, os eventos na vida das pessoas passam

por algum meio digital, e cada contato entre homem e tecnologia gera novas informações, que passam a fazer parte desse ciclo infinito.

A quantidade de informação gerada na atualidade é extremamente grande. O barateamento das estruturas de armazenamento e transmissão torna vantajoso armazenar tudo, mesmo que aquela informação não tenha nenhuma utilidade imediata. Além disso, há a diminuição de custo dos dispositivos geradores de dados: telefones celulares, computadores, câmeras, etiquetas RFID etc.

Big data é o nome genérico para se referir a esses conjuntos de dados tão grandes que as tradicionais técnicas de análise de dados demonstram-se insuficientes, ou, em outras palavras, é

[...] um fenômeno cultural, tecnológico e acadêmico que se baseia na interação entre: (1) Tecnologia: maximizando poder computacional e precisão algorítmica para coletar, analisar, conectar e comparar grandes conjuntos de dados. (2) Análise: baseada em grandes conjuntos de dados com o objetivo de identificar padrões e realizar afirmações de cunho econômico, social, técnico e legal. (3) Mitologia: a crença difusa de que grandes conjuntos de dados oferecem uma forma superior de inteligência, capaz de gerar compreensões que seriam anteriormente impossíveis, com uma aura de verdade, objetividade e precisão (BOYD e CRAWFORD, 2012, p. 663)¹⁷⁴.

O *big data* é, tradicionalmente, classificado pelo uso de três V's: velocidade, volume e variedade. O primeiro V faz referência à rapidez com que os dados são criados, armazenados, analisados e visualizados, o que ocorre em tempo real, seja através da coleta realizada por seres humanos, seja através de sensores e máquinas instalados nos quatro cantos do planeta – e também fora dele, como é o caso dos diversos telescópios e satélites fora do planeta.

O segundo V, volume, refere-se à quantidade de dados gerenciados por esses sistemas. Afinal, se a velocidade de coleta de dados tende ao infinito e o custo de armazenamento tende a ser cada vez mais baixo, faz sentido utilizar conjuntos enormes de dados. No passado, essa quantidade de dados seria um problema do ponto de vista da capacidade computacional necessária para analisá-los. Isso não

¹⁷⁴ No original: “[...] cultural, technological, and scholarly phenomenon that rests on the interplay of: (1) Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets. (2) Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims. (3) Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy.”

ocorre na atualidade, visto que surgiram novos *softwares* capazes de gerenciar e extrair conteúdo desses dados.

O terceiro V diz respeito à variedade dos tipos de dados que são armazenados, em razão de, em um passado não muito distante, a grande maioria dos dados criados eram estruturados, ou seja, distribuídos de modo organizado em colunas e linhas. Na atualidade, a maior parte dos dados é não estruturada, o que demanda o desenvolvimento de programas de computador que saibam gerenciar dados não organizados, isto é, capazes de lidar com informações sem que tenham sido especificamente instruídos sobre como elas são formatadas – técnica também chamada de *machine learning*.

Além dos tradicionais 3V's, David Lyon (2014) faz menção às outras características inerentes ao *big data*: 1) a exaustividade de escopo, uma vez que os dados coletados tendem a englobar um número cada vez maior de pessoas e sistemas; 2) a alta resolução dos dados, ou seja, o fato de que eles incluem uma enorme quantidade de detalhes; 3) a interconexão dos dados, o que significa que possuem campos em comum que permitem a junção de diferentes conjuntos de dados; 4) a extrema flexibilidade e escalabilidade horizontal – vez que permitem adicionar mais detalhes sobre uma mesma entrada de dados – e vertical – visto que possibilitam a fácil inclusão de novas entradas de dados.

Nesse ótica, fica claro que não se trata apenas de informações cuja quantidade torna impossível sua compreensão por um indivíduo; afinal, isso sempre aconteceu em grandes bibliotecas desde a Antiguidade. O grande diferencial do *big data* é a habilidade para dar novas funções a esses dados, permitindo análises extremamente sofisticadas e viabilizando a previsão de eventos incrivelmente complexos, como padrões de comportamento humano, tráfego, eventos climáticos etc. Nesse aspecto, Mark Andrejevic e Kelly Gates afirmam que

a biblioteca do congresso, por exemplo, existe já há algum tempo, mas conforme o seu conteúdo é digitalizado, algoritmos podem procurar padrões e correlações que foram, até então, impossíveis de detectar. Se, no passado, existiam limitações práticas na habilidade de rastrear simultaneamente o movimento de dezenas ou centenas de milhares de pessoas em uma grande cidade, por exemplo (seria proibitivamente caro contratar pessoas suficientes para perseguir todos e tomar notas), hoje, a habilidade para discernir padrões úteis e nada óbvios a partir de dados depende de sistemas técnicos complexos. Os humanos simplesmente não podem lidar com esse tipo de análise sem

ajuda (ANDREJEVIC e GATES, 2014)¹⁷⁵.

Os seres humanos estão fadados a viver toda a sua vida sem conseguir dar conta da totalidade de informações que gostariam de apreender. Sob tal perspectiva, o *big data* permite que o homem possa atribuir sentido a um conjunto de informações cada vez maior. A capacidade para analisar grandes conjuntos de dados torna-se um diferenciador para as entidades envolvidas – empresas e governos –, uma vez que melhores resultados podem ser obtidos através da elaboração de algoritmos de análise mais sofisticados. Esses algoritmos, contudo, pressupõem a existência de um sistema digital capaz de coletar esses dados, o que só pode ser feito em uma sociedade “mergulhada” no mundo tecnológico, onde todas as transações e interações típicas do cotidiano são mediadas, em algum momento, por uma estrutura virtual de dados.

O *big data* permite uma mudança de escala tão grande que cria um novo horizonte de perspectivas para a análise de dados. Além disso, esse fenômeno reforça o que foi defendido anteriormente, ou seja, de que não se pode confundir vigilância com *surveillance*. A natureza não sistematizada e não direcionada do *big data* faz com que apareça uma nova dimensão da *surveillance*, cujo objetivo, ao invés da seletividade da vigilância, é coletar a maior quantidade possível de dados sobre todos. O “alvo” da *surveillance* na era do *big data* não é uma pessoa, mas os sentidos ocultos dentro de vários conjuntos de dados.

Todavia, não se trata apenas de compreender os dados, mas de criar formas de modificar o mundo através dessa compreensão. Isso só é possível para aqueles que possuem o aparato tecnológico e o conhecimento técnico adequado. Para fazer o leitor compreender esse paradigma, é interessante demonstrar alguns exemplos de aplicação do *big data* na análise de dados, o que será feito no item a seguir.

3.3.3 Alguns exemplos das potencialidades probabilísticas do big data

¹⁷⁵ No original: “The Library of Congress, for example, has been around for a while, but as its contents are digitized, algorithms can search for patterns and correlations that have been hitherto impossible to detect. If, in the past, there were practical limitations on the ability to track the simultaneous movements of tens or hundreds of thousands of people through a major city, for example (it would be prohibitively expensive to hire enough people to tail everyone and take notes), today the ability to discern useful but non-obvious patterns from the data depends on complex technical systems. Humans simply cannot do that kind of data analysis unassisted.”

O *big data* é, sem dúvida, uma ferramenta extremamente poderosa. Ele permite aplicar, com facilidade, a lei dos grandes números às análises estatísticas. Esta lei, na probabilidade, demonstra que a repetição exaustiva de uma experiência – através de um grande espaço amostral – possibilita a obtenção da real probabilidade de ocorrência de um evento. Como uma análise da lei dos grandes números necessita de uma grande quantidade de eventos para obter uma média confiável, ela encontra no *big data* – cuja característica principal é a manipulação de enormes conjuntos de dados – o par perfeito para tal tipo de análise.

É a partir da análise pretérita de grandes conjuntos de dados que se torna possível chegar a um maior grau de confiança sobre a possibilidade de ocorrência de um evento no futuro. Isso permite o uso do *big data* para prever importantes eventos. Com efeito, esses mecanismos já foram usados – com relativo sucesso – para prever preços de ações no futuro; comportamento do mercado de trabalho; dos consumidores; demanda da indústria automotiva e destinos mais procurados nas férias. Aqui serão oferecidos alguns dos exemplos mais didáticos sobre a – também falta de – capacidade do *big data* de prever o futuro.

Veja-se, por exemplo, o desativado¹⁷⁶ *Google Gripe/Dengue Trends*, serviço que utilizava os dados relativos às buscas dos usuários do *Google* aliados às técnicas de *big data* para monitorar e prever os próximos surtos de dengue e gripe, inclusive no Brasil. O grande avanço é que os pesquisadores não precisaram indicar quais palavras o sistema deveria analisar, uma vez que o próprio sistema conseguia aprender quais as buscas que eram relacionadas às doenças, o que era feito através da comparação com os históricos epidemiológicos oficiais (GINSBERG, MOHEBBI, *et al.*, 2009).

Esse mecanismo, porém, não é perfeito. A pesquisa de Lazer *et al* (2014) demonstra que o algoritmo do *Google* teve dificuldade para criar modelos preditivos de dois grandes surtos de gripe, como foi o caso da gripe aviária (Influenza A/H5N1) dos anos de 2005-2006 e da gripe suína (Influenza A/H1N1) do ano de 2009. O algoritmo do *Google* previu um cenário muito pior que a realidade, deduzindo que iriam existir mais que o dobro dos casos efetivamente registrados pelos órgãos oficiais. Isso, possivelmente, ocorreu em virtude do efeito midiático de propagação do medo

¹⁷⁶ O projeto foi desativado em 20 de agosto de 2015, mas o *Google* continua fornecendo esses dados para pesquisas, inclusive para o CDC, centro de controle de doenças dos EUA.

da doença, o que fez com que o algoritmo fosse desbalanceado em virtude da excessiva quantidade de novas buscas por parte de pessoas que, embora não estivessem doentes, passaram a viver com medo de contrair o vírus.

Em uma outra publicação, que contou com o apoio da agência de redução de ameaças do departamento de defesa dos EUA – DTRA, na sigla em inglês para *Defense Threat Reduction Agency* –, pesquisadores utilizaram os metadados do posicionamento dos telefones celulares para inferir indicadores de desemprego em diversos níveis – micro e macro – (TOOLE, LIN, *et al.*, 2015). Os metadados telefônicos, como visto anteriormente¹⁷⁷, são de grande importância para determinar padrões de comportamento de indivíduos e grupos, especialmente, porque telefones celulares são, geralmente, utilizados por um único indivíduo, que carrega o dispositivo com ele durante todo o dia.

Segundo os pesquisadores, o modelo desenvolvido por eles permite “[...] não apenas melhorar as estimativas do atual estado da economia e oferecer previsões mais rápidas que os métodos tradicionais, mas também prever a situação futura e efetuar correções para se adequar às incertezas atuais” (TOOLE, LIN, *et al.*, 2015)¹⁷⁸. Além disso, eles acreditam que a aplicação desse algoritmo em larga escala é capaz de prever o comportamento de indicadores econômicos com meses de antecedência.

Ao contrário do problema que houve com o *Google Trends*, os algoritmos que se baseiam no uso do telefone celular são menos vulneráveis às oscilações externas e, portanto, menos suscetíveis a erros. Por outro lado, o uso de metadados de celulares pode introduzir outros erros na pesquisa, vez que o acesso a telefones celulares não é universal, o que retira da equação aqueles indivíduos que não possuem o equipamento.

Um último exemplo interessante envolve não apenas um sistema, mas um nome que ficou famoso no mundo inteiro. Nate Silver (2015), um estatístico e analista político e desportivo, desenvolveu métodos de análise massiva de dados de diversas fontes com o intuito de prever as eleições presidenciais dos EUA. A aproximação de Silver com o *big data* permitiu que ele utilizasse todas as fontes de dados disponíveis

¹⁷⁷ Item 2.5.1.

¹⁷⁸ No original: “[...] not only improve estimates of the current state of the economy and provide predictions faster than traditional methods, but also predict future states and correct for current uncertainties.”

para realizar uma derivação do método bayesiano – analisado supra – e prever, com sucesso, o resultado das eleições.

O método de Silver teve tanto sucesso que, em 2008, ele conseguiu prever o resultado das eleições presidenciais em 49 dos 50 Estados e de todas as 35 disputas para vagas do senado. Nas eleições presidenciais de 2012, o algoritmo de Silver foi ainda mais preciso e previu, corretamente, os resultados nos 50 estados e no *District of Columbia*.

Essas análises são extremamente beneficiadas pelo crescimento vertiginoso de informações coletadas através de sensores – ou de dispositivos que, embora tenham outra função aparente, atuam como sensores. No mundo do *big data*, como visto, toda informação pode ser usada para extrair padrões, ainda que elas que sejam aparentemente irrelevantes. Por isso, é possível afirmar que o *big data* só é completamente viabilizado em virtude da multiplicação de dispositivos passivos de coleta de dados. A multiplicação de sensores é um traço tão relevante das nossas sociedades que alguns, como Mark Andrejevic e Mark Burdon (2015), falam na existência de uma “sociedade dos sensores” – *sensor society* –, proposta que será abordada no item a seguir.

3.3.4 Sociedade dos sensores

Até o presente momento, deve ter ficado claro para o leitor que a *surveillance* é um fenômeno caracterizador da sociedade atual. Isso não deve criar uma falsa ideia de homogeneidade, visto que a *surveillance* se manifesta de diferentes modos, em diferentes lugares, com diferentes propósitos, dependendo das circunstâncias (LYON, 2007, p. 44).

Se, no passado, a coleta de dados ocorria em “pontos de controle” – ou seja, em determinados momentos, quando se entrava ou saía de um território, por exemplo –, hoje isso ocorre a todo instante. Praticamente todas as atividades – e as “não atividades”, afinal, um telefone celular coleta informações indicando, inclusive, que não está se movendo – do cotidiano geram fluxos discretos de dados, conforme analisado anteriormente no tópico referente à *dataveillance*.

Esses dados podem ser reunidos e separados com extrema flexibilidade, conforme demonstra a ideia de *surveillance society*, proposta por David Lyon (2007). Nessa esteira, o autor afirma que,

eventualmente, contudo, somos obrigados a ver que a [surveillance] contemporânea é muito influenciada pelo aparente imperativo de “unir-se”. O desejo de criar [assemblages] é forte, mesmo que isso não seja sempre acompanhado pela realidade, que pode ser tecnicamente deficiente ou pode encontrar resistência por parte dos usuários, ou ambos. Fluxos separados existem, mas são – ou podem ser – conectados cada vez mais através das redes eletrônicas de informação e comunicação (LYON, 2007, p. 25-26)¹⁷⁹.

Essa coleta de informações oriunda de diversas fontes é viabilizada pela multiplicação de dispositivos que, passivamente, capturam uma vasta gama de dados. A coleta automatizada de dados – como visto no tópico sobre metadados – permite chegar a conclusão de que

[...] a quantidade de dados que um *smartphone* gera sobre o seu usuário em um dia é provavelmente muito superior à quantidade de dados ativamente comunicada pelo seu usuário na forma de mensagens de texto, e-mails e chamadas telefônicas (inclusive porque cada uma dessas atividades gera mais dados sobre elas mesmas: onde o texto foi enviado, qual a duração da chamada, quais websites foram visitados etc. (ANDREJEVIC e BURDON, 2015, p. 20)¹⁸⁰.

Com isso, fica claro que qualquer dispositivo conectado a uma rede de dados, como é o caso dos smartphones, pode, também, servir como sensor. Além de gerarem informações sobre o seu uso e sobre o usuário¹⁸¹, a maioria desses dispositivos

¹⁷⁹ No original: “Eventually, however, we are obliged to see that contemporary surveillance is very much influenced by the apparent imperative to be joined-up. The desire to create assemblages is strong, even if these are not always matched by the reality, which may be technically deficient or may encounter user resistance, or both. Separate strands do still exist but increasingly, using electronic information and communication networks, they are or can be connected.”

¹⁸⁰ No original: “[...] the amount of data that a smart phone generates about its user in a given day is likely to far surpass the amount of data actively communicated by its user in the form of text messages, e-mails, and phone calls (not least because each of these activities generates further data about itself: where the text was sent, how long the call lasted, which websites were visited, and on and on).”

¹⁸¹ As manifestações contra a presidenta da república ocorridas em 13 de março de 2016 contaram, pelo menos na capital paulista, com o uso da tecnologia *SmartLok*, desenvolvida pela *startup* israelense *StoreSmarts*. A partir da quantidade de identificadores únicos emitidos por telefones celulares com tecnologia Wi-Fi ativada, foi possível determinar a quantidade de participantes da manifestação. Segundo entrevista com o dono da empresa, que cedeu “gratuitamente” a tecnologia, Eyal Ben Eliyahu, o mesmo sistema pode ser utilizado de maneira similar para analisar tanto manifestantes políticos, quanto consumidores: “We believe in taking data driven decisions, whether it’s politics or retail. The exposure we get by supporting such requests is very important for us and our partner, as we see Brazil as a very important market”. A matéria de Angelica Mari para o portal *ZDNet* está disponível em: < <http://surveillance.es/1w> >. Acesso em: 15 mar. 2016.

possui diversos sensores que viabilizam suas funções, como é o caso dos giroscópios e sensores de proximidade, de movimento, de luz, de umidade e de campo magnético. Uma das características desse tipo de coleta de dados é a possibilidade de reutilização dos dispositivos para fins diversos dos originais. Assim, um leitor de livros digitais como o *Kindle* pode, além de permitir o óbvio – a leitura de livros – coletar informações sobre as preferências literárias do usuário, a sua velocidade de leitura, os fragmentos dos livros que mais interessam etc.

Essa apreensão do mundo por sensores tem, como finalidade, aquilo que Andrejevic e Burdon chamam de “onisciência diacrônica” Com essa expressão, os autores querem dizer que, quando se reúnem dados suficientes, se torna possível, além de aplicar algoritmos preditivos do futuro, capturar também o passado. Conforme os autores,

o objetivo da “onisciência diacrônica” é a possibilidade de realizar um arquivo completo capaz de suplementar os inconstantes relatos e memórias através da sua externalização na forma de bancos e dados digitais. [...] Qualquer tentativa de viabilizar a chamada “onisciência diacrônica” necessariamente acarreta na formação de bancos de dados grandes o suficiente para reduplicar o mundo em formato digital, além da criação de ferramentas capazes de dar sentido a todos esses dados (2015, p. 30)¹⁸².

Embora, certamente, faça parte da ideia geral *surveillance society*, a análise da *sensor society* desvia o foco para o desenvolvimento de dispositivos que permitem a coleta e o uso de informações digitais capazes de afetar direitos humanos. Essa perspectiva permite perceber que a *surveillance* não é totalmente imaterial, mas depende de estruturas físicas que viabilizam a coleta e transmissão de dados. Logo, é possível concluir que, por mais líquida que se considere a *surveillance*, trata-se de um fenômeno que depende de meios físicos para existir, de modo que as relações de propriedade e de controle dessas estruturas são primordiais para a proteção dos direitos humanos.

Os sensores, contudo, apenas coletam e transmitem informações, sem realizar sofisticadas análises. Por isso, a verdadeira violação de direitos humanos

¹⁸² No original: “The goal of ‘diachronic omniscience’ invokes the possibility of a complete archive that could supplement the vagaries of reported actions and memories by externalizing them in the form of machine-readable databases. [...] Any attempt to approach so-called ‘diachronic omniscience’ necessarily entails the formation of databases large enough to re-duplicate the world in informational form and the development of analytic tools to make sense of these data.”

ocorre com o uso desses dados em modelos de computador capazes de determinar a probabilidade de ocorrência de um evento através de concatenações nada intuitivas que descubrem padrões cujo surgimento é impensável. Trata-se de algo extremamente comum no mundo contemporâneo e que, por isso, merecerá ser tratado no próximo item.

3.4 SURVEILLANCE E MODIFICAÇÕES NO TEMPO

3.4.1 Modelos preditivos e surveillance

A multiplicação de sensores e as análises do *big data* possibilitam o avanço de um campo específico da computação: inteligência artificial, ou, mais especificamente, do que é conhecido como aprendizado de máquinas – ou *machine learning* em inglês. Trata-se de uma área do saber cujo objetivo é criar sistemas computacionais capazes de acumular conhecimento, tomando decisões com base nas suas experiências anteriores, realizando análises dos resultados futuros das ações tomadas no presente. Em síntese: trata-se de um sistema capaz de ser treinado para tomar decisões diante de novos cenários.

Com a coleta de dados do passado, sistemas de computador tomam, no presente, decisões sobre o futuro. É possível afirmar, portanto, que o *big data* viabiliza o surgimento de instrumentos que cortam o tempo para muito além da instantaneidade da tecnologia vista, anteriormente, no capítulo sobre globalização¹⁸³.

Esse é o caso das ferramentas de análise preditivas – *predictive analytics* – que envolvem a criação de modelos de previsão de resultados com base em técnicas de *machine learning* e *data mining*. Tais técnicas estatísticas analisam padrões em um grande conjunto de dados para realizar previsões dos possíveis cenários futuros, sempre com o objetivo de dar conta da dinâmica do cotidiano.

Dessa maneira, pode-se dizer que as análises preditivas são uma tentativa de diminuir as incertezas da modernidade líquida, apostando na alta capacidade de geração e tratamento de dados que, aliados à matemática, seriam capazes de antecipar o futuro. Embora seja adequado dizer que a vida é muito complexa para caber em um algoritmo de computador, esse tipo de análise vem sendo utilizada, cada vez mais, com uma precisão impressionante.

¹⁸³ Item 1.2.

Estes mecanismos, conforme Oscar Gandy Jr. (2012, p. 125), geram o que pode ser traduzido como “informações utilizáveis” – *actionable intelligence*, no inglês. Essas, por sua vez, são utilizadas

[...] para situar indivíduos em uma matriz de identidades multidimensional e dinâmica. As características destas identidades refletem os interesses dos atores institucionais que buscam influenciar como os indivíduos entendem e respondem às opções que lhe são apresentadas. A apresentação estratégica de opções é feita para maximizar os benefícios e minimizar os riscos associados ao gerenciamento do comportamento destes indivíduos (GANDY JR., 2012, p. 125)¹⁸⁴

A finalidade desse tipo de análise, dentro do contexto da *surveillance*, é elaborar formas avançadas de identificação, classificação e avaliação. A primeira das finalidades, a identificação, refere-se ao processo de determinação da identidade dos indivíduos dentro de uma estrutura de poder, diferenciando-os dos demais.

Já a classificação tem como finalidade dizer “o que você é”, ou seja, agrupar distintos indivíduos em virtude de semelhanças compartilhadas entre eles. A tecnologia sob análise é extremamente hábil no reconhecimento de padrões em conjuntos de dados. Essa classificação não necessariamente corresponde à autoclassificação do sujeito, mas às categorias que forem estabelecidas pelo responsável pelo sistema. Como consequência dessa classificação, ocorre também a avaliação, ou seja, a análise preditiva do resultado esperado na interação do indivíduo com o ambiente, com o seu grupo e com outros indivíduos. Nas palavras de David Lyon,

atualmente, dados em massa são obtidos de diferentes fontes e reunidos antes mesmo de determinar os seus usos reais e potenciais e mobilizar algoritmos e análises não só para entender uma sequência de eventos do passado, mas também para prever e intervir antes que comportamentos, eventos e processos ocorram (LYON, 2014, p. 4)¹⁸⁵

¹⁸⁴ No original: “[...] to place individuals within a dynamic multidimensional matrix of identities. The character of these identities reflects the interests of the institutional actors seeking to influence how individuals understand and respond to the options that are set before them. The strategic presentation of options is designed to maximize the benefits and minimize the risks that are associated with managing the behavior of these individuals.”

¹⁸⁵ No original: “Now bulk data are obtained and data are aggregated from different sources before determining the full range of their actual and potential uses and mobilizing algorithms and analytics not only to understand a past sequence of events but also to predict and intervene before behaviors, events, and processes are set in train.”

O fenômeno da *dataveillance*, explorado anteriormente¹⁸⁶, é que conecta o *big data* à *surveillance*, o que ocorre através de quatro categorias principais de ação: observação monitorada, identificação e rastreamento, intervenção analítica e modulação de comportamentos (ESPOSTI, 2012).

A primeira categoria diz respeito à multiplicação de dispositivos capazes de coletar informações e armazená-las em formato digital. O tipo mais comum desses dispositivos são as tradicionais câmeras de CFTV. No entanto, em virtude da tendência de computação ubíqua – “Internet das coisas” –, a coleta de informações através de sensores diversos permite o aumento exponencial de informações coletadas sobre pessoas e sobre ambientes.

Existe, como visto no item anterior, uma tendência na tecnologia atual de embutir sensores em tudo que existe, habilitando que esses dispositivos se comuniquem entre eles. Desde relógios e pulseiras capazes de monitorar a atividade física e o sono do usuário – por todos, ver o *Pebble Watch* e o *Fitbit* – até roupas inteligentes capazes de medir frequência cardíaca e respiratória, bem como intensidade da atividade física, níveis de estresse e calorias gastas – como é o caso da *PoloTech Shirt*, da *Ralph Lauren*.

Além de coletar informações do corpo do usuário, como nos exemplos citados, os sensores podem ser utilizados para analisar tudo aquilo que entra em contato com ele, como é o caso do *SCiO*, da *startup* israelense *ConsumerPhysics*. Equipado com um espectrômetro infravermelho menor que uma moeda, esse dispositivo consegue identificar a composição química de um objeto através da captura da “assinatura molecular” única de cada substância. Toda a análise de espectro é realizada “na nuvem”, por servidores da empresa, que passam a armazenar a “assinatura molecular” de todas as substâncias com que o usuário entra em contato.

Um outro exemplo são os receptores de TV por assinatura da operadora Verizon (EUA) que, em 2012, patenteou¹⁸⁷ um dispositivo capaz de coletar imagens e sons do ambiente e dos telespectadores com a finalidade de oferecer publicidade direcionada para o que estiver acontecendo naquele momento no ambiente monitorado.

¹⁸⁶ Item 2.4.2.

¹⁸⁷ A patente descreve um equipamento que permitirá analisar a reação dos usuários à publicidade, “aprendendo” qual o tipo de anúncio desperta o interesse dos telespectadores. O requerimento de patente nº 20120304206 está disponível em < <http://surveillance.es/1q> >. Acesso em: 29 fev. 2016.

Um traço em comum a todos esses dispositivos é que eles possuem conectividade à Internet. Assim, cada um deles cria um fluxo de dados discreto, que é acumulado, processado pelos detentores da tecnologia e outras empresas que conseguem transformar aquelas informações em dinheiro ou poder.

A segunda categoria que conecta o *big data* à *surveillance* é a identificação e o rastreamento, que ocorrem com análise dos traços distintivos de um objeto ou pessoa e à possibilidade de seguir a sua movimentação. A identificação torna-se mais fácil em virtude da proliferação do uso da biometria – para pessoas – ou formas de identificação sem fio para objetos – como é o caso das etiquetas RFID ou sistemas NFC. Segundo Esposti (2012), essas categorias são importantes no contexto do *big data*, pois ajudam a resolver os problemas associados aos grandes conjuntos de dados – através da sua organização – e aumentam a velocidade de resposta dos sistemas, uma vez que viabilizam a coleta em tempo real de informações.

Exemplos desses sistemas são os já mencionados controles de fronteiras automatizados – *E-gates* – e passaportes com dispositivos RFID. Em virtude do baixo custo desse tipo de tecnologia, ela vem sendo utilizada pela iniciativa privada em identidades funcionais, como ocorre com cartões de acessos de universidades e empresas. Além de garantirem o acesso ao portador do cartão – identificando-o –, é possível distribuir antenas dentro do ambiente com a finalidade de detectar a exata localização do cartão – tecnologia conhecida como IPS, da sigla em inglês para *indoor positioning system*.

O mesmo tipo de rastreamento pode ocorrer com o uso de telefones celulares para obter sua localização tanto em ambientes abertos quanto fechados – através do uso de tecnologia de triangulação das torres de celular, GPS ou *Bluetooth*, por exemplo. Considerando que esses dispositivos são, geralmente, utilizados por uma única pessoa, é possível correlacionar o dispositivo com um indivíduo determinado.

A intervenção analítica, terceira categoria da proposta de Esposti, refere-se à utilização da *analytics* – ou seja, a análise de dados e estatísticas por sistemas digitais com a finalidade de encontrar padrões relevantes – para transformar as informações coletadas em conhecimento útil, isto é, na já mencionada “*actionable intelligence*” (GANDY JR., 2012, p. 125), o que ocorre através da criação de futuros simulados. Ou seja, é ela que gera a conexão entre o *big data* e a criação de modelos preditivos. Nas palavras de Esposti, o termo *analytics*

indica a análise dos chamados “dados não tratados” na busca de padrões e a consequente transformação destes dados no tipo de conhecimento que os responsáveis pela tomada de decisões necessitam para orientar, de forma otimizada, seu curso de ação (ESPOSTI, 2012, p. 211-212)¹⁸⁸.

A intervenção analítica é, na realidade, o principal ponto da compreensão do *big data*. As *analytics* agregam o real valor do *big data*, visto que, sem eles, seria como possuir uma enorme biblioteca sem fazer uso dela. Atualmente, são ferramentas bastante utilizadas por entidades públicas e privadas, mas o enfoque principal está no segmento publicitário. Isso porque essas ferramentas permitem, por exemplo, encontrar o preço máximo de um produto que o consumidor está disposto a pagar, maximizando os lucros, ou criar políticas de preços flexíveis para grupos populacionais distintos¹⁸⁹.

É problemático, contudo, acreditar que os resultados desse processamento de dados sejam “verdades matemáticas” – embora sejam derivados do uso da matemática. Os algoritmos de computador não são neutros – possuem erros, vieses e interesses políticos e econômicos –, de modo que o conhecimento derivado desses mecanismos deve ser sempre questionado. Quando eles são incorporados sem a necessária análise, tendem a tomar a forma de manipulação de comportamento, quarta categoria da proposta de Esposi.

A manipulação de comportamento ocorre quando as análises preditivas são transformadas em ações por aqueles que detêm poder para tanto, sempre com a finalidade de modificar um comportamento, geralmente sem consciência daquele que está no polo passivo da relação de poder.

Um dos exemplos mais notórios e polêmicos envolveu um estudo de 2014 realizado por pesquisadores do *Facebook* e da *Cornell University*. Os cientistas conseguiram verificar que o estado emocional das pessoas pode ser manipulado em virtude da exposição delas às emoções de outras pessoas sem que ocorra direta interação entre elas. Para demonstrar isso, manipularam o algoritmo de classificação

¹⁸⁸ No original: “[...] indicates the analysis of so-called ‘raw’ data in search of patterns, and the consequent transformation of these results into the kind of knowledge decision makers need to optimally orientate their course of action [...]”

¹⁸⁹ Em uma pesquisa realizada pelo *Wall Street Journal*, ficou evidente que os preços dos produtos vendidos na *Amazon* variavam conforme o site que levou o usuário até a sua página. Assim, consumidores que chegavam até a *Amazon* através de sites especializados em descontos pagavam um preço até 23% menor que os demais usuários. A matéria de Adam Tanner para a revista *Forbes* está disponível em < <http://surveillance.es/1h> >. Acesso em: 01 mar. 2016.

da “linha do tempo” – ou seja, aquilo que é demonstrado para o usuário quando ele entra no *site* – de 689.003 usuários do *Facebook*. De acordo com o estudo,

quando expressões positivas foram reduzidas, as pessoas produziram menos postagens positivas e mais postagens negativas; quando expressões negativas foram reduzidas, ocorreu o padrão oposto. Estes resultados indicam que emoções expressadas por outros no *Facebook* influenciam nossas próprias emoções, constituindo uma evidência experimental para o contágio em massa através de redes sociais. Este trabalho também sugere que, ao contrário das suposições mais aceitas, o contato pessoal e os sinais não-verbais não são estritamente necessários para o contágio emocional e que a observação das experiências positivas de terceiros constituem uma experiência positiva para as pessoas (KRAMERA, GUILLORY e HANCOCK, 2014, p. 8788)¹⁹⁰.

Trata-se de um estudo bastante perturbador, afinal, o *Facebook*, deliberadamente, manipulou as emoções de centenas de milhares de pessoas com o propósito de aumentar os seus lucros através do desenvolvimento de algoritmos mais sofisticados de publicidade direcionada. Considerando que tais algoritmos são opacos ao público, que sofre as consequências deles sem ter nenhuma chance de conhecê-los, a manipulação de comportamento por uma empresa privada é, nitidamente, uma violação de direitos humanos.

Por motivos como esses, Lyon acredita que é necessária cautela quando se aborda, com muito otimismo, o *big data*, visto que a sua aplicação deve ser analisada, cuidadosamente, sob a perspectiva de proteção dos direitos humanos. Se, por um lado, essas ferramentas podem ser utilizadas para a prestação de um serviço de melhor qualidade, ou mais personalizado, por outro, podem servir para reduzir a capacidade de ação dos indivíduos, visto que solidificam o futuro antes mesmo que ele aconteça – um pouco como no filme *Minority Report*.

Logo, é necessário distinguir entre três tipos principais de algoritmos preditivos. O primeiro tem, como finalidade, desenvolver estratégias para ajudar as pessoas a fazerem escolhas que lhes serão benéficas. O segundo está relacionado à possibilidade de deduzir desejos e traços de personalidade a partir de informações

¹⁹⁰ No original: “When positive expressions were reduced, people produced fewer positive posts and more negative posts; when negative expressions were reduced, the opposite pattern occurred. These results indicate that emotions expressed by others on Facebook influence our own emotions, constituting experimental evidence for massive-scale contagion via social networks. This work also suggests that, in contrast to prevailing assumptions, in-person interaction and nonverbal cues are not strictly necessary for emotional contagion, and that the observation of others’ positive experiences constitutes a positive experience for people.”

coletadas, como foi o caso da pesquisa de Kosinski et al (2013), já demonstrada anteriormente. Por fim, o terceiro e mais danoso tipo de algoritmo preditivo é aquele que, como na pesquisa de manipulação de sentimentos dos usuários do *Facebook*, transforma o futuro em presente, restringindo as opções de reação dos indivíduos através da sua classificação em categorias distintas.

Esses sistemas preditivos não fazem uma simples coleta ou representação de dados, mas constroem múltiplos tempos – passado, presente e futuro. Eles não simbolizam, necessariamente, uma tendência de desviar a *surveillance* do presente para o futuro, mas uma estratificação do passado e do futuro no presente, criando um presente alternativo que é apresentado como o único possível.

Quando ações preventivas são tomadas com base nesses modelos preditivos, transforma-se em verdade um futuro que era apenas uma probabilidade estatística¹⁹¹. No entanto, se os direitos humanos são violados para prevenir um possível atentado terrorista, por exemplo, pouco importa se o atentado foi concretizado ou não: o terrorismo já aconteceu, só que patrocinado pelos algoritmos preditivos.

Esse é o caso das listas que o governo estadunidense elabora de pessoas que não podem viajar de avião em virtude de serem potenciais terroristas – as chamadas *no fly lists* – que são elaboradas através de modelos preditivos, cujos critérios são secretos. Um caso específico, por sua peculiaridade, foi muito divulgado pela mídia internacional, pois envolveu um Senador dos EUA sendo classificado como terrorista¹⁹².

O caso do senador Kennedy demonstra que a precisão não é a maior das prioridades no mundo do *big data*. “Ao invés disto, o seu objetivo é intervir no mundo do modo mais efetivo possível, o que pode implicar em padrões mais baixos de abrangência e precisão” (ANDREJEVIC e GATES, 2014, p. 191)¹⁹³. O problema é que, mesmo sem precisão, tais sistemas são utilizados, cotidianamente, de maneira que afetam a vida das pessoas. Veja-se, por exemplo, os mecanismos de *score* de

¹⁹¹ Esse tema será aprofundado quando forem tratadas as violações de direitos humanos pela *surveillance*, item 4.2.2.

¹⁹² Em 2004, o senador estadunidense Edward Kennedy foi impedido de viajar em virtude de “T. Kennedy” ser – de acordo com o algoritmo – um nome falso comumente escolhido por terroristas. Ele, com todas as vantagens políticas do cargo que ocupava, levou cerca de três semanas para inserir na lista a informação de que não era terrorista. Ver a matéria de Gregory Krieg para o jornal *CNN*. Disponível em: < <http://surveillance.es/1j> >. Acesso em: 01 mar. 2016.

¹⁹³ No original: “Rather its goal is to intervene in the world as effectively as possible, which may well entail lower standards of comprehensiveness and accuracy.”

crédito, que estão se tornando cada vez mais comuns no Brasil. A partir de uma análise que reúne diversos bancos de dados e variáveis estatísticas – como idade, profissão, local de residência –, esses sistemas atribuem uma “nota” que é utilizada por instituições financeiras e empresas para o cálculo do risco de concessão de crédito. Como resultado, o acesso a um serviço tão importante nos dias de hoje – crédito – depende das análises de algoritmos de computador que permanecem opacos àqueles que têm suas vidas afetadas pelo sistema.

