doi: 10.5102/rbpp.v7i3.4840

O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da *dataveillance* em relação à utilização de metadados e seu impacto nos direitos humanos*

The draft law on personal data protection (PL 5276/2016) in the big data world: dataveillance through the use of metadata and its impacts on human rights

Elias Jacob de Menezes Neto**

Jose Luis Bolzan de Morais***

Tiago José de Souza Lima Bezerra****

Resumo

A utilização de metadados por entidades públicas e privadas é uma realidade que ganhou vida a partir dos avanços da tecnologia da informação com o fenômeno da Globalização. Ao abordar o tema da vigilância eletrônica, por meio de uma estratégia metodológica de caráter fenomenológico-hermenêutico e transdisciplinar, este artigo pretende analisar os impactos da utilização desses dados nos direitos humanos, e a tentativa de o Estado regulamentar seu uso por meio de instrumentos normativos, como o projeto de lei de proteção de dados no Brasil (PL 5276/2016). Verifica-se, por meio das análises feitas, que o fenômeno da surveillance atinge muito mais que a privacidade, sendo um fator determinante para a violação da dignidade, e propulsor da segregação social, sendo os instrumentos jurídicos atuais de controle da vigilância eletrônica insuficientes para a proteção efetiva dos dados pessoais diante das ideias de desterritorialidade e desespacialidade associadas ao enfraquecimento da soberania moderna. Finalmente, a originalidade deste trabalho demonstra-se por meio da falta de estudos no Brasil sobre a surveillance, e a superação da ideia simplória de que esse fenômeno atinge, apenas, a privacidade, sendo um fator determinante para a segregação social e desigualdade.

Palavras-chave: Dataveillance. Metadados. Dados pessoais. Big data. Direitos humanos.

Abstract

The use of metadata by public and private entities is a reality that has arisen from the advances of information technology with the phenomenon of Globalization. When discussing the topic of electronic surveillance, using a

* Recebido em 11/10/2017
Aprovado em 02/11/2017

** Mestre e Doutor em Direito Público pela Universidade do Vale do Rio dos Sinos. Professor adjunto do curso de Direito da Universidade Federal do Rio Grande do Norte, campus de Caicó/RN. Coordenador do Núcleo de Prática Jurídica e do Laboratório de Governança Pública, ambos da UFRN. E-mail: eliasjacob@ceres.ufrn.br

*** Mestre em Direito pela Pontifícia Universidade Católica do Rio de Janeiro. Doutor em Direito pela Universidade Federal de Santa Catarina. Bolsista de Produtividade em Pesquisa do CNPq – Nível 1D. Professor do Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – Mestrado e Doutorado. E-mail: bolzan@hotmail.com

**** Graduado em Direito pela Universidade Federal do Rio Grande do Norte (UFRN/CERES). Monitor do Núcleo de Prática Jurídica do CERES/UFRN. Bolsista de Iniciação Científica do Laboratório de Governança Pública da UFRN. E-mail: tiagobezerra@labgov.pub

phenomenological-hermeneutic and transdisciplinary methodological strategy, this article intends to analyze the impacts of the use of these data on human rights, and the State's attempt to regulate its use through normative instruments, as the draft law on data protection in Brazil. It's verified, through the analyzes made, that the phenomenon of surveillance reaches much more than privacy, being a determining factor for the violation of dignity, and a propeller of social segregation, being the current legal instruments of electronic surveillance insufficient for the effective protection of personal data, in the face of the ideas of deterritoriality and desaspaciality associated with the weakening of modern sovereignty. Eventually the originality of this work can be demonstrated by the lack of studies in Brazil about surveillance, and the overcoming of the simplistic idea that this phenomenon only affects privacy, being a determining factor for social segregation and inequality.

Keywords: Dataveillance. Metadada. Personal data. Big data. Human rights.

1. Introdução

Ao discutir o tema da vigilância eletrônica, geralmente, há uma associação com a metáfora do Big Brother de George Orwell, o que pode levar a equívocos teóricos. 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[1] da fabricante Samsung, as quais possuem um mecanismo de reconhecimento de voz capaz de enviar tudo que é falado no ambiente para a fabricante e suas parceiras, o que se assemelha muito à teletela prevista por Orwell —, sua aplicação ao mundo contemporâneo é bastante limitada. Isso se deve ao fato de a tarefa de monitoramento, como será visto neste artigo, ter sido expandida, tornando-se parte fundamental das estratégias de *marketing* da iniciativa privada. Como resultado, o mundo atual parece mais compatível com um conjunto de *little sisters* do que com um único *Big Brother*.

