Revista Jurídica vol. 03, n°. 70, Curitiba, 2022. pp. 770 - 791

DEMOCRACIA, FLUXO DE DADOS E SOCIEDADE EM REDE: LIMITES DE PROTEÇÃO E CONTROLE ESTATAL A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

DEMOCRACY, DATA FLOW AND NETWORK SOCIETY: PROTECTION AND CONTROL BOUNDARIES AFTER THE BRAZILIAN GENERAL DATA PROTECTION LAW

ELIAS JACOB DE MENEZES NETO

Doutor e Mestre 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 Laboratório de Governança Pública da UFRN. E-mail: eliasjacob@ceres.ufrn.br

JOSE LUIS BOLZAN DE MORAIS

Doutor em Direito pela Universidade Federal de Santa Catarina. Mestre em Direito pela Pontifícia Universidade Católica do Rio de Janeiro. Bolsista de Produtividade em Pesquisa do CNPq – Nível 1D. Professor do Programa de Pós-Graduação da Faculdade de Direito de Vitória.

VICTORIA LAYZE SILVA FAUSTO

Graduanda em Direito pela Universidade Federal do Rio Grande do Norte (UFRN). Bolsista do Laboratório de Governança Pública da UFRN e integrante do projeto de pesquisa "Tecnologia da informação e Governança Pública: o potencial dos dados abertos do Poder Judiciário no desenvolvimento de políticas públicas mais eficientes.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

RESUMO

Objetivo: analisar como a estrutura rígida e ainda característica do Estado brasileiro torna-se precária diante da flexibilidade das relações e a dinamicidade dos fluxos dedados, impossibilitando àquele o controle integral tanto das informações como de seu uso por entidades não governamentais.

Metodologia: pesquisa bibliográfica, com o apoio teórico de estudiosos como Manuel Castells e David Lyon. Ademais, consiste em método dedutivo, pois parte da sociedade em rede para a análise dos limites estatais brasileiros com o propósito de acrescentar perspectivas à discussão sobre Estado e democracia na sociedade líquida. Além disso, apresenta objetivo exploratório, uma vez que busca estender a noção de sociedade em rede para a necessidade de reestruturação do Estado nacional ao apontar limites e defeitos na atual tentativa de controle estatal sobre as informações.

Resultados: a organização em rede das relações sociais não confere espaço à atuação estática do Estado brasileiro como centralizador da proteção dos direitos humanos, obrigando esse último a adaptar-se à fluidez de trocas entre empresas e indivíduos para continuar a cumprir seus objetivos.

Contribuições: o debate sobre os limites de proteção do Estado na modernidade líquida e sobre a (in)capacidade estatal de proteger todos os direitos violados pela manipulação de fluxos de dados.

Palavras-Chave: Lei Geral de Proteção de Dados do Brasil; Limites estatais; Proteção dos direitos humanos; *Surveillance.*

ABSTRACT

Objective: *to analyze how the rigid structure and yet characteristic of the BrazilianState becomes precarious before the flexibility of relationships and dynamics of datastreams, making it impossible to the State full control as much in the information asits use by non-governmental entities.*

Methodology: *a bibliographical research,based on scholars such as Manuel Castells and David Lyon. Moreover, it consists ofa deductive method as part of the network society for the analysis of the Brazilian State boundaries to add perspectives to discussion of state and democracy in theliquid society. Furthermore, it has an exploratory objective as it seeks to extend thenotion of liquid society to the need for restructuring of the national state pointing limitsand flaws in the current attempt to state control over information.*

Results: *thenetwork organization of social relations does not give space to static performance ofBrazilian State as centralizing the protection of human rights, forcing*

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

the latter toadapt to the fluidity of exchanges between companies and individuals to continue tofulfil their goals.