As análises preditivas do *big data* possibilitam que a criação de categorias como risco sejam o resultado de um conjunto complexo de algoritmos que não podem ser explicados de modo tradicional. Isso ocorre porque a complexidade das suas análises não funciona da mesma forma que as deduções do pensamento humano.

As formas de conhecimento que resultam das análises desses algoritmos preditivos são extremamente opacas – embora deixem o indivíduo transparente à análise pelos detentores do poder. Como resultado, “o banco de dados pode gerar padrões que possuem poder preditivo, mas não explicativo” (ANDREJEVIC e GATES, 2014, p. 186)¹⁹⁴. Pode-se afirmar, assim, que o *big data* e as análises preditivas permitem elaborar cenários de aplicação de conjecturas, ou seja, perguntar “e se?” (ELMER e OPEL, 2006), sem, necessariamente, explicar “como?”.

3.4.2 Simulação e pós-panoptismo

As sociedades disciplinares dos séculos XVIII e XIX foram situadas por Foucault no panóptico, a partir da ideia de confinamento (DELEUZE, 1992). Nesse tipo de sociedade, os seres humanos estão sempre transitando entre espaços fechados.

Porém, na esteira do que já foi defendido anteriormente a respeito da superação do paradigma do panóptico, Deleuze afirma que Foucault sabia da brevidade de prevalência do modelo disciplinar de sociedade, o que ocorreu após a Segunda Guerra Mundial. Além disso, cabe ressaltar que o trabalho de Foucault era menos uma análise das sociedades que lhe eram contemporâneas e mais uma obra historiográfica das sociedades do século XVIII e XIX.

¹⁹⁴ No original: “The database can generate patterns that have predictive power but not necessarily explanatory power.”

Segundo Deleuze, “encontramo-nos numa crise generalizada de todos os meios de confinamento, prisão hospital, fábrica, escola, família” (DELEUZE, 1992, p. 220). Essa crise do confinamento, fortalecida, sobretudo, pela necessidade de mobilidade inerente à globalização, ocorre porque as estruturas das sociedades disciplinares são inflexíveis, incapazes de se adaptar às demandas de um mundo cada vez mais líquido. A distinção entre interior e exterior, necessária para o pleno funcionamento do modelo panóptico, é incapaz de absorver a natureza descentralizada das redes de poder típicas da sociedade em rede, o que demanda uma nova forma de pensar a *surveillance*.

Assim, Deleuze explica que os confinamentos são moldes independentes, ou seja, o indivíduo começa do zero a cada passagem de um molde para o outro. Nas sociedades disciplinares, havia sempre recomeços a cada transição dos moldes. Os controles, por sua vez, são modulações autodeformantes, que mudam continuamente (DELEUZE, 1992, p. 221). Essa modulação, do ponto de vista da física, “[...] é o controle variável das características de uma onda. Ela não é aplicada aos indivíduos, mas às oscilações, especificamente, às tendências ou movimentos tendenciais que possuem uma propriedade estatística definida” (BOGARD, 2012, p. 32)¹⁹⁵.

Esse tipo de controle não depende da existência de um interior, ainda que funcione como uma espécie de invólucro. Isso somente se torna factível em virtude do surgimento das novas tecnologias de informação, que garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos.

Tal fato que se acabou de afirmar sobre os efeitos no espaço da passagem das sociedades disciplinares para as sociedades do controle também é válido para o tempo. Nas sociedades disciplinares – nos mesmos moldes do que foi escrito anteriormente sobre o tempo e a modernidade sólida –, o confinamento é acompanhado por formas rígidas de controle do tempo de maneira linear. Além disso,

um molde não pode alterar a sua forma, e o objeto que ele produz é fixo. O controle modular adapta-se à desterritorialização das forças produtivas que marca a mudança da organização industrial para a sociedade em rede contemporânea. Ao invés de gerar um objeto fixo, o indivíduo, um invólucro que modula pode variar sua estrutura e o

¹⁹⁵ No original: “[...] is a variable control over the characteristics of a wave. It is not applied to individuals, but to oscillations, specifically, to ‘trends’ or ‘tendential’ movements that have defined statistical properties [...]”.

produto que ela produz em resposta às mudanças contingenciais da produção, por exemplo, aquelas geradas pela velocidade e complexidade das comunicações modernas ou o rápido fluxo dos mercados globais (BOGARD, 2012, p. 33)¹⁹⁶.

Em virtude dessa mudança, da disciplina para o controle, William Bogard (2012) defende que as sociedades do controle necessitam do paradigma da simulação de Baudrillard para a sua correta compreensão. Dessa maneira, o autor explica que as modernas formas de simulação tiveram origem nos métodos estatísticos de amostragem militares, que permitiram a coleta de dados mínimos populacionais com o propósito de prever o seu comportamento futuro.

O trabalho de Bogard deriva das análises de Baudrillard sobre a simulação e o controle pós-panóptico. Com efeito, o autor entende que o objetivo máximo da simulação não é refletir a realidade, mas tornar-se a realidade. Em suas palavras,

a verdade do signo, a partir de então, é autorreferenciada, não necessitando mais, para a sua verificação, da medida em relação a uma realidade independente. Sistemas de signos constituem a sua própria realidade, ou, como Baudrillard diz, tornam-se ‘hiperreaís’ (BOGARD, 2012, p. 34)¹⁹⁷

Com base nesse conceito, Bogard estabelece a ideia de *surveillance* simulada ou de *surveillance* como moduladora. Através do *big data* e dos mecanismos preditivos de análise, a *surveillance* atinge o seu potencial máximo de prever o futuro através de sofisticadas simulações capazes de prever o maior número possível de contingências. Isso porque, nas sociedades do controle da modernidade líquida, o objetivo dos mecanismos preditivos não é representar a realidade de modo fiel, “[...] mas auxiliar na construção e aplicação de modelos. O que é monitorado, antes de tudo, é a informação sobre a performance do modelo, não os eventos que ele representa” (BOGARD, 2012, p. 35)¹⁹⁸.

¹⁹⁶ No original: “A mold cannot alter its form, and the object it produces is fixed. Modulation control adapts to the deterritorialization of productive forces that marks the shift from industrial to network organization in con-temporary society. Rather than generate a fixed object, the individual, an enclosure that modulates can vary its structure and the product it produces in response to changing contingencies of production, for example, those generated by the speed and complexity of modern communications, or the rapid flux of global markets.”

¹⁹⁷ No original: “The truth of the sign henceforth is self-referential and no longer needs the measure of an independent reality for its verification. Sign systems constitute their own reality, or as Baudrillard says, they become ‘hyperreal’.”

¹⁹⁸ No original: “[...] but to assist in the construction and application of models. What is monitored first of all is information on the performance of the model, and not the event it models.”

A ideia de que os sistemas de análise preditiva – realidades simuladas – derivam de altíssima tecnologia acaba por obscurecer o que eles, de fato, são: modelos especulativos de futuro. Tomar decisões com base nesses sistemas, sob o falso argumento de que suas conclusões são verdades científicas, possui consequências diretas para os direitos humanos. Por isso, os juristas e responsáveis pela elaboração de políticas precisam compreender essas ferramentas pelo que elas realmente são: simulações.

3.4.3 Surveillance e o novo biopoder

Se a proposta panóptica de Michel Foucault é, como visto, amplamente difundida – embora cada vez mais questionada – como paradigma da *surveillance* no mundo contemporâneo, o mesmo não se pode dizer sobre a ideia de biopoder, tema muito menos abordado pela *surveillance studies*. Para o francês, o biopoder é aquele com a função de gerir a vida, especialmente, através do exercício de controles reguladores do corpo como processo biológico.

Substitui-se, assim, a “potência de morte” do poder soberano do medievo pela gestão calculista da vida por meio de técnicas de controle populacional, que se desenvolvem a partir do século XVII. O conhecimento técnico desenvolvido nesse período permitiu as “[...] regulações de população, a demografia, a estimativa da relação entre recursos e habitantes, a tabulação de riquezas e de sua circulação, das vidas com sua duração provável” (FOUCAULT, 1998, p. 132).

Ainda da análise de Foucault, depreende-se que o biopoder está associado à ideia do Estado, mais especificamente de um Estado que viabiliza o desenvolvimento do capitalismo através do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos. Esse poder, no entanto, demanda um exercício diferente, uma vez que deve ser cada vez mais dócil, ou seja, necessita garantir a sua manutenção do modo mais assimilável possível, sem causar perturbações ou dificuldades na vida cotidiana dos governados.

Ao dissertar sobre o biopoder, Foucault relaciona os dispositivos de segurança ao tratamento do aleatório (FOUCAULT, 2008, p. 39), que ele considera um dos principais objetivos dos governos liberais. Assim, a finalidade dos dispositivos de segurança é prever a ocorrência de determinados eventos, como é o caso da escassez de alimentos no exemplo utilizado pelo autor.

Por essa razão, é interessante a análise realizada por Ayse Ceyhan (2012). Para a professora do *Institut d'études politiques de Paris*, a *surveillance* não é apenas uma forma de buscar maior eficiência no controle e gerenciamento de populações através da observação e classificação dos indivíduos, mas, conforme demonstrado no item anterior sobre o *big data* e as *predictive analytics*, é uma forma de capturar e controlar as incertezas inerentes à condição humana.

Essa incerteza não é exclusividade dos tempos contemporâneos, visto que a eliminação do incerto foi sempre uma busca humana. Conforme assevera Ceyhan,

se, nos tempos de Hobbes, [a incerteza] foi gerada pelas características humanas brutas, como a ganância e o egoísmo, ela é atualmente produzida tanto pelas transformações da modernidade tardia, cujas principais características, conforme Zygmunt Bauman, estão sendo “leve, líquida, móvel, escorregadia” quanto pelas mudanças que ocorrem nos regimes de segurança em virtude das novas formas de violência e a sua disseminação através de redes transnacionais, privadas e virtuais. Essas dinâmicas impactam as alegações de verdade, conhecimento e poder, que já não podem mais contar com os tradicionais marcadores de certeza, como é o caso do território, da hierarquia e da racionalidade que a modernidade tinha definido após o século XVII (CEYHAN, 2012, p. 38)¹⁹⁹.

Desde modelos climáticos gerados por computadores de última geração até análises como aquelas do *Google Trends* para gripe e dengue, é possível perceber que, na atualidade, os dispositivos de segurança correspondem às tecnologias capazes de prever os riscos associados ao meio ambiente, à ciência, à tecnologia e à saúde das populações. Assim, “o conceito de aleatório aparece, então, como a variável explanatória que justifica o foco nas tecnologias de gerenciamento de risco que permite a previsão destas mudanças antes delas ocorrerem” (CEYHAN, 2012, p. 41)²⁰⁰.

Diante desse cenário, é possível falar da aplicação da ideia de biopolítica à *surveillance*, já que as informações geradas pelo corpo – por exemplo, identificação

¹⁹⁹ No original: “If in Hobbes’s times it was generated by crude human characteristics like greediness and selfishness, it is now produced both by the transformations of late modernity whose main features, says Zygmunt Bauman, are being “light, liquid, mobile, slippery” and the changes occurring in security regimes by the new forms of violence and their dissemination through transnational, private and virtual networks. These dynamics impact the claims to truth, knowledge and power which no longer rely on the traditional markers of certainty like territory, hierarchy and rationality that modernity had set after the seventeenth century.”

²⁰⁰ No original: “The concept of the aleatory appears then as the explanatory variable that justifies the focus on the technologies of risk management that enable the prediction of these changes before they occur.”

biométrica – ou pelo seu movimento – como é o caso da geolocalização de pessoas – são utilizadas na tentativa de domesticar as incertezas especialmente aquelas relacionadas à segurança do mundo em constante medo, conforme ressaltado anteriormente.

Isso se deve ao fato, conforme Foucault (1998), o biopoder não precisar ser exercido exclusivamente através do Estado, mas pode partir de qualquer organização que seja capaz de realizar a coleta e o processamento de informações. Com isso, em uma sociedade cuja expansão das tecnologias de informação ocorre de maneira vertiginosa, é possível verificar o surgimento de uma nova modalidade de biopoder, capaz de “[...] desterritorializar e conectar pontos que não foram feitos para serem conectados. Além disso, o poder é agora exercido em locais não tradicionais, como centros de dados, programas de computador e empresas aéreas e telefônicas” (CEYHAN, 2012, p. 38)²⁰¹. Como resultado, surge um novo tipo de biopoder, que gerencia a vida dos indivíduos de forma eletrônica, através de algoritmos desenvolvidos dentro das grandes empresas e sem que haja grande capacidade de intervenção das tradicionais estruturas estatais de regulamentação e controle.

Assim como na perspectiva original de Foucault, a diminuição das incertezas – ou seja, o tratamento do aleatório – depende de procedimentos estatísticos e de cálculos, cujo conhecimento é necessário para o desenvolvimento da força do Estado, até porque, lembra o autor, a própria etimologia da palavra “estatística” remonta à ideia de “conhecimento do Estado” (FOUCAULT, 2008, p. 365).

A partir do tratamento da aleatoriedade como forma de exercício de poder, é possível concluir que os mecanismos preditivos associados à *surveillance* podem ser considerados instrumentos para controle da probabilidade e do risco, o que se torna verdade especialmente na sociedade contemporânea, onde as análises preditivas são amplamente utilizadas na tentativa de capturar o futuro antes da sua ocorrência. Essas ferramentas estão fundamentadas na aplicação de técnicas de cálculos probabilísticos e estatísticos, uma das principais características do biopoder de Foucault.

Contudo, a globalização e a fluidez da *surveillance* na modernidade líquida modificam a ideia presente em Foucault, motivo pelo qual Ceyhan prefere se referir a

²⁰¹ No original: “[...] deterritorializes and connects dots which are not in the first place designed to be connected. Moreover, power is now exercised in non-traditional locations like data warehouses, software, airline and phone companies.”

uma nova e híbrida forma de biopoder (2012, p. 43), porque, embora o biopoder de Foucault esteja fundamentado na regulação de fluxos, as características do mundo contemporâneo modificam o espaço onde esses fluxos ocorrem. Logo,

Não apenas o espaço da mobilidade foi estendido para fora das fronteiras estatais e alcançou o mundo todo, mas ele também se tornou virtualizado e aberto, com a exibição de uma variedade de tecnologias da informação e da comunicação, assim como o desenvolvimento de enormes bancos de dados onde os fluxos de informação são processados e os dados são extraídos.[...] Isso nos permite definir uma nova forma de governamentalidade e poder regulador que está localizado em lugares não tradicionais como a Internet (o Google, por exemplo), shoppings centers, serviços de marketing, companhias telefônicas, empresas e corporações de alta tecnologia. (CEYHAN, 2012, p. 44)²⁰²

O exemplo do *Google* é recorrente neste e em outros trabalhos sobre o tema, pois a empresa de *Mountain View* é uma das principais a coletar e analisar grandes volumes de dados sobre pessoas e grupos diversos, sempre com a finalidade de extrair sentido de dados aparentemente desconexos. O já mencionado serviço do *23andme*²⁰³, por exemplo, permite que o *Google* vá além e possa incorporar, nas suas análises preditivas, os dados genéticos das pessoas. Tal fato permite que a empresa possa criar diversos modelos de futuro, inclusive, prevendo o aparecimento de características físicas²⁰⁴ ou doenças.

Assim, essa nova forma de biopoder viabilizada pela *surveillance* e pelo *big data* faz parte do que Ceyhan chama de sistema híbrido, ou seja, sistemas “[...] heterogêneos projetados para [a realização] de múltiplas tarefas sem seguir uma direção determinada a priori” (2012, p. 44)²⁰⁵. Tais sistemas são fluidos o suficiente para permitirem a sua adaptação às necessidades dos seus desenvolvedores em

²⁰² No original: “Not only has the space of mobility been extended outside the state borders and embraced the whole globe, but it has also become virtualized and open-ended with the display of a variety of technologies of information and communication as well as the development of huge databases where flows of information are processed and data mined. [...] This makes us define a new form of governmentality and regulative power that is located in non-traditional places like the Internet (Google, for instance), shopping malls, marketing services, phone companies, businesses and high-tech corporations.”

²⁰³ Item 3.2.1.

²⁰⁴ Veja-se, por exemplo, que os dados coletados pelo *23andme* foram utilizados para determinar quais genes contribuem para a calvície masculina. Para mais informações, consultar o estudo completo: Li Riu et al. Six Novel Susceptibility Loci for Early-Onset Androgenetic Alopecia and Their Unexpected Association with Common Diseases. **PLoS Genetics**, San Francisco, v. 2, n. 5, doi: 10.1371/journal.pgen.1002746. Disponível em: < <http://surveillance.es/1k> >. Acesso em: 09 mar. 2016.

²⁰⁵ No original: “[...] heterogeneous systems designed for multiple tasks implemented without following an overarching direction from the beginning.”

tempo real, possibilitando a elaboração de modelos preditivos diversos a partir do mesmo conjunto de dados. Esse fenômeno reforça a ideia de que a *surveillance* não é um fenômeno único, mas uma *assemblage*, conforme demonstrado anteriormente.

Como resultado, é possível concluir que o modelo de biopoder de Foucault, embora útil, necessita de modificações a fim de poder contribuir para a compreensão da *surveillance* na era do *big data*. O biopoder agora é híbrido, vez que congrega uma diversidade enorme de tecnologias distintas, sempre com a finalidade de identificar e rastrear indivíduos e grupos, bem como criar modelos preditivos de comportamento e risco. Outra evidência dessa natureza híbrida do biopoder é a modificação do espaço onde ocorrem os fluxos de poder e dados, agora globalizado e virtualizado, fora dos tradicionais limites do Estado nacional. Esta modificação do espaço é o tema do item a seguir.

3.5 SURVEILLANCE E MODIFICAÇÃO DO ESPAÇO

3.5.1 A desterritorialização das fronteiras

Até o momento, o leitor deve ter percebido que existe uma relação entre a *surveillance* e o espaço, o que ocorre por dois motivos principais: o primeiro, em virtude da relação entre as novas tecnologias da informação e a desconstrução dos espaços na modernidade líquida, conforme demonstrado no primeiro capítulo deste trabalho. O segundo é consequência da análise do panóptico, feita anteriormente²⁰⁶, especialmente no que diz respeito à passagem do modelo panóptico para o pós-panóptico, o que está diretamente vinculado à ideia de desterritorialização.

Essa desterritorialização não gera mais liberdade, mas o contrário, como visto na ideia de mudança da sociedade disciplinar para a sociedade do controle. Isso tende a fortalecer novos tipos de estruturas de poder capazes de gerar efeitos negativos para os direitos humanos sem o necessário contraponto do aparato jurídico estatal, cuja possibilidade de controle se vê reduzida diante da diminuição de importância de elementos típicos de constituição do Estado, como é o caso do território. Nesse mesmo sentido, William Bogard afirma que

[...] nenhum poder de polícia é capaz de controlar a desterritorialização da [surveillance], porque o número de conexões virtuais em uma rede rizomática sempre supera o número de pontos que podem ser

²⁰⁶ Item 2.2.1.

verdadeiramente monitorados (se um caminho está bloqueado, outro pode ser encontrado). Se a [surveillance] está relacionada ao controle e à polícia, ela também pode possuir tendências 'anti-polícia' e 'anti-controle', ambas inerentes à sua desterritorialização (BOGARD, 2006, p. 101)²⁰⁷.

Nessa direção, a ideia de *surveillance assemblage* trabalhada anteriormente ²⁰⁸ é extremamente útil, por ser capaz de demonstrar que a reconfiguração horizontal e rizomática da *surveillance* viabiliza o exercício do controle independentemente da vinculação a um território específico e das fronteiras.

No entanto, as fronteiras são, tradicionalmente, os limites de um determinado território e de um Estado. Por um lado, a globalização necessita de que tais fronteiras sejam permeáveis o suficiente para permitir que pessoas, bens e capitais circulem livremente. Por outro, as fronteiras também são locais de controle, ou seja, devem ser capazes de impedir a entrada de indivíduos indesejados. Nas palavras de David Lyon, “[...] em um mundo acelerado e móvel, a ideia de que fronteiras são barreiras ao movimento é uma irritação inaceitável. Contudo, em um mundo dominado pelo medo e inseguro, tais fronteiras fazem muito sentido” (2007, p. 132)²⁰⁹.

Essa necessidade de permeabilidade das fronteiras é extremamente difícil, especialmente, em um mundo onde vigora a ameaça difusa e indeterminada do terrorismo. Como possibilitar a livre circulação de pessoas e, ao mesmo tempo, evitar a entrada de potenciais ameaças? Trata-se de uma situação-modelo para a compreensão da *surveillance*, especialmente, quando entendida como uma forma de discriminar indivíduos em grupos de interesse e risco²¹⁰.

As fronteiras, sob a perspectiva da coleta e análise massiva de dados, deixaram de ser um espaço físico localizado nos limites geográficos dos Estados. Sob esse aspecto, Peter Adey explica que

pessoas e coisas cruzam, fluem e intrometem-se contra fronteiras que não são mais encontradas nas bordas dos Estados. As fronteiras podem até mesmo se localizar dentro, e agora fora, dos containers territoriais como corpos muito alongados, informatizados e puxados e empurrados para dentro e através das fronteiras nacionais. A

²⁰⁷ No original: “[...] no police power is capable of controlling the deterritorialization of surveillance, because the number of virtual connections in a rhizomatic network always exceeds the number that can actually be monitored (if one path is blocked, another can be found). If surveillance is about control and the police, it also has these ‘anti-police’, ‘anti-control’ tendencies too, immanent to its deterritorialization.”

²⁰⁸ Item 2.4.1.

²⁰⁹ No original: “[...] in a speeding and mobile world, the idea of borders as barriers to movement is an unacceptable irritation, but in a fearful and unsafe world such borders make a lot of sense.”

²¹⁰ Mais detalhes sobre esse tema serão trabalhados no item 4.2.2.

[surveillance] parece desrespeitar os tradicionais limites jurisdicionais do Estado-nação através de sistemas transfronteiriços e interoperáveis nacionais e internacionais, paradoxalmente, com o objetivo de fortalecer as suas fronteiras (ADEY, 2012, p. 193)²¹¹.

Desde os atentados terroristas de 11 de setembro, o aeroporto passou a ser um dos locais onde a mais alta tecnologia é utilizada para controlar o fluxo de pessoas e objetos. Veja-se, por exemplo, o uso de *scanners* que verificam os corpos dos viajantes para “enxergar” através das roupas na busca por armas, explosivos e itens ilegais (tais tecnologias são conhecidas como *backscattered x-ray* e *millimeter wave scanner*). Embora não seja o propósito deste trabalho, tal nível de tecnologia permite visualizar a quantidade de investimentos que são realizados no segmento de segurança e controle de fronteira.

Porém, tais tecnologias são visíveis somente nos “*checkpoints*” dos aeroportos. Ao contrário delas, o que importa para este trabalho são as formas invisíveis de assegurar o controle do fluxo de pessoas pelas fronteiras. Isso acontece em virtude da capacidade que a tecnologia da informação possui para “desmaterializar” aquilo que é sólido. As pessoas são “virtualizadas” em forma de *data-doubles*, ou seja, agregados de informações reunidas sobre elas. Essas informações são coletadas de bancos de dados diversos – públicos, privados, nacionais, internacionais – e, também, do próprio corpo do indivíduo – veja-se, por exemplo, a inserção de informações biométricas em passaportes. Perde relevância o “ser humano real”, uma vez que ele somente pode ser analisado quando entra nas bases de dados.

Essa interação entre fronteiras e bancos de dados de origem privada – como os programas de milhagens das companhias aéreas, empresas de cartão de crédito etc. – faz com que as fronteiras percam cada vez mais a sua natureza de limites políticos da soberania de um Estado e passem a ser, cada vez mais, relacionadas aos interesses econômicos dos controladores das bases de dados.

²¹¹ No original: “Peoples and things cross, flow and butt up against borders which are no longer found at the edges of states. Borders might even be located within and now outside territorial containers as bodies too are stretched, made informational and pulled and pushed within and across national boundaries. Surveillance seems to disrespect the traditional jurisdictional limits of nation-states by transborder supranational and interoperable surveillance systems in order to, paradoxically, reinforce their borders.”

Nessa tendência de virtualização, as fronteiras também são transformadas em iterações de programas de computadores e, com isso, passa a predominar a tendência da desvinculação entre a fronteira e o território. Nas palavras de Peter Adey,

em virtude da conjugação contemporânea de todos esses sistemas distribuídos de captura de dados, distribuição e de tomada de decisões, a [surveillance] nas fronteiras é melhor descrita por Mark Salter como deslocalizadas – a fronteira é movida para fora do centro e da costa. A afinidade do Estado pelo “controle remoto” [...] é particularmente evidente em programas de liberação prévia do controle de fronteira [...] vemos novas ideias sobre fronteiras serem propostas através de uma linguagem aprimorada de segurança de fronteira que tem cada vez menos a ver com a ideia enclausurada de controle territorial e mais com o gerenciamento dos fluxos populacionais (ADEY, 2012, p. 198)²¹².

Com isso, as fronteiras, assim como as pessoas, deixam de ser consideradas em sua característica física, como uma linha desenhada no mapa. As fronteiras passam a “acontecer” no momento em que as informações são concatenadas e decisões são tomadas com base nessas concatenações. Dessa maneira, a tecnologia da informação possibilita a desvinculação entre fronteiras e territórios, de modo que os potenciais riscos são avaliados antes mesmo de se concretizarem.

Esse deslocamento de fronteiras fica claro, por exemplo, quando um brasileiro pretende viajar para os Estados Unidos. Pelas regras atuais, é necessário solicitar uma autorização prévia de viagem (visto) nos consulados localizados no Brasil. Embora a obtenção de um visto não impeça que ocorra nova análise do viajante quando da sua chegada ao território estadunidense, a não concessão dessa autorização prévia impossibilita até mesmo o embarque do passageiro no avião.

Nessa situação, a fronteira estadunidense é “materializada” dentro do Brasil, quando um sistema de computador e um oficial de imigração daquele país decide se o solicitante pode ou não receber o visto. Situação similar ocorre com o indivíduo que pretende viajar ao Canadá, conforme explicado, anteriormente, na introdução deste capítulo. Ambas constituem aquilo que Mark Salter vê como “um exemplo concreto de

²¹² No original: “Bearing witness to the contemporary assembling of all of these distributed systems of data capture, distribution and decision-making, border surveillance is best described by Mark Salter as delocalized – the border is moved off-center and off-shore. The state’s affinity for “remote control” [...] is particularly evident in border pre-clearance programs. [...] we see new ideas about the border being proposed through an enhanced language of border security which has less and less to do with container-like territorial control but rather the management of population flows.”

desterritorialização da soberania, onde o Estado desfruta de autoridade e preferência legal fora do seu território nacional” (2006, p. 170)²¹³.

Além disso, diversos sistemas permitem uma análise de elegibilidade para entrada em um determinado território antes mesmo de o viajante adentrar nele. Além dos já mencionados API e PNR, sistemas como o *Electronic System for Travel Authorization* (ESTA), nos EUA e a segunda versão do *Schengen Information System* (SIS II), na União Europeia verificam, previamente, se o viajante cumpre determinados requisitos de segurança²¹⁴. Caso esses sistemas não aprovem o viajante, ele é impedido de embarcar na aeronave.

Um outro exemplo de sistema é aquele utilizado pela agência de transportes dos EUA, a TSA, para gerar a já mencionada “*no fly list*”, um banco de dados formado por pessoas com potenciais vínculos com o terrorismo e que não podem embarcar em aviões cujo destino ou origem seja aquele país. No exemplo do brasileiro com um visto válido, caso ele vá parar, posteriormente, naquela lista, a fronteira dos EUA será fechada para ele no momento em que ele efetuar a reserva do bilhete aéreo. Como esse tipo de sistema separa a fronteira do território e o *data-double* da pessoa, é extremamente difícil demonstrar que um nome está naquela lista por um engano. Dá-se mais confiança ao sistema do que ao ser humano concreto, exceto, obviamente, nos casos absurdos – geralmente, envolvendo pessoas poderosas – quando fica claro que a identidade do indivíduo não pode corresponder àquele *data-double*²¹⁵.

3.5.2 As fronteiras como controle de fluxos: o banóptico

É a partir desse controle das fronteiras que Didier Bigo trabalha a ideia de banóptico (2008) (2006). Ainda que tenham sido feitas as ressalvas em relação ao modelo panóptico, é interessante a metáfora elaborada pelo autor em relação à lógica de exclusão de grupos formados por pessoas mais frágeis – pobres, imigrantes,

²¹³ No original: “a concrete example of the deterritorialization of sovereignty, where a state enjoy authority and legal precedence outside of its national territory.”

²¹⁴ Diversos outros sistemas possuem, dentre várias funções, a de controlar os fluxos de pessoas antes mesmo de elas chegarem ao território do país de destino. Vejam-se os exemplos estadunidenses do *Terrorist Identities Datamart Environment* (TIDE); *Secondary Security Screening Selection* (SSSS); *Secure flight program*.

²¹⁵ Além do exemplo do Senador T. Kennedy, demonstrado anteriormente, existiram situações absurdas quando, até mesmo, crianças de 4 anos de idade foram colocadas na “no fly list” por suspeita de envolvimento com o terrorismo. A matéria da agência *Associated Press* publicada no portal *NBC News* está disponível em < <http://surveillance.es/1-> >. Acesso em: 26 mar. 2016.

refugiados etc. –, viabilizadas pelas técnicas da *surveillance* – pública ou privada. Embora faça alusão ao panóptico, Bigo busca deixar claro que as práticas da *surveillance* são descentralizadas e que funcionam a partir de uma *assemblage* entre fluxos de dados públicos e privados em diversos lugares do planeta. Isso possibilita a compreensão do “*ban-optique*” mais como um jogo de palavras do que como um modelo teórico fundamentado no panóptico.

A palavra “*ban-optique*” é fruto da junção de “bando” (abandono, banimento), empregada por Giorgio Agamben (AGAMBEN, 2007) e o panóptico de Foucault. Serve para indicar a capacidade que as tecnologias da informação, ao viabilizarem a coleta, transmissão, armazenamento e processamento de dados, possuem para separar grupos de interesses político ou econômico.

No exemplo de Didier Bigo, fica claro como essas técnicas da *surveillance* surgem para fundamentar novos discursos que pregam uma situação de insegurança global e que têm como objetivo ajudar no controle do deslocamento dos indesejados. Esses mecanismos de uso ubíquo – visto que é difícil distinguir entre público e privado, como ficou evidente na associação entre a NSA e empresas privadas no caso Edward Snowden –, possibilitam não apenas a exclusão de uma categoria social em um determinado Estado, mas, em virtude da sua indeterminação e fluidez, de diversas estruturas de poder globalmente interconectadas. Nesse sentido, Zygmunt Bauman e David Lyon afirmam que “o banóptico opera nos espaços globalizados além do Estado-nação, assim, os efeitos do poder e da resistência não são mais sentidos somente entre Estado e sociedade” (BAUMAN e LYON, 2013, p. 62)²¹⁶.

É a associação entre o banóptico – viabilizado pela *surveillance* – e a globalização que permite o paradoxal surgimento simultâneo de mobilidade de fluxos de pessoas e a securitização das fronteiras. Para Stephen Graham (2010, p. 89), essa mudança decorre da transformação da natureza do Estado nacional, que se distancia, cada vez mais, do seu papel de garantidor de uma comunidade de cidadãos dentro de um território. Para o autor, o Estado torna-se, cada vez mais, um ator dentro de sistemas organizadores internacionais cujo objetivo é viabilizar o controle dos fluxos de pessoas, separando entre aqueles que merecem adentrar no território e outros, infelizes, que não são “merecedores” desse direito.

²¹⁶ No original: “the ban-opticon operates in globalized spaces beyond the nation-state, so the effects of power and resistance are no longer felt merely between state and society.”.

As fronteiras, assim, tornam-se semipermeáveis, uma vez que permitem o trânsito de pessoas, bens e capitais, mas com o contínuo controle desses fluxos. Essa reconfiguração das fronteiras é viabilizada pelas “guerras” desterritorializadas da modernidade líquida, como é o caso da já mencionada “guerra contra o terror”, centrada em ideais vagos de segurança pública ao invés da busca pela conquista de territórios, como eram as guerras da modernidade sólida. Como resultado, é possível concluir que essa nova “fronteira virtual” deixa de ser uma estrutura rígida, tornando-se um espaço flexível que se modifica conforme as necessidades de controle dos fluxos (GRAHAM, 2010).

Pelo exposto, fica óbvio que os tradicionais limites do Estado-nação são modificados pela *surveillance*, que deve ser entendida não apenas como um olhar vigilante unidirecional, mas como um fenômeno da vida contemporânea que atinge a todos os membros das sociedades altamente interconectadas. Como resultado, deslocam-se também as fronteiras, que deixam de ser apenas um limite territorial do Estado e passam a fazer parte desses fluxos de dados.

Uma vez que pessoas e fronteiras são “virtualizadas”, as comunicações entre esses dois componentes passam a ocorrer também em um ambiente virtual que é independente da sua localização geográfica. Isso faculta que riscos sejam avaliados antes mesmo que as potenciais ameaças cheguem ao território do Estado, além de permitir a passagem daqueles que, pelas regras do sistema, são considerados viajantes “legítimos” – ou seja, de interesse comercial.

É por isso que a ideia de *surveillance* como violadora dos direitos humanos e da democracia é essencial para compreender o fenômeno de desterritorialização das fronteiras. Os critérios para decisão e as fontes dos dados que alimentam esses sistemas, dificilmente, passam pelo crivo democrático, o que facilita a perpetuação de tratamento desigual e discriminatório.

O “local” onde as portas de um país são abertas ou fechadas não corresponde, necessariamente, aos limites do território desse local. Assim, é possível concluir que, para aqueles que se enquadram no “modelo” de viajante desejável, a globalização está, realmente acontecendo e o trânsito de pessoas está cada vez mais fácil. Por outro lado, as minorias e os indivíduos que não se enquadram naquele “modelo” encontram, sempre, mais dificuldade para transitar livremente. Para essas

peessoas, os “muros” das fronteiras estão cada vez mais altos e aparecem antes mesmo que cheguem ao seu destino.

Desse modo, é imprescindível analisar como a coleta e o processamento de dados viola a democracia e os direitos humanos, especialmente daquelas pessoas que são colocadas nas categorias cujas restrições são maiores. Esses temas serão abordados no próximo capítulo.

4 SURVEILLANCE PARA ALÉM DO ESTADO: DEMOCRACIA, DIREITOS HUMANOS E CONSTITUCIONALISMO

*What shall we use
To fill the empty spaces
Where we used to talk?
How shall I fill
The final places?
How should I complete the wall*

(Pink Floyd – Empty Spaces)

“Senhor(a), o seu nome não consta no sistema”. Quem nunca foi impedido de concretizar algum objetivo em virtude da negativa ou indisponibilidade de um sistema de computador? Essa frase demonstra o surgimento de uma entidade poderosa, capaz de controlar a vida das pessoas e garantir – ou impedir – que consiga obter algum bem da vida: o sistema.

Mas que sistema é esse? Quem foi que o elaborou? Qual o critério utilizou para garantir ou impedir o acesso? Se todos já se sentiram frustrados com uma negativa, por exemplo, para cancelar uma linha telefônica, o que dizer das dezenas de *Mohammeds* pelo mundo que sequer conseguem embarcar em um avião em virtude da ordem de um sistema preditivo?

Pelo que foi exposto até o presente momento, fica nítido que as novas tecnologias da informação criam problemas igualmente novos, o que deixa um espaço vazio de regulamentação que não pode ser preenchido pelo tradicional direito atual, que, historicamente ligado a uma perspectiva centrada no Estado, acaba ficando desorientado, sem saber como preencher esse vazio – ou, no máximo, tentando preenchê-lo com suas antigas ferramentas.

Em virtude desse vácuo, ocorre a apropriação do espaço digital pelo poder privado, o que agrava, ainda mais, a coleta, armazenamento e processamento de dados que caracterizam a *surveillance*. Essa situação, conforme será visto neste capítulo, atinge, especificamente, a democracia e os direitos humanos. Nesse sentido, será demonstrado que a democracia necessita de visibilidade e de *accountability*, elementos que não são encontrados nas novas tecnologias da informação.

Buscar-se-á demonstrar que, embora a *surveillance* envolva uma relação de transparência, trata-se de um tipo de visibilidade que é completamente distinto

daquela relacionada aos regimes democráticos. Tal fenômeno ocorre porque a *surveillance* possibilita a formação de uma visibilidade assimétrica, como acontece com um espelho falso: de um lado, Estados e empresas coletam e analisam, cada vez mais, dados sobre as pessoas com finalidades diversas; de outro, sempre aumenta a opacidade sobre como esses dados são capturados e processados.

Em virtude da sua obscuridade, os critérios para utilização desses dados, permanecem fora do debate democrático, além de serem elaborados por indivíduos que não foram eleitos democraticamente, o que somente torna ainda mais grave o fato de que não existe uma distinção entre quem cria e quem aplica a “lei” desse direito paralelo – nesse caso, simbolizado pelos códigos de computador. A incerteza gerada por um código de *modus operandi* desconhecido e que possui autoexecutoriedade, sem a mínima possibilidade de resistência é, sem dúvida, um risco para a democracia.