Para superação dessas metáforas, será apresentado um modelo diferenciado chamado "*surveillance assemblages*", proposto por Richard Ericson e Kevin Haggerty. Esse modelo dá ênfase aos fluxos discretos de dados, ou seja, ao aspecto da *surveillance* que se convencionou chamar de *dataveillance*, propondo-se o uso da obra "O processo", de Franz Kafka como uma alternativa para se pensar esse modelo.

Utilizando-se uma estratégia metodológica de caráter fenomenológico-hermenêutico e transdisciplinar, será abordada a relação do tema com as insuficiências presentes no cenário jurídico nacional. No caso, este artigo analisará o problema de fluxos de dados — e metadados — e como a ausência de compreensão das tecnologias da informação e comunicação (TICs) gera consequências nefastas para o PL 5276/2016 e o que nele é classificado como "dados anônimos".

Para compreender o fenômeno das TICs, será necessário, primeiramente, demonstrar quais os motivos para a adoção da palavra "*surveillance*" (em inglês) na construção dessa categoria, o que possibilitará ver o seu estreito e inseparável vínculo com a tecnologia da informação. É justamente nesse sentido que será abordada 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[2]. Por essa razão, será analisado esse modelo, verificando sua aplicabilidade ao cenário jurídico nacional, 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*.

1 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://www.samsung.com/hk_en/info/privacy/smarttv/ >. Acesso em: 22 out. 2017.

2 ORWELL, G. *1984*. Tradução: Wilson Velloso. São Paulo: Companhia das Letras, 2009. Não paginado.

2. Dataveillance como metáfora para o mundo atual

Nos últimos anos, o panóptico, de Jeremy Bentham[3] e Michel Foucault[4], foi o modelo padrão nos estudos sobre a vigilância. Ainda que as práticas de vigilância sejam tão antigas quanto a própria civilização ocidental, elas adquiriam 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 por meio do panóptico. Isso porque 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.

Embora a tradução literal — vigilância — seja linguisticamente adequada, a palavra em Língua Inglesa — bem como Língua Francesa — possui uma polissemia que não é alcançada pelo termo em Língua Portuguesa do Brasil. Logo, será sempre uma aproximação de um conceito, não o próprio conceito.

Ao utilizar o conceito em Língua Inglesa, forma-se um novo sentido para a palavra *surveillance*, incapaz de ser abarcado pela sua tradução literal. O conceito de *surveillance* ultrapassa os limites da concepção tradicional de vigilância, uma vez que permite trazer a tecnologia para dentro das relações sociais. Em vez 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. Dataveillance

Um outro modo de pensar a *surveillance* é trazido por Kevin D. Haggerty e Richard V. Ericson. Com base nos trabalhos de Gilles Deleuze e Félix Guattari 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.[5] 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 d*ata doubles,* ou seja, os alteregos digitais.

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* (multiplicidade de objetos distintos cuja unidade provém do fato de que eles funcionam em conjunto como uma entidade funcional), 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. Trata-se da aglutinação das palavras *data* e *surveillance* e pode ser definida como o uso sistemático de sistemas de dados pessoais na investigação e monitoramento de ações e comunicações de um ou mais

3 BENTHAM, Jeremy. *The Works of Jeremy Bentham*. Edinburgh: William Tait, 1843. v. 4.

4 FOUCAULT, Michel. *Vigiar e punir*: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

5 ERICSON, Richard; HAGGERTY, Kevin. The surveillant assemblage. *British Journal of Sociology,* London, v. 51, n. 4, p. 605-622, dez. 2000.

indivíduos[6].

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 dados. 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[7]. 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, 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*, 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[8] Manaus[9] com o intuito de verificar

6 CLARKE, Roger. Information technology and dataveillance. *Communications of the ACM*, v. 31, n. 5, p. 498-512, maio 1988.

7 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.