Contributions: *the debate about the protection limits of the State inthe liquid modernity and about the (in)ability of the State to protect all rights violatedby the manipulation of data flows.*

Keywords: *Brazilian General Data Protection Regulation; State boundaries; Human rights protection; Surveillance.*

1 INTRODUÇÃO

Em junho de 2018, a rede social *Facebook* entregou ao Senado dos Estados Unidos um documento (BOYD,2012, p.662–679) que responde a uma série de questões elaboradas pelos parlamentares sobre a coleta, o monitoramento e o uso de dados dos usuários. Esta participação da rede compõe, na verdade, a audiência intitulada *Facebook, Social Media Privacy, and the Use and Abuse of Data* em que a mesma empresa esteve presente para esclarecer questões de transparência logo após o vazamento de dados dos usuários da plataforma para uso destinado a campanhas eleitorais e fabricantes de celulares (NY TIMES,2018).

O escape das informações supracitadas gerou grande movimento em esferas econômico-sociais distintas cujos usuários foram afetados, uma vez que os dados de mais de 50 milhões (NY TIMES,2018) daqueles que se utilizam da rede foram utilizados para alcançar interesses particulares sem conhecimento e autorização prévios dos envolvidos.

A repercussão gerada suscitou discussões sobre assuntos que vão desde a transparência de empresas que se utilizam de dados pessoais dos usuários ao controle estatal de uso e tratamento dos fluxos de dados coletados por grandes corporações. Avaliando a dimensão de impacto de manipulação dos dados no momento atual em que a sociedade se organiza, é acertado referenciar a informação como fundamento base das relações no mundo contemporâneo.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Nesse sentido, este trabalho tem o objetivo de discutir os limites do Estado nacional no controle os fluxos de dados, razão de ser da Era da Informação, para entender a insuficiência de sua atuação quando solitária na proteção dos direitos humanos. Para isso, é necessário compreender a configuração do próprio Estado no contexto atual da sociedade em rede, assim definida pelo sociólogo catalão Manuel Castells (2010).

Como resultado de inúmeras transformações e modelagens sociais proporcionadas por estruturas complexas, por exemplo, de comunicação e globalização, a nova forma de organizar a sociedade baseia-se na distribuição de poder e ação em focos difusos, os nós, partes menores de uma dimensão extensa e dinâmica, a rede.

Esta alteração afeta diretamente o Estado, uma vez que desloca o controle governamental para uma quantidade de nós ilimitados que fazem parte da nova forma de se pensar a dinâmica social, agora mais ágil e difusa. Antes o centro do movimento de todas as informações, o Estado torna-se um dos “nós” por meio dos quais a informação é organizada. Todas as consequências desta adaptação, por interferir nas modelagens convencionais de distribuição do poder, afeta o mesmo Estado, esse criado a partir de elementos sólidos, opostos à flexibilidade e ao movimento que caracterizam as tecnologias da informação.

Com isso, noções de espaço, tempo, comunicação, previsibilidade e permanência são forçadas a uma nova composição para ajustar-se às demandas dos fluxos de dados alheios a elementos tão intrínsecos ao regime convencional, como a territorialidade. Nessa perspectiva, conceitos como *surveillance* e metadados são indispensáveis para a presente análise, uma vez que o primeiro termo se refere à caracterização abrangente do momento atual das relações; ao passo que o outro diz respeito a uma definição indispensável ao estudo que envolve fluxos de dados.

O primeiro elemento, a *surveillance*, é um dos objetos de estudo do relevante sociólogo David Lyon, aqui utilizado como uma das principais referências teóricas. O termo em questão é referenciado em sua forma original, em inglês,

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

porque se acredita que reduzir este fenômeno à tradução correspondente em língua portuguesa seria diminuir a dimensão a que diz respeito o próprio objeto da *surveillance*, não comportada pelo termo vigilância. A distância entre essa última e aquela está na extensão e envolvimento de todas as camadas da sociedade com as tecnologias da informação, característica da *surveillance*; diferentemente quando da concentração daqueles instrumentos para controle centralizado de informações e influência sobre a maioria, em que ocorre a vigilância, mas não mais condizente ao estado atual de fluidez das relações.