Além desse problema de visibilidade, a *surveillance* permite a criação do chamado filtro-bolha, que consiste na construção de um espaço de experiência virtual pasteurizada, onde não há lugar para a construção de perspectivas que divirjam do mundo criado para o usuário. Isso se faz possível através da personalização, que é viabilizada pelas técnicas de *data-mining* e *big data*.

Essas técnicas permitem que sejam determinados os interesses dos indivíduos com a finalidade de criar uma experiência prazerosa e sem atritos no uso da Internet. No entanto, esse “filtro” impede que as pessoas se conectem às outras, inviabilizando a oxigenação de ideias e pluralidade de perspectivas, tão essenciais à formação de uma esfera pública diversa, o que tem efeitos deletérios para a democracia.

No mesmo sentido, será visto que a proliferação de espaços privados na Internet – invólucros digitais – destrói o seu potencial democrático, uma vez que toda interação do usuário passa a ser feita em ambientes sofisticadamente desenhados para, cada vez mais, coletar informação e exercer contínua influência sobre os indivíduos. Ainda que, em muitos casos, se queira dar um falso ar de democratização desses espaços, trata-se, na realidade, de um simulacro.

Por essa razão, ficará visível que as relações assimétricas de poder, a ausência de transparência e de *accountability* – todos eles elementos essenciais à democracia – fazem com que a Internet seja um ambiente antidemocrático, que, ao invés de redistribuir, reforça as relações de poder, concentrando-o nas mãos de

entidades privadas. A grande maioria dos indivíduos opera um sistema operacional de código fonte fechado, acessa redes sociais de software-proprietário e utiliza serviços de e-mail que pertencem a uma empresa privada.

Embora já tenha ficado nítido o potencial que a tecnologia da informação possui para violar direitos humanos, será questionado qual o papel do Estado na sua proteção. Para tanto, será demonstrado que as abordagens tradicionais, vinculadas ao Estado-nação, embora reconheçam que tais direitos são violados por atores privados, não propõem respostas adequadas para a solução desses problemas, em razão de essas matrizes teóricas entenderem que os Estados – através da sua constituição política – são capazes de, sozinhos, resolver esse tipo de problema.

Por isso, será discutida a concepção sistêmica de que os direitos humanos são formas de controlar o poder através da delimitação da atuação dos sistemas sociais. A vantagem da teoria sistêmica para a análise da *surveillance*, nesse caso, é sua capacidade de lidar com a violação dos direitos humanos fora dos tradicionais lugares do poder e sem o contínuo retorno ao Estado nacional.

Sobre esse tema, será ressaltado que a igualdade, embora frequentemente ignorada, é um dos mais importantes direitos humanos violados, o que só é possível em virtude da capacidade que os sistemas de processamento digitais possuem para analisar e classificar dados.

Ocorre que esses sistemas são alimentados com dados sobre seres humanos reais, e essa classificação acaba por colocar pessoas em grupos diversos – seja de risco, de interesse, de saúde etc. Com a criação dos *data doubles* – dossiês digitais ilimitados sobre as pessoas –, é possível categorizar indivíduos e grupos de modo cada vez mais eficiente e preciso.

Além da igualdade, a privacidade é outro direito fundamental que sofre os influxos da *surveillance*, o que é de amplo conhecimento dos meios de comunicação e dos teóricos em geral. No entanto, ao invés de fazer retomadas históricas sobre a privacidade – tarefa melhor realizada por monografias dedicadas ao tema –, serão abordados fenômenos recentes que fazem com que outros pontos da privacidade mereçam mais atenção. Isso será feito através da ideia de que, no mundo habitado pelas *little sisters*, a privacidade transformou-se em moeda de troca, servindo para “pagar” serviços que – apenas em aparência – são gratuitos.

Na sequência, será demonstrado que o Estado é um palco fragilizado na proteção dos direitos humanos. Isso não ocorre por conta de uma “falha” do modelo estatal atual, mas em virtude da sua limitação, uma vez que ele foi pensado para viabilizar a imposição de limites jurídicos apenas para os poderes políticos.

Assim, será trazida a abordagem de Stefano Rodotà (2008, 2014) para reforçar o argumento de que a Internet é uma dimensão sem precedentes na história da humanidade, o que torna insuficientes as apostas nos tradicionais mecanismos teóricos – ou seja, o retorno à legislação nacional e à constituição política. De modo correto, Rodotà não acredita que a descentralização proporcionada pela tecnologia da informação possa ser considerada um retorno ao medievo. No entanto, como será visto, a tese de Rodotà deve ser adotada com parcimônia, em virtude de não captar, adequadamente, o fenômeno da *surveillance*.

Como resultado dessa análise, demonstrar-se-á a necessidade de retomar o trabalho de Gunther Teubner, proposta que parece ser muito mais adequada para compreender os conflitos viabilizados pela *surveillance* no universo do direito, especialmente em virtude de o referido autor deslocar-se das perspectivas tradicionais – que pensam os problemas transnacionais exclusivamente a partir de perspectivas que dependem do Estado nacional ou da sua aplicação em escala global.

Para tanto, serão trazidas os aportes sobre a teoria do constitucionalismo societário, que possibilita lidar com problemas associados aos sistemas sociais que adquiriram autonomia em relação ao Estado. Como será visto, constitucionalizar a Internet demanda um duplo, simultâneo e delicado movimento: de generalização – isto é, separar a constituição das características inerentes ao sistema político e estatal – e a reespecificação – que engloba a transposição do constitucionalismo para esse meio digital.

Sob esse aspecto, Teubner (2004, 2011a, 2011b) propõe a transição de um pensamento centrado na construção constitucional pelo Estado-nação em direção a um pluralismo constitucional, seja transnacional, seja societário. Afinal, no século XXI, está aumentando – e continuará a aumentar – o papel das corporações multinacionais na violação dos direitos humanos.

Essa multiplicidade de poderes – policentrismo –, que caracteriza a globalização, intensifica as crises das premissas do Estado-nação. Ainda assim, este continua sendo um ente fundamental na organização mundial das sociedades e, por

isso, deve ser sempre considerado, ainda que se defenda a constitucionalização de outros sistemas sociais. Isso poderá ser visto com a proposta do constitucionalismo híbrido nos moldes colocados por Gert Verschraegen (2011).

A ideia de globalização policêntrica permitirá chegar à conclusão de que somente através da renovação do direito constitucional, será possível controlar, eficazmente, os poderes selvagens. Isso requer um esforço da teoria do direito, para que saia da sua zona de conforto centrada exclusivamente no Estado e reconheça que, sozinho, o ente estatal possui capacidade de ação limitada.

4.1 SURVEILLANCE E DEMOCRACIA

4.1.1 Democracia, *accountability* e visibilidade

As maiores disputas de poder da história, afirma Manuel Castells (2010a), tiveram, como objetivo, a conquista da mente das pessoas. Considerando que a *surveillance* é caracterizada, especialmente, pela revolução na tecnologia da informação e, também, que o modo de fazer política na sociedade contemporânea²¹⁷ está diretamente associado ao tipo e à quantidade de informações disponíveis sobre os indivíduos, as instituições democráticas tradicionais passam, simultaneamente, tanto a sofrer os influxos de novos processos políticos, quanto a utilizar as novas tecnologias da informação para atingir os seus objetivos.

A democracia tem a visibilidade e a *accountability* como elementos essenciais para a sua existência. Infelizmente, ao contrário do que se gostaria de imaginar, a tendência atual das tecnologias da informação demonstra que elas são utilizadas mais como ferramenta de manipulação política e econômica do que como instrumento de emancipação democrática. Tal fato se dá porque a “transparência” democrática, que permite a *accountability* dos detentores de poder, é diametralmente oposta à visibilidade proporcionada pela *surveillance*.

Embora a democracia esteja sendo constantemente reinventada conforme as mudanças do mundo, ela não pode evitar a *accountability* dos detentores do poder, que é primordial para a existência de qualquer regime democrático representativo. Sob tal aspecto, Deborah Johnson e Kent Wayland, ao tratarem sobre o tema, afirmam

²¹⁷ Por todos, remete-se ao uso de bancos de dados digitais na campanha presidencial dos EUA em 2012.

que, embora a *surveillance* e a transparência envolvam a visibilidade, a ideia por trás de cada uma delas é diametralmente oposta. A visibilidade da *surveillance* não possui, ao contrário da transparência democrática, a conotação positiva. Isso porque, diferentemente da *surveillance*, “[...] a transparência sugere a operação da democracia, dos poderosos sendo responsabilizados” (2010, p. 26)²¹⁸.

Como resultado, ainda que seja frequente a aposta na democratização como solução para o crescente número de problemas associados à *surveillance* – já que a visibilidade democrática poderia, em tese, conter seus impulsos autoritários –, existem diversos fatores que limitam as possibilidades de uma significativa invasão da *accountability* democrática para dentro das tecnologias da informação.

O primeiro desses fatores limitantes está ligado ao caráter eminentemente técnico dos avanços nessa área, uma vez que eles surgem dentro de laboratórios, não no espaço público. Tais avanços dificilmente são debatidos publicamente, sendo diretamente implementados nos diversos âmbitos da vida social sem a possibilidade de controle democrático prévio. Essa dificuldade de controle prévio decorre, também, da menor velocidade do direito, da política e da democracia, incapazes, por sua natureza, de acompanhar a rapidez do desenvolvimento científico e das inovações tecnológicas.

A democracia, nesse sentido, chega tarde, pois o debate só se torna possível quando as tecnologias já foram inventadas, implementadas e, portanto, “normalizadas” no âmbito social. Isso ficou claro, por exemplo, no caso da alta aceitação, por parte do eleitorado estadunidense, do *Patriot Act* como instrumento na luta da suposta “guerra contra o terror”. Essa legislação demonstra que é questionável a possibilidade de formação de um consenso não manipulado dos eleitores a respeito da *surveillance*, pois, normalmente, a implementação de novas técnicas da *surveillance* ocorre em períodos de forte comoção popular, como foi o caso dos atentados de 11 de setembro de 2001.

Sob tal aspecto, uma das maiores alavancas para a “legitimação pública” da *surveillance* é o combate ao medo incerto e líquido gerado pelo terrorismo²¹⁹. A legislação de exceção estadunidense após os atentados contra o *World Trade Center* sofreu poucos questionamentos públicos, uma vez que surgiu como um remédio que,

²¹⁸ No original: “[...] transparency suggests the operation of democracy, of the powerful being held accountable.”

²¹⁹ Sobre o tema, ver item 3.2.2.

embora amargo, seria imprescindível na suposta luta por um “bem maior”. Os reflexos disso são visíveis, por exemplo, na opinião, extremamente comum nos EUA, de que Edward Snowden é um traidor e deve ser julgado e condenado à morte por divulgar os segredos da NSA²²⁰.

Infelizmente, a história demonstra que, em períodos de considerável medo, é mais provável que apareçam posturas nacionalistas e radicais do que debates fundamentados a respeito dos riscos de utilização da infraestrutura estatal para controlar os indivíduos. O exemplo da “guerra contra o terror” acentua o antagonismo entre a visibilidade democrática e os segredos de Estado – ainda que justificado para fins de “segurança nacional”.

A sociedade contemporânea organiza-se através dos regimes de visibilidade, cada um com as suas assimetrias. Se a tecnologia da informação tem o poder de aumentar a visibilidade da coisa pública na democracia – veja-se, por todos, os avanços relacionados aos portais de transparência nas diversas esferas do governo – a *surveillance*, por sua vez, tende a diminuir a visibilidade, especialmente nas sociedades do controle (DELEUZE, 1992). No entanto, a única promessa não cumprida da modernidade que denota incompatibilidade total com a democracia é a manutenção e o fortalecimento de poderes invisíveis. A grande proposta dos primeiros regimes democráticos foi desvelar o núcleo duro e oculto do poder exercido por pequenos grupos. Essa foi, inclusive, uma das razões da superioridade desses regimes em relação ao Estado absoluto, em que eram defendidos os poderes ocultos – *arcana imperii* (BOBBIO, 1997).

Ao contrário das outras promessas não cumpridas, o segredo é o único tema que Norberto Bobbio considera ter sido pouco abordado pelos cientistas políticos. Para o autor, dentro do Estado visível, a tendência é que exista sempre um outro Estado, paralelo ou superior, invisível. Com isso, é possível afirmar que “o tema mais interessante, com o qual é possível realmente colocar à prova a capacidade do poder visível debelar o poder invisível, é o da publicidade dos atos de poder que [...] representa o verdadeiro momento de reviravolta na transformação do estado moderno” (BOBBIO, 1997, p. 103).

²²⁰ Na pesquisa feita pela agência Reuters, 23% dos entrevistados consideravam Snowden um traidor; 31% um patriota e 46% não souberam opinar. A matéria de Andy Sullivan para a agência *Reuters*, está disponível disponível em < <http://surveillance.es/2c> >. Acesso em: 26 abr. 2016.

A existência de subgovernos e criptogovernos divide o poder não mais vertical ou horizontalmente, mas em relação à profundidade da sua ocultação, de modo que é possível classificar os poderes com base nesse critério. Curiosamente, tais poderes operam sob o argumento de proteção da privacidade que, na relação entre *surveillance* e democracia, tem o condão de reforçar formas não recíprocas de visibilidade, em que os detentores do poder se escondem ao mesmo tempo em que as massas se tornam cada vez mais visíveis (HAGGERTY e SAMATAS, 2010).

Como resultado, os avanços da tecnologia da informação estão diretamente relacionados à ideia de visibilidade. Essa, por óbvio, não pode ser reduzida àquilo que pode ser captado pela visão, mas como um

[...] campo simbólico de significação social: ver e ser visto não correspondem simplesmente a determinadas posições de poder. As relações de visibilidade são também constituídas por outras formas – não diretamente perceptuais – de perceber, gerenciar a atenção e determinar a significância de eventos e sujeitos. Em síntese, a visibilidade corresponde à intersecção entre a estética – relações de percepção – e a política – relações de poder (BRIGHENTI, 2010, p. 52).²²¹

Por essa razão, uma ideia mais ampla de visibilidade e do controle do poder deve estar diretamente relacionada à democracia. Seguindo essa ideia, Bobbio afirma que “o Estado democrático é aquele em que a opinião pública deve ter peso decisivo na formação e controle das decisões políticas [...]” (BOBBIO, 1985, p. 21)²²². Não se deve confundir, portanto, as autocracias – nas quais os detentores do poder são vistos como forma de exibição do seu poder – com a visibilidade dos regimes democráticos, que exige a visibilidade dos atos de poder, o que viabiliza o seu controle.

Essa visibilidade, quando contaminada por relações de poder não democráticas, tende a ser assimétrica, já que os detentores do poder podem tornar visível apenas aquilo que lhes for interessante. Protegidos pela “vantagem do pequeno número”, os detentores do poder podem sustentar a sua posição através do controle da visibilidade dos seus atos. Isso os fortalece ainda mais e dificulta a quebra

²²¹ No original: “[...] a symbolic field of social meaning: seeing and being seen do not simply correspond to given power positions. Visibility relationships are also constituted by many other, not directly perceptual, forms of noticing, managing attention, and determining the significance of events and subjects. In short, visibility lies at the intersection of aesthetics (relations of perception) and politics (relations of power).”

²²² No original: “El estado democrático es el estado donde la opinión pública debería tener un peso decisivo para la formación y el control de las decisiones políticas [...]”.

do seu “núcleo duro”, de maneira que é possível afirmar que “toda dominação que pretenda continuidade é, em algum ponto decisivo, dominação secreta” (WEBER, 1999, p. 196).

Um tema central na tentativa de proporcionar visibilidade democrática para a *surveillance* diz respeito à dinâmica entre os Estados e as entidades privadas. Como visto anteriormente²²³, um dos aspectos centrais do processo de globalização é a modificação das estruturas de soberania nacional em virtude da pluralidade de poderes, públicos e privados, que surgem no cenário contemporâneo. Essa descentralização, especialmente quando ocorre na esfera privada – em que, para lembrar a denúncia de Norberto Bobbio (1997), nem mesmo a democracia como procedimento foi implementada²²⁴ –, retira das regras e dos usos da *surveillance* a possibilidade de controle democrático por parte daqueles que sofrerão as consequências da sua implementação.

Esse controle passa a ser feito por quem não foi eleito democraticamente, uma vez que os critérios de coleta e uso das informações de grandes empresas de tecnologia da informação não são passíveis de legitimação por parte dos usuários, cabendo, quando muito, apenas a possibilidade de se recusar a usufruir determinados serviços. Essa opção, no entanto, não existe de modo substancial, uma vez que a exclusão do mundo da informação e da comunicação não é, realmente, uma possibilidade para a grande maioria das pessoas²²⁵. Afinal, “[...] quando a submissão

²²³ Item 1.2.

²²⁴ Nesse sentido, Norberto Bobbio (1997, p. 55) já advertia que, com relação ao processo de democratização, “[...] não tanto, como erroneamente muitas vezes se diz, na passagem da democracia representativa para a democracia direta quanto na passagem da democracia política em sentido estrito para a democracia social, ou melhor, consiste na extensão do poder ascendente, que até agora havia ocupado quase exclusivamente o campo da grande sociedade política (e das pequenas, minúsculas, em geral politicamente irrelevantes associações voluntárias), para o campo da sociedade civil nas suas várias articulações [...] Em outras palavras, podemos dizer que o que acontece hoje quanto ao desenvolvimento da democracia não pode ser interpretado como a afirmação de um novo tipo de democracia, mas deve ser entendido como a ocupação, pelas formas ainda tradicionais de democracia, como é a democracia representativa, de novos espaços, isto é, de espaços até agora dominados por organizações de tipo hierárquico ou burocrático.”

²²⁵ Na opinião de Tim Wu, professor da *Columbia Law School* e um dos mais renomados especialistas sobre o tema nos Estados Unidos, os usuários devem deixar de utilizar os serviços das empresas envolvidas no escândalo *PRISM/Upstream/XKeyscore*. O pesquisador afirmou em entrevista ao jornalista Chris Baraniuk: “Quit Facebook and use another search engine. It’s simple. It’s nice to keep in touch with your friends. But I think if you find out if it’s true that these companies are involved in these surveillance programs you should just quit.”

Contudo, considerando que, além das empresas mencionadas por ele, foram comprometidas informações de usuários de uma infinidade de outros serviços, inclusive de telefonia móvel, seria muito simplista acreditar que os usuários pudessem simplesmente abandonar o uso de ferramentas tão importantes como e-mails, sistemas de busca e telefone celular. Veja-se, por exemplo, o caso brasileiro: o Ministério do Desenvolvimento Social incentiva o cadastramento de um telefone celular até mesmo

ao monitoramento torna-se a condição para o acesso não apenas ao trabalho, mas aos bens e serviços (desde comida até telefonia), as relações de acesso e de controle sobre os recursos estruturam os termos de entrada” (ANDREJEVIC, 2007, p. 132)²²⁶.

Por essa razão, é de extrema relevância retomar Norberto Bobbio, para quem o processo de alargamento da democracia política contemporânea atingiu uma situação limítrofe, visto que há pouco espaço para ampliação dos direitos políticos dentro da estrutura estatal. No entanto, o limite de crescimento da democracia representativa não significa que o próximo passo seja um retorno à democracia direta proporcionada pela tecnologia da informação.

Isso em razão de a evolução democrática, para Bobbio, estar relacionada à expansão participativa para além da esfera estatal, ou seja, à extensão do método democrático – indireto e, quando possível e desejável, direto – para áreas distintas daquela da tradicional arena política. Dessa maneira, “[...] através de todas aquelas formas de ‘socialização do poder’ [...] que permitem um controle a partir da base da direção pública da economia, ou através de outra fórmula, a instauração de um sistema de ‘programação descentralizada e participada’” (BOBBIO, 1999, p. 70).

Nessa esteira, pode-se afirmar que a evolução democrática consiste na passagem da democracia da esfera política para a democracia social. Existe tal necessidade, porque, após a conquista do direito de participação política, os integrantes das democracias avançadas perceberam que as relações de poder estabelecidas na esfera política correspondem apenas a uma parte, condicionada pelo todo que compõe a sociedade civil, de forma que se passou a sentir necessidade de democratizar, também, a vida social, avanço indispensável à manutenção do Estado democrático de direito.

Logo, torna-se evidente que a democracia política, limitada ao Estado-nação, tem se demonstrado insuficiente para proteger os indivíduos contra o despotismo dos poderes privados. Disso resulta a clássica afirmação, feita por Bobbio (2007, p. 157), segundo a qual o desenvolvimento da democracia não deve mais estar relacionado

para aqueles que recebem o “bolsa família” e que, portanto, são oficialmente reconhecidos como miseráveis. A matéria Chris Baraniuk para a revista *Wired* está disponível em: < <http://surveillance.es/2d> >. Acesso em: 26 abr. 2016.

²²⁶ No original: “[...] when submission to monitoring becomes a condition of access not just to work, but to goods and services (from food to telephony), relations of unequal access to and control over resources structure the terms of entry.”

apenas aos legitimados para votar – quem vota –, mas, especialmente, deve verificar em quais espaços o voto democrático pode ser exercido – ou seja, onde se vota.

Torna-se nítido, portanto, que a principal característica dos regimes de visibilidade proporcionado pela *surveillance* nas sociedades contemporâneas é a incerteza gerada pelo desconhecimento sobre quais as regras a serem usadas para coletar e tratar os dados dos grupos e indivíduos. O risco para a democracia, nesse caso, está relacionado ao fato de que a *surveillance* torna visível uma quantidade maior de dados das pessoas e, ao mesmo tempo, não oferece *accountability* sobre o uso desses dados. Por essa razão, percebe-se que “[...] existe um risco maior do que a criação de perfis das pessoas por agências (relativamente) invisíveis: é o fato de que os próprios critérios de criação desses perfis são invisíveis” (BRIGHENTI, 2010, p. 64)²²⁷.

No entanto, a assimetria das relações de visibilidade constitui apenas um risco que a *surveillance* gera para a democracia. A seguir, serão analisados outros problemas dessa complexa relação.

4.1.2 Democracia e pluralismo político: o problema do filtro-bolha

Com base no exposto até o momento, é de se perguntar: será possível compatibilizar a *surveillance* com a democracia? Essa resposta, assim como outras sobre o tema deste trabalho, é ambígua. Por um lado, essa tecnologia tem muito a oferecer à democracia, como é o caso dos portais de transparência ou das tecnologias que permitem aprofundar o conhecimento sobre a saúde da população e sua situação econômica. Por outro, essas mesmas ferramentas podem ser utilizadas para aumentar o poder daqueles que controlam as tecnologias. Trata-se, enfim, de uma questão aberta, extremamente dependente do contexto em que é feita a análise e da forma como são utilizados esses sistemas.

Para alguns, os computadores interconectados representam uma nova era de participação democrática, visto que tais máquinas possibilitariam, simultaneamente, a manutenção da visibilidade dos detentores de poder e o *feedback* imediato dos governados. A era da interatividade, sob esse aspecto, seria marcada, também, pela

²²⁷ No original: “There exists a greater threat than the fact that people are profiled by (relatively) invisible agencies: it is the fact that profiling criteria themselves are invisible.”

coleta de dados por parte do Estado, que seria capaz de criar políticas públicas mais adequadas aos cidadãos (HAGGERTY e SAMATAS, 2010). Nesse sentido, por exemplo,

[...] a Internet é vista por muitos como um meio revolucionário que oferece igualdade de vozes a todos os cidadãos, especialmente quando comparada aos meios pré-existentes (por exemplo, televisão, jornal e rádio), que são comumente caracterizados como *top-down*, canais de comunicação unilaterais controlados pelas elites das *medias*. As capacidades técnicas da Internet são colocadas como prova de que a Internet é, pela sua essência, uma ameaça às relações de poder centralizadas e hierárquicas [...] (WHITSON, 2010, p. 232)²²⁸.

Por outro lado, é preciso ter cautela a respeito dos efeitos da *surveillance* nos regimes democráticos, em virtude de a dinâmica das relações de poder no mundo real ser fundamental para as tecnologias. Ao invés de permitir a ampliação da democracia, alterando as hierarquias sociais de poder, as novas tecnologias acabam por reforçá-las. Por isso, a personalização tem consequências negativas para a democracia e torna mais fácil manipular a formação da opinião na esfera pública (ANDREJEVIC, 2007). Nesse aspecto, conforme Gunther Teubner,

considerando que, no seus primórdios anárquicos, a Internet foi construída sobre os princípios da inclusão de todos, do anonimato, da liberdade contra controle e da heterarquia, cresce cada vez mais a tendência atual, motivada pela política e pela economia, de surgimento das chamadas intranets, ou seja, de redes fechadas, baseadas na exclusão, no controle, na hierarquia e na orientação restrita a determinados objetivos (TEUBNER, 2004, p. 23)²²⁹.

Essa ambiguidade das novas tecnologias da informação é bem colocada por Antonio-Enrique Pérez Luño (PÉREZ LUÑO, 2003)²³⁰ através do contraste entre

²²⁸ No original: “[...] the internet is seen by many as a revolutionary medium that gives equal voice to all citizens, especially when compared to pre-existing media forms (e. g. television, newspaper, and radio networks), that are commonly characterized as top-down, one-way communication channels controlled by media elites. The technical capabilities of the internet are held as proof that the internet is an inherent threat to centralized, hierarchical power relations [...]”.

²²⁹ “Whereas in its anarchical beginnings the internet was built up on the principles of the inclusion of all, of anonymity, freedom from control and heterarchy, today the politically and economically motivated tendencies towards the emergence of so-called intranets, i.e. closed networks, based on exclusion, control, hierarchy, and strict goal-orientation, are growing stronger.”

²³⁰ Adepto do positivismo jurídico, Pérez-Luño move-se em um nível completamente diferente da proposta deste trabalho. Embora não se concorde com as soluções para o problema da *surveillance* por ele apontadas – o retorno ao Estado como protetor dos direitos humanos violados pelas novas tecnologias da informação – a análise das premissas do problema feita pelo autor espanhol é de extrema relevância para os juristas.

“ciberdidadani@” e “cidadania@.com”. A primeira seria a dimensão “positiva”²³¹, capaz de viabilizar a maior participação política dos indivíduos e, portanto, fortalecer o regime democrático. Já a “cidadania@.com” simbolizaria o lado negativo das novas tecnologias da informação, visto que está relacionada à desconstrução da esfera pública e de fortalecimento das relações de poder e submissão existentes. Na síntese do próprio auto,

[...] se, em suma, pode-se conceber as novas tecnologias e, em particular, a Internet, como um novo tecido comunitário para a sociedade civil ou como um instrumento de submissão universal, são alternativas sobre o emprego dessa nova técnica de conhecimento e poder sobre as quais se coloca o destino social do homem de hoje (PÉREZ LUÑO, 2012, p. 82)²³².

Essa dualidade é bastante nova no imaginário teórico, porque a Internet, até pouco tempo atrás – e, para muitos, ainda hoje –, era considerada uma forma de conectar-se com o outro, ouvi-lo e deixar-se ouvir. Essa “alteridade”, extremamente importante para a democracia, seria estimulada pela Internet.

No entanto, ocorreu uma mudança invisível nesse ideal. Em 04 de dezembro de 2009²³³, uma nova era para a democracia começou silenciosamente. A partir daquele dia, o *Google* passou a utilizar quase sessenta indicadores eletrônicos individuais para prever os resultados que seriam de maior interesse para o usuário.

²³¹ Aqui vale a crítica ao que Pérez Luño considera “[...] las experiencias más estimulantes para la afirmación de la polaridad positiva [...]”. Segundo o autor, faz parte desse grupo “el Manifiesto por el ejercicio de una ciber ciudadanía activa, responsable y comprometida. Dicha declaración fue elaborada por el primer Congreso ONLINE del Observatorio para la Ciber-Sociedad, celebrado en septiembre de 2002, donde fue aprobada mayoritariamente y en todos sus puntos. El Congreso reunió a 700 cibernautas de todo el mundo.” (PÉREZ LUÑO, 2012, p. 82-83). A importância que Pérez Luño dá ao referido documento demonstra a fragilidade das matrizes teóricas tradicionais que, na ausência de uma “declaração” de direitos cibernéticos de um Estado ou de organização internacional, buscam socorro em documentos de baixa relevância no contexto geral.

²³² No original: “[...] si, en suma, puede concebirse a las NT y, en particular, a Internet como un nuevo tejido comunitario para la sociedad civil o como un instrumento de sujeción universal, son alternativas sobre el empleo de esta nueva técnica de conocimiento y poder sobre las que se juega el destino social del hombre de hoy.”

²³³ Em 2009, sob o título de “busca personalizada para todos”, o Google passou a oferecer resultados personalizados de pesquisa inclusive para aqueles usuários que não tinham feito o *login* com a sua conta do *Google*. Através da inserção de um arquivo *cookie* no computador do usuário, a empresa passou a monitorar as pesquisas realizadas em cada dispositivo, independente da expressa manifestação de vontade do usuário para fazer parte deste serviço. A postagem de Bryan Horling e Matthew Kulick, empregados do *Google*, no blog da empresa, embora ensine como o usuário pode desativar este serviço, informa que tal desligamento só ocorrerá para aqueles que seguirem um procedimento que, para a maioria, é demasiado completo. Trata-se, pois, de um sistema *opt-out*, não *opt-in*. Disponível em: < <http://surveillance.es/28> >. Acesso em: 25 abr. 2016.

Como resultado, caso duas pessoas diferentes façam exatamente a mesma pesquisa, os resultados obtidos podem ser absolutamente diversos.

Pouco tempo depois, diversas outras empresas passaram a utilizar algoritmos similares para categorizar informações que fossem mais “adequadas” para o usuário. É o caso, por exemplo, da “linha do tempo” da rede social *Facebook* que, ao invés de mostrar as postagens em ordem cronológica, prioriza aquelas que poderão ser de maior interesse do usuário, com base em todas as interações dele e dos seus amigos na rede social²³⁴.

A criação de modelos preditivos, analisados anteriormente neste trabalho, passou a atingir em cheio a democracia. Isso se deve ao fato de que um regime democrático exige simetria comunicativa e de visibilidade na formação da esfera pública democrática.

Craig Calhoun lembra que a democracia requer tanto a inclusão quanto a conexão entre os indivíduos, ou seja, que eles se tornem capazes de acessar informações relevantes e de comunicar-se entre si para além dos limites impostos pelas associações privadas. Segundo o referido autor,

os públicos conectam pessoas que não fazem parte da mesma família, comunidades, clubes; pessoas que não são iguais às outras. A vida urbana é pública, logo, de certa forma, a vida em um vilarejo não é. Os meios de comunicação modernos amplificam essa capacidade de comunicar com estranhos. E a própria comunicação é vital, pois ela tanto cria uma cultura compartilhada quanto possibilita o debate (CALHOUN, 2005, p. 5)²³⁵.

Essa necessidade de pluralismo de ideia é essencial para a democracia. Nesse sentido, Norberto Bobbio entende que o pluralismo político é uma proposta que visa a manter um modelo centrífugo de sociedade, em que o poder é distribuído em diversos pontos, mesmo que conflitantes. Essa divisão permite a limitação da criação de um centro de poder dominante, tradicionalmente vinculado ao Estado (BOBBIO, 1997).

²³⁴ Em 30 de março de 2016, o *Instagram*, rede social que pertence ao *Facebook*, anunciou que também utilizaria algoritmos para selecionar as fotos que seriam exibidas para os seus usuários. Segundo entrevista de seu presidente, “what this is about is making sure that the 30 percent you see is the best 30 percent possible”. A postagem de Ashley Caran para o portal *The Verge* está disponível em: < <http://surveillance.es/2m> >. Acesso em: 25 abr. 2016.

²³⁵ No original: “Publics connect people who are not in the same families, communities, and clubs; people who are not the same as each other. Urban life is public, thus, in a way village life is not. Modern media amplify this capacity to communicate with strangers. And communication itself is vital, for it both creates shared culture and enables debate.”.

Assim, o pluralismo é o traço diferenciador da democracia dos modernos, para usar a terminologia de Bobbio. Conforme o autor, desde que o dissenso seja mantido dentro dos limites das regras do jogo democrático, ele possui a capacidade de promover a democracia, de modo que “[...] uma sociedade em que o dissenso não seja admitido é uma sociedade morta ou destinada a morrer” (BOBBIO, 1997, p. 61). Obviamente, não se está afirmando que a democracia necessita sempre do dissenso – afinal, exige uma concordância final na tomada de decisões. O que se pretende afirmar é que a democracia não existe nos regimes que, ao invés de aceitar o dissenso, buscam pasteurizar o pensamento divergente.

Da mesma forma, o conflito, oriundo da diversidade do pensamento, é um traço marcante dos regimes democráticos na acepção de Robert Dahl. Corroborando tal ideia, o autor americano lembra que, já na constituição dos EUA do ano de 1787, James Madison defendia que a diversidade e o conflito de pontos de vista eram traços inerentes da sociedade democrática (DAHL, 1984). De acordo com ele, já que a existência de “organizações independentes pode ser suprimida apenas pela supressão das instituições da poliarquia, [...] não é acidente que pluralismo e poliarquia andem juntos” (DAHL, 1984, p. 234)²³⁶. O conflito, muito mais que o consenso, é considerado por Dahl como característica imprescindível para as sociedades modernas, dinâmicas e pluralistas – “MDP”²³⁷ (DAHL, 2012).

Sob a mesma perspectiva, John Rawls entende que a pluralidade de opiniões completamente divergentes é o traço delineador dos regimes democráticos. Para ele, “[...] uma pluralidade de doutrinas razoáveis, ainda que incompatíveis, é o resultado

²³⁶ No original: “Independent organizations can be suppressed only by suppressing the institutions of polyarchy [...] it is no accident that pluralism and polyarchy go together [...]”.

²³⁷ A sociedade “moderna, dinâmica e pluralista” (MDP), definida por Dahl (2012, p. 396), “[...] pode ser resumida em duas características gerais: (1) uma sociedade MDP dispersa o poder, a influência, a autoridade e o controle para além de um único centro e os aproxima de uma variedade de indivíduos, grupos, associações e organizações. E (2) ela promove atitudes e convicções favoráveis às ideias democráticas. Embora essas duas características sejam geradas independentemente, elas também se reforçam mutuamente. O que é crucial numa sociedade MDP é que, por um lado, ela inibe a concentração de poder num só conjunto unificado de atores e, por outro, ela dispersa o poder entre uma série de atores relativamente independentes. Devido a seu poder e autonomia, esses atores podem resistir à dominação unilateral, competir entre si por certas vantagens, envolver-se em conflitos e negociações e buscar ações independentes por si mesmos. São características de uma sociedade MDP: a dispersão dos recursos políticos, tais quais o dinheiro, o conhecimento, o status e o acesso às organizações; a dispersão das localizações estratégicas, particularmente em assuntos econômicos, científicos, educacionais e culturais; e a dispersão das posições de negociação, tanto manifestas quanto latentes, nos assuntos econômicos, na ciência, nas comunicações, na educação e em outras áreas”.

normal do exercício da razão humana no contexto das instituições livres de um regime constitucional democrático” (RAWLS, 1996, p. xvi)²³⁸.

Dessarte, são três os fatores que compõem a cultura política de uma sociedade democrática: 1) a possibilidade de dissenso; 2) a inexistência de uma doutrina única amparada pela força (Rawls refere-se, expressamente, ao poder estatal, mas, para os fins deste trabalho, deve-se ampliar a sua concepção de modo a abranger qualquer poder, público ou privado) e 3) a necessidade de suporte da democracia pela maioria dos seus cidadãos politicamente ativos.

Rawls entendia que a manutenção de uma única opinião somente poderia ocorrer através da opressão do poder estatal. Para ele, “se considerarmos uma sociedade política como uma comunidade unida na afirmação de uma única doutrina, então o uso opressivo do poder estatal será necessário para a comunidade política” (RAWLS, 1996, p. 37)²³⁹. No entanto, como se pretende demonstrar com este trabalho, o uso dos algoritmos que fornecem conteúdo personalizado é, também, uma interferência de um poder – só que, desta vez, privado e sedutor – capaz de diminuir o dissenso, pedra angular das sociedades democráticas.

Esse algoritmo funciona de maneira relativamente simples: eles analisam a atividade *online* do usuário – páginas que visita, e-mails que recebe, pessoas com quem tem amizade – e cria um perfil preditivo sobre quem é aquele usuário e o que ele gostará de acessar. Esses algoritmos, chamados “filtros-bolha” – *filter bubble* – por Eli Pariser, criam um universo de informação único para cada usuário, alterando as formas como os indivíduos obtêm conhecimento sobre o mundo (PARISER, 2011).