8 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. Para maiores detalhes: KANNEBERG, Vanessa. 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: <https://gauchazh.clicrbs.com.br/geral/noticia/2015/06/camera-vai-fotografar-usuarios-para-coibir-fraude-no-uso-do-passe-livre-em-onibus-da-regiao-metropolitana-4792089.html >. Acesso em: 22 out. 2017.

9 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 Transporte Urbanos conseguiu impedir gastos

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/RS[10], 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 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 reais[11]. 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 dividas.

Se, anteriormente, 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[12], 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 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.

equivalentes a R$230.000,00 mensais com fraudes. Para maiores detalhes: SEVERIANO, Adneilson. Ônibus terão biometria facial após fraudes de R$ 230 mil por mês, no AM. *G1 Amazonas*, Manaus, 23 nov. 2015. Disponível em: <http://g1.globo.com/am/amazonas/noticia/2015/11/onibus-terao-biometria-facial-apos-fraudes-de-r-230-mil-por-mes-no-am.html>. Acesso em: 22 out. 2017.

10 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. Para maiores detalhes: HENTZ, Tatiane. Câmeras devem ajudar a identificar carros roubados em Novo Hamburgo. *Jornal NH*, Novo Hamburgo, 6 ago. 2014. Disponível em: <http://www.jornalnh.com.br/_conteudo/2014/08/noticias/regiao/70867-cameras-devem-ajudar-a-identificar-carros-roubados-em-novo-hamburgo.html>. Acesso em: 22 out. 2017.

11 Sob as acusações de que o sistema e-Financeira 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. Os detalhes sobre a referida nota da RFB estão disponíveis em <http://idg.receita.fazenda.gov.br/noticias/ascom/2016/fevereiro/nota-de-esclarecimento-sobre-a-e-financeira>. Acesso em: 22 out. 2017.

12 LISBOA, Vinícius. Renda média do brasileiro cai 1,9% em maio, informa IBGE. *EBC,* Brasília, 6 ago. 2014. Disponível em: <http://www.ebc.com.br/noticias/economia/2015/06/renda-media-do-brasileiro-cai-19-em-maio-informa-ibge>. Acesso em: 22 out. 2017.

2.2. Franz Kafka e a metáfora da *dataveillance*

Diante do que foi exposto neste artigo, diversos aspectos da *surveillance* não foram capturados nem por Foucault[13] 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.

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[14].

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 por meio 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.[15]

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 na audiência. Após o 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*. Por meio 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.

13 FOUCAULT, Michel. *Vigiar e punir*: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.
14 KAFKA, Franz. *O processo*. Tradução: Gervásio Álvaro. Lisboa: Livros do Brasil, 1999. 285 p.
15 KAFKA, Franz. *O processo*. Tradução: Gervásio Álvaro. Lisboa: Livros do Brasil, 1999. 285 p.

É possível, pois, argumentar que Kafka 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.

3. O PODER DOS METADADOS E O PL 5276/2016

3.1. 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"[16].

De modo simplificado, é possível utilizar a metáfora de uma carta ordinária. 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 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 Snowden, 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. 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.[17]

16 NATIONAL INFORMATION STANDARDS ORGANIZATION. *Understanding Metadata*. Bethesda: NISO Press, 2004. 17 p.
17 RODOTÀ, S. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. 382 p.

Existe um experimento em andamento cujo intuito é demonstrar para as pessoas a relevância dos metadados. Intitulado *MetaPhone*, 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 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[18].

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 veí-

18 MAYER, J.; MUTCHER, P. MetaPhone: The Sensitivity of Telephone Metadata. *Web Policy*, [S.l.], 12 mar. 2014.

culo 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* para determinar riscos, preferências e hábitos das pessoas. A sofisticação técnica dos programas que realizam análises de *big data* surpreende o "usuário comum" — vide, por todos, o estudo de Kosinski Stillwell e Graepel[19] que construiu um sistema capaz de identificar traços de personalidade do usuário a partir das suas "curtidas" na rede social *Facebook*.

3.2. O PL 5276/2016 e a ilusão de que existem (meta)dados "anônimos"

Embora exista projeto similar tramitando no Senado (PLS 330/2013), a massiva participação popular no texto que resultou no PL 5276/2016 torna a proposta da Câmara muito mais relevante do ponto de vista democrático. Isso porque, após a aprovação do marco civil da internet (Lei 12.965/2014), 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 que ocorreu depois de mais de 1300 colaborações no site da consulta pública[20]. Desse APL surgiu o PL 5276/2016, daí a sua maior importância na análise aqui realizada.