Além disso, convém citar o conceito de metadados como sendo o conjunto organizado de informações que permite localizar, identificar ou definir outro conjunto de dados ou informações. É comum referir-se ao metadado, portanto, como a informação sobre a informação. Em diversas situações, estes dados sobre os dados são mais importantes para a coleta e análise do que apenas os elementos em si, como ainda será visto em momento oportuno.

Com o propósito de analisar a capacidade do Estado para controlar o fluxo de dados (1), este trabalho utilizar-se-á de dispositivos legais para projetar a extensão dos limites estatais ainda ligados a conceitos fixos e sólidos. O marco civil da internet (2), conhecido oficialmente como a Lei nº 12.965/14, é abordado com o objetivo de delimitar a capacidade de proteção a que se destina. Com o mesmo propósito, dando continuidade ao estudo dos instrumentos legais brasileiros de proteção de dados, analisa-se um dos pontos frágeis da Lei nº 13.709/2018 (3). A Rede Tor ainda é abordada (4) como forma de estender a discussão para como a consequência da dinamicidade da sociedade em rede afeta os Estados estrangeiros, como, neste caso, acontece com a França.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

2 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 deste 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, de 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 destes 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)[1]. Sob essa perspectiva, observa-se que a prática

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

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

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. Esta 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 todos os lugares. Como resultado, "[...] faz funcionar, ao arrepio 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, 2011, 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 deste "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 a seguir apresentados: a Lei nº 12.965/2014 – marco civil da Internet no Brasil, a Lei nº 13.709/2018 – lei geral de proteção de dados, e a tentativa de bloqueio da rede Tor pela França.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

3 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 nº 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, 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?

Estas 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 parece querer a doutrina tradicional – que a elaboração de uma nova lei seria capaz de evitar a interferência nos fluxos de dados mundiais[2]. As legislações de proteção de dados são essenciais para

[2]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 de limites técnicos em que 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

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

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 é demonstrado neste artigo. Isso porque dá início ao capítulo que, justamente, trata dos direitos e garantias dos usuários, mas restringe estes 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 analisados 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 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 fazer[3]. Certamente, alguma proteção é melhor que nenhuma, de maneira que há possibilidade de

desterritorializados. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1449738&filename=REL+2/2016+CPICIBER+=%3E+RCP+10/2015. Acesso em: 4 maio 2018.

[3]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.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

(pouca) efetividade dos trechos da legislação em questão[4]. Porém, seria ingênuo acreditar que este tipo de solução sólida (dispositivo legal) tem condições para lidar com a liquidez dos fluxos de dados – embora esta 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-papo[5]. 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 12.965/2014[6], por qual motivo dever-se-ia acreditar que esta legislação será respeitada por outras empresas com muito menos vínculos no Brasil ou por agências de inteligência?

Ainda, sua utilização causou uma mudança importante no conceito daquilo que é "informação 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 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,

[4]Veja-se, por exemplo, a importância que a neutralidade da rede possui na proteção da liberdade de informação dos usuários da Internet. Em virtude desta 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.

[5]"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: https://policies.google.com/terms?hl=pt-BR&gl=uk. Acesso em: 29 jul. 2018.

[6]Observe-se que, nos termos desta 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.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

análise e processamento de metadados permite identificar e fazer inferências sobre os mais íntimos segredos do ser humano.

Alguns exemplos deste 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 dispositivos[7]; 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.

Esta 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 et al, 2014, p. 74)[8].

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"[9]. Atualmente, grande parte da vida

[7]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: https://money.cnn.com/2014/08/01/technology/social/russian-soldier-ukraine-instagram/. Acesso em: 28 abr. 2018.

[8]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."

[9] Neste último caso, por exemplo, o *Facebook* deixa claro: "Se você está conectado ao Facebook e visita um site com o botão Curtir, seu navegador nos envia informações sobre sua visita. [...] Como

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, este vínculo entre "real" e "virtual". Nenhuma destas 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 deste 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 da nova lei de proteção de dados pessoais. 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 sofrem da mesma miopia da Lei 13.709/2018, a Lei Geral de Proteção de Dados do Brasil.