Por um lado, existe algo positivo no filtro-bolha. Afinal, a quantidade de informações na Internet demanda formas de organizá-las, sob risco de as pessoas nunca encontrarem aquilo que desejam. No entanto, esse filtro-bolha é invisível aos indivíduos. Uma vez que não existe transparência nenhuma sobre a origem das fontes de dados sobre os usuários e de que maneira esses dados são processados, é impossível saber o que o sistema exclui de cada bolha individual. Além disso, é

²³⁸ No original: “[...] a plurality of reasonable yet incompatible comprehensive doctrines is the normal result of the exercise of human reason within the framework of the free institutions of a constitutional democratic regime”.

²³⁹ No original: “[...] can be maintained only by the oppressive use of state power. If we think of political society as a community united in affirming one and the same comprehensive doctrine, then the oppressive use of state power is necessary for political community”.

extremamente problemático o fato de que o usuário não possui a opção de “sair” ou entrar na bolha.

No mesmo sentido, Cass Sunstein entende que essa revolução da customização é incrível, já que as recomendações de serviços como *Amazon* e *Netflix* são magicamente adequadas aos gostos dos usuários e, provavelmente, uma infinidade de pessoas já descobriu um novo filme, ou música, ou livro favorito por conta dessas recomendações. Por outro lado,

[...] isso pode ser também perturbador se sua consequência for encorajar as pessoas a estreitar os seus horizontes, ou alimentar os seus gostos atuais ao invés de permiti-las formar outros novos. Isto é um problema real para filmes e música, mas é provavelmente muito mais sério para o campo democrático. Suponha, por exemplo, que pessoas com certas convicções políticas encontram-se aprendendo cada vez mais sobre autores com o mesmo ponto de vista e, com isso, fortalecendo os seus julgamentos preexistentes, somente porque a maior parte do que eles encontraram para ler possui o mesmo conteúdo. Em uma sociedade democrática, não poderia isto ser preocupante? (SUNSTEIN, 2007, p. 21)²⁴⁰

Para entender esse problema, Sunstein analisa a ideia de fórum público a partir do conceito de liberdade de expressão²⁴¹. Em 1939, a Suprema Corte dos EUA²⁴², ao proibir que ruas e parques fossem fechados para o acesso do público, delimitou o que ficou conhecido como “teoria do fórum público”, que consiste, basicamente, na liberdade de reunião em locais públicos como forma de proteção da liberdade de expressão.

Posteriormente²⁴³, ao julgar sobre a aplicabilidade da referida teoria aos aeroportos, a Suprema Corte reconheceu que a participação política depende, cada vez mais, dos meios eletrônicos. Ainda que não tenham decidido sobre a aplicação

²⁴⁰No original: “[...] it might well be disturbing if the consequence is to encourage people to narrow their horizons, or to cater to their existing tastes rather than to allow them to form new ones. The problem is a real one for movies and music, but it is probably most serious in the democratic domain. Suppose, for example, that people with a certain political conviction find themselves learning about more and more authors with the same view and thus strengthening their preexisting judgments, only because most of what they are encouraged to read says the same thing. In a democratic society, might this not be troubling?”

²⁴¹ Sobre a liberdade de expressão e formação da esfera pública com foco na propriedade dos meios de comunicação de massas, remete-se à leitura da dissertação de mestrado do autor deste trabalho. JACOB NETO, E. **Concentração proprietária dos meios de comunicação de massas na democracia constitucional**. 2012. 216 f. Dissertação (Mestrado em Direito) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 11 set. 2012. Disponível em: < <http://surveillance.es/2a> >. Acesso em: 25 abr. 2016.

²⁴² *Hague v. CIO*, 307 U.S. 496 (1939).

²⁴³ *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727, 803 (1996).

da referida teoria à Internet, ela é importante por diversos motivos, em especial, por garantir que os participantes do debate democrático tenham acesso a um leque amplo e heterogêneo de pessoas e opiniões.

O filtro-bolha impossibilita o encontro casual com opiniões e interesses diversos, diminuindo a oxigenação de ideias, o que é extremamente prejudicial para a democracia. Isso porque os

encontros não planejados e não escolhidos frequentemente acabam tendo efeitos positivos para os indivíduos e para a sociedade em geral. [...] talvez leve-o a reavaliar os seus próprios pontos de vista e até mesmo revisá-los. No mínimo, você terá aprendido sobre o que os seus concidadãos pensam e porque pensam desta forma (SUNSTEIN, 2007, p. 30)²⁴⁴.

Por esse motivo, o filtro-bolha, ao retroalimentar opiniões e pontos de vista preexistentes, acaba por enfraquecer o debate plural exigido pela democracia²⁴⁵. O pluralismo político, necessário para os regimes democráticos, só pode ser obtido através da fertilização cruzada de ideias. Nesse contexto, vale a máxima de John Stuart Mill, que considerava impossível “[...] superestimar o valor, no atual baixo estado do aperfeiçoamento humano, de colocar os seres humanos em contato com outras pessoas diferente deles, com modos de pensar e agir diversos daqueles com os quais está familiarizado” (MILL, 1909, Livro III, Capítulo XVI, §5º)²⁴⁶.

Infelizmente, a personalização viabilizada por algoritmos preditivos – o filtro-bolha – permite que indivíduos vivam em universos paralelos, porém separados – ou seja, suas vidas, por mais que coexistam, nunca se tocam. A democracia só funciona quando os seus participantes conseguem pensar fora das suas esferas individuais, o que se torna extremamente difícil sem uma visão de mundo compartilhada,

²⁴⁴ No original: “Unplanned and unchosen encounters often turn out to do a great deal of good, for individuals and society at large. [...] it might prompt you to reassess your own view and even to revise it. At the very least, you will have learned what many of your fellow citizens think and why they think it.”

²⁴⁵ No mesmo sentido, Zygmunt Bauman, em recente entrevista, afirmou que “o diálogo real não é falar com gente que pensa igual a você. As redes sociais não ensinam a dialogar porque é muito fácil evitar a controvérsia. Muita gente as usa não para unir, não para ampliar seus horizontes, mas ao contrário, para se fechar no que eu chamo de zonas de conforto, onde o único som que escutam é o eco de suas próprias vozes, onde o único que veem são os reflexos de suas próprias caras. As redes são muito úteis, oferecem serviços muito prazerosos, mas são uma armadilha.” A entrevista de Zygmunt Bauman, realizada por Ricardo de Querol para o jornal *El País* está disponível em: < <http://surveillance.es/2w> >. Acesso em: 04 maio 2016.

²⁴⁶ No original: “[...] overrate the value, in the present low state of human improvement, of placing human beings in contact with persons dissimilar to themselves, and with modes of thought and action unlike those with which they are familiar.”

conhecendo o outro e as suas necessidades. Em sentido diametralmente oposto, o filtro-bolha cria a ilusão de que os interesses do indivíduo correspondem à totalidade do mundo. A vida torna-se pasteurizada, autorreferenciada em um movimento centrípeto ao redor do indivíduo. Destrói-se, assim, o potencial democrático da Internet, tão aplaudido na década de 1990 e, ainda hoje, festejado por alguns teóricos.

4.1.3 Democracia e invólucro digital

Uma ideia similar à do filtro-bolha e que possui extrema relevância na análise da relação entre *surveillance* e democracia é a de invólucro digital – *digital enclosure* (ANDREJEVIC, 2007, p. 2). Essa proposta faz alusão aos cercamentos legais das terras – *land enclosure* – que ocorreram na Inglaterra dos séculos XVII e XVIII e que marcaram o começo da revolução industrial. Antes desse movimento, a terra era entendida como um bem comum onde todos poderiam cultivar. Com a transição do modo de produção feudal para o capitalista, a terra passou a ser vista como um bem de produção, o que fez com que os senhores feudais passassem a construir cercas delimitando suas terras e exigindo pagamento daqueles que tivessem interesse em cultivá-las.

De forma similar, o conceito de invólucro digital – que também pode ser chamado de “cercamento digital” – parte da ideia de que o espaço virtual era um lugar que pertencia a todos, especialmente se considerada a inexistência de governos eleitos no âmbito virtual. Esse tipo de espaço desregulamentado acaba se tornando ambiente propício para a colonização pelos detentores dos poderes, o que aconteceu com a Internet através da apropriação, cada vez maior, dos espaços digitais por empresas de tecnologia. Por isso,

como no caso do movimento de cercamento da terra, aqueles que controlam os recursos dentro do invólucro digital, – neste caso, as tecnologias de coleta de informações e os bancos de dados – podem se apropriar do valor gerado por aqueles que “livremente” entram no invólucro (ANDREJEVIC, 2007, p. 132)²⁴⁷.

²⁴⁷ No original: “As in the case of the land enclosure movement, within the digital enclosure, those who control the resources – in this case, information-gathering technologies and databases – can lay claim to the value generated by those who enter ‘freely’ into the enclosure.”

Agora, com os novos “cercamentos” realizados pelas empresas de tecnologia, as pessoas têm que pagar para participar – seja com dinheiro, seja com os seus dados. Uma vez considerado ambiente livre do controle, esse novo “cercamento digital” fez com que a Internet se tornasse ambiente privatizado. Na realidade,

é uma piada cruel que espaços desregulados, idealizados pelos tecno-libertários dos anos 1990, tenham se tornado lugares de [surveillance] e controle. O espaço deixado pelos governos eleitos, especialmente aqueles dos Estados-nação, permitem que corporações online conquistem espaço. Diferente dos governos eleitos, estas corporações não são responsáveis pelos seus “cidadãos”, não podem ser depositas e suas práticas e modos de funcionamento interno são opacos (WHITSON, 2010, p. 231).²⁴⁸

Com efeito, passa a ser insustentável a ideia de que a internet é um local de livre circulação de ideias, aberta ao debate. Existem regras que são impostas por entidades que não foram eleitas democraticamente e cuja única legitimidade é a propriedade da tecnologia que viabiliza a comunicação. Utilizando-se da estrutura descentralizada da rede, as empresas instalaram espaços privados sob o seu controle absoluto.

Tal caso é facilmente ilustrado no embate ocorrido, em 2015, entre o *Facebook* e o Ministério da Cultura brasileiro. No dia 16 de abril daquele ano, a rede social decidiu bloquear uma foto postada pelo Ministério por entender que ela continha nudez²⁴⁹, o que seria contrário à política da empresa. Na conversa inicial entre o representante do *Facebook* e o Ministro da Cultura, a rede social insistiu que a fotografia permaneceria bloqueada e que o *Facebook*, por ser uma empresa global, não estava sujeito às legislações nacionais de liberdade de expressão.

O traço fundamental desses invólucros digitais é a assimetria de visibilidade do poder, ou seja, o seu funcionamento como uma espécie de falso espelho – ou one way mirror, para utilizar a expressão de Frank Pasquale (2015)²⁵⁰. Isso acontece

²⁴⁸ No original: “It is a cruel joke that the unregulated spaces idealized by techno-libertarians of the nineties have now become sites of surveillance and control. The gap left by elected governments, especially nation-state governments, allows corporations to conquer online spaces. Unlike elected governments, these corporations are not accountable to their ‘citizens’, cannot be disposed of, and their practices and internal workings are opaque.”.

²⁴⁹ Tratava-se de um ensaio fotográfico feito por Walter Garbe em 1909 que mostrava uma índia com os seios expostos. Somente após diversas ameaças de judicialização do problema e em virtude da pressão pública, a rede social resolveu autorizar a publicação da fotografia. A matéria de Aline Leal para a Agência Brasil está disponível em < <http://surveillance.es/2g> >. Acesso em: 28 abr. 2016.

²⁵⁰ Embora já exaustivamente repetido, vale lembrar que a metáfora do espelho não deve levar à conclusão de que a visibilidade da surveillance diz respeito apenas aos olhos.

porque, além das empresas serem pouco transparentes, a própria natureza digital do espaço onde operam permite alcançar níveis de coleta de dados muito maiores que nos espaços físicos. Afinal, trata-se de um meio ótimo para a coleta de metadados²⁵¹, pois se todas as operações ocorrem de modo digital, todas elas geram metadados. Por isso, Mark Andrejevic (2007) considera que esses invólucros digitais permitem o acúmulo, nas mãos de poucas empresas, de uma quantidade enorme de dados e, portanto, de controle sobre os indivíduos através de práticas de visibilidade assimétrica e, por consequência, antidemocrática.

Ainda que existam discursos alegando que o usuário é livre para abster-se dos invólucros digitais caso esteja insatisfeito com a dinâmica de (in)visibilidade do sistema – como visto anteriormente em nota sobre Tim Wu –, essas estruturas virtuais – sejam redes sociais, serviços de e-mail, mecanismos de busca – são essenciais para as atividades cotidianas nas sociedades contemporâneas. Assim, é impossível escapar de, pelo menos, algum tipo de invólucro digital e, por isso, é necessário repensar as relações entre o poder e a propriedade do *hardware* e do *software*.

Em razão dessa assimetria das relações de poder entre usuários e empresas, Jennifer Whitson entende que os invólucros digitais são espaços totalitários; afinal,

[...] a ausência de governo cria oportunidades para a exploração. A democracia, em parte, depende da simetria das relações. Em troca dos votos dos cidadãos, os governos eleitos são obrigados a concretizar a vontade do público, permanecendo responsáveis perante ele. Existe uma simetria de visibilidade, onde os governantes fornecem ao público o acesso às suas deliberações e das regras que são criadas. As regras corporativas, por outro lado, são assimétricas: as decisões e ações das entidades privadas permanecem opacas mesmo que os usuários sejam cada vez mais transparentes aos publicitários e anunciantes (WHITSON, 2010, p. 240).²⁵²

Um dos componentes fundamentais da produção dessa assimetria é o código, ou seja, a estrutura lógica que determina as regras de funcionamento de um sistema e que, salvo raros casos de erros, são tão inescapáveis quanto as leis da física. Tanto a produção quanto o conhecimento exclusivo sobre o modo como o código opera

²⁵¹ Sobre os metadados, ver item 2.5.1.

²⁵² No original: “absence of government creates opportunities for exploitation. Democracy, in part, relies on a symmetry of relations. In exchange for citizens' votes, elected governments are mandated with carrying out the will of the public and remain accountable to the public. There is a symmetry of visibility wherein rulers provide the public with access to their deliberations and the policy they form. Corporate rule is, by contrast, asymmetrical: the decisions and actions of corporate entities remain opaque even as users are rendered increasingly transparent to marketers and advertisers.”

permitem que as empresas de tecnologia tenham poder sobre os indivíduos. A manutenção dos códigos como *segredo*, contudo, remete novamente ao debate bobbio sobre o núcleo duro do poder e os *arcana imperii*²⁵³.

Por fim, é preciso ter cuidado para evitar confundir democracia com o seu simulacro – como ocorre, por exemplo, com a criação de uma página de governança e as “votações” que o *Facebook* realiza antes de algumas alterações dos seus termos de uso²⁵⁴. Para tanto, é preciso entender a diferença que Mark Andrejevik (2007, p. 241) faz entre “interatividade cibernética” e “interatividade democrática”.

Sob tal aspecto, as “votações” do *Facebook* servem para auxiliar publicitários, já que o objetivo da rede social não é criar propostas de deliberação coletiva, mas tornar a coleta de dados em massa mais “palatável” em virtude da falsa ideia de que o usuário participa da definição dos parâmetros do sistema. É possível afirmar, na esteira do que Andrejevic fala sobre o programa *American Idol*, que as votações no *Facebook* são

[...] um convite à participação na própria manipulação através do fornecimento de informações cada vez mais detalhadas sobre preferências sociais, atividades e históricos [entregando-lhes] para quem utiliza esse conhecimento com a finalidade de gerenciar o consumo. [...] as pessoas não apenas pagarão para participar no espetáculo da sua própria manipulação, mas também, graças à promessa de participação, elas irão, às suas próprias expensas, ratificar políticas que beneficiam os interesses das elites no poder. É como se, de alguma forma, o suporte interativo transformasse em seus aqueles interesses (ANDREJEVIC, 2007, p. 242)²⁵⁵.

Com isso, é possível concluir que a assimetria nas relações de poder, a ausência de *accountability* e de transparência fazem com que o ambiente virtual, longe daquilo que é pregado pelas posturas mais otimistas, seja eminentemente antidemocrático. Ao invés de redistribuir o poder na sociedade, a Internet reforça a sua concentração nas mãos de poucos, o que anula o potencial democratizador da

²⁵³ Item 4.1.1.

²⁵⁴ Em virtude do caráter dinâmico das postagens, algo natural ao *Facebook*, é imprescindível remeter à consulta da página de governança da empresa. Disponível em < <http://surveillance.es/2h> >. Acesso em: 28 abr. 2016.

²⁵⁵ No original: “[...] the invitation to participate in one's own manipulation by providing increasingly detailed information about personal preferences, activities, and background to those who would use the knowledge to manage consumption. [...] people will not only pay to participate in the spectacle of their own manipulation, but that, thanks in part to the promise of participation, they will ratify policies that benefit powerful elites and vested interests at their own expense, as if their (inter)active support might somehow make these vested interests their own.”

tecnologia da informação. Diante desse contexto, deve-se pensar quais são os efeitos dessa falta de democracia na proteção dos direitos humanos. Esse é o assunto do próximo segmento deste trabalho.

4.2 SURVEILLANCE E DIREITOS HUMANOS

4.2.1 Notas introdutórias sobre o papel dos Estado na proteção dos direitos humanos violados pela *surveillance*

Face às atuais tecnologias da informação, que permitem a coleta, armazenamento, processamento, análise e transmissão de uma quantidade de dados – pessoais ou não²⁵⁶ – sem precedentes, fica nítido que a *surveillance* coloca em risco os direitos humanos – liberdade, privacidade e, especialmente, igualdade.

Por mais “virtual” que todas essas tecnologias possam ser consideradas, as consequências da presença ou ausência de dados em determinados sistemas são sentidas de maneira real na vida das pessoas. Cada uma delas possui um *data double*, uma espécie de *alter ego* digital, com perfis detalhados das suas vidas, elaborados a partir da análise de dados gerados enquanto os indivíduos se movem pelo mundo e efetuam transações típicas do cotidiano.

Como visto, a *surveillance* oferece uma dupla e paradoxal transparência. As formas de coleta, os critérios de utilização e as regras utilizadas no processamento desses dados atuam de maneira “transparente”, ou seja, são pouco conhecidas ou completamente ocultas.

Por outro lado, os indivíduos têm suas vidas, cada vez mais “transparentes”, uma vez que, constantemente, são produzidas e utilizadas – tanto pelos poderes públicos quanto pelos privados – as informações sobre eles. Essa dupla transparência significa, na realidade, uma relação de (in)visibilidade extremamente desigual, de modo que se conhecem cada vez menos as maneiras como os próprios dados são coletados e quais sentidos são atribuídos àqueles dados.

Como visto, as quase inexistentes tentativas de abordar o tema – pelo menos no cenário jurídico brasileiro – incorrem no mesmo equívoco: o de atribuir traços

²⁵⁶ Embora os fluxos de dados nem sempre sejam pessoais – isto é, não diretamente vinculados a uma pessoa –, podem ser de extrema relevância para a vida humana. Veja-se, por exemplo, o uso de satélites e sistemas computacionais para a previsão do tempo, gerenciamento de colheitas, desmatamento de florestas, monitoramento da qualidade de água, ar etc.

puramente panópticos ao que entendem como “vigilância”. Com isso, uma situação extremamente fluida é solidificada nos limites das relações de “visibilidade” exigidas tanto pelo ideal do panóptico, quanto pela produção de sentido da palavra “vigilância”. As análises jurídicas derivadas desse equívoco teórico, como resultado, limitam-se ao problema da violação da privacidade, ou seja, da esfera íntima individual.

Uma perspectiva para além desse lugar-comum teórico, aqui proposta como teoria da *surveillance*, permite ressaltar que a informação viabiliza a divisão, muitas vezes, antidemocrática, das pessoas em grupos sociais distintos. A categorização dos seres humanos cria barreiras eletrônicas com efeitos reais, capazes de garantir ou impedir o acesso aos elementos indispensáveis para uma vida digna.

Assim, existe uma ambiguidade entre a democracia e a identificação/classificação possibilitada pela *surveillance*. Se, por um lado, a *surveillance* viabiliza o acesso diferenciado a determinados benefícios jurídicos típicos do Estado democrático de direito – basta lembrar, por exemplo, os cadastros dos programas de transferência direta de renda atualmente em vigor no Brasil –, pode, por outro, servir para criar divisões que violam direitos humanos, situação que ocorre quando não há controle democrático dos critérios de classificação.

Tendo em vista que as possibilidades de acesso ou exclusão passaram a ser definidas por sistemas automatizados, são necessárias formas capazes de proteger os direitos humanos contra violações através da tecnologia. No entanto, os modelos de direito e Estado vigentes demonstram pouca habilidade para lidar com conflitos que envolvem as novas tecnologias, intrinsecamente desespacializadas. Logo, vale repetir que não se trata de propor o fim do Estado, mas, pelo contrário, de reconhecer que a coleta e processamento de dados são questões de relevância pública que escapam, em grande parte, ao controle tradicional pelo ente estatal.

As clássicas abordagens dos direitos humanos – por todos, veja-se Luigi Ferrajoli (2007) –, embora reconheçam que tais direitos são violados por atores privados, entendem que os Estados – através da sua constituição política – são capazes de conter as tendências totalizantes de todos os demais sistemas sociais. Contudo, os direitos humanos violados pela *surveillance* não podem ser adequadamente protegidos pelo direito centrado no Estado nacional, o que ficou nítido nos exemplos dos capítulos anteriores.

Os direitos fundamentais podem ser compreendidos como formas de controlar o poder e, desde que surgiram nas cartas constitucionais, permitiram que o sistema político controlasse o poder estatal. Isso aconteceu através da delimitação da sua atuação em outros sistemas sociais. Por isso, a concepção dos direitos humanos como instrumentos capazes de garantir a diferenciação funcional dos sistemas é extremamente relevante para os estudos da *surveillance*. Isso em razão de os conflitos analisados nos capítulos anteriores deixarem claro como o sistema social da tecnologia da informação tende à incessante expansão – que Verschraegen (2011, p. 220) chama de “totalização da sociedade” –, o que afeta negativamente outros sistemas sociais.

Na condição de possibilidade teórica adequada à *surveillance*, Teubner demonstra como os direitos humanos na esfera transnacional podem ser levados a sério sem que, para isso, seja necessário um retorno às teorias centradas somente no Estado e na política, o que é típico da maioria das teorias constitucionais e dos direitos fundamentais. Tal fato é extremamente importante, especialmente em virtude de a *surveillance* viabilizar a violação de direitos humanos fora dos tradicionais *loci* do poder do Estado-nação e dos controles da política, ou seja, na esfera privada, por atores transnacionais.

Isso não demonstra uma “falha” do modelo estatal atual, mas sua limitação, uma vez que ele foi pensado para viabilizar a imposição de limites jurídicos apenas para os poderes políticos, como visto anteriormente na discussão a respeito do surgimento do Estado²⁵⁷. Isso impede, por exemplo, o sucesso das propostas que, de uma forma ou de outra, pretendem efetuar uma mudança de escala do modelo estatal para a esfera global.

Nesse estado da arte, Teubner (2011b) defende a possibilidade de ocorrência de uma autoconstitucionalização dos sistemas autorreferenciados, como é o caso da Internet. Embora ainda não seja tão desenvolvida quanto a economia – *lex mercatoria* –, a *lex digitalis* demonstra ser um caso típico de sistema capaz de criar ele mesmo as suas regras que, com a devida pressão externa, tendem a deixar de ser apenas regras constitutivas – ou seja, que organizam seu funcionamento e formação – para se tornarem também limitativas – isto é, regras capazes de controlar a natureza inerentemente incontrolável do poder.

²⁵⁷ Item 1.1.1 sobre o surgimento Estado

Deve-se, então, propor a seguinte pergunta: como situar corretamente a proteção dos direitos humanos diante dos fenômenos da *surveillance* e dos fluxos globais de dados, especialmente levando-se em conta que a desterritorialidade e a fluidez, características desses fenômenos, desafiam os tradicionais mecanismos de controle jurídico, arraigados na centralidade, exclusividade e territorialidade do Estado-nação? Essa será a temática do restante deste trabalho.

4.2.2 Surveillance como violadora dos direitos humanos

Até o momento, todos os tópicos apresentados sobre a *surveillance* foram capazes de mostrar a habilidade que os computadores têm para violar direitos humanos, especialmente em virtude da sua capacidade de classificar coisas e pessoas com base em critérios pré-estabelecidos.

A ideia de que a *surveillance* tem, como finalidade, a classificação social foi inicialmente desenvolvida por Oscar Gandy Jr, no ano de 1993, quando escreveu sobre o *panoptic sort* – uma “classificação panóptica”. Posteriormente, essa ideia foi aperfeiçoada por David Lyon (1994, 2001, 203a, 2003b, 2007, 2014), para quem a “classificação social’ enfatiza o principal objetivo da *surveillance* contemporânea” (LYON, 2003b).

Como visto nos capítulos referentes ao *data mining*, ao *big data* e às análises preditivas²⁵⁸, os códigos de computadores classificam dados para os mais variados propósitos: desde a criação de perfis sobre qual a melhor estratégia de marketing a ser adotada com um consumidor específico, até a análise de informações que levam um sistema a categorizar alguém como potencial terrorista, como ficou evidente quando se discutiu as *no fly lists*. Consequentemente, é possível afirmar que os códigos de computadores

[...] são portas invisíveis que permitem o acesso ou excluem da participação um grande número de eventos, experiências e processos. As classificações resultantes são desenhadas para influenciar e gerenciar populações e pessoas, afetando direta ou indiretamente as chances daqueles a quem se referem os dados. Os portões e barreiras que contêm, canalizam e classificam populações tornaram-se virtuais (LYON, 2003b)²⁵⁹.

²⁵⁸ Item 3.4.1.

²⁵⁹ No original: “[...] are the invisible doors that permit access to or exclude from participation in a multitude of events, experiences, and processes. The resulting classifications are designed to influence

Na mesma linha de raciocínio, Oscar Gandy Jr. (2010) entende que a discriminação é o resultado de um processo tecnologicamente aprimorado de identificação, classificação e avaliação. As análises estatísticas realizadas por algoritmos acabam por multiplicar situações sociais de discriminação, seja na fila de um banco – para concessão de um empréstimo, por exemplo –, ou na fila de um aeroporto – para determinar qual passageiro não cumpre com determinados critérios de “segurança”.

Da mesma forma, Luigi Ferrajoli entende que as novas técnicas de classificação de dados pessoais produzem um desenvolvimento exponencial de desigualdade, capaz de gerar novas castas sociais e divisões das pessoas em grupos com finalidade discriminatória. Para o referido autor,

a formação, o acesso e a disponibilidade, pela polícia ou pelas empresas, de grandes bancos de dados sobre qualquer indivíduo, incluindo talvez os seus dados genéticos e de saúde, com o seu conjunto de anomalias e de prognósticos ameaçadores, é, na verdade, destinada não somente a operar, no plano econômico e social, como um novo fator de discriminação, colocando em risco vagas de emprego e sistemas de previdência, mas, também, para gerar, no plano cultural e no senso comum, uma nova antropologia da desigualdade (FERRAJOLI, 2007, p. 335)²⁶⁰.

Com efeito, demonstrada a necessidade de superação os modelos panóptico e orwelliano da *surveillance* e a importância de se considerar a participação da iniciativa privada nesse fenômeno, fica evidente que tanto práticas estatais, quanto corporativas da *surveillance* são capazes de gerar desigualdades sociais.

No entanto, o senso comum tende a associar o problema da *surveillance* à privacidade e, raramente, à liberdade²⁶¹. Obviamente, não se trata de um erro, pois, realmente, existe uma ligação óbvia e forte entre a *surveillance* e a privacidade. Todavia, é uma abordagem restrita, pois

and to manage populations and persons thus directly and indirectly affecting the choices and chances of data subjects. The gates and barriers that contain, channel, and sort populations and persons have become virtual.”

²⁶⁰ No original: “La formazione, o l’accesso e la disponibilità, da parte della polizia o delle imprese, di grandi banche dati su ciascun individuo, inclusi magari i suoi dati genetici e sanitari con il loro corredo di anomalie e di prognosi infauste, è infatti destinata non soltanto ad operare, sul piano economico e sociale, come un nuovo fattore di discriminazioni, mettendo a rischio posti di lavoro e sistemi di previdenza, ma anche a generare, sul piano culturale e nel senso comune, una nuova antropologia della disuguaglianza.”

²⁶¹ Veja-se, por todos, o fato de que a igualdade sequer é mencionada no debate público gerado pelas revelações de Edward Snowden.

embora essas questões [de privacidade] continuem sendo importantes, está cada vez mais claro, para muitos, que elas não contam a história completa. Porque a [surveillance], na atualidade, classifica as pessoas em categorias, atribuindo-lhes valor ou risco de uma maneira que possui efeitos reais nas oportunidades das suas vidas. Ocorre uma discriminação profunda, o que transforma a [surveillance] não em um simples problema de privacidade pessoal, mas de justiça social (LYON, 2003a, p. 1).²⁶²

Nesse mesmo sentido, Zygmunt Bauman trata a relação entre o consumo e a criação de divisões sociais (BAUMAN e LYON, 2013) (BAUMAN, 2001). Segundo Bauman, a *surveillance*, especialmente aquela relacionada às *little sisters*, é fundamental para incentivar o consumo no mundo contemporâneo. A Internet possibilita que essa relação entre *surveillance* e consumo se dê de maneira ainda mais forte e invisível, uma vez que a crescente virtualização do comércio implica também a criação de um comércio de outro tipo, muitas vezes, oculto: o de metadados. No mundo digital, cada transação gera uma informação sobre ela mesma, de modo que, além de obter o lucro na venda de produtos, as grandes empresas de varejo na Internet ganham a habilidade de criar perfis diversos sobre cada indivíduo e grupo.

Ao se libertar do panopticismo, a análise da *surveillance* pode compreender como ela se desvinculou do Estado-nação e passou a ser uma característica central da vida contemporânea. Longe de um “*Big Brother*” onisciente, uma infinidade de “*little sisters*” coletam, armazenam, processam e compartilham informações diversas para diversos objetivos centrados no planejamento, previsão e prevenção de condutas a partir de elaboração de perfis de riscos. Por isso, a ideia de

‘classificação social’ enfatiza o viés classificador da [surveillance] contemporânea. Também neutraliza alguns dos supostos aspectos mais sinistros dos processos da [surveillance] (não se trata de uma conspiração com intenções malignas ou de um processo incansável e inexorável)” (LYON, 2003b, p. 13)²⁶³.

²⁶² No original: “While these issues are still significant, it is becoming increasingly clear to many that they do not tell the whole story. For surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice.”

²⁶³ No original: “‘Social sorting’ highlights the classifying drive of contemporary surveillance. It also defuses some of the more supposedly sinister aspects of surveillance processes (it’s not a conspiracy of evil intentions or a relentless and inexorable process).”

A sistemática coleta e processamento dos fluxos de informação possibilita a classificação pouco – ou nada – democrática das pessoas em categorias sociais de seu interesse. Com base na análise das informações de uma troca de e-mails, por exemplo, é possível – sem sequer ter acesso ao conteúdo da mensagem – classificar indivíduos em grupos específicos, classificações estas que possuem consequências significativas para suas vidas.

A categorização dos seres humanos tem, como finalidade, a sua inclusão ou exclusão em determinados grupos. E os critérios para a obtenção e uso dessas informações, reitera-se, não se submetem aos tradicionais controles e limites democrático-territoriais, sendo geridos, tratados e utilizados a partir da ideia de segredo: seja de Estado, seja comercial, visto que tais informações e as análises que delas derivam são consideradas propriedade da empresa que as obtêm e oferece o serviço.

Obviamente, a vida humana seria impensável sem a possibilidade de categorizar pessoas e grupos sociais. Isso é feito instintivamente. Contudo, as novas tecnologias da informação possibilitam que essa categorização ocorra de maneira automática, a partir de algoritmos de computadores cuja função é classificar todas as informações com base em critérios predeterminados pelos seus criadores. Dessarte, é possível entender que tais algoritmos são “portas virtuais” que possibilitam, por meio de vários critérios desconhecidos, quem “entra” e quem “não entra” – em “lugares” físicos ou naqueles, não menos importantes, virtuais, que determinam a elegibilidade para diversos benefícios.

De igual maneira, vale lembrar que a categorização de grupos sociais também não é nenhuma novidade. Trata-se de um processo inescapável da vida humana em sociedade e que teve um maior crescimento a partir da modernidade. Naquele período, porém, os dados coletados eram arquivados e geralmente esquecidos, ou seja, possuíam baixa capacidade de gerar consequências discriminatórias.

Com o surgimento dos *data doubles*, as informações são transformadas em códigos binários extremamente fluidos. Os sistemas de computadores passam, portanto, a ter enorme importância, uma vez que os resultados das análises das pessoas dependem dos critérios estabelecidos nos seus algoritmos²⁶⁴. Em outras

²⁶⁴ O crescimento do uso da surveillance para criar categorias sociais não se deve somente às novas tecnologias disponíveis, mas o contrário, pois estas somente são desenvolvidas em virtude das necessidades sociais. Uma dessas necessidades se dá em virtude da crise do welfare state, cujo

palavras, a decisão final é o resultado da concatenação lógica de um sistema automatizado a partir de critérios previamente estabelecidos no – “famoso” e sempre culpado – sistema.

A ideia de que a *surveillance* seja utilizada como instrumento gerador de desigualdades sociais é sintetizada de forma percuciente por David Lyon, para quem

o fato de que as formas como as nossas vidas são moldadas [...] depende fortemente de quais os tipos de dados que estão disponíveis sobre nós significa que a política da informação é uma área cada vez mais importante para o debate [...] a categorização social afeta as escolhas e as oportunidades das pessoas comuns (LYON, 2007, p. 8).²⁶⁵

Por isso, a simples presença do nome em determinada lista eletrônica pode limitar as ações dos seres humanos e, até mesmo, tolher sua liberdade de ir e vir. Os fundamentos para elaboração dessas categorias permanecem opacos, de modo que, na ausência de mecanismos de proteção, critérios prejudiciais e discriminatórios podem ser facilmente inseridos dentro dos “códigos”, reproduzindo e multiplicando desigualdades.

Além da igualdade, a privacidade é extremamente violada pela *surveillance*. Essa violação é a mais conhecida – seja nos trabalhos científicos, seja nos meios de comunicação – de modo que, para aprofundamento, se remete o leitor às obras que tratam exaustivamente sobre o tema²⁶⁶. Todavia, alguns fenômenos recentes envolvendo a privacidade merecem atenção neste espaço.

desmantelamento “[...] teve, como efeito, a individualização dos riscos. Uma vez que o conceito de Estado de bem-estar envolve o compartilhamento social dos riscos, o inverso ocorre quando esse Estado de bem-estar declina” (LYON, 2007, p. 20). Esse fenômeno alavanca uma busca, cada vez maior, por mecanismos automatizados de classificação social e previsão de riscos.

²⁶⁵ No original: “the fact that the way in which our lives are shaped [...] depends heavily on the kinds of data available about us means that the politics of information is an increasingly important arena for debate. [...] social categorization affects ordinary people’s choices and chances.”

²⁶⁶ Por todos, ver a excelente tese de doutoramento de Vinícius Borges Fortes (2015) sobre o direito fundamental à privacidade e as propostas que o autor faz para a legislação brasileira com base no estudo comparado das leis dos Estados Unidos e da União Europeia. Ao contrário da crítica aqui realizada à maioria dos trabalhos jurídicos sobre o tema, os quais acreditam no retorno ao Estado-nação como forma de controlar em absoluto as tecnologias da informação, Fortes deixa claro que “[...] esta tese não tem por objeto o tema vinculado à teoria do Estado, visto que concentra-se na proposta de incorporação conceitual para a construção normativa brasileira, voltada à proteção da privacidade e dos dados pessoais na internet. Apesar disso, ao tratar do tema da vigilância em massa e da *surveillance*, a pesquisa sugere uma proposta de incorporação conceitual como uma das respostas institucionais de solução parcial, e restrita ao âmbito nacional, dos episódios de vigilância realizados por governos, empresas e indivíduos, convergindo para a tratativa do tema da privacidade e da proteção dos dados pessoais e não para a contradição conceitual da soberania dos Estados frente à natureza transnacional da rede” (FORTES, 2015, p. 152).

Isso acontece porque, sob a perspectiva das *little sisters*²⁶⁷, acaba ocorrendo um desvio daquilo que se entende como privacidade, que deixa de ser considerada um direito fundamental para se transformar uma moeda de troca virtual. Nesse sentido, “[...] os invólucros digitais exemplificam uma mudança na conceituação de privacidade como uma *commodity* a ser trocada por outros bens e serviços [...]” (WHITSON, 2010, p. 234)²⁶⁸

Tal fato é facilmente percebido através da proliferação de diversas empresas gratuitas de busca, redes sociais, e-mails etc., em que os serviços são pagos através da exploração das informações privadas dos usuários. No mesmo sentido é o já mencionado caso do *23andme*. Ora, a diferença entre o preço pago pelo usuário e o verdadeiro custo do teste é compensada pela coleta daquilo que talvez seja a mais privada das informações: o DNA, bloco com todas as “instruções” sobre a composição do indivíduo.