Ressalte-se: 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 sofre de um problema fundamental, pois considera que, ainda, se está lidando, apenas, com dados pessoais. Isso torna-se evidente já no artigo 1º, em que 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.*[21]*"*

Com uma definição desse tipo, o PL 5276/2016 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 PL 5276/2016 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 PL 5276/2016 fosse considerada um mero "esquecimento", suas consequências para a proteção dos direitos humanos seriam igualmente prejudiciais, especialmente quando

19 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*, v. 110, n. 15, p. 5802-5805, 9 abr. 2013.

20 PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. *EBC*, Brasília, 19 out. 2015. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet>. Acesso em: 22 out. 2017.

21 BRASIL. *Projeto de Lei de proteção de dados pessoais: PL 5276/2016*. Brasília: Câmara dos Deputados, 2016.

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 PL 5276/2016 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 locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa".

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 politicas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou politico, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos.

Por fim, os dados anônimos, conforme inciso IV do artigo 5º do PL 5276/2016, seriam aqueles "[...] dados relativos a um titular que não possa ser identificado".

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. Esses 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 PL 5276/2016 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 PL 5276/2016 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 — anônimos[22]. 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, por meio de consultas de bases de dados de acesso público, inferir informações como orientação sexual e traços de personalidade[23]

22 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: <https://33bits.org>. Acesso em: 22 out. 2017.

23 ACQUISTI, Alessandro; GROSS, Ralph; STUTZMAN, Fred. Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, Pittsburgh, v. 6, n. 2, p. 1-20, 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[24]. Como isso ocorreu?

Em 2006, o Netflix — o maior serviço de *steaming* 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:

> 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?[25].

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 reunir um conjunto de dados completamente anônimos e cruzá-los 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 etc.

É preciso 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 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".

4. Considerações finais

A visão de George 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

24 NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets. In: *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 2008, Washington: IEEE Computer Society. 2008. p. 111-125

25 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?"

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, relembrando, assustadoramente, aspectos da atualidade, questões sobre direitos humanos, como igualdade e dignidade, são tocadas pela obra de Orwell, associadas à impossibilidade de construir uma identidade própria, distinta das massas; e do exercício de controle de acordo com cada grupo social, o que se assemelha muito com a ideia de *dataveillance* e utilização de metadados.

Ao contrário das propostas de Foucault, Bentham e Orwell, 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, como comumente ocorre com a literatura tradicional sobre o tema[26].

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[27], modifica a expectativa de resposta dos sistemas tecnológicos, que devem deixar de ser reativos e conservativos — ou seja, preservar a ordem por meio 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.

Também, verificou-se que, embora importantes, os mecanismos de controle estatais (como PL 5276/2016, para a proteção dos dados pessoais no Brasil) são incapazes de proteger, adequadamente, os direitos humanos, o que ocorre como consequência de alguns fenômenos: da globalização; do surgimento de novos centros de poder não estatais; e 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.

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 da 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 PL 5276/2016 — das cruéis violações da igualdade e da liberdade patrocinadas pela tecnologia da informação.

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.

26 PÉREZ-LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución*. 5. ed. Madrid: Tecnos, 1995. 550 p.; PÉREZ-LUÑO, Antonio Enrique. **Los derechos fundamentales**. Madrid: Tecnos, 2005. 233 p.

27 HARDT, Michael; NEGRI, Anthony. *Multitude*: war and democracy in the age of empire. New York: The Penguin Press, 2004. 405 p.

Por isso, é possível — e necessário — compreender que as TICs atingem muito mais que a privacidade, podendo servir como um instrumento de segregação social e caracterizador da violação à isonomia e à dignidade. São insuficientes as tentativas de restringir os fluxos de dados na sociedade em rede[28] por meio de mecanismos rígidos, centrados em territórios, como é o caso das legislações derivadas do Estado-nação.

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 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 por meio 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*. É necessário, portanto, repensar os modelos de proteção de direitos na contemporaneidade, o que fugiria do escopo do presente artigo, mas deve servir como provocação para o leitor atento.