4 DADOS "ANÔNIMOS" E A LEI Nº 13.709/2018

Como mais uma forma de demonstrar as barreiras que a estrutura sólida do Estado possui para gerência de informações, torna-se conveniente falar sobre a Lei de nº 13.709, aprovada recentemente, em agosto de 2018. Além de alterar o dispositivo abordado anteriormente, o Marco Civil da Internet, este novo dispositivo

outros sites da internet, recebemos informações sobre a página da Web que você está visita[n]do, a data e hora as outras informações relacionadas ao navegador. Registramos essas informações como auxílio para melhorar nossos produtos." Acontece que, no caso do vazamento de dados como esses que envolveu a referida rede e a empresa *Cambridge Analytica*, informações tão sensíveis ao conteúdo particular tornam-se expostas a usos e abusos motivados por interesses corporativos distintos e, muitas vezes, vulneráveis a violação dos direitos humanos. Nessa situação, por exemplo, muito além de anúncios direcionados, os dados foram destinados à manipulação político-partidária deliberada dos votos usuários em período eleitoral. Para mais informações sobre os dados obtidos pelo *Facebook*, disponível em: <https://www.facebook.com/help/186325668085084>. Acesso em: 23 jul. 2018.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

cuida da proteção de dados pessoais, esses últimos definidos pelo texto legal como a “informação relacionada à pessoa natural identificada ou identificável”.

Dentre as formas de territorialidade, sendo essa última o aprisionamento estático-espacial do Estado, a lei caracteriza-se como elemento chave para a existência estatal, uma vez que vincula os sujeitos a ela relacionados aos critérios legais que permitem o controle da organização administrativa.

Nesse sentido, a regulamentação do uso de dados pessoais deixa claro o objetivo do Estado de estabelecer a gerência sobre como as informações dos usuários devem ser dispostas dentro do território nacional. Apenas observando esta dimensão do seu propósito é possível compreender a importância indiscutível da iniciativa legislativa de abordar este aspecto de proteção estatal sobre os elementos que dizem respeito à vida de seus cidadãos. Especialmente quando se leva em conta que o abuso destas informações pode comprometer a proteção de direitos humanos sobre a qual o Estado possui responsabilidade.

Entretanto, antes mesmo da discussão da nova lei em comento e levando em consideração as abordagens feitas sobre a rede que caracteriza a sociedade atual, é possível observar a limitação que possui um instrumento jurídico que depende do território para surtir efeitos. A sociedade em rede, na dimensão da *surveillance*, não cabe nesta pequena projeção de controle, já que toma proporções amplas e diretas nas relações e, por isso, não é influenciada por Estados nacionais, uma vez que esses são limitados a agir no que diz respeito ao seu perímetro territorial.

Além deste problema, cabe mencionar a relação que o texto legal faz com os tipos de dados para que seja possível compreender a perspectiva sob a qual as informações dos usuários são protegidas. Nesse sentido, além do conceito de dado pessoal, já delineado anteriormente como a informação a qual é possível relacionar uma pessoa natural identificável, existem no texto, ainda, duas outras espécies de informações: os dados sensíveis e anonimizados.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Dados sensíveis, em acordo com o inciso II do artigo 5º da Lei 13.709/18[10], referem-se às informações que categorizam o indivíduo de que os dados tratam, permitindo a inserção da pessoa, por exemplo, em grupos religiosos, tipos sanguíneos, ideologias políticas e grupos de saúde. Já os dados anonimizados ou anônimos[11] representam o exato oposto dos dois primeiros tipos, uma vez que, ainda que se tenha acesso aos dados equivalentes a uma pessoa, não é possível relacioná-los a um indivíduo específico ou identificável. Os dados, segundo o dispositivo, neste caso, são despersonalizados.