Além disso, as noções de privacidades tendem a vê-la como um direito do indivíduo contra a invasão de um terceiro. Por essa razão, é interessante a visão de Valerie Steeves da privacidade como uma construção de atores sociais através da comunicação intersubjetiva (STEEVES, 2006), o que permite analisar, com melhor nitidez, as situações em que o indivíduo participa voluntariamente de atividades violadoras da privacidade.

Por conseguinte, compreender a privacidade como limite da identidade construído intersubjetivamente possibilita entender a sua violação não apenas como um problema de coleta de dados – com ou sem consentimento –, mas como a abertura do mundo interior dos indivíduos aos olhos dos grandes detentores de poder, que utilizam essa informação especialmente com finalidade publicitária. Essa compreensão impede que a privacidade seja “domesticada”, ou seja, inviabiliza que organizações, sob o manto de “boas práticas” de privacidade – de caráter eminentemente técnico – continuem a praticar a coleta desleal de dados pessoais (LYON, 2015, pos. 2565). Dessa forma,

esse tipo de publicidade levanta sérios questionamentos sobre a natureza da comunicação que é despojada de intersubjetividade. Ela constitui uma invasão da privacidade porque a corporação penetra no espaço privado da criança e extrai dados para finalidades

²⁶⁷ Item 2.3.

²⁶⁸ No original: “[...] digital enclosures exemplify a shift from conceptualizing privacy as a right to conceptualizing privacy as a commodity to be exchanged for other goods and services [...]”.

instrumentais através da manipulação da criança. Essa interação, por definição, não é recíproca, já que as palavras da criança são capturadas pelo observador sem o filtro da interpretação intersubjetiva. A criança não é mais colocada como consumidora interagindo com um vendedor, mas como um amigo conversando com outro, de modo que ocorre o colapso da fronteira entre os papéis – amigo, consumidor, membro da sociedade civil (STEEVES, 2006, p. 186-187)²⁶⁹.

Embora se refira às experiências das crianças, essa análise é facilmente expansível, por exemplo, para os adultos que utilizam serviços de redes sociais. Embora não exista pesquisa sobre o tema, parece justo conjecturar que usuários do *Facebook*, por exemplo, não entendem que a sua relação com aquela empresa é de consumo, mas veem a empresa como uma espécie de confidente, já que são incentivados a fornecer cada vez mais informações sobre como estão se sentindo.

Tanto é assim que, na versão em português da rede social, na tela de publicação de postagens, está escrito “Gostaria de compartilhar algo?”. O usuário é levado a crer que está “dividindo” com os seus amigos quando, na verdade, está fornecendo informações sobre os seu sentimentos e pensamentos. Da mesma maneira, só que sem a utilização de eufemismos, a versão em inglês pergunta incisivamente ao usuário “*What’s on your mind?*”.

As políticas tradicionais de uso da informação privada não podem proteger esse tipo de violação da privacidade, pois não questionam a respeito da validade social das finalidades dessas coletas de dados. Por outro lado, essa proposta de privacidade entendida como comunicação intersubjetiva conecta as práticas de coleta com as consequências sociais, uma vez que reconhece que a privacidade está vinculada à formação da identidade do indivíduo, ou seja, não apenas que é um “espaço” que merece ser “deixado em paz”. Por isso, Steeves acredita que somente o consentimento não é suficiente para validar as práticas violadoras da privacidade no meio virtual. Isso requer a criação de mecanismos que tornem claro que se está

²⁶⁹ No original: “This kind of marketing raises serious questions about the nature of communication that is stripped of inter-subjectivity. It constitutes an invasion of privacy because the corporation penetrates the child’s private spaces and extracts data for instrumental purposes by manipulating the child communicatively. The interaction is, by definition, non-reciprocal; the child’s words are captured by the watcher without the filter of inter-subjective interpretation. The child is no longer situated as a consumer interacting with a salesperson, but as a friend talking to a friend, and the boundary between roles – friend, consumer, anonymous member of civil society – collapses.”

coletando dados com finalidade publicitária – de modo similar ao que já existe hoje em relação à obrigatoriedade de identificar uma peça publicitária como tal²⁷⁰.

Por fim, um último ponto na análise sobre a privacidade diz respeito aos “cavaleiros do apocalipse”, que pregam o seu fim, como foi o caso da afirmação feita, em 1999, por Scott McNealy, o então presidente da *Sun Microsystems*: “*You have zero privacy anyway. Get over it*” (SPRENGER, 1999).

Na realidade, a privacidade não acabou. Muito pelo contrário, em virtude das mudanças na sua natureza, especialmente como resultado do uso dos metadados, é possível afirmar que se trata, na verdade, de uma mudança assimétrica de privacidade, como visto anteriormente. Sob esse enfoque,

a privacidade, muito longe de estar morta, também é o fundamento do valor de toda informação detalhada sobre consumidores e cidadãos. Empresas lucram milhões de dólares ao coletarem informações detalhadas sobre consumidores e alegam que elas são sua propriedade privada. Ao fazer isso, elas impedem que os membros do público tenham acesso à informação que foi coletada sobre eles, invocando o seu próprio direito à privacidade. [...] o retorno da privacidade como uma vingança: descobrimos que é quase impossível aprender o que é feito com toda a informação que coletam sobre nós graças ao escudo da privacidade, alegado pelas empresas, e o do segredo e da segurança nacional, invocados pelos Estados (ANDREJEVIC, 2007, p. 6-7)²⁷¹.

Como resultado, ao invés de se falar sobre o fim da privacidade, deve-se questionar como a iniciativa privada utiliza o argumento da privacidade e da propriedade, ou seja, da proteção daquilo que é privado – no caso, seus algoritmos e bancos de dados – com a finalidade de esconder o seu modo de funcionamento.

Nesse diapasão, qualquer debate sobre privacidade deve levar em consideração a elaboração de legislação de acesso à informação que inclua o setor privado, uma vez que sua ausência gera graves consequências para os direitos humanos. Logo, ainda que diversas críticas tenham sido feitas ao anteprojeto de lei de proteção de dados pessoais, ele é um avanço nesse aspecto, pois viabiliza uma

²⁷⁰ Art. 28 do Código Brasileiro de Autorregulamentação Publicitária: “O anúncio deve ser claramente distinguido como tal, seja qual for a sua forma ou meio de veiculação.”

²⁷¹ No original: “Privacy itself is not only far from dead, it also forms the very basis for the value of detailed information about consumers and citizens. Companies make billions of dollars by gathering detailed information about consumers and claiming it as their private property. In so doing, they prevent members of the public from accessing information that has been gathered about them by invoking their own right to privacy. [...] is the return of privacy with a vengeance: we find it next to impossible to learn what is being done with all of information about us, thanks to the shield of privacy claimed by commercial organizations and that of secrecy and national security invoked by the state.”

maior visibilidade dos dados que a iniciativa privada guarda sobre os indivíduos. Contudo, deve-se sempre ter em mente que a proteção dos direitos humanos violados por esse tipo de tecnologia vai muito além do Estado, como será visto a seguir.

4.2.3 O Estado como palco fragilizado na proteção dos direitos humanos

Por esses motivos, uma teoria dos direitos humanos adequada à *surveillance* não pode depender exclusivamente dos mecanismos e categorias jurídicas tradicionais. Em igual sentido, Steffano Rodotà afirma que “não estamos diante de uma questão de ordem pública, mas de uma nova forma de distribuição do poder” (2014, pos. 541)²⁷².

Isso porque, “[...] logo percebemos a inadequação das tradicionais definições jurídico-institucionais diante dos novos problemas impostos pela realidade dos sistemas informativos atuais” (RODOTÀ, 2008, p. 25). Essas novas relações de poder, para o autor, são desnudadas pela própria rede, como é o caso do *Google*, empresa que o autor italiano não considera somente uma empresa multinacional, mas um poder em si mesmo.

O *Google* é mais poderoso que uma infinidade de Estados nacionais, além de ser um “[...] interlocutor cotidiano de centenas de milhões de pessoas para quem oferece a possibilidade de entrar e mover-se dentro do universo digital. Governa corpos, consciências e e relações sociais” (RODOTÀ, 2014, pos. 695)²⁷³. No entanto, esse poder carece de legitimidade democrática, porque privado. Isso significa que os poderes privados, no contexto da *surveillance*, podem ser facilmente categorizados como “poderes selvagens”, na terminologia de Luigi Ferrajoli (2011a).

As soluções para essa situação, no entanto, não são as mesmas propostas por Ferrajoli, que aposta sempre na posituação – pelo Estado – dos direitos fundamentais através do fortalecimento das constituições ou declarações de direitos. Isso porque “[...] no momento em que se entra em uma dimensão completamente

²⁷² No original: “Non siamo di fronte a questioni d’ordine pubblico, ma a nuove forme di distribuzione del potere.”

²⁷³ No original: “È interlocutore quotidiano di centinaia di milioni di persone alle quali offre la possibilità di entrare e muoversi nell’universo digitale.”

diversa, como a da Internet, mesmo essas aberturas revelam-se totalmente insuficientes” (RODOTÀ, 2014, pos. 718)²⁷⁴.

Rodotà defende a necessidade de que diversos *players* dessa rede de poderes – ainda que em níveis diversos – possam dialogar e desenvolver regras comuns de acordo com um modelo *multistakeholder* e multinível, como é o caso das propostas de Gunther Teubner, a serem trabalhadas nos próximos fragmentos do trabalho. Porém, para Rodotà (2014, pos. 761), a tese de Teubner – ao entender que, na atualidade, predominam as constituições “setoriais”, ou seja, múltiplas constituições civis relacionadas às dinâmicas sociais e econômicas – acaba por fragilizar os direitos humanos. Segundo o italiano, esse modelo de constitucionalismo societário somente reconhece os direitos humanos compatíveis com a lógica econômica, o que ele entende inaceitável para aqueles preocupados com os poderes selvagens privados.

Nessa linha de pensamento, embora Rodotà defenda a existência de uma *Bill of Rights* para a Internet, afirma que esta não deve ser imaginada como uma transposição, para a o mundo virtual das lógicas tradicionais das convenções internacionais e da positivação constitucional dos direitos humanos. Isso ocorre porque,

[...] em virtude da natureza da rede, o reconhecimento dos princípios e direitos não pode ocorrer de cima para baixo. Deve ser o resultado de um processo, de uma grande participação de uma multiplicidade de sujeitos que possam intervir de modo ativo, graças, sobretudo, a uma tecnologia que torna todos capazes de formular um projeto, compará-los, modificá-los, enfim, submetê-los ao controle e à elaboração comum, transferindo para o setor da regulação jurídica as formas e procedimentos típicos do “método wiki”, com o progressivo ajuste e configuração do texto proposto (RODOTÀ, 2014, pos. 734)²⁷⁵.

Sob tal aspecto, ainda que se concorde com Rodotà em relação à necessidade de participação, o autor italiano acaba por cair em uma armadilha muito comum nas leituras que são feitas sobre tecnologias: a de que a solução para os

²⁷⁴ No original: “Ma nel momento in cui si entra in una dimensione completamente diversa, come quella di Internet, anche queste aperture si rivelano del tutto insufficienti.”

²⁷⁵ No original: “[...] conformemente alla natura della rete, il riconoscimento di principi e diritti non può essere calato dall’alto. Deve essere il risultato di un processo, di una partecipazione larga di una molteplicità di soggetti che possono intervenire in modo attivo, grazie soprattutto a una tecnologia che mette tutti e ciascuno in grado di formulare progetti, di metterli a confronti, di modificarli, in definitiva di sottoporli a un controllo e a una elaborazione comuni, di trasferire nel settore della regolazione giuridica forme e procedure tipiche del ‘metodo wiki’, dunque con progressive aggiustamenti e messe a punto dei testi proposti.”

problemas criados por ela é a implementação de mais tecnologias²⁷⁶. É paradoxal que Rodotà, ao mesmo tempo em que reconhece o problema do exercício de poder pela tecnologia e a sua natureza de propriedade privada, aposta na mesma tecnologia ou nas estruturas físicas para a sua utilização – ambas propriedades de alguém – como solução para o problema de falta de democracia criado pela tecnologia da informação.

Essa “aposta” do autor na Internet, como instrumento emancipatório, fica clara quando ele defende uma dualidade entre a tecnologia da informação – supostamente dotada da capacidade de reconstruir um novo modelo de democracia – e as técnicas de *surveillance* –, capazes de viabilizar o controle total dos indivíduos. Nas palavras do autor italiano,

“Orwell in Athens” era o feliz título de um livro que buscava colher a tensão permanente entre todos os sistemas democráticos de difusão do poder e os controles sobre os cidadãos, que a dimensão identificada das inovações tecnológicas desvela e enfatiza de maneira particularmente evidente. [...] Isto é, às tecnologias da informação e da comunicação é confiada a tarefa de construir uma nova democracia dos cidadãos; às técnicas de vigilância é confiada a tarefa de construir o controle capilar sobre os cidadãos. Precisamente a passagem da Web 1.0 para a Web 2.0, das redes sociais, criaram uma nova dimensão da relação entre a democracia e o direto. Foram enriquecidas as possibilidades de ação organizada, não apenas e não somente em termos de quantidade, mas também em relação à qualidade dos indivíduos que agora são capazes de articular as relações sociais de uma nova maneira e, juntos, criar formas variadas de ação política (RODOTÀ, 2014, pos. 97)²⁷⁷.

Não obstante, deve ter ficado claro até o momento que a Internet não é, exclusivamente, um instrumento emancipatório. Muito pelo contrário: as ideias de filtro-bolha, por exemplo, tendem a diminuir os traços democratizantes da tecnologia da informação. Considerando que as interações sociais ocorrem dentro de uma

²⁷⁶ Existe uma corrente nitidamente otimista a respeito do papel da tecnologia na democratização, como é o caso das perspectivas de e-governo e cyberdemocracia. Como visto, salvo raras exceções, não se compactua com essas correntes teóricas, especialmente por entender que a democracia não pode ser alcançada a partir de debates que dependem de estruturas – de *hardware* e *software* – eminentemente privadas para o seu funcionamento.

²⁷⁷ No original: “Orwell in Athens era il felice titolo di un libro che voleva cogliere una tensione permanente in tutti i sistemi democratici tra diffusione del potere e controlli sui cittadini, che la dimensione individuata dalle innovazioni tecnologiche disvela ed enfatizza in maniera particolarmente evidente. [...] Vale a dire, alle tecnologie dell’informazione e della comunicazione viene affidato il compito di costruire dal basso una nuova democrazia dei cittadini; alle tecniche della sorveglianza viene affidato il compito di costruire dal basso il controllo capillare sui cittadini. Proprio il passaggio dal Web 1.0 al Web 2.0, quello delle reti sociali, ha attribuito una dimensione nuova al rapporto tra democrazia e diritti. Si sono arricchite le possibilità di azione organizzata, non solo e non tanto dal punto di vista quantitativo, quanto piuttosto per la qualità dei soggetti che sono ormai in grado di articolare in modo nuovo le relazioni sociali e, insieme, di dar vita a forme variegiate di azione politica.”

estrutura privada – como é o caso do *Facebook* e do *WhatsApp* –, cujo objetivo é a coleta e a monetização das informações dos seus usuários, as capacidades democráticas da Internet devem ser vistas com certo ceticismo.

Ainda sobre o trecho acima, é possível perceber que Rodotà, inadvertidamente, contrapõe a tecnologia – “essencialmente” boa – com aquilo que aqui se denomina *surveillance* – que seria “essencialmente” má. Como visto anteriormente, além ser impossível separá-las, tecnologia da informação e *surveillance* não são “naturalmente” positivas ou negativas. Sistemas de coleta e análise de dados, inclusive de criação de perfis, são utilizados, cotidianamente, para melhorar a qualidade de serviços prestados tanto pela iniciativa pública quanto pela privada. Assim, a *surveillance* também serve para otimizar o uso de recursos, sendo descabido associá-la como algo inerentemente negativo. Por todos, veja-se o uso da *surveillance* para prevenção de doenças ou até mesmo as interessantes e relevantes sugestões de livros fornecidas pela *Amazon*. Embora seu objetivo seja aumentar o lucro da empresa, certamente, há ganho para o usuário quando ele recebe sugestões de leitura que irá apreciar.

Além desse maniqueísmo, a tese de Rodotà parece apostar em uma inclusão digital generalizada, o que dificilmente pode ser considerado verdade, especialmente se for avaliado que apenas 57.6% dos brasileiros possuíam acesso à Internet no ano de 2015 (INTERNATIONAL BANK FOR RECONSTRUCTION AND DEVELOPMENT, 2016). Ainda que esse número fosse maior, é de se questionar se uma população carente dos mais básicos direitos humanos – como a brasileira – seria capaz de gerir um tipo de construção democrática no formato *wiki*.

Por outro lado, o autor italiano percebe, corretamente, que os questionamentos jurídicos tradicionais – ou seja, “quem é o legislador?” e “que tribunal irá aplicar os direitos proclamados na era digital?” – são incompatíveis com os mecanismos criadores dos direitos vinculados à tecnologia da informação e, por isso, ultrapassam os tradicionais limites estatais de controle.

Com base nisso, é possível estabelecer um paralelo entre a ideia de Rodotà sobre o papel das instituições existentes na construção do “novo” cenário jurídico-democrático no contexto da rede de poderes e a proposta de Saskia Sassen, apresentada anteriormente, sobre a reconstrução das capacidades das instituições existentes. Afinal, para o autor italiano, esse novo mundo sem fronteiras –

protagonizado pela Internet – “[...] acontece em um contexto no qual as instituições tradicionais não são expurgadas, mas contribuem para um compromisso de renovação que, simultaneamente, pode modificar e reforçar o seu papel” (RODOTÀ, 2014, pos. 749)²⁷⁸.

O autor italiano toca no ponto fulcral da problemática da criação de direito no Estado em rede quando questiona sobre a possibilidade de, em uma sociedade caracterizada por essa topologia sem centro definido, ainda se fazer referência a uma formação institucional – como é o caso do Estado – que não apenas necessita da criação de regras comuns a todos os seus membros, mas também centraliza a produção normativa e decisória.

Como resultado, Rodotà compreende que se está diante de novos fenômenos, cujos efeitos nocivos para a democracia e os direitos humanos não possuem uma resposta adequada nos mecanismos jurídicos tradicionais. Isso em razão de a aposta na centralização da produção jurídica não ser mais uma forma efetiva de proteção da democracia e dos direitos humanos.

Ainda que as novas tecnologias tendam a gerar um movimento centrípeto, é possível, como visto anteriormente na descrição do modelo de sociedade em rede de Manuel Castells²⁷⁹, a predominância de determinados nós na topologia da rede, o que ocorre sempre de modo precário. Essa maior importância – chamada de “centralização” por Rodotà – não é incompatível com a ideia de uma rede. A causa disso é que

[...] as novas tecnologias da informação e da comunicação não produzem somente efeitos de policentrismo, de dispersão “dos poderes soberanos entre diferentes atores, entre eles não hierarquizados e que não insistem sobre o mesmo território”, mas também uma possibilidade sem precedentes de centralização, como demonstra a experiência de diversos países, sobretudo no que diz respeito à criação de sistemas totais de vigilância (RODOTÀ, 2014, pos 772)²⁸⁰.

²⁷⁸ No original: “[...] accade in un contesto in cui le istituzioni tradizionali non vengono tagliate fuori, ma contribuiscono a una impresa di rinnovamento che, al tempo stesso, può mutare e rafforzare il loro ruolo.”

²⁷⁹ Item 1.4.1.

²⁸⁰ No original: “[...] le nuove tecnologie dell’informazione e della comunicazione non producono soltanto effetti di policentrismo, di dispersione “dei poteri sovrani fra attori diversi tra loro non gerarchizzati e che non insistono sul medesimo territorio”, ma anche possibilità senza precedenti di centralizzazione, come dimostra l’esperienza di diversi paesi soprattutto per quanto riguarda la creazione di sistemi di sorveglianza totale.”

Por esse motivo, Rodotà entende que se está adentrando em um tempo cujas características não podem ser descritas pelos mecanismos forjados na modernidade, especialmente aqueles derivados do Estado e da democracia representativa. Essas mudanças, no entanto, não garantem que o cenário a ser posto será o de uma “pós-democracia”, até mesmo porque essa terminologia não resolve os problemas oriundos das novas tecnologias da informação no âmbito democrático. Como resultado, ele questiona se não seria o caso de “[...] nos perguntarmos, na realidade, se não estamos correndo o risco de uma regressão em direção à pré-modernidade” (RODOTÀ, 2014, p. 780)²⁸¹.

Assim como Saskia Sassen, Rodotà não acredita que se trate de um retorno ao medieval. Na realidade, ele critica, com veemência, aqueles que associam a descentralização do poder na sociedade em rede com uma espécie de situação neomedieval. Esse tipo de conclusão, afirma, é consequência de uma “[...] fraqueza do pensamento político e jurídico que, diante da crise da soberania nacional e do nascimento de uma complexa organização supranacional, é incapaz de elaborar categorias interpretativas adequadas, refugiando-se naquelas do passado” (RODOTÀ, 2014, pos. 790)²⁸².

Sob esse aspecto, concorda-se com Rodotà quando ele afirma que o direito não pode fingir que nada está acontecendo na relação entre Estado, direito e tecnologia; afinal, o direito não pode ser indiferente às inovações trazidas pela *surveillance*. Como resultado, o direito não pode se valer de “[...] critérios hermenêuticos pré-tecnológicos, acreditando que a inovação pode ser conhecida e assume relevância somente quando adentra no universo jurídico” (RODOTÀ, 2014, pos. 806)²⁸³. Por essa razão, o referido autor entende que perde sentido a distinção entre “novo” e “velho”, uma vez que os direitos e liberdades fundamentais só podem ser protegidos, no contexto da *surveillance*, através de uma completa releitura do catálogo de direitos fundamentais elaborados pelo constitucionalismo moderno.

²⁸¹ No original: “Dobbiamo chiederci, infatti, se non si stia correndo anche il rischio di una regressione verso la premodernità.”

²⁸² No original: “[...] debolezza del pensiero politico e giuridico che, di fronte alla crisi della sovranità nazionale e alla complessa nascita di una organizzazione sovranazionale, non è capace di elaborare categorie interpretative adeguate e si rifugia in quelle del passato.”

²⁸³ No original: “[...] criteri ermeneutici pretecnologici e ritenendo che l’innovazione possa essere conosciuta, e assumere rilevanza, solo quando s’incarna in apposite e diverse situazioni giuridiche.”

Em razão disso, as tentativas de “subsumir” as novas tecnologias aos direitos elaborados através de Estados possuem sucesso limitado – ainda que sejam imprescindíveis. Um exemplo recente disso é o caso da justiça brasileira e o aplicativo *WhatsApp*, de propriedade do *Facebook*.

Em 1º de março de 2016, o vice-presidente do *Facebook* na América Latina foi preso pela Polícia Federal em São Paulo (FAGUDEZ; SERRA, 2016). A prisão ocorreu em virtude de a empresa ter se negado a cumprir as determinações da justiça do estado de Sergipe, que solicitava a quebra de sigilo das mensagens trocadas por investigados de participação no crime organizado. O *WhatsApp* alegou, em síntese, que, por não armazenar, em seus servidores, as mensagens trocadas pelos usuários, não seria possível quebrar o sigilo das comunicações, como queria a justiça brasileira. O Poder Judiciário, no entanto, negou-se a aceitar as justificativas da empresa e passou a aplicar pesadas multas, incluindo o bloqueio de valores das contas do *Facebook* no Brasil²⁸⁴.

Embora as tecnologias da informação modifiquem completamente o papel do direito estatal na proteção da democracia e dos direitos humanos, as situações que se apresentam, embora inéditas, não são desconhecidas, afinal, estão acontecendo a todo instante, modificando-se com incrível velocidade. Tais processos devem ser, antes de tudo, compreendidos e, justamente em virtude do seu ineditismo, isso não pode ser feito através dos mecanismos existentes.

Assim, é imprescindível aceitar que o Estado, nos moldes em que é conhecido, é insuficiente para a proteção dos direitos humanos. Deve-se pensar, portanto, em modalidades democráticas de elaboração de controles capazes de “domar” os poderes selvagens associados à tecnologia da informação. Por óbvio, não se pode importar a solução dada por Luigi Ferrajoli no sentido de que a democracia e os direitos fundamentais só podem ser protegidos “[...] pela introdução e reforço das garantias constitucionais e legislativas adequadas” (FERRAJOLI, 2011a, p. 107)²⁸⁵.

²⁸⁴ Talvez como resposta à justiça brasileira, em 05 de abril de 2016, o *WhatsApp* passou a utilizar criptografia ponto a ponto, de modo que, ainda que eventual comunicação seja interceptada pela justiça, ela só poderá ser decodificada pelos aparelhos celulares dos participantes da conversa. Ver a matéria de Camila Costa para o jornal BBC Brasil. Disponível em: < <http://surveillance.es/24> >. Acesso em: 13 abr. 2016.

²⁸⁵ No original: “[...] por la introducción y el reforzamiento de garantías constitucionales y legislativas adecuadas.”

Isso se deve ao fato de que, embora seja possível afirmar que, no caso da *surveillance*, também se tratam de poderes selvagens, o problema que Ferrajoli buscava solucionar – a fragilização da democracia constitucional em virtude do “berlusconismo” – ocorria dentro das estruturas tradicionais do Estado. Os problemas da crise da democracia e do Estado derivados da *surveillance*, por outro lado, são externos às estruturas estatais, sendo impossível solucioná-los a partir do interior das instituições estatais.

As respostas dadas por Rodotà para esse problema parecem ser insuficientes. O autor aposta na possibilidade de proteção dos direitos humanos por uma “comunidade global de tribunais” (RODOTÀ, 2014, pos. 825), capazes de agregar a sociedade civil organizada e, com referência aos documentos internacionais, elaborar garantias concretas aos direitos humanos. Além disso, o autor italiano defende que alguns valores básicos da Internet devem ser preservados – embora não indique como isto possa ser realizado.

Como resultado, Rodotà também propõe a proteção da Internet contra o exercício do poder privado. Para ele, a lógica da propriedade da Internet – ou, especificamente, das suas estruturas físicas e lógicas – não pode ser utilizada para diminuir o seu aspecto democrático. Nesse sentido, as propostas do autor são similares àquelas de Luigi Ferrajoli, que identifica o problema na tendência que os sistemas jurídicos atuais têm em conjugar liberdade e propriedade como se ambos fizessem parte do mesmo grupo de direitos.

Ambos os autores concordam que a polissemia da expressão “direito de propriedade” pode induzir ao erro de considerar, como se fossem a mesma coisa, “[...] o direito de se tornar proprietário e de dispor dos próprios direitos de propriedade [...] [e também o] concreto direito de propriedade sobre aquele ou este bem [...]” (FERRAJOLI, 2011b, p. 19). A confusão entre direitos fundamentais e direitos patrimoniais, dirá Luigi Ferrajoli, é um grande equívoco teórico que trouxe resultados políticos negativos tanto para o pensamento liberal, com a valorização da propriedade a ponto de torná-la equivalente à liberdade, quanto para a teoria marxista, que, através da mesma equiparação, desvalorizou o direito de liberdade como um “direito burguês”.

Embora as propostas de Ferrajoli e Rodotà possibilitem a diferenciação entre propriedade dos meios físicos e digitais – *hardware* e *software* – e os direitos humanos atingidos pela *surveillance*, é impossível negar que o poder econômico exerce forte

pressão na dinâmica da Internet. Isso porque, como visto anteriormente, é justamente esse poder econômico que melhor explora a *surveillance* com a finalidade de maximizar os lucros, sendo impossível ignorar essa realidade.

Por essa razão, devem ser analisadas perspectivas teóricas alternativas, como é o caso das propostas de constitucionalismo societário e os impactos dos direitos humanos no espaço transnacional, de Gunther Teubner. O aparato teórico proposto por Teubner parece ser mais adequado para compreender os imbrólios ocasionados pela *surveillance* no universo do direito, especialmente em virtude de se deslocar das perspectivas tradicionais que pensam os problemas transnacionais, exclusivamente, a partir de perspectivas que dependem do Estado nacional – ou da sua aplicação em escala global.

Como visto no item relativo à democracia, a manutenção de estruturas que possibilitam a assimetria nas relações de visibilidade fragiliza o regime democrático e coloca em risco os direitos humanos. Por isso, torna-se necessária a construção de mecanismos adequados para lidar com as perplexidades das novas tecnologias, utilizadas pelos poderes tanto públicos quanto privados. Ainda que, a princípio, isso demonstre o fortalecimento de alguns Estados – em virtude, especialmente, do controle da tecnologia da informação –, parece claro que, como resultado da multiplicidade dos atores envolvidos na *surveillance*, há a fragilização das tradicionais estruturas de proteção dos direitos humanos e da democracia.

Não é nenhuma novidade que a democracia ainda não encontrou – se é que encontrará – lugar dentro das empresas privadas, nem mesmo na sua forma mais básica, ou seja, como procedimento. Além disso, o atual processo de apropriação privada da internet (SASSEN, 2006) estimula a formação de espaços virtuais que possuem cada vez mais importância na vida das pessoas, mas cujas regras não estão submetidas ao controle democrático.

Em um mundo globalizado e sempre mais digital, demonstra-se extremamente difícil submeter essas empresas aos diversos interesses nacionais. Como resultado, cada vez mais espaços da vida humana estão confinados nos limites privados das empresas²⁸⁶, onde a democracia é irrelevante.

²⁸⁶ Para um exemplo de como a estrutura da Internet é privada, vide a batalha entre *Comcast* e *Netflix* em virtude de aquela cobrar um ‘pedágio’ para que os usuários desta pudessem utilizar o serviço sem restrições. Essa situação, contudo, não poderia acontecer caso as empresas estivessem no Brasil, visto que o art. 9º do Marco Civil da Internet estabelece que “o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem

É de extrema importância reiterar que, ao contrário do que alguns mais otimistas acreditam, a Internet não é um “lugar” público e democrático. Isso em razão de ser dominada pela iniciativa privada, seja sob uma perspectiva das estruturas físicas (servidores, cabos de fibra ótica, satélites etc.); seja sob o ponto de vista do software (websites, sistemas operacionais, navegadores, protocolos de comunicação).

Até mesmo do ponto de vista da esfera pública, é retirada a possibilidade de controle democrático do uso das tecnologias da informação por parte daqueles que a ela estão sujeitos. Essa situação ficou clara recentemente, uma vez que, por maior que fosse possibilitada a participação dos cidadãos estadunidenses nos eventos divulgados por Edward Snowden, indivíduos de todos os lugares do mundo são afetados pelos sistemas de coleta de dados desenvolvidos pelo governo dos EUA. Pessoas que vivem fora das fronteiras dos EUA não podem participar democraticamente da gestão dos sistemas *PRISM*, *Fairview*, *Upstream*, *XKeyscore* etc. Os senadores daquele país, como é óbvio, não foram eleitos, por exemplo, pelos brasileiros, mas, ainda assim, estima-se, estes tiveram cerca de 2,3 bilhões²⁸⁷ de telefonemas e mensagens interceptadas pela NSA.

Para monitorar o fluxo de dados de residentes ou empresas instaladas nos Estados Unidos, a NSA precisa de autorização da *Foreign Intelligence Surveillance Court*. A situação fica ainda pior para aqueles que não são cidadãos ou que estão fora das fronteiras dos EUA, pois o monitoramento passa a ser feito sem necessidade de ordem judicial. Não obstante, o sistema utilizado em ambas as situações é o mesmo, situação que demonstra a facilidade que a tecnologia da informação tem para ignorar fronteiras jurídicas e políticas.

Esse aspecto extranacional da *surveillance* também é disseminado de maneira indireta, uma vez que, no mundo real, existe pouca possibilidade de reação por parte de qualquer Estado nacional, inclusive dos mais fortes. Isso ficou claro, conforme demonstrado anteriormente²⁸⁸, na (falta de) força das respostas tanto do

distinção por conteúdo, origem e destino, serviço, terminal ou aplicação”. Sobre a discussão nos EUA, ver a matéria de Victor Luckerson para a revista *Time*. Disponível em: < <http://surveillance.es/2f> >. Acesso em: 27 abr. 2016.

²⁸⁷ Este número foi obtido através da análise, feita por jornalistas, dos documentos vazados por Snowden. Para acesso aos documentos, ver a matéria Glenn Greenwald, Roberto Kaz e José Casado para o jornal O Globo. Disponível em: < <http://surveillance.es/2e> >. Acesso em: 26 abr. 2016.

²⁸⁸ Item 1.5.3.

Brasil em relação ao *PRISM* – que resultou em uma conversa diplomática – quanto da União Europeia em relação ao *ECHELON* – cuja resposta foi a elaboração de um relatório do Parlamento Europeu.

Tudo isso culmina com um dos mais problemáticos pontos na relação entre *surveillance* e democracia: o papel fundamental do poder privado no desenvolvimento e utilização de mecanismos de gerenciamento de dados²⁸⁹. Isso demonstra a imprescindibilidade do questionamento democrático a respeito da *surveillance* e da busca, por parte do direito, de instrumentos capazes de lidar com essas perplexidades da democracia no mundo líquido da tecnologia da informação.

Por estarem fundamentadas na centralidade e territorialidade do Estado-nação, as respostas tradicionais demonstram-se incapazes para, sozinhas, exercerem sua função no contexto da transformação do poder na era do *bit*. Na sociedade em rede, o poder adquire grande fluidez e passa a atuar, de modo descentralizado e desespacializado, na tentativa de definir, controlar e limitar o ser humano.

Essas circunstâncias exigem a superação da fórmula dogmatizada do Estado através de estruturas cuja porosidade seja compatível com a liquidez do mundo, mas, seguindo os avisos de Jose Luis Bolzan de Moraes, “[...] sem perder de vista as consequências de tais possibilidades, assim como o papel fundamental das estruturas públicas estatais no contexto das sociedades periféricas o enfrentamento das desigualdades [...]” (BOLZAN DE MORAIS, 2012, p. 35). Nesse sentido, o direito precisa de respostas igualmente descentralizadas, sob pena de tornar-se obsoleto. Esse será o tema do próximo item.

4.3 SURVEILLANCE E CONSTITUCIONALISMO PARA ALÉM DO ESTADO-NAÇÃO

4.3.1 Constituição para além do Estado nacional: notas sobre o constitucionalismo societário

Uma interessante perspectiva para a análise de como pode atuar o direito diante da *surveillance* no mundo globalizado é aquela trazida por Gunther Teubner. Em texto escrito junto com Anna Beckers (2013), os autores utilizam a história de

²⁸⁹ Vale ressaltar o fato de que os reais responsáveis pelo desenvolvimento e utilização dos sistemas de associados à NSA são empresas privadas por ela contratada, gigantes da telemática como *Booz Allen Hamilton* e *Dell Corporation*.

Ulisses e as sereias para demonstrar a necessidade de uma análise dos direitos humanos que não esteja centrada no controle do poder exercido pelo Estado.

Em síntese, o recurso à história de Ulisses e o canto das sereias permite verificar que, através da imposição prévia de um acordo que não pode ser desobedecido nem mesmo por aquele que o estabelece – ou seja, através da criação de uma Constituição – se pode atingir não apenas a sobrevivência, mas um grau superior de liberdade – que, no caso de Ulisses, permitiu que ele não apenas permanecesse vivo, mas desfrutasse o belo canto das sereias.

No entanto, diferentemente da maioria dos juristas que utiliza a metáfora de Ulisses para ilustrar a importância do constitucionalismo, Teubner e Beckers percebem que não existe apenas uma sereia cantando para Ulisses. Como resultado, eles entendem que

o maior erro do Estadocentrismo na teoria e prática constitucional é que ele apenas cuida de uma tentação. Concentrar nos excessos do poder estatal significa ignorar tentações de todas as outras sereias. Não apenas Thelxiepia, mas também Molpe, Aglaope, Pisinoe, Parténope, Ligéia, Leucosia, Raidne e Teles tentam encantar a tripulação de Ulisses com as suas vozes sedutoras. De maneira similar, os perigos constitucionais não são apenas criados pelo poder, mas também pelo dinheiro, conhecimento, tecnologia e medicina. Atualmente, os maiores conflitos constitucionais não são apenas relacionados à constituição estatal, mas também às várias constituições na sociedade global [...] A sociedade pós-moderna está exposta às tendências expansiva, até mesmo totalitária, de uma variedade de racionalidades parciais: monetização, mercantilização, cientificação, juridificação e medicalização (BECKERS e TEUBNER, 2013, p. 524)²⁹⁰.

Logo, há de se reconhecer que o modelo de direitos humanos baseado somente na proteção contra a violação do Estado só funciona enquanto o Estado é identificado com a sociedade, ou, ao menos, quando o Estado é visto como a forma de organização da sociedade, e a política é entendida como sua forma de coordenação hierárquica.