Referências

ACQUISTI, Alessandro; GROSS, Ralph; STUTZMAN, Fred. Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, Pittsburgh, v. 6, n. 2, p. 1-20, 2014.

BRASIL. *Projeto de Lei de proteção de dados pessoais: PL 5276/2016*. Brasília: Câmara dos Deputados, 2016.

BENTHAM, Jeremy. *The Works of Jeremy Bentham*. Edinburgh: William Tait, 1843. v. 4.

BOLZA DE MORAIS, Jose Luis; JACOB NETO, Elias. 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, George Salomão; LEMOS, Ronaldo. *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 417-439.

CASTELLS, Manuel. *The rise of the network society*: The information age – economy, society and culture. 2. ed. Chichester: Wiley-Blackwell, 2010. v. 1.

CLARKE, Roger. Information technology and dataveillance. *Communications of the ACM*, v. 31, n. 5, p. 498-512, maio 1988.

ERICSON, Richard; HAGGERTY, Kevin. The surveillant assemblage. *British Journal of Sociology,* London, v. 51, n. 4, p. 605-622, dez. 2000.

FOUCAULT, Michel. *Vigiar e punir*: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

HARDT, Michael; NEGRI, Anthony. *Multitude*: war and democracy in the age of empire. New York: The Penguin Press, 2004. 405 p.

HENTZ, Tatiane. Câmeras devem ajudar a identificar carros roubados em Novo Hamburgo. *Jornal NH*, Novo Hamburgo, 6 ago. 2014. Disponível em: < http://www.jornalnh.com.br/_conteudo/2014/08/noticias/regiao/70867-cameras-devem-ajudar-a-identificar-carros-roubados-em-novo-hamburgo.html>. Acesso em: 22 out. 2017.

KAFKA, Franz. *O processo.* Tradução: Gervásio Álvaro. Lisboa: Livros do Brasil, 1999. 285 p.

KANNEBERG, Vanessa. 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: <https://gauchazh.clicrbs.com.br/geral/noticia/2015/06/camera-vai-fotografar-usuarios-para-coibir-fraude-no-uso-do-passe-

28 CASTELLS, Manuel. *The rise of the network society*: The information age – economy, society and culture. 2. ed. Chichester: Wiley-Blackwell, 2010. v. 1.

livre-em-onibus-da-regiao-metropolitana-4792089.html>. Acesso em: 22 out. 2017.

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*, v. 110, n. 15, p. 5802-5805, 9 abr. 2013.

LISBOA, Vinícius. Renda média do brasileiro cai 1,9% em maio, informa IBGE. *EBC*, Brasília, 6 ago. 2014. Disponível em: < http://www.ebc.com.br/noticias/economia/2015/06/renda-media-do-brasileiro-cai-19-em-maio-informa-ibge >. Acesso em: 22 out. 2017.

MAYER, J.; MUTCHER, P. MetaPhone: The Sensitivity of Telephone Metadata. *Web Policy*, [S.l.], 12 mar. 2014.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets. In: *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 2008, Washington: IEEE Computer Society. 2008. p. 111-125.

NATIONAL INFORMATION STANDARDS ORGANIZATION. *Understanding Metadata*. Bethesda: NISO Press, 2004. 17 p.

ORWELL, G. *1984*. Tradução: Wilson Velloso. São Paulo: Companhia das Letras, 2009. Não paginado.

PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. *EBC*, Brasília, 19 out. 2015. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet>. Acesso em: 22 out. 2017.

PÉREZ-LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución*. 5. ed. Madrid: Tecnos, 1995. 550 p.

PÉREZ-LUÑO, Antonio Enrique. *Los derechos fundamentales*. Madrid: Tecnos, 2005. 233 p.

RODOTÀ, S. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. 382 p.

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.

SEVERIANO, Adneilson. Ônibus terão biometria facial após fraudes de R$ 230 mil por mês, no AM. *G1 Amazonas*, Manaus, 23 nov. 2015. Disponível em: <http://g1.globo.com/am/amazonas/noticia/2015/11/onibus-terao-biometria-facial-apos-fraudes-de-r-230-mil-por-mes-no-am.html>. Acesso em: 22 out. 2017.