Entretanto, esta classificação é completamente alheia à realidade de tratamento e análise de dados. Especialmente quando se aborda os atuais mecanismos de extração e tratamento massivo de dados, como o procedimento de mineração de dados. No atual contexto de desenvolvimento das tecnologias é ingênuo e longe do fenômeno contemporâneo da *surveillance* acreditar que a omissão de informações personalizadas qualifica o dado como anônimo e, portanto, impossível de individualização.

Ao contrário, o processo inverso de identificação dos dados acontece facilmente a partir do acesso a uma base de dados com grande disponibilidade de informações, o que significa que, quanto mais dados "anônimos", maior a possibilidade de personalização. Nessa perspectiva, esta espécie de dados pode ser ainda mais valiosa do que os dados propriamente sensíveis, uma vez que, por dar acesso a uma extensa gama de informações para identificação, os dados anônimos permitem uma variação mais ampla de categorização dos indivíduos.

Esta fantasia de "anonimização" dos dados acontece comumente e, por isso, diversas pesquisas já foram desenvolvidas para desmistificar a ilusão que tantos Estados alimentam ao dar publicidade a dados considerados "não pessoais" e, por

[10]Art. 5º Para os fins desta Lei, considera-se: [...] II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...].

[11]Art. 5º Para os fins desta Lei, considera-se: [...] III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...].

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

isso, não ameaçadores à privacidade dos cidadãos. Como exemplo destes esforços científicos, é possível citar a pesquisa desenvolvida por um grupo de cientistas de dados que analisou as transações de cartões de crédito realizadas por mais de um milhão de pessoas no período de três meses (DE MONTJOYE et al, 2015).

Os conjuntos de dados avaliados consistiam no que pode ser denominado de conteúdo "anônimo", pois os detalhes continham as datas de cada transação, o valor monetário relacionado e o local da operação, não incluídas informações personalizadas dos envolvidos, como nomes e números de conta. Apesar disso, 90% dos usuários tiveram suas identidades descobertas, sobre o que foi dito pelos autores que "os metadados financeiros, quando em larga escala e simplesmente anônimos, podem ser facilmente reidentificados"[12]. De modo mais específico,

> Assim como metadados de cartões de créditos e telefones celulares, os conjuntos de dados referentes a navegações ou transporte são consequências da interação do homem com a tecnologia, estão sujeitos às mesmas particularidades do comportamento humano, além de serem esparsos e de extensa dimensão (por exemplo, a quantidade de sites que se pode visitar ou o número de possíveis combinações de entrada e saída das estações de metrô). Isso significa que estes dados podem ser reidentificados de modo relativamente fácil se forem disponibilizados simplesmente de forma anônima e que eles provavelmente não podem ser anonimizados simplesmente omitindo dados[13]. (DE MONTJOYE et al, 2015, p. 539).

Ainda no texto da Lei 13.709/2018, em seu artigo 12, fala-se sobre considerar os dados anônimos como pessoais nos casos de inversão da anonimização ou de sua possibilidade. Com isso, mais uma vez é possível notar a desatualização do direito em relação ao funcionamento das tecnologias. Os dados anonimizados não existem em si mesmos, de modo que desconsiderar sua

[12]No original: "Simply anonymized large-scale financial metadata can be easily reidentified via spatiotemporal information."

[13]No original: "Like credit card and mobile phone metadata, Web browsing or transportation data sets are generated as side effects of human interaction with technology, are subjected to the same idiosyncrasies of human behavior, and are also sparse and high-dimensional (for example, in the number of Web sites one can visit or the number of possible entry-exit combinations of metro stations). This means that these data can probably be relatively easily reidentified if released in a simply anonymized form and that they can probably not be anonymized by simply coarsening of the data."

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

existência é uma redundância. Tratar esta espécie de dados como “anônimos” é ignorar os mecanismos facilmente acessíveis de reidentificação.