²⁹⁰ No original: “The great error of state centrism in constitutional theory and practice is that it only addresses one temptation. Concentrating on the excesses of state power meant turning a blind eye to the manifold other sirenic temptations. Not only Thelxiepia, but also Molpe, Aglaophonos, Peisithoe, Parthenope, Ligeia, Leucosia, Raidne, and Teles try to lure Ulysses’ crew with their seductive voices. Similarly, constitutional dangers are not only created by power but also by money, knowledge, technology, and medicine. Today, the great constitutional conflicts are not only about the state constitution but also about the many constitutions within global society. [...] Postmodern society is exposed to expansive, even totalitarian, tendencies of a variety of partial rationalities: monetarization, commodification, scientification, juridification, and medicalization.”

Quando outros *medium* de comunicação altamente especializados – como é o caso da tecnologia da informação – adquirem autonomia em relação ao Estado, esse modelo torna-se insuficiente para proteção dos direitos humanos. Como resultado, esses direitos não podem ser limitados às relações entre o indivíduo e o e o Estado. Por esse motivo,

a questão dos direitos humanos, no seu sentido mais estrito, deve ser vista hoje como o comprometimento da integridade do corpo e da mente dos indivíduos por uma multiplicidade de processos comunicativos que são anônimos, autônomos e, atualmente, globalizados. A fragmentação da sociedade mundial em subsistemas autônomos cria não apenas novas fronteiras, fora da sociedade, entre o subsistema e o ser humano, mas também novas fronteiras entre os vários subsistemas dentro da sociedade, cujas tendências expansionistas funcionam de modo específico (TEUBNER, 2011b, p. 211)²⁹¹.

Em razão disso, ainda que os direitos humanos oriundos das constituições estatais funcionem como modelo para os seus equivalentes transnacionais, não se deve pensar que se trata de viabilizar a “expansão” dos direitos humanos estatais para o contexto transnacional. Isso se deve ao “[...] fato de que decisões e argumentações no sistema legal formam ciclos fechados, que podem muito bem se irritarem reciprocamente, mas que não se fundem” (TEUBNER, 2011b, p. 192-193)²⁹².

Somente afirmar que ocorre a “expansão” dos direitos estatais para outra esfera não explica nada sobre como os direitos humanos adquirem poder normativo nos regimes transnacionais. Isso exige um ato de validação através dos processos legislativos institucionalizados nessa esfera, o que não ocorre com a simples transferência de “escala”, ou, seja,

nunca é demais enfatizar que é a atividade de tomada de decisões dos próprios regimes transnacionais que valida os direitos fundamentais nas suas fronteiras. Logo, acima e além da positivação estatal, a positivação “social” dos direitos fundamentais é a força motora por trás da sua universalização (TEUBNER, 2011b, p. 195-

²⁹¹ No original: “The human-rights question in the strictest sense must today be seen as endangerment of individuals’ integrity of body and mind by a multiplicity of anonymous, autonomised and today globalised communicative processes. The fragmentation of world society into autonomous subsystems creates not only new boundaries outside society between subsystem and human being, but also new boundaries between the various subsystems inside society, on which the expansionist tendencies of the subsystems work in their specific ways.”

²⁹² No original: “[...] fact that decisions and argumentations in the legal system form closed cycles, which may well be reciprocally irritating but do not merge one another.”

196)²⁹³.

Tal fenômeno ocorre através da simultânea generalização – ou seja, a separação da constituição das vicissitudes do sistema político e estatal – e da reespecificação – isto é, a transposição da constituição para o sistema social da tecnologia. Trata-se, contudo, de tarefas delicadas “[...] em virtude da grande interpenetração dos aspectos constitucionais e políticos”, bem como por causa “[...] das peculiaridades do subsistema, suas operações, estruturas, *media*, códigos e programas específicos que requerem um abrangente repensar das instituições constitucionais” (TEUBNER, 2004)²⁹⁴.

Por essa razão, a crítica de Teubner e Beck é extremamente relevante para o debate da *surveillance*; afinal, os direitos humanos são constantemente violados por uma infinidade de atores ligados à tecnologia da informação e não apenas pelos Estados, como ficou claro na análise de como o paradigma das “*little sisters*” sobrepõe-se ao do “*Big Brother*”. Assim como o canto das sereias, o caráter sedutor das vantagens e facilidades de um mundo “facilitado” pela *surveillance* produz um benefício imediato que, muitas vezes, têm consequências negativas posteriores.

Por óbvio, a aposta no constitucionalismo societário não significa a proposição do fim do constitucionalismo tradicional – apenas a sua adaptação ao novo cenário de forças existentes, em razão de o constitucionalismo societário reconhecer a existência dos “momentos constitucionais”, ou seja, aquele instante de crise tão aguda que a única saída é a mudança radical. Esse é o caso, por exemplo, da Declaração Universal dos Direitos Humanos de 1945, que surgiu como resposta às atrocidades cometidas pelos regimes totalitários. Essa crise ocorre de modo similar à estrutura que Thomas Kuhn (1998) criou para explicar as mudanças de paradigmas na ciência, ou seja, as distorções contrárias ao paradigma em vigor vão se acumulando, paulatinamente, até chegar ao ponto em que acontece o colapso do paradigma em virtude da sua impossibilidade de explicar a imensa quantidade de anomalias.

²⁹³ No original: “It thus cannot be emphasised strongly enough that it is the decision-making practice of transnational regimes themselves that is sufficient to validate fundamental rights within their borders. Thus, above and beyond state positivisation, the ‘social’ positivisation of fundamental rights is the driving force behind their universalisation.”

²⁹⁴ No original: “[...] in view of the close interpenetration of constitutional and political aspects [...] the peculiarities of the sub-system, its specific operations, structures, media, codes and programmes require a far-reaching rethinking of constitutional institutions.”

Não obstante, o constitucionalismo societário reconhece que esses momentos constitucionais ocorrem em outros lugares, ou seja, além da política tradicional. Isso porque, em todos esses outros *loci*, “[...] desenvolve-se um grande crescimento das energias que são excessivamente ambíguas na sua produtividade e no seu potencial destrutivo” (BECKERS e TEUBNER, 2013, p. 526)²⁹⁵. Os autores fazem menção às crises do sistema bancário mundial dos anos de 1929 e 2008, que desencadearam, no mundo, reações dos movimentos sociais na busca pela criação de uma constituição mundial que regulasse o setor. Além disso, também consideram que o ano de 2011, em virtude do desastre na usina termonuclear de *Fukushima*, foi um “momento constitucional” em virtude do maior enfoque ao problema das matrizes energéticas nucleares.

Mais importante: para fins deste trabalho, Beckers e Teubner afirmam que “estamos esperando que o momento constitucional ocorra no mundo digital. As manipulações de dados do *Google* e do *Facebook* parecem avisos antecipados” (2013, p. 526)²⁹⁶. Para os mais esperançosos, o caso das revelações de Edward Snowden poderia ter potencial para ser considerado o *tipping point* – apropriando-se da expressão de Saskia Sassen (2006) – para o surgimento do momento constitucional do mundo virtual. No entanto, como ficou claro, isso não ocorreu por uma série de fatores, especialmente em virtude de a situação não ter causado comoção social, vez que colocada apenas como um dualismo do tipo “privacidade vs terrorismo”.

A transformação da crise em um momento constitucional exige, simultaneamente, controles internos e externos dos participantes, o que não ocorreu no caso da *NSA* e das grandes empresas de tecnologia. Além disso, a resposta que se procurou dar ao redor do mundo foi a de que se deveria apostar no fortalecimento da função estatal no controle dos fluxos de dados – veja-se, por todos, os debates sobre a CPI da espionagem, demonstrados anteriormente²⁹⁷. Esse tipo de postura é exatamente oposta àquilo que Teubner propõe para quando houver o surgimento de um momento de colapso. Conforme o autor,

²⁹⁵ No original “[...] develop massive growth energies that are excessively ambiguous in their productivity and in their destructiveness.”

²⁹⁶ No original: “And we are waiting for the constitutional moment to occur in the digital world. Google and Facebook’s data manipulations sound like early warnings.”

²⁹⁷ Item 15.3.

quando os processos em um subsistema social saem do controle dessa maneira, uma escolha deve ser feita entre a intervenção estatal e a constitucionalização. Após as experiências do totalitarismo político do último século, a permanente subordinação ao Estado não é uma opção [que deva ser] seriamente discutida. Uma ordem constitucional global precisa encarar o seguinte desafio: como pode a pressão externa suficiente ser exercidas sobre os subsistemas de modo que se torne eficaz a autolimitação dos seus possíveis cursos de ação? (TEUBNER, 2011a, p. 224-225)²⁹⁸.

A autovinculação interna da teoria do constitucionalismo societário não necessita, contudo, da motivação voluntária dos atores sociais para o autocontrole, até mesmo porque acreditar “[...] que essas regras de autolimitação são desenvolvidas voluntariamente implicaria [na aceitação] de um falso idealismo e sobrestimaria o potencial que a autorregulação possui para resolver estes conflitos constitucionais” (BECKERS e TEUBNER, 2013, p. 527).

Afinal, no mundo real, ainda que os responsáveis pelos momentos de crise – como é o caso das empresas de tecnologia na análise da *surveillance* – sejam os únicos atores capazes de se autocontrolarem, a limitação do poder por ele próprio é dificilmente obtida de maneira voluntária. Trata-se do “dilema competência-motivação”, que só pode ser superado através das pressões externas capazes de desencadear o processo interno de autorreflexão que, posteriormente, é estabilizado por forças também externas, capazes de fazer com que os atores sociais continuem agindo da maneira autoimposta (BECKERS e TEUBNER, 2013).

Essa pressão externa – forte o suficiente para constranger os atores sociais a agirem de modo diferente – é a primeira condição que os autores colocam para a existência de um momento constitucional. Para eles, “apenas pressões externas e internas fortes permitem que as sociedades superem o dilema competência-motivação e ‘forçam’ o setor social em direção a um processo de autorrestrrição” (BECKERS e TEUBNER, 2013, p. 527). Tais forças externas podem partir dos movimentos sociais, dos meios de comunicação, das organizações internacionais e dos próprios mecanismos tradicionais de regulamentação jurídica do Estado.

²⁹⁸ No original: “[...] When processes in a social subsystem spin out of control in this manner, a choice must be made between state intervention and constitutionalisation. After the experience of political totalitarianism during the last century, permanent subordination to the state is not an option that is seriously discussed. [...] A global constitutional order must face the challenge: how can sufficient external pressure be brought to bear on the subsystems so that the self-limitation of their possible courses of action becomes effective?”

Vale salientar, contudo, que afirmar que o controle dos mecanismos políticos e jurídicos do Estado é uma das forças externas capazes de desencadear um processo interno de autocontrole não significa que a regulamentação estatal é suficiente como modo de intervenção direta para controlar o exercício do poder. Essa pretensão de controle externo – como é o caso das propostas que defendem exclusivamente a constitucionalização estatal dos poderes selvagens (FERRAJOLI, 2011a) – não é suficiente, uma vez que

as experiências do passado demonstram igualmente como, em muitos casos, falharam as tentativas de controlar processos internos através da intervenção externas, em virtude da falta de conhecimento e competência das autoridades externas. As iniciativas regulatórias também foram regularmente criticadas em virtude da inerente limitação do seu alcance, permitindo que as corporações identificassem potenciais brechas para evitarem a intervenção regulatória. Se essa experiência também for tomada em consideração, torna-se muito difícil retornar ao tradicional conceito de intervenção político-jurídica (BECKERS e TEUBNER, 2013, p. 530).²⁹⁹

Obviamente, a ideia de constitucionalismo societário não tem, como consequência, a abolição da intervenção do direito e da política estatal, ambos imprescindíveis como forma de pressão externa aos atores sociais. Essa corrente teórica apenas reconhece que, em muitos casos, os processos internos de autocontrole surtem efeito maior que as tradicionais tentativas de intervenção estatais. As empresas de tecnologia da informação e o debate sobre a *surveillance* são exemplos privilegiados disso, especialmente se forem considerados os casos – trazidos no decorrer deste trabalho – das tentativas infrutíferas de controle dos fluxos de dados pelos Estados.

Além disso, o constitucionalismo societário não defende, como as teorias de matriz cosmopolita, por exemplo, a construção de uma constituição global unitária. Para Teubner (2011a), trata-se de um equívoco teórico que ocorre como resultado da tentativa de transferir acriticamente os conceitos do direito constitucional nacional para a sociedade mundial. Essa “constitucionalização” do direito internacional apresenta

²⁹⁹ No original: “Past experience has equally shown how in many cases attempts to control internal processes through external intervention failed due to the lack of knowledge and competence of external authorities. And regulatory initiatives were also regularly criticized because of their inherent limited reach, allowing corporations to identify potential gaps and thus circumventing regulatory intervention. If this experience is also taken into consideration, it becomes indeed difficult to fall back on the familiar concept of political-legal intervention.”.

uma “comunidade internacional” como ponto central para o surgimento de um direito constitucional global. Todavia,

a própria natureza fragmentada da sociedade mundial, enfatizada pela análise sociológica, causa reais dificuldades para esse tipo de constitucionalismo unitário. [...] As condições sociais que permitiram ao Estado-nação estabelecer uma constituição unitária não ocorrem, a princípio, na esfera transnacional. O constitucionalismo transnacional terá que se conformar com os requerimentos de uma sociedade mundial duplamente fragmentada. Como resultado da primeira fragmentação, os setores sociais globais autônomos da modernidade insistem, teimosamente, nas suas próprias constituições, em competição com as constituições dos Estados-nação. Além disso, padrões unitários de uma constituição global tornam-se ilusórios em virtude da segunda fragmentação em várias culturas regionais, cada uma baseada em conjuntos de princípios sociais organizacionais diferentes daqueles do mundo ocidental. Caso deseje-se conceber um tipo de ‘constituição global’, o único diagrama possível é aquele das constituições particulares para cada fragmento global – nações, regimes transnacionais, culturas regionais – e as inter-relações jurídicas entre essas constituições através de um conflito constitucional de leis (TEUBNER, 2011a, p. 216)³⁰⁰.

Esse “nacionalismo metodológico” – ou seja, a tendência de seguir metodologias derivadas da centralidade do Estado nacional – das perspectivas que pretendem uma constituição global reconhecem apenas entidades estatais como parte das relações globais. Ao identificar que o Estado não é a única fonte produtora de normatividade de caráter constitucional, fica fácil perceber, também, que o constitucionalismo societário é adequado para a compreensão da sociedade em rede, onde o Estado é apenas um dos nós que compõem os complexos e sempre mutantes fluxos de poder. Como resultado, percebe-se que o direito estatal é importante, tanto quanto os demais nós nas redes de poder e influência, como forma de iniciar uma forte pressão capaz de fazer surgir um momento constitucional no caso de crise.

Por outro lado, o constitucionalismo societário não pressupõe que todo

³⁰⁰ No original: “The very marked fragmentation of world society emphasized by sociological analyses causes real difficulties for such a unitary constitutionalism. [...] The social conditions which allowed the nation-state to establish a unitary constitution, in principle, do not obtain in the transnational sphere. A transnational constitutionalism will have to conform with the requirements of a doubly fragmented world society. As a result of the first fragmentation, the autonomous global social sectors of modernity insist stubbornly on their own constitutions, in competition with the constitutions of nation-states. Moreover, unitary standards of a global constitution are rendered illusory by the second fragmentation into various regional cultures, each based upon sets of social principles of organisation different to those of the western world. If one wishes to conceive at all of a ‘global constitution’, the only possible blueprint is that of particular constitutions for each global fragment – nations, transnational regimes, regional cultures – and the legal interrelation of these constitutions by means of a constitutional conflict of laws.”

processo de autorreflexão tem como consequência a autolimitação, já que seria extremamente ingênuo crer que os poderes selvagens se autolimitariam sem que houvesse pressão externa. É sempre necessário, para evitar ilusões, retomar a máxima de Montesquieu, para quem o poder se conserva sempre selvagem, ou seja, “[...] todo homem que possui poder é levado a dele abusar; ele vai até onde encontra limites [...] Para que não se possa abusar do poder, é preciso que, pela disposição das coisas, o poder limite o poder” (MONTESQUIEU, 2000, p. 166).

Por isso, mesmo as autolimitações que surtem efeitos necessitam de poderes externos para estabilizá-las, ou seja, para viabilizar a permanência da autovinculação exógena do constitucionalismo societário. Isso equivale – retomando a metáfora do canto das sereias – à manutenção da obediência dos marinheiros para que eles não desamarrassem Ulisses do mastro mesmo que ele ordenasse o contrário. Seguindo nessa linha de pensamento, Beckers e Teubner afirmam que “a constituição do Estado-nação não é somente uma instância de autolimitação do sistema político, mas também está conectada ao processo autorreflexivo do direito [...]” (2013, p. 536)³⁰¹.

Logo, é imprescindível a existência de um processo legal externo. Isso ocorre, na maioria das vezes, de duas maneiras: por intermédio de autoridades certificadoras de práticas das empresas, que controlam as atividades dos seus membros para que possam receber determinada certificação de boas práticas³⁰² ou por meio do direito do Estado-nação, que permite a vinculação dos códigos internos das empresas a uma temporalidade diferente, mais rígida e resistente às paixões momentâneas. Ainda assim, Beckers e Teubner entendem que, em virtude da pouca quantidade de pesquisas que demonstrem essa capacidade estabilizadora das constituições nacionais em relação aos códigos internos das empresas, sua validade ainda é incerta (2013).

Trata-se, assim, da transição de um pensamento centrado na construção constitucional pelo Estado-nação em direção a um pluralismo constitucional transnacional. Esse modo de pensar pode parecer problemático, especialmente para

³⁰¹ No original: “The nation-state constitution is not solely an instance of self-limitation of the political system, but also connected to the self-reflexive process of the law [...]”

³⁰² Veja-se, por todos, o exemplo da iniciativa do IBD para certificar produtos orgânicos. Com base nas legislações do Brasil, EUA e União Europeia, o selo “IBD Orgânico” garante que os produtores que desejam manter essa certificação permaneçam dentro de rígidos padrões de produção que são reavaliados anualmente. Maiores informações sobre esta certificação podem ser acessadas no manual do IBD. Disponível em: < <http://surveillance.es/25> >. Acesso em: 20 abr. 2016.

os teóricos ligados à teoria constitucional tradicional. Pensar a proteção dos direitos humanos para além das constituições estatais pode fazer parecer que se está “entregando” a guarda desses direitos ao mercado, o que ficou claro em virtude da opinião de Stefano Rodotà, analisada anteriormente.

Essa transição é essencial se for considerado que, com os avanços da tecnologia da informação e o seu vínculo com as empresas privadas, esclareceu-se que, no século XXI, aumentará, cada vez mais, o papel das corporações multinacionais na violação dos direitos humanos. Isso demonstra que a questão constitucional atual diverge daquelas que foram colocadas nos séculos XVIII e XIX.

Naquela época, a principal preocupação do constitucionalismo era “[...] liberar as energias do poder político nos Estados nacionais e, ao mesmo tempo limitar efetivamente esse poder através do Estado de direito” (TEUBNER, 2011a, p. 210)³⁰³. No século XXI, diversas forças associadas à *surveillance* também foram “liberadas”, sendo capazes de se movimentarem além (e através) dos compartimentos territoriais dos Estados.

Ao mesmo tempo em que carregam potencial construtivo – afinal, como demonstrado anteriormente, a *surveillance* não é inerentemente negativa –, essas forças, como todo poder, tendem a buscar sua expansão ilimitada caso não sejam controladas. Transformadas em “poderes selvagens”³⁰⁴, elas adquirem potencial destrutivo capaz de violar, com imensa facilidade, os direitos humanos.

Segundo Teubner (2011a), existe uma polarização no debate sobre o constitucionalismo transnacional. De um lado, há aqueles que pregam o declínio do constitucionalismo moderno vinculado ao Estado-nação sem que existam alternativas aplicáveis para o contexto transnacional. Essa aplicação torna-se impossível em virtude da inexistência, fora da esfera nacional, das bases que fundamentam o constitucionalismo tradicional

No outro lado do debate, também há o entendimento de que se está presenciando o esfacelamento do constitucionalismo moderno. A diferença é que, para esses teóricos, há a possibilidade de que tal crise seja compensada pela criação de novos domínios globais da política, especialmente através da transposição das estruturas estatais para a esfera global.

³⁰³ No original: “[...] release the energies of political power in nation-states and at the same time to limit that power effectively, according to the rule of law.”.

³⁰⁴ Item 4.3.3.

Discordando de ambos, Teubner propõe uma terceira via – que, segundo ele, não deve ser entendida como um meio-termo das duas anteriores. Para isso, ele desvincula o constitucionalismo da relação entre política e direito, afirmando que os debates constitucionais devem englobar toda a sociedade. Logo,

[...] além do papel que as constituições possuem na política internacional, torna-se claro que elas também têm importância em outros setores da sociedade. Assim como o constitucionalismo tem o potencial para reagir às tendências expansionistas do sistema político global, ele também possui o potencial para reagir contra aqueles outros subsistemas quando eles colocarem em risco a autonomia dos indivíduos ou das instituições (TEUBNER, 2011a, p. 211)³⁰⁵.

Para compreender adequadamente a proposta de Teubner, é necessário se desfazer de alguns equívocos teóricos. O primeiro deles é a ideia de que o constitucionalismo societário deriva do seu vínculo com a globalização, em especial da debilidade das relações políticas na escala transnacional.

Obviamente, é impossível desvincular os efeitos da globalização dos mercados no direito. Porém, a problemática que levou à necessidade de se pensar um constitucionalismo para além das relações entre política e direito decorre da fragmentação da sociedade e da autonomização desses fragmentos durante o auge do projeto estatal. O elemento mais relevante dessas novas legislações transnacionais diz respeito à diferenciação entre o direito e a política que, até meados do século XX, fundamentava as relações hierarquizadas/verticalizadas das normas.

A globalização aparece como uma força que agrava essa fragmentação, pois, em decorrência da fraqueza da política transnacional, os problemas oriundos da ausência de soluções institucionalizadas aparecem com mais vigor. Com efeito, é possível afirmar que a globalização permitiu que diversos sistemas sociais pudessem liberar-se das amarras territoriais do Estado. Por essa razão,

a teoria dos sistemas contemporânea reflete essa evolução argumentando que uma sociedade moderna, diferenciada funcionalmente, não pode ser vista como uma entidade territorial orgânica. Sistemas funcionalmente especializados possuem um alcance universal e global, não podendo ser contidos na forma territorial. Formas territoriais de diferenciação interna, na forma de subsistemas do Estado-nação, surgiram como elementos

³⁰⁵ No original: “[...] in addition to the role which constitutions play in international politics, it becomes clear that they also play a role in other sectors of world society. Just as constitutionalism has the potential to react to the expansionist tendencies of the global political system, it also has the potential to react to those of other subsystems when they endanger individual or institutional autonomy.”

estabilizadores no início da modernidade, mas, do ponto de vista dos sistemas globais, tornaram-se cada vez mais obstáculos da evolução. Consequentemente, somente em uma sociedade globalizada é que se torna visível a força integral do constitucionalismo societário (VERSCHRAEGEN, 2011, p. 221)³⁰⁶.

No caso da *lex digitalis*, por exemplo, trata-se uma ordem com ambição global, cujos limites não são territoriais – como no caso do Estado –, mas temáticos. Em consequência, não se pode aplicar a estrutura verticalizada e hierárquica típica do Estado-nação, pois determinados sistemas se desenvolveram de modo totalmente diferente, com outros tipos de limites que são incompatíveis com a territorialidade dos tradicionais mecanismos políticos e jurídicos vinculados ao Estado-nação.

Não se trata, assim, de tentar compensar os limites do Estado nacional diante do surgimento de novas esferas sociais não constitucionalizadas, mas, na realidade, de descobrir como se pode transformar a relação – que sempre existiu – entre o Estado-Nação e as instituições do constitucionalismo societário, agora sob a nova ótica da globalização (TEUBNER, 2011a). Em uma sociedade global caracterizada por sua estrutura em rede – ou seja, sem centro –, as diferentes racionalidades dos sistemas sociais prosseguem em direções distintas, o que torna impossível permanecer com a ideia de unidade do Estado.

Além de ignorar que as subconstituições sociais já existiam – antes mesmo da globalização – junto com o (e dentro do) Estado nacional, a maioria das análises também pressupõe que o espaço internacional é “vazio” e que, pois, deve ser constitucionalizado a partir do zero. Todavia, essas constituições globais já existiam, de modo que o propósito do constitucionalismo transnacional, ao invés de construir algo inteiramente novo, é transformar a atual estrutura constitucional transnacional. Isso se dá através da evolução para além das já existentes regras constitutivas, ou seja, pela criação de regras limitativas capazes de constranger as tendências selvagens desses poderes.

O objetivo central de Teubner é, portanto, desvincular a tradicional ligação entre o constitucionalismo e a política, materializada no Estado, bem como demonstrar

³⁰⁶ No original: “Contemporary systems theory reflects this evolution by arguing that modern, functionally differentiated society cannot possibly be seen as an organic, territorial entity. Functionally specialised systems have a universal and global reach, and cannot be contained in a territorial form. Territorial forms of internal differentiation, in the form of nation-state subsystems, emerged as stabilising elements in early modernity, but from the point of view of global function systems they have increasingly become obstacles to further evolution. Consequently, it is only in globalised society that the full force of societal constitutionalism has become visible.”

que os direitos humanos são uma forma de proteger indivíduos e sistemas sociais da dinâmica expansionista dos outros sistemas. Logo, são os direitos humanos que permitem a sua diferenciação funcional.

4.3.2 Constitucionalismo híbrido

Uma outra perspectiva que complementa a proposta de Teubner é aquela trazida por Gert Verschraegen (2011). Embora concorde com a proposta de distanciar o vínculo existente entre o constitucionalismo e a política, Verschraegen reitera o ponto abordado durante todo este trabalho: que é preciso deixar claro que propor o constitucionalismo societário não pode significar o fim do constitucionalismo político tradicional, tampouco do Estado.

Embora o fim do Estado, por óbvio, não seja o objetivo da proposta de Teubner, Verschraegen acredita que as “questões estatais” são pouco abordadas nos textos de Teubner sobre direitos humanos, de modo que é necessário aprofundar a temática sob o risco de, não o fazendo, gerar confusões na compreensão adequada do papel estatal no cenário do constitucionalismo societário.

Verschraegen entende que se deve dar enfoque ao papel crucial do Estado na dinâmica de inclusão/exclusão da sociedade. Isso em virtude de uma das distinções mais importantes no dia de hoje para a concretização dos direitos humanos ser o pertencimento do indivíduo a um determinado Estado. Logo, o autor entende que,

até mesmo em uma sociedade mundial sem centro – onde sistemas, redes e organizações globais e heterárquicos criaram formas de filiação e inclusão em multicamadas sobrepostas – a antiga distinção jurídica entre cidadão e estrangeiro continua a ser de maior importância (VERSCHRAEAGEN, 2011, p. 223)³⁰⁷.

Assim, Verschraegen acredita que embora, a globalização policêntrica tenha intensificado a crise das premissas do Estado-nação, esta forma de organização política continua a ser a pedra angular da sociedade mundial. Isso fica evidente, por exemplo, quando até mesmo um gigante da tecnologia como o *Google* – uma

³⁰⁷ No original: “Even in a centreless world society, where heterarchic, globally operating systems, networks and organisations have created multilayered and overlapping forms of membership and inclusion, the old legal distinction between citizens and strangers remains of major importance.”.

corporação transnacional por excelência – esbarra com determinações estatais, como foi o caso do direito ao esquecimento na União Europeia. Além disso, quase todos os habitantes do mundo estão vinculados a algum Estado em virtude dos laços de nacionalidade, de modo que a “[...] diferenciação da política mundial em Estados ainda não possui clara alternativa” (VERSCHRAEGEN, 2011, p. 223)³⁰⁸.

Por essa razão, a concretização dos direitos humanos na sociedade contemporânea ainda depende, em muito, da filiação dos indivíduos a um determinado Estado. Consequentemente, essa forma de organização política em um território demonstra-se essencial na tarefa de incluir ou excluir as pessoas dos sistemas globais, como é o caso da tecnologia da informação. Afinal, se um somali não pode sequer contar com a segurança de manutenção da sua vida, como poderá ser adentrar no mundo virtual?

O Estado deve, portanto, ser visto como condição de possibilidade para a inserção dos seres humanos na “esfera global”, de modo que não existe nenhuma contradição entre o desenvolvimento de estruturas globais não estatais e a permanência do Estado nacional. Como resultado,

[...] Estados que cuidam dos direitos e interesses dos seus cidadãos precisarão se conectar as evoluções globais; ao invés de “renacionalizar” essas questões, os Estados apenas podem proteger os seus cidadãos através da sua inserção nas matrizes comunicativas globais, ou seja, aumentando sua dependência em relação aos mercados, ciência, educação, medicina e outras esferas sociais globais (VERSCHRAEGEN, 2011)³⁰⁹.

Logo, o debate sobre as finalidades do Estado na sociedade contemporânea não deve ser tratado como uma “superação do velho pelo novo”, mas como uma sobreposição de sistemas cujos limites, objetivos e capacidades são distintos. E esse é o laço em comum entre a teoria sistêmica e o paradigma da *surveillance* analisado neste trabalho: reconhecer que o exclusivo retorno ao Estado e à política estatal não é mecanismo hábil para lidar com as crises do próprio Estado – e os efeitos dessa crise no constitucionalismo estatal e na proteção dos direitos humanos pelas constituições.

³⁰⁸ No original: “[...] the segmentary differentiation of world politics into states is still without a clear alternative.”

³⁰⁹ No original: “[...] states which look after the rights and interests of their citizens will have to connect to worldwide evolutions; they can only protect citizens by enabling them to plug into the global communicative matrixes, that is, by increasing their dependence on global markets, science, schooling, medicine and so forth, rather than by ‘re-nationalising’ these issues.”

O Estado, por óbvio, ainda é extremamente importante na manutenção de direitos humanos – basta ver que a regra global é que os Estados mais desenvolvidos são capazes de assegurar mais direitos aos seus cidadãos. É justamente por essa razão que Verschraegen entende que a constitucionalização de outras áreas da sociedade não deve ocorrer como fenômeno excludente da constitucionalidade estatal. Até mesmo porque, como se viu anteriormente, a legislação estatal é, além de pressão externa capaz de forçar a autorregulação privada, força estabilizadora que contribui para mantê-la pelo tempo.

Tendo isso em mente, fica fácil concordar com Verschraegen quando ele afirma que o “[...] constitucionalismo societário pressupõe a existência de Estados funcionais – ou qualquer outra forma efetiva de política capaz de monopolizar a força e garantir a jurisdição interna [...]” (2011, p. 227)³¹⁰. Por outro lado, deve-se retomar o ponto segundo o qual o Estado é pré-condição para o desenvolvimento dos direitos humanos não significa que ele – e a sua constituição política – deve ter primazia em relação às constituições sociais, tampouco que incumbe ao ente estatal controlar as regras básicas de outros subsistemas sociais.

No mesmo sentido, ao abordar a possibilidade de um constitucionalismo da Internet, Verschraegen explica que a regulação da Internet – seja na esfera nacional ou na internacional – tende a falhar em virtude da natureza transnacional da comunicação digital, o que não exclui a possibilidade de que continuem a ser utilizadas ambas as ferramentas com sucesso parcial. Isso porque, em virtude de possuir os próprios meios de controle – os códigos – a nova tecnologia “[...] pode [regular] amplamente sem a regulação controlada pelas expectativas sócio-jurídicas, mas os meios eletrônicos, por sua vez, são controlados por normas meta-legais. Essa tendência vai no claro sentido de um regime regulatório híbrido” (TEUBNER, 2004, p. 17)³¹¹.

Por essas razões, um constitucionalismo híbrido – capaz de combinar normatividades estatal e privada – parece ser uma forma efetiva de se proteger os direitos humanos sem as ilusões do estatismo. Essa combinação permite a minimização das fraquezas de cada uma dessas formas de constitucionalismo, o que

³¹⁰ No original: “[...] societal constitutionalism presupposes functioning states – or whatever effective political form is available to monopolise force and guarantee internal jurisdiction [...]”.

³¹¹ No original: “[...] it can largely do without regulation controlled by socio-legal expectations, but the electronic means are in turn controlled by meta-legal norms. The trend thus clearly goes in the direction of hybrid regulatory regimes.”.

é interessante para a proteção dos direitos humanos contra os poderes selvagens que, nos dias de hoje, atuam em diversas “camadas”, muito além da tradicional marcação territorial. Esse é o tema do próximo item.

4.3.3 Controle não estatal dos poderes selvagens

Segundo Luigi Ferrajoli (2011a), os poderes selvagens são aqueles que funcionam ao arrepio das normas constitucionalmente estabelecidas e que, por isso, fragilizam a democracia política. Isso ocorre porque, segundo Ferrajoli (1995), desde o século XIX, viu-se acontecer a expansão dos direitos humanos para as esferas privadas. Desde então, o avanço do constitucionalismo tem sido o avanço dos direitos humanos nessas esferas como forma de controlar o poder privado.

No entanto, com o passar do tempo, novas formas de poder foram se desenvolvendo sem a correspondente evolução do constitucionalismo, o que viabiliza a atuação selvagem daqueles poderes e a violação de direitos. Esse fenômeno de manifestação selvagem do poder ocorre naquelas áreas da vida em que o direito não se desenvolveu como instrumento de preservação contra o arbítrio – nos âmbitos das vidas privadas dos indivíduos e nas relações internacionais entre os Estados.

Nessas esferas infra e suprajurídicas, articulam-se os extralegais ou ilegais micro e macropoderes selvagens e, contra eles, “[...] não se coloca nenhum problema de obediência, nem política nem jurídica. Eles são poderes de fato, cuja simples existência demonstra, algumas vezes, a prevalência da força sobre o direito” (FERRAJOLI, 1995, p. 933)³¹². Trata-se, pois, de forças na esfera internacional (outros Estados, organizações internacionais, órgãos supranacionais etc), nacional (em especial, por intermédio do pluralismo de poder próprio dos regimes democráticos) e transnacional (como ocorre, por exemplo, com ONGs internacionais, agências de *rating*, instituições financeiras globais, empresas de tecnologia avançada de comunicação etc).

Ainda segundo Ferrajoli, o modelo que ele denomina de paleoliberal demonstrou-se incapaz de regulamentar adequadamente essas situações, em virtude de esse modelo apenas estabelecer vínculos e limites em relação aos poderes

³¹² No original: “[...] no se plantea ningún problema de obediencia, ni política ni jurídica. Estos son poderes de hecho, cuya sola existencia testimonia en ocasiones la prevalencia de la fuerza sobre el derecho.”

estatais. Com efeito, o autor italiano concorda com o fato de que, na atualidade, a proteção dos direitos humanos requer a limitação do exercício do poder privado, transformando a democratização – entendida, aqui, como limites e vínculos representados pela garantias constitucionais – num dos passos necessários para a diminuição das arbitrariedades e para a maximização dos direitos humanos, em especial da igualdade.

No entanto, para compreender os problemas dos direitos humanos nas esferas sociais, é necessário fugir da tradicional fixação entre tais direitos e o Estado. Como, corretamente, lembra Luigi Ferrajoli (2011a), as constituições devem servir para controlar a selvageria dos poderes – inclusive privados. Da mesma maneira, Teubner explica que a principal tarefa do constitucionalismo é “[..] limitar as tendências expansionistas das lógicas particulares dos subsistemas sociais [...]” (2011a, p. 215)³¹³.

Para tanto, Teubner, ao contrário de Ferrajoli, entende que não se pode continuar a defender que os direitos humanos devem ser analisados sob uma ótica que leve em consideração somente o Estado ou que considere que tais direitos podem ser violados somente por atores sociais – individuais ou coletivos. Com isso, Teubner quer dizer que os direitos humanos devem ser efetivos na proteção contra os diversos “*medium de comunicação*” (TEUBNER, 1989, p. 263).

Persistir na busca por mecanismos estatais tradicionais – ou da sua adaptação a uma ordem internacional – é um equívoco. Os poderes selvagens que operam em escala transnacional não são controláveis pelos mecanismos de produção jurídica do Estado nacional. A globalização facilita para que, “[...] aliviados das restrições do Estado-nação, os sistemas estão agora livres para seguir irrestritamente, em escala global, o programa de maximizar a sua racionalidade parcial” (TEUBNER, 2011a, p. 224)³¹⁴.

Contudo, a concentração do constitucionalismo clássico exclusivamente no campo da política excluiu os outros campos sociais do processo de constitucionalização e, portanto, do controle do poder. O constitucionalismo societário busca reconhecer a natureza política existente mesmo nos setores sociais não

³¹³ No original: “[...] to use constitutional means to limit the expansionist tendencies of the particular logics of social subsystems [...]”

³¹⁴ No original: “[...] Unburdened by nation-state restrictions, the systems are now free to follow without constraints, globally, a programme of maximising their partial rationality.”

políticos – como é o caso da tecnologia da informação – e viabilizar a sua constitucionalização – através das regras constitutivas e limitativas.

Qualquer que seja a perspectiva jurídica ou sociológica adotada – Ferrajoli³¹⁵ ou Teubner – vê-se que a expansão unilateral de um setor social permite que os poderes se desenvolvam de modo destrutivo, ou seja, selvagem. Sem sofrerem o devido contrapeso dos mecanismos existentes, as racionalidades dos sistemas sociais geram uma força destrutiva, que coloca em risco os demais sistemas sociais. Por esse motivo, devem ser elaboradas constituições que sejam parte, cada uma, do respectivo setor da sociedade. Com isso, o direito constitucional terá efetividade no controle dos poderes selvagens através da contenção das tendências colonizadoras dos sistemas sociais, transformando as irritações externas em autocontrole interno.

³¹⁵ Professor de Luigi Ferrajoli, Norberto Bobbio compartilha as mesmas opiniões sobre a forma de controlar os poderes privados. Nas palavras de Bobbio (1999, p. 19), “queremos romper o domínio inteiramente avassalador do poder público e caímos na ‘selvageria’ dos poderes privados, naquela privatização do público de que falou recentemente Pizzorno”. No mesmo sentido, veja-se a contundente crítica de Robert Dahl, para quem “[...] relatively autonomous organizations – or, more commonly, coalitions of organizations – may take on what are essentially public functions. However distasteful this must be to an advocate of monistic democracy like Rousseau, in itself it need not be particularly alarming. But it does alert us to some possibilities that must give concern even to one who accepts the inherent relation of organizational pluralism to large scale democracy. One such possibility is that control over some important public matters will be transferred to organizations that are not themselves controllable, as a practical matter, by the demos and its representatives in parliament and the executive. [...] The seminal work, published nearly twenty years ago, was an essay by Rokkan on Norway, the thesis of which may be summed up in his own words: ‘Numerical Democracy and Corporate Pluralism: Votes Count but Resources Decide’. [...] That systems combining numerical democracy with corporate pluralism have great advantages seems to me undeniable; but it is also undeniable that they raise perplexing problems for democratic theory and institutions. [...] Yet to the extent that it allows control over crucial public matters to be alienated, it would seem to violate democratic criteria” (DAHL, 1984, p. 235-236).

CONSIDERAÇÕES FINAIS

*It doesn't have to be like this
Our greatest hopes could become reality in the future
With the technology at our disposal, the possibilities are unbounded
All we need to do is make sure we keep talking.*

(Stephen Hawking em Pink Floyd – Keep Talking)

O problema que se buscou enfrentar nesta tese foi a necessidade de proteger os direitos afetados pela *surveillance*, considerando que isto não pode ocorrer, exclusivamente, através dos meios de regulação jurídica associados ao Estado, dada a sua impossibilidade de lidar com problemas que escapam à esfera da política e ao *container* territorial, o que torna imprescindível a participação da iniciativa privada nessa discussão. Para tanto, deve-se levar em conta que a desterritorialidade e a fluidez, características desses fenômenos, desafiam os tradicionais mecanismos de controle jurídico, arraigados na centralidade, exclusividade e territorialidade do Estado-nação.

Isso foi realizado a partir do uso, no direito, da matriz dos *surveillance studies* e da construção da categoria *surveillance* como pressuposto teórico para a superação da ideia de mera vigilância. Esta, por sua vez, está vinculada a um paradigma em crise, o que ocorre, especialmente, em virtude do surgimento dos meios eletrônicos de tratamento de dados.

A delimitação da categoria da *surveillance*, intrinsecamente relacionada à globalização e às novas tecnologias da informação, também possibilitou a análise dos efeitos dessa realidade nas estruturas do Estado-nação. Embora sempre tenha sofrido com ameaças externas, essa forma de organização política encontra-se diante de um novo cenário, capaz de alterar os seus fundamentos não apenas de modo quantitativo, mas, principalmente, qualitativo.

Isso ficou claro nas críticas que foram realizadas a cinco casos de tentativas nacionais de controlar os fluxos de dados globais: 1) a de proteção da privacidade das comunicações armazenadas no Marco Civil da Internet; 2) a falha de compreensão, por parte da CPI da espionagem, sobre o que constituíam os eventos de coleta de dados pela NSA; 3) as tentativas infrutíferas do governo francês de controlar a rede Tor; 4) a fragilidade do conceito de informação anônima no anteprojeto da lei de

proteção de dados pessoais e 5) a proliferação de legislações de segurança após os eventos envolvendo Edward Snowden.

No primeiro caso, da tentativa de proteção da privacidade das comunicações armazenadas pelo Marco Civil da Internet no Brasil, a impossibilidade de controle nacional dos fluxos de dados em face do poder da iniciativa privada ficou clara no caso emblemático do uso de informações privadas pelo *Google*. Isso porque os termos de serviço da empresa de *Mountain View* garantem que ela acesse todas as mensagens e conversas dos usuários dos seus serviços de e-mail e bate-papo.

Logo, se até mesmo os termos de serviço do *Google* – uma empresa com representação no Brasil que provê serviços a milhões de brasileiros, empresas e órgãos da administração pública e que, portanto, está totalmente enquadrada nos critérios do Marco Civil – afrontam abertamente o disposto no art. 7º, inciso III da lei 12.965/2014 – que trata da inviolabilidade e sigilo das informações privadas armazenadas, salvo por ordem judicial –, por qual motivo se deveria acreditar que essa legislação será respeitada pelas agências de inteligência estrangeiras ou por outras empresas com muito menos vínculos no Brasil?

Além disso, ficou claro que a utilização de metadados modifica o conceito de informação privada, que passa a englobar muito mais do que aquilo que o Marco Civil brasileiro considera como “informações privadas armazenadas”. Esses metadados podem dizer mais detalhes sobre a vida privada de um indivíduo do que o conteúdo de e-mails, por exemplo. A coleta e tratamento dos metadados permite identificar indivíduos e fazer inferências sobre os seus mais íntimos segredos. Mesmo assim, esse tipo de informação não está abrangida pela proteção de inviolabilidade da lei 12.965/2014.

A segunda crítica às propostas de controle nacional dos fluxos globais de dados foi aquela relacionada à CPI da espionagem realizada pelo Senado, cujo relatório, desde o seu título, faz uso da palavra espionagem para explicar seu objeto, embora se tenha deixado claro, nesta tese, que o problema deixou de ser mera espionagem ou vigilância.

Isso porque se ultrapassa a ideia de que se está diante de um evento específico e dirigido contra determinados sujeitos – vigilância –, para a compreensão de que a coleta e tratamento dos fluxos de dados globais é uma característica inevitável das sociedades contemporâneas – *surveillance*. Não apenas potências

militares, como os EUA, mas, especialmente, grandes grupos privados dedicam cada vez mais esforços no desenvolvimento de tecnologia para coletar, analisar e processar informações.

Existe, no relatório, uma mistura entre eventos pontuais de espionagem – como, por exemplo, a invasão de servidores da Petrobrás ou da Presidência da República – e eventos generalizados que, de maneira alguma, podem ser considerados espionagem. Dessarte, o problema da CPI é considerar equivalentes eventos que são intrinsecamente distintos – espionagem de autoridades pela NSA e coleta massiva de dados de todos os indivíduos pela iniciativa pública e privada.

A terceira crítica, feita quando se falou sobre a rede Tor, teve o intuito de dar materialidade à discussão sobre a inviabilidade do recurso aos mecanismos territoriais para solucionar problemas em redes descentralizadas de alta tecnologia. Pelo que foi exposto, a tentativa do governo francês de impedir o uso dessa rede no seu território será frustrada em decorrência da própria forma como ela foi desenvolvida – ou seja, descentralizada e com criptografia forte. Isso fica claro em virtude desse tipo de tecnologia não poder ser controlada sequer pelo seu criador, maior potência tecnológica e militar existente – EUA.

O quarto exemplo de tentativa frustrada de limitar os fluxos de dados referiu-se ao anteprojeto de lei de proteção de dados que está em debate no Poder Executivo brasileiro. O APL faz uma classificação fantasiosa dos dados em três categorias: pessoais, sensíveis e anônimos.

Ocorre que os dados não possuem uma essência – no sentido aristotélico – que permita caracterizá-los em um desses três grupos de maneira abstrata. Isto só acontece no momento da aplicação do algoritmo, de maneira que dados aparentemente anônimos podem sofrer o processo inverso e se tornarem identificáveis, revelando informações sensíveis sobre os indivíduos.

Como ficou claro pelo farto uso de exemplos trazidos da tecnologia da informação, a concatenação de bases de dados é inversamente proporcional ao anonimato. Logo, a classificação *a priori* entre dados pessoais, sensíveis e anônimos, como faz o APL, coloca em risco os direitos humanos, uma vez que permitirá a proteção insuficiente de dados potencialmente sensíveis, facilitando a identificação dos indivíduos e, conseqüentemente, afetando diretamente as suas vidas.

A quinta crítica realizada diz respeito não a um evento específico, mas à tendência de proliferação de leis que garantem o acesso, pelos Estados, aos fluxos de dados dentro das suas fronteiras. Os escândalos envolvendo Edward Snowden inauguraram uma nova era de recurso à legislação nacional que tende a aumentar os poderes do Estado na coleta e processamento de informações. Essa propensão demonstra que a *surveillance*, entendida como fenômeno que permeia o mundo atual, não tem como consequência, a implosão do Estado. Em alguns casos, como ficou claro com os EUA, ela pode até mesmo fortalecer Estados específicos, embora fragilize a presença dos demais Estados em rede.

Tal situação de instabilidade irá colapsar quando as diversas leis nacionais tentarem impor às grandes empresas de tecnologia da informação restrições que sejam mutuamente excludentes ou, ainda pior, quando as disposições nacionais contrariarem os seus interesses. Em um mundo onde o *Google* é mais poderoso que grande parte dos países existentes, pouco poderá ser feito quando aquela empresa resolver não cumprir a lei, o que ficou claro na primeira crítica realizada *supra*.

Todos os cinco exemplos acima possuem, como pano de fundo, a equivocada crença de que a legislação nacional é capaz de regulamentar o fluxo de dados. No entanto, demonstrou-se que perde qualquer sentido sustentar que o mecanismo lei – associado ao Estado vinculado a um território – possa ser capaz de conter fenômenos globais.

Isso porque, através da análise da literatura sobre a globalização, verificou-se que, embora importantes, os mecanismos de controle estatais são incapazes de proteger, adequadamente, os direitos humanos. Isso ocorre como consequência de alguns fenômenos: 1) da globalização; 2) do surgimento de novos centros de poder não estatais e 3) da expansão das tecnologias da informação. Todos eles possuem, em comum, a extrema facilidade para transpor espaços físicos – o foi referido através das ideias de desterritorialidade e desespacialidade.

Desterritorialidade, contudo, não significa o fim o território, mas denota a aptidão que as novas tecnologias da informação possuem para tornar a análise territorial secundária. E daí surge o problema, pois, partindo-se de uma teoria tradicional do Estado, o território é uma das suas pedras angulares. Logo, esta tese questionou se a crise nesse fundamento específico do Estado significa o fim desse modelo de organização política.

A resposta para essa pergunta foi negativa, porque se concluiu que não existe contradição entre o enfraquecimento do elemento territorial e a manutenção do modelo estatal de organização política. Isso porque a globalização não pode ser vista como um fenômeno de desconstrução do Estado, pois não é a sua totalidade que está sendo desnacionalizada, mas apenas alguns dos seus elementos específicos.

Veja-se, por exemplo, que o caso mais famoso de coleta de dados em escala mundial – um fenômeno notoriamente desterritorializado – somente foi possível através do uso de estruturas estatais fortes – NSA e agências reguladoras nos EUA. As consequências globais não poderiam ter acontecido sem o uso de estruturas locais, simbolizadas por um aparato estatal incrivelmente desenvolvido e bem-estabelecido.

Além disso, a partir da literatura consultada, verificou-se que o Estado não é “vítima” da globalização, mas parte dela. Essa participação estatal em um mundo cada vez mais interdependente, com estruturas espaço-temporais diferentes daquelas associadas ao Estado-nação tradicional, demanda uma nova teoria, capaz de compreender tais mudanças como modificações das capacidades estatais.

Não se tratou, portanto, de propor o fim do Estado, mas de reconhecer uma reconfiguração mundial da soberania, o que pode ser visto na modificação dos pressupostos do Estado, especialmente em virtude da desnacionalização de algumas das suas capacidades diante do contexto daquilo que se convencionou chamar de modernidade líquida e sociedade em rede.

Essa organização em rede, fortemente relacionada às novas tecnologias da informação, viabiliza importantes mudanças na compreensão do papel do Estado nas suas relações com outros participantes das estruturas de poder globais, sejam eles públicos – outros Estados ou blocos econômicos – ou privados – corporações transnacionais. Isso porque ele perde o seu papel de ator central, tornando-se apenas um dos *players* na complexa rede de poderes da sociedade em rede.

Com efeito, o Estado-nação, com sua autoridade soberana, é antagonizado pelos diversos poderes que também são nós da rede. Isso acontece, por exemplo, quando os *data-doubles* dos indivíduos circulam livremente, sem possibilidade de controle pelos mecanismos territorializados, entre empresas quem monetizam os dados (e metadados) gerados naturalmente pelos indivíduos durante as suas atividades cotidianas.

Como resultado, fragiliza-se a ideia de soberania, pelo menos no seu conceito tradicional, uma vez que, sob tal perspectiva, ela deveria ser indivisível. Nessa nova função, embora mantenha certo poder decisório em determinados assuntos, o Estado passa, também, a ser influenciado pelas decisões de uma pluralidade de poderes que integram a rede descentralizada de atores globais.

Isso demonstra importância da discussão que foi realizada a respeito dos limites do conceito de soberania. Para alguns, como Saskia Sassen, a soberania está sendo descentralizada e o território parcialmente desnacionalizado, o que é um efeito das práticas de empresas transnacionais e do surgimento de um regime jurídico paralelo, ainda que incipiente.

Como resultado, ao invés de destruída, a soberania está sendo transformada pela globalização. Há uma proliferação dos *loci* onde ela é exercida, processo que ocorreu nos últimos anos através da reconfiguração da intersecção entre soberania e território. Para essa corrente, a globalização viabiliza a mudança das capacidades do Estado – dentre elas, a sua exclusividade territorial – e permite formar sistemas globais particulares que não requerem territorialidade nem exclusividade.

Essa não é, contudo, a perspectiva mais amplamente difundida na literatura sobre o tema. Na maioria dos casos, entende-se que o Estado está perdendo sua soberania, especialmente, porque esse conceito, desde Bodin, exige a exclusividade do poder de decisão. Nessa visão, adotada, dentre outros, por Manuel Castells, acredita-se que a capacidade de reação do Estado está fatalmente comprometida, especialmente, em virtude da globalização das atividades econômicas, do crime e das tecnologias da informação.

Independentemente da corrente escolhida, vê-se que a incapacidade de controle da *surveillance* por parte dos mecanismos tradicionalmente associados ao Estado – e que, reitera-se, dependem fortemente do elemento territorial – não deve levar à falsa percepção de que o ambiente virtual – em especial, a Internet – é uma terra sem lei. Qualquer conclusão nesse sentido é, no máximo, ingênua, dado que considera somente a existência do ente estatal como fonte de poder normativo. Sob essa ótica, demonstrou-se, com exemplos, que os poderes privados constituem importantíssima fonte reguladora do espaço virtual, em especial através da imposição de técnicas, padrões e protocolos, que constituem verdadeiras “leis” do mundo virtual.

Tais leis – que, na realidade, são códigos digitais – possuem extrema importância para a *surveillance*, já que a tecnologia da informação é um dos seus elementos diferenciadores. É essa tecnologia que permite romper com as perspectivas tradicionais de vigilância comumente associadas ao Big Brother, de George Orwell, ou do panóptico, de Michel Foucault e Jeremy Bentham.

Ao contrário dessas propostas, a *surveillance* não depende do elemento territorial, tampouco do uso da coação ou do sentido da visão. Isso porque os conceitos de *surveillance assemblage* e de *dataveillance* deslocam o problema da coleta de dados do mundo físico para o virtual. Isso permite que as novas tecnologias violem os direitos humanos de modos completamente imprevisíveis para aqueles que não compreendem adequadamente essa categoria.

Trata-se de um fato de grande relevância para o mundo jurídico, especialmente para que se possa garantir a permanência das conquistas oriundas das lutas históricas do segundo pós-guerra relativas à expansão da democracia e dos direitos humanos. Naquela época, esses direitos voltavam-se, em grande parte, contra as violações perpetradas pelo Estado. De modo diverso, a expansão da *surveillance*, no século XXI, desloca esse embate especialmente para dentro da iniciativa privada, como ficou evidente quando se defendeu a superação do modelo do *Big Brother* pelo das *little sisters*. Isso porque, embora alguns poucos Estados façam uso da coleta e tratamento sistematizado de dados, tal situação ocorre, geralmente, através do uso das estruturas da iniciativa privada e, ainda assim, em escala muito menor – veja-se que mesmo a NSA analisa, proporcionalmente, muito menos informações que as gigantes do *big data*.

Há que se ressaltar, todavia, que esse deslocamento não deve levar à conclusão de que não há mais lutas pela proteção dos direitos humanos e da democracia contra violações do Estado. Exemplo disso foram as informações divulgadas por Edward Snowden, que demonstraram a imensa capacidade dos Estados Unidos da América para coletar e tratar dados com finalidades secretas.

O caso protagonizado por Edward Snowden demonstra a complexidade do problema; afinal, não se trata de uma situação de exclusão – de coleta de dados pública vs. Privada –, mas de uma relação mutualística, ou seja, é pública e privada, ou melhor, é pública através da estrutura privada, consoante ficou evidente nas

notícias de que as grandes empresas de tecnologia colaboram ativamente com a NSA.

Sejam públicas ou privadas, todas as entidades que coletam e analisam dados, na atualidade, possuem em comum a busca pela categorização e pelo reconhecimento de padrões – *data mining* – em enormes conjuntos de dados – *big data*. Isso decorre da transição do modelo da defesa em direção à atual sociedade securitizada, na qual o medo líquido preenche as vidas de incertezas que precisam ser eliminadas a partir de novas tecnologias.

Essa securitização, para utilizar a expressão de Michael Hardt e Antonio Negri modifica a expectativa de resposta dos sistemas tecnológicos, que devem deixar de ser reativos e conservativos – ou seja, preservar a ordem através de interferências somente quando perturbados –, para se tornarem ativos e construtivos – antecipar essas interferências e modificar a ordem social antes mesmo que elas ocorram.

Como resultado, esse fenômeno enfraquece a soberania moderna em virtude da sua capacidade para normalizar uma situação de guerra constante, que deveria ser excepcional. Como resultado, desestabiliza-se o poder, que passa a migrar em direção aos atores públicos – vinculados às grandes potências – e privados – detentores da tecnologia da informação.

Uma das consequências fundamentais derivada da matriz teórica dos *surveillance studies* é a superação da ideia de que informações pessoais e comunicações privadas dizem respeito apenas às violações privacidade. Esse lugar-comum no direito, resultado da não compreensão da categoria da *surveillance*, faz com que os juristas já comecem a encarar o problema de maneira equivocada, conforme foi demonstrado pela ausência do enfrentamento – pelo Marco Civil da Internet, pela CPI da espionagem e pelo anteprojeto de lei de proteção de dados – das cruéis violações da igualdade e da liberdade patrocinadas pela *surveillance*.

Desde concessões de benefícios somente para indivíduos caracterizados como “de interesse comercial”, até a impossibilidade de utilizar meios de transporte aéreo, os seres humanos sofrem, cotidianamente, as consequências de sistemas que coletam e, acima de tudo, categorizam informações com critérios que não passam por qualquer tipo de controle democrático,

Por isso, é possível – e necessário – compreender que a *surveillance* atinge muito mais que a privacidade. Utilizando-se de grandes quantidades de dados,

programas de computador extremamente sofisticados conseguem violar os direitos humanos em quatro vieses principais: 1) da liberdade de locomoção; 2) do direito à informação; 3) da liberdade de agir; 4) da igualdade.

A liberdade de locomoção é afetada em razão da existência de sistemas automatizados que permitem ou impossibilitam o movimento das pessoas nas sociedades contemporâneas. Tratam-se de instrumentos amplamente utilizados nos controles de fronteira e que dependem de informações biométricas, ou seja, extraídas do próprio corpo do indivíduo, para classificá-lo como desejável ou perigoso.

O segundo viés indicado, do direito à informação, é ameaçado em virtude da personalização de informações, fenômeno que foi explicado, nesta tese, como filtro bolha. Com base na teoria dos direitos fundamentais de Luigi Ferrajoli, pode-se concluir que esse direito à informação é, muito além da mera não proibição – liberdade de informação –, uma expectativa positiva, indispensável à liberdade de consciência e de pensamento. Por isso, deve ser protegido contra a manipulação das informações através da garantia de independência política e econômica, bem como da pluralidade de opiniões na esfera pública. Por filtrarem as informações e permitirem que cheguem até os indivíduos apenas aquilo que seja do seu interesse e conforme a sua visão do mundo, os sistemas de computadores inviabilizam a fertilização de ideias necessária para a evolução do pensamento humano.

O terceiro viés, a liberdade de agir, é violada por força das análises estatísticas e comportamentais, notadamente aquelas de natureza publicitária e política, que permitem prever quais os “gatilhos” corretos para “disparar” desejos nos indivíduos – sejam eles econômicos, como a decisão de comprar de um produto, sejam políticos, como escolha de qual candidato irá votar no próximo pleito eleitoral.

A quarta perspectiva de ameaça aos direitos humanos, da igualdade, ocorre como consequência dos mecanismos de classificação social que reforçam as desigualdades em escala geométrica, especialmente na era da chamada guerra contra o terror da atual sociedade securitizada. Assim, ao ser colocado em uma determinada categoria, o ser humano passa a sofrer restrições inerentes àquela classificação, o que só reforça o estereótipo do grupo onde foi colocado.

Uma análise a partir da ideia de *surveillance*, portanto, possibilita a compreensão de que os sistemas de computadores são alimentados com informações sobre seres humanos reais e essa classificação, por mais virtual que pareça, acaba

por colocar pessoas em grupos diversos – sejam eles de risco, de interesse, de saúde etc. –, afetando, de modo relevante, as suas vidas.

Essas violações, embora frequentemente ignoradas, são de extrema importância e só podem ser percebidas a partir do paradigma da *surveillance*. Afinal, a abordagem da mera vigilância é incapaz de demonstrar que outros direitos humanos – além da privacidade – podem ser violados como decorrência da capacidade que os sistemas de processamento digitais possuem para analisar e classificar dados.

Diante disso, a categoria da *surveillance* deve ser utilizada como condição de possibilidade para perceber o vínculo comum entre todas aquelas violações. Trata-se dos algoritmos de análise preditivas – *predictive analytics* –, amplamente empregados como forma de diminuir as incertezas na sociedade securitizada. Através de cálculos probabilísticos complexos, essa tecnologia busca antecipar o futuro para gerar respostas – sejam elas políticas, jurídicas, econômicas ou militares – antes mesmo que o potencial evento danoso aconteça.

A análise desses mecanismos e a compreensão das modificações nas relações de tempo que eles proporcionam fazem sentido somente se for considerado, como defendido nesta tese, que houve a superação da sociedade disciplinar em direção às sociedades do controle. Ultrapassa-se, assim, a necessidade de confinar aqueles que necessitam ser controlados. A flexibilidade e a ubiquidade da tecnologia da informação garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos – *containers* territoriais.

Ao encontro dessa tendência de calcular os riscos com a finalidade de prever o futuro está a ideia de biopoder, que viabiliza o desenvolvimento do capitalismo através do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos. O biopoder é exercido de um modo oposto à proposta panóptica, visto que ele precisa ser cada vez mais dócil, dando a sensação de liberdade. Para tanto, deve garantir a sua manutenção do modo mais assimilável possível, sem causar perturbações ou dificuldades na vida cotidiana.

Esse traço torna o modelo do biopoder extremamente compatível com o caráter sedutor da *surveillance* na sociedade do consumo, sobretudo se for atualizado a fim de poder contribuir para a compreensão da *surveillance* na era do *big data*. O biopoder agora é híbrido, congregando um amplo leque de tecnologias distintas,

sempre com a finalidade de identificar e rastrear indivíduos e grupos, bem como criar modelos preditivos de comportamento e risco.

A desnecessidade do elemento confinador – espacial ou territorial – viabilizada pela *surveillance* modifica, também, as relações do homem com o espaço através do deslocamento das fronteiras referido nesta tese. Tal fenômeno desvincula a tradicional concepção de fronteira como um lugar físico, transformando os limites territoriais dos Estados em um “acontecimento” que surge no momento em que decisões são tomadas por sistemas de computador para permitir ou impedir o fluxo de pessoas pelo globo.

É possível, pois, perceber que as fronteiras não permaneceram incólumes. Além das evoluções na tecnologia da informação, isso decorre da mudança do cenário político, que viabiliza a incessante busca pela criação e ampliação das “áreas seguras”. Essas alterações ficam ainda mais claras quando colocadas a partir do paradigma da *surveillance*. Partindo-se dessa categoria, percebe-se que o controle dos fluxos de pessoas não tem um alvo específico: todos os indivíduos e grupos devem ser constantemente analisados para a determinação do risco que representam.

Uma leitura a partir da *surveillance* permite concluir que, ao contrário do que poderiam deduzir as visões ingênuas sobre a globalização, o fato do mundo estar cada vez mais conectado não extinguiu as fronteiras. Os limites territoriais do poder político estatal são agora, extremamente moduláveis, o que não significa que sejam inexistentes. Para aqueles que se encontram fora dos modelos estatísticos de risco aceitável, as fronteiras nunca foram tão presentes e intransponíveis como são hoje.

Está-se, portanto, diante de outro efeito da *surveillance* no território, que é pressuposto da teoria do Estado. Os limites territoriais são transformados em concatenações de quantidades inimagináveis de dados oriundos de entidades públicas e privadas. Nos mais diversos lugares do mundo, aquelas análises estatísticas servem como fundamento para que um *software* garanta ou impeça a mobilidade das pessoas. Como resultado, o exercício de um direito fundamental – a liberdade de locomoção – fica condicionado às iterações de um sistema cujos critérios de funcionamento são extremamente opacos.

Essa opacidade está relacionada à predominância dos poderes privados vinculados à *surveillance* – ou, nos poucos casos envolvendo poderes estatais, dos *arcana imperii* a que se referia Norberto Bobbio. Por isso, pode-se afirmar que o

problema da *surveillance* diz respeito, sobretudo, à questão de ausência de visibilidade democrática. Nos espaços privados, retomando Norberto Bobbio, a democracia não chegou sequer como procedimento.

Essa colonização pela iniciativa privada decorre, de modo especial, da incapacidade do modelo estatal tradicional para lidar com os fenômenos desterritorializados, como é o caso da *surveillance*. Cria-se, assim, um vácuo normativo, que passa a ser preenchido pelos poderes privados que se desenvolvem no mundo virtual sem restrições, ou seja, de modo selvagem, para utilizar a expressão de Luigi Ferrajoli.

Dessarte, os critérios para coleta e tratamento de dados permanecem fora do debate democrático, pois elaborados por indivíduos que não foram eleitos. Para tornar a situação ainda mais grave, não existe, nesses sistemas, um equivalente à teoria de separação dos poderes. Em outras palavras: criadores e executores da “lei” – neste caso, os códigos de computador – são os mesmos. A incerteza gerada por um algoritmo cujo modo de funcionamento é desconhecido e que possui auto-executividade, sem a mínima possibilidade de resistência, é kafkiana, o que a torna inaceitável do ponto de vista da democracia.

Por tal razão, falham, novamente, as abordagens tradicionais, uma vez que o Estado – salvo raras exceções – não participa do desenho desse novo sistema legal, composto de algoritmos computacionais. Essa nova “lei” não encontra precedentes históricos e, como resultado, não é percebida como tal pela teoria do direito, que está habituada a lidar com leis derivadas do Estado nacional.

Forma-se, assim, um segundo vácuo, desta vez da teoria do direito e da constituição, que se veem incapazes de proteger os direitos humanos das violações desse novo tipo de instrumento com características de lei. Por essa razão, é possível, parafraseando Paulo Bonavides, afirmar que ontem vigoravam os códigos, hoje, as constituições e, amanhã, novamente, os códigos – agora, claro, digitais e elaborados segundo critérios ignorados pelos seus destinatários.

Sem as restrições típicas do constitucionalismo na elaboração desses códigos, fica fácil perceber como a tecnologia da informação ganha a capacidade de violar direitos humanos, o que reforça a ideia defendida de que o Estado é um palco fragilizado para a sua proteção. Disso não se deve concluir que se trata de uma “falha” do modelo estatal, possível de ser sanada através do seu redesenho. O que ocorre é

exatamente o oposto, ou seja, trata-se de um limite intransponível que demonstra a insuficiência desse formato de organização política para, sozinho, proteger os direitos humanos na era do *big data*.

Para solucionar esse imbróglio, são necessárias propostas teóricas que reconheçam o poder normativo dos códigos de computadores gestados dentro do segredo da iniciativa privada. Essas teorias devem ser capazes de propor soluções para garantir que aquele primeiro vácuo – relativo à ausência de poder legitimado democraticamente no meio virtual – seja preenchido por normas constitucionais, protetoras dos direitos humanos.

Esse é o caso, por exemplo, das teorias de matrizes sistêmicas, como aquelas trabalhadas nesta tese. Tratam-se de propostas que parecem ser muito mais adequadas para compreender os conflitos decorrentes da *surveillance* no universo do direito, sobretudo em virtude de se deslocarem das perspectivas tradicionais – que pensam os problemas transnacionais exclusivamente a partir de abordagens que dependem do Estado nacional ou da aplicação do modelo estatal em escala global.

A categoria da *surveillance*, conjugada com a matriz sistêmica, demonstra que a teoria do direito precisa se deslocar em direção a uma concepção de constituição desvinculada da política, ou seja, deve reconhecer a possibilidade de constitucionalização de outros sistemas sociais. Em síntese: o constitucionalismo não pode permanecer atrelado ao Estado nacional caso pretenda proteger, efetivamente, os direitos humanos e a democracia no mundo contemporâneo.

A proteção dos direitos afetados pela *surveillance* não pode depender somente dos meios de regulação jurídica associados ao Estado, dada a sua impossibilidade de lidar com problemas que escapam à esfera da política e ao *container* territorial, o que torna imprescindível a participação da iniciativa privada nessa discussão.

Diante do exposto, resta confirmada a hipótese levantada nesta tese, ou seja, verificou-se que o desenvolvimento da tecnologia da informação e o seu uso para a coleta, transmissão, armazenamento e processamento de informações, em virtude do seu impacto direto na vida humana, cria novas situações de perigo para os direitos humanos. Isso fica mais nítido se for levado em consideração que a vida cotidiana depende, cada vez mais, dos resultados das análises feitas por computadores a partir de uma ampla variedade de bancos de dados interconectados. Aqueles que sofrem

os efeitos concretos dessas análises, no entanto, desconhecem como ela é realizada e de onde são coletadas as informações que lhe fundamentam.

Este trabalho, efetivamente, construiu uma nova categoria na teoria jurídica nacional, qual seja, a *surveillance*. Em síntese, esta deve ser entendida transdisciplinarmente, como um fenômeno inerente à sociedade contemporânea, onde ocorre a sistemática coleta de informações em praticamente todos os momentos da vida, especialmente por parte da iniciativa privada.

O elemento diferenciador dessa categoria é a natureza líquida da tecnologia que ela utiliza para buscar padrões estatísticos com o propósito de influenciar, categorizar e controlar pessoas ou grupos, em geral na busca por maior segurança e consumo. Isto possibilitou um olhar crítico dos atuais instrumentos legais que tentam proteger os direitos humanos violados pelas tecnologias da informação e viabilizou um novo recorte teórico para a construção de mecanismos mais adequados para exercer aquela tarefa.

Cumpridos os objetivos inicialmente traçados, esta tese contribuiu para a evolução da teoria do Estado no atual cenário de mudanças extremamente relevantes nos seus pressupostos. Essa contribuição decorre da discussão sobre como a categoria elaborada impacta os tradicionais elementos que compõem o Estado, dos efeitos que ela possui na proteção dos direitos e das suas consequências para o regime democrático.

Superados esses pontos construtivos, objetiva-se, também, que esta tese tenha um caráter desconstrutivo, ou seja, que possa servir para gerar novas dúvidas. Isso porque, tendo refletido sobre o que é a *surveillance* e como ela afeta os direitos humanos e a democracia, a teoria jurídica deve repensar como encarar o problema para além das soluções associadas ao Estado territorial da modernidade, reconhecendo as suas possibilidades, mas também as suas restrições.

Demonstrou-se a necessidade de questionar como o Estado, dentro dessa nova dinâmica de poder, é capaz de ainda fazer frente aos diversos *players* globais da tecnologia da informação. Em outras palavras: a tradicional teoria do Estado – que fundamenta o mito de que ele pode proteger os direitos humanos frente à liquidez das tecnologias da informação – não pode dar todas as respostas aos problemas do mundo atual. É necessário, pois, perguntar quais os seus novos limites e papéis na contemporaneidade.

Diante desse novo cenário, é necessário reconhecer a remodelação da soberania como uma consequência do surgimento de novas estruturas não estatais de autoridade e poder. Agora vulnerável aos ataques cada vez menos específicos – e, por isso mesmo, mais inevitáveis – das diversas fontes de poder do mundo contemporâneo, o Estado tem suas funções reformuladas, agindo não mais como centro, mas como nó de uma rede descentralizada de poder.

Ainda que a soberania e o território continuem sendo características fundamentais do sistema mundial, ocorreu um desvio parcial em direção a outras arenas institucionais fora do Estado e da sua vinculação a um determinado espaço geográfico. Dado que a exclusividade daqueles dois elementos, do ponto de vista histórico, é essencial para o Estado-nação, essa mudança representa uma reviravolta do seu próprio conceito.

Ainda é necessária uma teoria do Estado, visto que as relações de poder, embora não confinadas exclusivamente na esfera estatal, continuam a fazer parte de toda a sua atividade. No entanto, e aí está a contribuição desta tese, uma adaptação da teoria do Estado ao cenário protagonizado pela *surveillance* impõe a sua abertura para os novos influxos não estatais e, portanto, deve ir no sentido de transformá-la em uma teoria do poder.

É lamentável perceber que, ao ignorar o mundo e confinar sua compreensão do direito aos limites do Estado e do constitucionalismo do sistema político, os juristas impedem que as inovações de outras áreas fertilizem o pensamento jurídico. Com isso, diminuem a sua capacidade de responder às violações de direitos humanos quando elas são causadas por mecanismos que escapam aos tradicionais recortes jurídicos. Por isso, esta tese teve como esforço superar a linha de raciocínio mais comum, que parte do direito para entender a tecnologia. Neste trabalho, tecnologia e direito estão imbricados de modo indissolúvel.

Somente através da compreensão adequada da *surveillance* como uma característica inerente à modernidade líquida será possível perguntar qual a legitimidade democrática das categorias em que os indivíduos são classificados. A correta percepção desse fenômeno, para além dos limites teóricos tradicionais, irá permitir que o direito faça perguntas relevantes na busca pela proteção dos direitos humanos e da democracia, cuja função primordial é tornar mais visíveis as relações de poder.

Ao que parece, existem duas abordagens possíveis: pode-se, por um lado, aumentar a produção legislativa, criar emendas constitucionais, resolver as possíveis violações de direitos nos tribunais nacionais e dar-se por satisfeito; ou, por outro, pode-se reconhecer a incapacidade desses mecanismos para, sozinhos, controlar algo tão líquido quanto o fluxo de dados e discutir outras propostas para proteger os direitos humanos.

A primeira abordagem fornece uma segurança jurídica que, infelizmente, é falsa. Embora sejam uma herança da modernidade sólida, os direitos humanos são, inquestionavelmente, essenciais para se manter a humanidade em tempos líquidos e, por mais paradoxal que pareça, somente será possível protegê-los através de ferramentas caracterizadas pela liquidez, adjetivo tão pouco apreciado pela teoria jurídica.

Como bem afirmou Stephen Hawking na epígrafe desta conclusão, a tecnologia à disposição do homem permite a realização de coisas inimagináveis. No entanto, é preciso o debate sobre quais as melhores formas de utilizar essa tecnologia para fins que engrandecem a existência humana, não que aprisionem o homem dentro de si mesmo.

O que o direito precisa reconhecer é que o mundo, assim como a vida, é demasiado complexo e caótico para caber no espaço rígido e seguro da lei associada ao Estado nacional. Tendo sempre em consideração a ideia de ambivalência, inerente à modernidade líquida, o jurista deve poder pensar o caos e a unidade juntos, em uma construção dialética. Em outras palavras, para retomar a maestria de Luis Alberto Warat (2000), deve-se tornar essa ambiguidade disponível ao pesquisador do direito, pois a audácia presente no surgimento do novo depende da capacidade de cultivar a ambiguidade.

Dessa maneira, ao invés de tentar simplificar o mundo para que ele caiba no porto seguro da lei, o trabalho do jurista é fazer parte do caos que o cerca e, dentro dele, compreendê-lo, tornando-se capaz de encontrar novas e efetivas formas de proteger os direitos humanos.

REFERÊNCIAS

4-YEAR-OLD turns up on government 'no-fly' list. **NBC News**, New York, 05 jan. 2006. Disponível em: < <http://surveillance.es/1-> >. Acesso em: 26 mar. 2016.

ACQUISTI, A.; GROSS, R.; STUTZMAN, F. Face Recognition and Privacy in the Age of Augmented Reality. **Journal of Privacy and Confidentiality**, Pittsburgh, 6, n. 2, 2014. 1-20. Disponível em:< <http://surveillance.es/s> >. Acesso em: 15 fev. 2016.

ADEY, P. Borders, identification and surveillance: new regimes of border control. In: BALL, K.; HAGGERTY, K.; LYON, D. **Routledge Handbook of Surveillance Studies**. New York: Routledge, 2012. p. 193-200.

AEROPORTO de campinas implanta controle automatizado de passaportes.**Portal Brasil**, Brasília, 14 jan. 2016. Disponível em: < <http://surveillance.es/3> >. Acesso em: 04 fev. 2016.

AGAMBEN, G. **Homo sacer**: o poder soberano e a vida na rua. Tradução de Henrique Burigo. Belo Horizonte: UFMG, 2007. 207 p.

ANDREJEVIC, M. **iSpy**: Surveillance and Power in the Interactive Era. Lawrence: University Press of Kansas, 2007. 325 p.

ANDREJEVIC, M. Ubiquitous surveillance. In: BALL, K.; HAGGERTY, K. D.; LYON, D. **Routledge Handbook of Surveillance Studies**. New York: Routledge, 2012. p. 91-98.

ANDREJEVIC, M.; BURDON, M. Defining the Sensor Society. **Television & New Media** , 16, n. 1, jan. 2015. 19-36. DOI: 10.1177/1527476414541552.

ANDREJEVIC, M.; GATES, K. Big Data Surveillance: Introduction. **Surveillance & Society**, Kingston, 2, n. 12, 2014. 185-196.

APRÈS Google, le moteur de recherche Bing lance son formulaire de « droit à l'oubli » en Europe. **Le Monde**, Paris, 17 jul. 2014. Disponível em: < <http://surveillance.es/2o> >. Acesso em: 01 maio 2016.

BALL, J.; BORGER, J.; GREENWALD, G. Revealed: how US and UK spy agencies defeat internet privacy and security. **The Guardian**, London, 06 set. 2013. Disponível em: < <http://surveillance.es/1s> >. Acesso em: 10 mar. 2016.

BARANIUK, C. 'Quit Google, Facebook' suggests tech expert as surveillance scandal deepens. **Wired**, London, 10 jun. 2013. Disponível em: < <http://surveillance.es/2d> >. Acesso em: 26 abr. 2016.

BARRETTO, V. D. P. **O fetiche dos direitos humanos e outros temas**. 2. ed. Porto Alegre: Livraria do Advogado, 2013. 372 p. Kindle Edition.

BAUMAN, Z. **Globalização: as consequências humanas**. Tradução de Macus Penchel. Rio de Janeiro: Jorge Zahar, 1999. 148 p.

BAUMAN, Z. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001. 258 p.

BAUMAN, Z. **Medo líquido**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2008. 239 p.

BAUMAN, Z.; LYON, D. **Liquid Surveillance: A Conversation**. Cambridge: Polity, 2013. 152 p.

BECK, U. **La sociedad del riesgo: hacia una nueva modernidad**. Tradução de Jorge Navarro; Daniel Jiménez e Maria Rosa Borrás. Barcelona: Paidós, 1998. 304 p.

BECKERS, A.; TEUBNER, G. Expanding constitutionalism. **Indiana Journal of Global Legal Studies**, Bloomington, 20, n. 2, 2013. 523-550.

BENNET, C. J. et al. **Transparent Lives: Surveillance in Canada**. Edmonton: Athabasca University Press, 2014. 239 p.

BIGO, D. Security, exception, ban and surveillance. In: LYON, D. **Theorizing Surveillance: The panopticon and beyond**. Cullompton: Routledge, 2006. p. 46-68.

BIGO, D. Globalized (In) Security: The field and the Ban-Opticon. In: BIGO, D.; TSOUKALA, A. **Terror, Insecurity and Liberty: iliberal practices of liberal regimes after 9/11**. New York: Routledge, 2008. p. 10-48.

BOBBIO, N. **O futuro da democracia**. Tradução de Marco Aurélio Nogueira. 6. ed. Rio de Janeiro: Paz e Terra, 1997. 171 p.

BOBBIO, N. **As ideologias e o poder em crise**. Tradução de João Ferreira. 4. ed. Brasília: Universidade de Brasília, 1999. 240 p.

BOBBIO, N. **Estado, governo, sociedade**: para uma teoria geral da política. Tradução de Marco Aurélio Nogueira. 14. ed. Rio de Janeiro: Paz e Terra, 2007. 173 p.

BOGARD, W. Surveillance assemblages and lines of flight. In: LYON, D. **Theorizing surveillance**: the panopticon and beyond. Cullompton: Willan Publishing, 2006. p. 97-122.

BOGARD, W. Simulation and post-panopticism. In: BALL, K.; HAGGERTY, K. D.; LYON, D. **Routledge Handbook of Surveillance Studies**. New York: Routledge, 2012. p. 30-37.

BOLZAN DE MORAIS, J. L. As crises do Estado contemporâneo. In: VENTURA, D. D. F. L. **América Latina**: Cidadania, Desenvolvimento e Estado. Porto Alegre: Livraria do Advogado, 1996. p. 37-50.

BOLZAN DE MORAIS, J. L. **A subjetividade do tempo**: Uma perspectiva transdisciplinar do Direito e da Democracia. Porto Alegre: Livraria do Advogado, 1998. 124 p.

BOLZAN DE MORAIS, J. L. **As crises do estado e da constituição e a transformação espacial dos direitos humanos**. 2. ed. Porto Alegre: Livraria do Advogado, 2011. 143 p.

BOLZA DE MORAIS, J.L; JACOB NETO, E. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. In: LEITE, G. S; LEMOS, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 417-439,

BOLZA DE MORAIS, J.L; JACOB NETO, E. A “liquidez” da surveillance cabe nos limites da “solidez” do marco civil da Internet? **Empório do Direito**. 05 maio 2015. ISSN 2446-7405. Não paginado. Disponível em: < <http://surveillance.es/2s> >. Acesso em: 02 maio 2016.

BOLZA DE MORAIS, J.L.; JACOB NETO, E. Liberté, égalité, fraternité et... “surveillé”: O leviatã contra-ataca **Empório do Direito**. 18 maio 2015. ISSN 2446-7405. Não paginado. Disponível em: < <http://surveillance.es/2t> >. Acesso em: 02 maio 2016.

BOLZA DE MORAIS, J.L.; JACOB NETO, E. Quem é anônimo no mundo dos metadados? O problema do anteprojeto de lei para proteção de dados pessoais. **Empório do Direito**. 06 nov. 2015. ISSN 2446-7405. Não paginado. Disponível em: < <http://surveillance.es/2r> >. Acesso em: 02 maio 2016.

BOLZAN DE MORAIS, J. L.; STRECK, L. L. **Ciência política e teoria do estado**. 7. ed. Porto Alegre: Livraria do Advogado, 2007. 211 p.

BOSKER, B. Siri Rising: The Inside Story Of Siri's Origins — And Why She Could Overshadow The iPhone. **The Huffington Post**, New York, 22 jan. 2013. Disponível em: < <http://surveillance.es/x> >. Acesso em: 15 fev. 2015.

BOYD, D.; CRAWFORD, K. Critical Questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. **Information, Communication & Society**, 15, n. 5, jun. 2012. 662-679. Disponível em:< <http://surveillance.es/1a> >. Acesso em: 25 fev. 2016.

BRASIL. **Anteprojeto de lei de proteção de dados pessoais**. Ministério da Justiça. Brasília. 2015. Disponível em: < <http://surveillance.es/p> >. Acesso em: 15. fev. 2016.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 24 abr. 2014a.

BRASIL. Relatório final da comissão parlamentar de inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. **Senado Federal**, Poder Legislativo, DF, 09 abr. 2014b. Disponível em: <http://surveillance.es/2v> >. Acesso em: 04 maio 2016.

BRASIL. Relatório final da comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país. **Câmara dos Deputados**, Poder Legislativo, DF, 20 abr. 2016. Disponível em: <http://surveillance.es/2u> >. Acesso em: 04 maio 2016.

BRIGHENTI, A. M. Democracy and its visibilities. In: HAGGERTY, K.; SAMATAS, M. **Surveillance and democracy**. London: Routledge, 2010. p. 51-68.

CALHOUN, C. Rethinking the Public Sphere. Presentation to the Ford Foundation. **Social Science Research Council**, 07 fev 2005. Disponível em: < <http://surveillance.es/29> >. Acesso em: abr 25 2016.

CARAN, A. Instagram will start showing posts out of order, like Facebook. **[s.l.]**, London, 15 mar. 2016. Disponível em: < <http://surveillance.es/2m> >. Acesso em: 25 abr. 2016.

CASADO, J.; GREENWALD, G.; KAZ, R. EUA espionaram milhões de e-mails e ligações de brasileiros. **O Globo**, Rio de Janeiro, 06 jul 2013. Disponível em: < <http://surveillance.es/2e> >. Acesso em: 26 abr. 2016.

CASTELLS, M. **The power of identity**: The information age – economy, society and culture. 2. ed. Chichester: Wiley-Blackwell, v. 2, 2010a. 538 p.

CASTELLS, M. **The rise of the network society**: The information age – economy, society and culture. 2. ed. Chichester: Wiley-Blackwell, v. 1, 2010b. 597 p.

CEYHAN, A. Surveillance as biopower. In: BALL, K.; HAGGERTY, K.; LYON, D. **Routledge handbook of surveillance studies**. New York: Routledge, 2012. p. 38-45.

CHEVALLIER, J. **O Estado pós-moderno**. Tradução de Marçal Justen Filho. Belo Horizonte: Fórum, 2009. 309 p.

CLARKE, R. Information technology and dataveillance. **Communications of the ACM**, 31, n. 5, maio 1988. 498-512. Disponível em: < <http://surveillance.es/c> >. Acesso em: 12 fev. 2016.

CLARKE, R. **Dataveillance - 15 Years On**. Privacy Issues Forum. Canberra: New Zealand Privacy Commissioner. 2003. Não paginado. Disponível em: < <http://surveillance.es/d> >. Acesso em: 12 fev. 2016.

COSTA, C. Quatro coisas que mudam com a criptografia no WhatsApp – e por que ela gera polêmica. **BBC Brasil**, Londres, 06 abr. 2016. Disponível em: < <http://surveillance.es/24> >. Acesso em: 13 abr. 2016.

DAHL, R. Polyarchy, Pluralism, and Scale. **Scandinavian Political Studies**, [s.l.], 7, n. 4, 1984. p. 225-240.

DAHL, R. **A democracia e seus críticos**. Tradução de Patrícia de Freitas Ribeiro. São Paulo: WMF Martins Fontes, 2012. 625 p.

DELEUZE, G. Post-scriptum sobre as sociedades de controle. In: DELEUZE, G. **Conversações**. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 219-226.

DELEUZE, G.; GUATTARI, F. **Mil Platôs: Capitalismo e Esquizofrenia**. Rio de Janeiro: 34, 1997. 715 p.

ECO, Umberto. **Como se faz uma tese**. Tradução de Gilson Cesar Cardoso de Souza. 21. ed. São Paulo: Perspectiva, 2007.

ELMER, G.; OPEL, A. Pre-empting panoptic surveillance: surviving the inevitable war on terror. In: LYON, D. **Theorizing Surveillance: The panopticon and beyond**. Cullompton: Willan Publishing, 2006. p. 139-160.

ENGELMANN, W. As Nanotecnologias e a Gestão Transdisciplinar da Inovação. In: ENGELMANN, W. **As novas tecnologias e os direitos humanos: Os desafios e as possibilidades para construir uma perspectiva transdisciplinar**. Curitiba: Honoris Causa, 2011. P. 297-336.

ERICSON, R. V.; HAGGERTY, K. D. The surveillant assemblage. **British Journal of Sociology**, London, 51, n. 4, dez. 2000. p. 605-622.

ESPOSTI, S. D. When big data meets dataveillance: The hidden side of analytics. **Surveillance & Society**, Kingston, 2, n. 12, 2012. p. 209-225.

FAGUNDEZ, I; SERRA, R. Executivo do Facebook é libertado em SP. **BBC Brasil**, São Paulo, 02 mar. 2016. Disponível em: < <http://surveillance.es/23> >. Acesso em: 13 abr. 2016.

FERRAJOLI, L. **Derecho y razón: teoría del garantismo penal**. Tradução de Perfecto Andrés Ibáñez. Madrid: Trotta, 1995. 991 p.

FERRAJOLI, L. Processo deconstituinte. In: GALLO, D.; IPPOLITO, F. **Salviamo la costituzione**. Taranto: Chimienti, 2005. p. 93-110.

FERRAJOLI, L. **Principia iuris**: Teoria del diritto e della democrazia. Bari: Laterza, v. 2, 2007. 713 p.

FERRAJOLI, L. **Poderes salvajes**: la crisis de la democracia constitucional. Tradução de Perfecto Andrés Ibáñez. Madrid: Trotta, 2011a. 109 p.

FERRAJOLI, L. **Por uma teoria dos direitos e dos bens fundamentais**. Tradução de Alexandre Salim; Alfredo Copetti Neto, *et al.* Porto Alegre: Livraria do Advogado, 2011b. 122 p.

FORD, H.; CROWTHER, S. **My life and work**. New York: Doubleday, Page & Company, 1923. 289 p.

FOUCAULT, M. **História da sexualidade I**: a vontade de saber. Tradução de Meria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 13. ed. Rio de Janeiro: Graal, v. 1, 1998. 152 p.

FOUCAULT, M. **Vigiar e punir**: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

FOUCAULT, M. **Segurança Território, População**: Curso dado no Collège de France (1997-1978). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008. 572 p.

FORTES, V. B. **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**. 2015. 225 f. Tese (Doutorado em Direito) – Universidade Estácio de Sá, Rio de Janeiro, 01 jun. 2015.

GANDY JR., O. H. Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems. **Ethics and Information Technology**, 12, n. 1, mar. p. 2010. 29-42. DOI: 10.1007/s10676-009-9198-6.

GANDY JR., O. H. Statistical surveillance: Remote sensing in the digital age. In: BALL, K.; HAGGERTY, K. D.; LYON, D. **Routledge Handbook of Surveillance Studies**. London: Routledge, 2012. p. 125-132.

GIBBS, S. Snowden: FBI's claim it can't unlock the San Bernardino iPhone is 'bullshit'. **The Guardian**, London, 09 mar. 2016. Disponível em: < <http://surveillance.es/1q> >. Acesso em: 10 mar. 2016.

GIDDENS, A. **Essential Concepts in Sociology**. Cambridge: Polity Press, 2014. 6059 po. Kindle Edition.

GIDDENS, A. **The Nation-State and Violence**. Cambridge: Polity Press, v. 2, 1985. 399 p.

GIDDENS, A. The Globalizing of Modernity. In: HELD, D.; MCGREW, A. **The Global Transformations Reader: An Introduction to the Globalizing Debate**. 2. ed. Cambridge: Polity, 2003. p. 60-66.

GIDDENS, A. **Sociology**. 6. ed. Cambridge: Polity, 2009. 1194 p.

GINSBERG, J. et al. Detecting influenza epidemics using search engine query data. **Nature**, n. 457, 19 fev. 2009. p. 1012-1014. Disponível em:< <http://surveillance.es/1c> >. Acesso em: 25 fev. 2016.

GRAHAM, S. **Cities under siege: the new military urbanism**. London: Verso, 2010. 402 p.

GREENBERG, A. These Are the Emails Snowden Sent to First Introduce His Epic NSA Leaks. **WIRED**, San Francisco, 13 out. 2014. Disponível em: < <http://surveillance.es/18> >. Acesso em: 19 fev. 2016.

GREENWALD, G *et al.* Microsoft handed the NSA access to encrypted messages. **The Guardian**, London, 12 jul. 2013. Disponível em: < <http://surveillance.es/1p> >. Acesso em: 10 mar. 2016.

GRIFFIN, A. France could ban public Wi-Fi and Tor anonymous browsing following Paris attacks. **Independent**, London, 07 dez. 2015. Disponível em: < <http://surveillance.es/2n> >. Acesso em: 01 maio 2016.

HABERMAS, J. **A constelação pós-nacional: ensaios políticos**. Tradução de Márcio Seligmann-Silva. São Paulo: Littera Mundi, 2001. 220 p.

HABERMAS, J. **Mudança estrutural da Esfera Pública**: investigações quanto a uma categoria da sociedade burguesa. Tradução de Flávio R. Kothe. Rio de Janeiro: Tempo Brasileiro, 2003. 398 p.

HAGGERTY, K. D. Tear down the walls: on demolishing the panopticon. In: LYON, D. **Theorizing surveillance**: The panopticon and beyond. Cullompton: Willan Publishing, 2006. p. 23-45.

HAGGERTY, K. D.; SAMATAS, M. Surveillance and democracy: an unsettled relationship. In: HAGGERTY, K. D.; SAMATAS, M. **Surveillance and Democracy**. New York: Routledge, 2010. p. 1-16.

HARDT, M.; NEGRI, A. Globalization as Empire. In: HELD, D.; MCGREW, A. **The Global Transformations Reader**: An Introduction to the Globalizing Debate. 2. ed. Cambridge: Polity, 2003. p. 116-119.

HARDT, M.; NEGRI, A. **Multitude**: war and democracy in the age of empire. New York: The Penguin Press, 2004. 405 p.

HELD, D. **Democracy and the Global Order**: From the Modern State to Cosmopolitan Governance. Stanford: Stanford University Press, 1995. 324 p.

HELD, D.; MCGREW, A. The Great Globalization Debate: An Introduction. In: HELD, D.; MCGREW, A. **The Global Transformations Reader**: An Introduction to the Globalizing Debate. 2. ed. Cambridge: Polity, 2003. p. 1-50.

HEIDEGGER, Martin. **Ser e tempo**: Parte I. Tradução de Marcia Sá Cavalcante. 8. ed. Petrópolis: Vozes, 1999. 325 p.

HENTZ, T. Câmeras devem ajudar a identificar carros roubados em Novo Hamburgo. **Jornal NH**, Novo Hamburgo, 06 ago. 2014. Disponível em: < <http://surveillance.es/h> >. Acesso em: 13 fev. 2016.

HORLING, B.; KULICK, M. Personalized Search for everyone. **Google Official Blog**, Mountain View, 04 dez. 2009. Disponível em: < <http://surveillance.es/28> >. Acesso em: 25 abr. 2016.

INNIS, H. **Empire and communications**. Toronto: Press Porcépic, 1986. 184 p.

INNIS, H. **The bias of communication**. Toronto: University of Toronto Press, 2008. Kindle Edition. 5695 pos.

INTERNATIONAL BANK FOR RECONSTRUCTION AND DEVELOPMENT. **World development report: digital dividends**. Washington: The World Bank, 2016. 330 p. DOI: 10.1596/978-1-4648-0671-1. Disponível em: < <http://surveillance.es/22> >. Acesso em: 11 abr. 2016.

JACOB NETO, E. **Concentração proprietária dos meios de comunicação de massas na democracia constitucional**. 2012. 216 f. Dissertação (Mestrado em Direito) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 11 set. 2012. Disponível em: < <http://surveillance.es/2a> >. Acesso em: 25 abr. 2016.

JOHNSON, D.; WAYLAND, K. Surveillance and transparency as sociotechnical systems of accountability. In: HAGGERTY, K.; SAMATAS, M. **Surveillance and democracy**. London: Routledge, 2010. p. 19-33.

KAFKA, F. **O processo**. Tradução de Gervásio Álvaro. Lisboa: Livros do Brasil, 1999. 285 p. Disponível em: < <http://surveillance.es/y> >. Acesso em: 15 fev. 2015.

KAHNEMAN, D.; TVERSKY, A. Belief in the law of small numbers. **Psychological Bulletin**, s.l, 72, n. 2, 1971. p. 105-110. DOI: 10.1037/h0031322.

KANNEBERG, V. Câmera vai fotografar usuários para coibir fraude no uso do passe livre em ônibus da Região Metropolitana. **ZH Notícias**, Porto Alegre, 30 jun. 2015. Disponível em: < <http://surveillance.es/f> >. Acesso em: 13 fev. 2016.

KASSAM, A. Spain's everyday internet warrior who cut free from Google's tentacles. **The Guardian**, London, 13 maio 2014. Disponível em: < <http://surveillance.es/21> >. Acesso em: 27 mar. 2016.

KELION, L. Bots now 'account for 61% of web traffic'. **BBC News**, London, 12 dez. 2013. Disponível em: < <http://surveillance.es/e> >. Acesso em: 12 fev. 2016.

KOSINSKI, M.; STILLWELL, D.; GRAEPEL, T. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences of the United States of America**, 110, n. 15, 9 abr. 2013. p. 5802-5805. Disponível em: < <http://surveillance.es/o> >. Acesso em: 15 fev. 2016.

KRAMERA, A.; GUILLORY, J.; HANCOCK, J. Experimental evidence of massive-scale emotional contagion through social networks. **Proceedings of the National Academy of Sciences of the United States of America**, 2 jun. 2014. p. 8788-8790. Disponível em: < <http://surveillance.es/1d> >. Acesso em: 29 fev. 2016.

KRIEG, G. No-fly nightmares: The program's most embarrassing mistakes. **CNN Politics**, Atlanta, 07 dez. 2015. Disponível em: < <http://surveillance.es/1i> >. Acesso em: 01 mar. 2016.

KUHN, T. **A estrutura das revoluções científicas**. Tradução de Beatriz Boeira. 5. ed. São Paulo: Perspectiva, 1998. 257 p.

LEAL, A. Facebook desbloqueia foto de índios botocudos. **EBC**, Brasília, 17 abr. 2015. Disponível em: < <http://surveillance.es/2g> >. Acesso em: 28 abr. 2016.

LANE, N. D. et al. **MoodScope**: building a mood sensor from smartphone usage patterns. Proceeding of the 11th annual international conference on Mobile systems, applications, and services. New York: ACM. 2013. p. 389-402. Disponível em:< <http://surveillance.es/1x> >. Acesso em: 24 mar. 2016.

LAPLACE, P. S. M. D. **Essai philosophique sur les probabilités**. 6. ed. Paris: Bachelier, 1840. 274 p.

LAZER, D. et al. The Parable of Google Flu: Traps in Big Data Analysis. **Science**, 343, n. 6176, 14 mar. 2014. p. 1203-1205. DOI: 10.1126/science.1248506. Disponível em: < <http://surveillance.es/1j> >. Acesso em: 02 mar. 2016.

LISBOA, V. Renda média do brasileiro cai 1,9% em maio, informa IBGE. **EBC**, Brasília, 06 ago. 2014. Disponível em: < <http://surveillance.es/j> >. Acesso em: 13 fev. 2016.

LI RIU et al. Six Novel Susceptibility Loci for Early-Onset Androgenetic Alopecia and Their Unexpected Association with Common Diseases. **PLoS Genetics**, San Francisco, v. 2, n. 5, DOI: 10.1371/journal.pgen.1002746. Não paginado. Disponível em: < <http://surveillance.es/1k> >. Acesso em: 09 mar. 2016.

LUCKERSON, V. Netflix Gets a Speed Boost, Courtesy of Comcast. **Time**, New York, 12 maio 2014. Disponível em: < <http://surveillance.es/2f> >. Acesso em: 27 abr. 2016.

LYON, D. **The Electronic Eye: The Rise of Surveillance Society**. Minneapolis: University of Minnesota Press, 1994. 270 p.

LYON, D. **Surveillance society: Monitoring everyday life**. Buckingham: Open University Press, 2001. 189 p.

LYON, D. Introduction. In: LYON, D. **Surveillance as Social Sorting: Privacy, risk and digital discrimination**. London: Routledge, 2003a. p. 1-9.

LYON, D. Surveillance as social sorting: computer codes and mobile bodies. In: LYON, D. **Surveillance as Social Sorting: Privacy, risk and digital discrimination**. London: Routledge, 2003b. p. 13-30.

LYON, D. **Surveillance Studies: An Overview**. Cambridge: Polity, 2007. 243 p.

LYON, D. Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies. **International Political Sociology**, 4, n. 4, 1 dez. 2010. p. 325-338. DOI: 10.1111/j.1749-5687.2010.00109.x.

LYON, D. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, 1, n. 2, Jul. 2014. p. 1-13. DOI: 10.1177/2053951714541861.

LYON, D. **Snowden Surveillance after**. Cambridge: Polity Press, 2015. Kindle Edition.

MANN, M. Has Globalization Ended the Rise and Rise of the Nation-State? In: HELD, D.; MCGREW, A. **The Global Transformations Reader: An Introduction to the Globalizing Debate**. 2. ed. Cambridge: Polity, 2003. p. 135-146.

MARI, A. Protest organizers in Brazil use analytics to measure attendance. **ZDNet**, [s.l.], 14 mar. 2016. Disponível em: < <http://surveillance.es/1w> >. Acesso em: 15 mar. 2016.

MARX, G. T. What's New about the "New Surveillance"?: Classifying for Change and Continuity. **Surveillance & Society**, Kingston, 1, n. 1, 2002. p. 9-29.

MAYER, J; MUTCHER, P. MetaPhone: The Sensitivity of Telephone Metadata. **Web Policy**, [s.l.], 12 mar. 2014. Disponível em: < <http://surveillance.es/n> >. Acesso em: 15 fev. 2016.

MCCULLOCH, J.; WILSON, D. **Pre-crime**: pre-emption, precaution and the future. New York: Routledge, 2016. 154 p.

MCLUHAN, M. Playboy interview Marshall McLuhan: a candid conversation with the high priest of popcult and metaphysician of media. **Playboy**, Chicago, 16, n. 3, mar. 1969. p. 53-75.

MENN, J. NSA infiltrated RSA security more deeply than thought - study. **Reuters**, London, 31 mar. 2014. Disponível em: < <http://surveillance.es/8> >. Acesso em: 07 fev. 2016.

MILL, J. S. **Principles of Political Economy**. 7. ed. London: Longmans, Green and Co., 1909. Não paginado. Disponível em:< <http://surveillance.es/2b> >. Acesso em: 25 abr. 2016.

MITROU, L. The impact of communications data retention on fundamental rights and democracy: the case of the EU Data Retention Directive. In: HAGGERTY, K.; SAMATAS, M. **Surveillance and democracy**. New York: Routledge, 2010. p. 127-147.

MLODINOW, L. **The Drunkard's Walk**: How Randomness Rules Our Lives. New York: Pantheon Books, 2008. 252 p.

MONTESQUIEU, C. D. S.-B. D. **O espírito das leis**. Tradução de Cristina Murachco. 3. ed. São Paulo: Martins Fontes, 2000. 851 p.

MORIN, E. **Cultura e barbárie européias**. Tradução de Ana Paula de Viveiros. Lisboa: Instituto Piaget, 2005. 75 p.

MURAKAMI WOOD, D. Beyond the Panopticon? Foucault and Surveillance Studies. In: CRAMPTON, J. W.; ELDEN, S. **Space, Knowledge and Power**: Foucault and Geography. Aldershot: Ashgate, 2007. p. 245-263.

MURAKAMI WOOD, D. Globalization and surveillance. In: BALL, K.; HAGGERTY, K. D.; LYON, D. **Routledge Handbook of Surveillance Studies**. London: Routledge, 2012. p. 333-342.

NARAYANAN, A.; SHMATIKOV, V. **Robust De-anonymization of Large Sparse Datasets**. Proceedings of the 2008 IEEE Symposium on Security and Privacy. Washington: IEEE Computer Society, 2008. p. 111-125. Disponível em: < <http://surveillance.es/t> >. Acesso em: 15 fev. 2016.

NATIONAL INFORMATION STANDARDS ORGANIZATION. **Understanding Metadata**. Bethesda: NISO Press, 2004. 17 p. ISBN 1880124629. Disponível em: < <http://surveillance.es/l> >. Acesso em: 14 fev. 2016.

NATIONAL SECURITY AGENCY. **SIGINT Strategy: 2012-2016**. [s.l.], 5 p. 2012. Disponível em: < <http://surveillance.es/1u> >. Acesso em: 10 mar. 2016.

NETFLIX. Netflix Prize FAQ. **Netflix Prize**, 02 out. 2006. Não paginado. Disponível em: < <http://surveillance.es/u> >. Acesso em: 15 fev. 2016.

NIXON, R. U. S. Postal Service Logging All Mail for Law Enforcement. **The New York Times**, New York, 03 jul. 2013. Disponível em: < <http://surveillance.es/m> >. Acesso em: 14 fev. 2016

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **2014 Report on Security Clearance Determinations**. Director of National Intelligence. Washington, D.C., 10 p. 2015. Disponível em: < <http://surveillance.es/11> >. Acesso em: 16 fev. 2016.

ORWELL, G. **1984**. Tradução de Wilson Velloso. São Paulo: Companhia das Letras, 2009. Kindle Edition. Não paginado.

PEDUZZI, P. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. **EBC**, Brasília, 19 out. 2015. Disponível em: < <http://surveillance.es/k> >. Acesso em: 01 maio 2016.

PÉREZ LUÑO, A. E. **¿Ciberciudadaní@ o ciudadaní@.com?** Barcelona: Gedisa, 2003. 142 p.

PÉREZ LUÑO, A. E. **Los derechos humanos en la sociedad tecnológica**. Madrid: Editorial Universitas, 2012. 140 p.

PARISER, E. **The filter bubble: What the Internet is Hiding from You**. New York: The Penguin Press, 2011. 294 p.

PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY. **The darknet and online anonymity**. Houses of Parliament. London, 4 p. 2015.

PASQUALE, F. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. 311 p.

QUEROL, R. Zygmunt Bauman: “As redes sociais são uma armadilha”. **El País**, Madrid, 09 jan. 2016. Disponível em: < <http://surveillance.es/2w> >. Acesso em: 04 maio 2016.

RAMSEY, L. 23andMe CEO defends practice of sharing genetic info with pharma companies. **Business Insider**, New York, 07 jul. 2015. Disponível em: < <http://surveillance.es/19> >. Acesso em: 19 fev. 2016.

RAWLS, J. **Political Liberalism**. New York: Columbia University Press, 1996. 464 p.

ROCHA, L. S.; KING, M.; SCHWARTZ, G. **A verdade sobre a autopoiese no direito**. Porto Alegre: Livraria do Advogado, 2009. 148 p.

RODOTÀ, S. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. 382 p.

RODOTÀ, S. **Il mondo nella rete**: Quali i diritti, quali i vincoli. Roma: Laterza / la Repubblica, 2014. Kindle Edition. 1307 pos.

SALTER, M. B. The global visa regime and the political technologies of the international self: borders, bodies, biopolitics. **Alternatives**, 31, n. 2, abr. 2006. p. 167-189. doi: 10.1177/030437540603100203.

SASSEN, S. **Losing control? Sovereignty in an Age of Globalization**. New York: Columbia University Press, 1996. Não paginado.

SASSEN, S. **Territory, authority, rights**. Woodstock: Princeton University Press, 2006. 493 p.

SASSEN, S. **Sociology of globalization**. New York: W. W. Norton & Company, 2007. 308 p.

SCHIOCCHET, T. A regulamentação da base de dados genéticos para fins de perseguição: reflexões acerca do uso forense do DNA. **Novos Estudos Jurídicos**, [s.l.], 18, n. 3, dez. 2013. p. 518-529. Disponível em: < <http://surveillance.es/15> >. Acesso em: 18 fev. 2016.

SCHNEIER, B. **Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World**. New York: W. W. Norton & Company, 2015. 398 p.

SCHOPENHAUER, A. **A arte de escrever**. Tradução de Pedro Sússekind. Porto Alegre: L&PM, 2009. 176 p.

SEGALL, L. Oops! Russian soldier Instagrams himself in Ukraine. **CNN Money**, Atlanta, 01 ago. 2014. Disponível em: < <http://surveillance.es/2i> >. Acesso em: 28 abr. 2016.

SEVERIANO, A. Ônibus terão biometria facial após fraudes de R\$ 230 mil por mês, no AM. **G1 Amazonas**, Manaus, 23 nov. 2015. Disponível em: < <http://surveillance.es/g> >. Acesso em: 13 fev. 2016.

SILVER, N. **The Signal and the Noise: Why Most Predictions Fail – but Some Don't**. 2. ed. New York: Penguin, 2015. 560 p. ISBN: 978-1-59-420411-1.

SOLOVE, D. J. **The digital person: technology and privacy in the information age**. New York: New York University Press, 2004. 283 p.

SORENSEN, G. **La transformación del Estado: más allá del mito del repliegue**. Tradução de Ramón Cotarelo. Valência: Tirant lo blanch, 2010. 229 p.

SPRENGER, P. Sun on Privacy: 'Get Over It'. **Wired**, London, 26 jan. 1999. Disponível em: < <http://surveillance.es/2k> >. Acesso em: 29 abr. 2016.

STAPLES, W. **Everyday surveillance: vigilance and visibility in postmodern life**. 2. ed. Lanham: Rowman & Littlefield, 2014. 6751 p. Kindle Edition. 6571 pos.

STEEVES, V. It's Not Child's Play: The Online Invasion of Children's Privacy. **University of Ottawa Law & Technology Journal**, 3, n. 1, 2006. 169-188. Disponível em: < <http://surveillance.es/2j> >. Acesso em: 29 abr. 2016.

STRECK, L. L. As portarias, o mensalção de o “fator Carminha”. **Consultor Jurídico**. 9 ago. 2012. Disponível em < <http://surveillance.es/2-> >. Acesso em: 01 jun. 2016.

STRECK, L. L. **Jurisdição constitucional e decisão judicial**. 4. ed. São Paulo: Revista dos Tribunais, 2014. 980 p.

STRECK, L. L. **Verdade e Consenso**: constituição, hermenêutica e teorias discursivas. 4. ed. São Paulo: Saraiva, 2011. 639 p.

SULLIVAN, A. More Americans see man who leaked NSA secrets as 'patriot' than traitor - poll. **Reuters**, London, 13 jun. 2013. Disponível em: < <http://surveillance.es/2c> >. Acesso em: 26 abr. 2016.

SUNSTEIN, C. R. **Infotopia**: How Many Minds Produce Knowledge. New York: Oxford University Press, 2006. 273 p.

SUNSTEIN, C. R. **Republic.com 2.0**. Princeton: Princeton University Press, 2007. 251 p.

TANNER, A. Different Customers, Different Prices, Thanks To Big Data. **Forbes**, New York, 26 mar. 2014. Disponível em: < <http://surveillance.es/1h> >. Acesso em 01 mar. 2016.

TEUBNER, G. **O direito como sistema autopoietico**. Tradução de José Engrácia Antunes. Lisboa: Fundação Calouste Gulbenkian, 1989. 357 p.

TEUBNER, G. Societal Constitutionalism: Alternatives to State-centred Constitutional Theory. **Storrs Lectures 2003/04 Yale Law School**, [s.l.], 24 p. 2004. Disponível em:< <http://surveillance.es/2l> >. Acesso em: 29 abr. 2016.

TEUBNER, G. Constitutionalising Polycontextuality. **Social & Legal Studies**, 20, n. 2, jun. 2011a. p. 210-229. doi:10.1177/0964663911400245.

TEUBNER, G. Transnational Fundamental Rights: Horizontal Effect? **Netherlands Journal of Legal Philosophy**, 40, n. 3, 2011b. p. 191-215. Disponível em: < <http://surveillance.es/26> >. Acesso em: 20 abr. 2016.

TOOLE, J. L. et al. Tracking employment shocks using mobile phone data. **Journal of the royal society interface**, 12, n. 107, 27 maio 2015. 1-9. DOI: 10.1098/rsif.2015.0185.

VERSCHRAEGEN, G. Hybrid Constitutionalism, Fundamental Rights and the State: A Response to Gunther Teubner. **Netherlands Journal of Legal Philosophy**, v. 40, n. 3, p. 216-229, 2011. ISSN: 213-0721. Disponível em:< <http://surveillance.es/27> >. Acesso em: 23 abr. 2016.

WARAT, Luis Alberto. **A Ciência Jurídica e seus dois maridos**. 2. ed. Santa Cruz do Sul: EDUNISC, 2000. 200 p.

WEBER, M. **Economia e sociedade**: fundamentos da sociologia compreensiva. Tradução de Regis Barbosa e Karen Elsabe Barbosa. Brasília: Universidade de Brasília, v. 2, 1999. 586 p.

WHITSON, J. R. Surveillance and democracy in the digital enclosure. In: HAGGERTY, K.; SAMATAS, M. **Surveillance and democracy**. London: Routledge, 2010. p. 231-246.