Para além disso, continuar a tratar de dados anônimos faz permanecer a ilusão não somente em relação à fantasia de anonimização deste tipo de informação, mas, também, quanto à proteção estatal dos direitos humanos, que permanecem expostos ao abuso na medida em que dados sensíveis ainda estão ao alcance de quem possui os mecanismos tecnológicos necessários.

Apesar da relevante discussão levantada pela Lei, a abordagem jurídica ainda ignora aspectos fundamentais inerentes à *surveillance*, o que provoca estas lacunas de proteção no dispositivo em questão. Tratar problemas, ainda que nacionais, de modo restrito e sem levar em consideração os fluxos globais e desterritorializados de dados leva a imprecisões como a que foi demonstrada brevemente pela análise acima disposta.

Este problema 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.

5 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 o 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.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Na rede Tor, os dados são roteados múltiplas vezes, garantindo que seja extremamente difícil[14] rastrear a sua origem. Em virtude de assegurar um maior grau de anonimato aos usuários, a rede é amplamente utilizada para finalidades diversas, sendo algumas benéficas – divulgação de informações por *whistleblowers* como Julian Assange e Edward Snowden ou pesquisadores, jornalistas e ativistas que desejam fugir da censura imposta por um país –, e 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*. No 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, compondo o que pode ser denominado de "efeito hidra"[15].

Logo, até mesmo o mais potente Estado-nação, detentor do maior aparato tecnológico e militar existente, os EUA têm 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, além de, obviamente, ser irônico[16] o fato de que um *software* criado por um departamento do governo estadunidense não possa por ele ser controlado.

[14]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.
[15]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. Possuia 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.
[16]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.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Após os eventos envolvendo o atentado terrorista na França nos dias 07 e 09 de janeiro de 2015, o governo francês 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 a referida rede para troca de mensagens[17]. 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.

Este exemplo, assim como os anteriores, possui um liame comum: demonstra 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; LYON, 2013), especialmente diante daquilo que aqui se denomina *surveillance*.

6 CONSIDERAÇÕES FINAIS

A análise desenvolvida por este artigo pretendeu avaliar como atuam os instrumentos de proteção dos direitos humanos pelo Estado brasileiro em relação ao abuso de tratamento de dados. Com o propósito de fundamentar a abordagem, conceitos como sociedade em rede, fluxo de dados, *surveillance* e metadados foram trabalhados, uma vez que tais definições compõem o estado atual de movimento dinâmico global.

A maioria dos exemplos abordados por este trabalho utilizou-se de dispositivos jurídico-normativos para demonstrar como a recorrência isolada ao Estado para solucionar problemas de ordem global e, portanto, desterritorializada, é

[17]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: <https://www.independent.co.uk/news/world/europe/france-could-ban-public-wi-fi-and-tor-anonymous-browsing-after-paris-attacks-a6763001.html>. Acesso em: 1 maio 2018.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

ingênua e alheia às configurações atuais da sociedade, que trabalha em rede de dados.

Inicialmente, a Lei nº 12.965/2014, também conhecida como o marco civil da internet, foi analisada a partir de sua preocupação com a proteção da privacidade. Como demonstrado pelo texto, apesar dos benefícios do referido instrumento legal, a dimensão estrita que a lei nacional representa é insuficiente para assegurar a não violência a uma garantia tão ampla como a privacidade no mundo interconectado.

Percebe-se, no mundo atual, o esgotamento da noção ultrapassada de espionagem e vigilância enquanto ações de coleta de dados direcionadas, noções vencidas pela *surveillance* enquanto tratamento massivo e difuso de informações sobre indivíduos. A preocupação insuficiente quanto à privacidade – ao invés de, também, a igualdade – configura-se como mais um dos problemas das perspectivas tradicionais, acompanhadas da característica de desterritorialização dos fluxos, questão ainda não abarcada pelo pensamento jurídico tradicional.

Em seguida, a Lei nº 13.709/2018, que disciplina o tratamento de dados pessoais dos cidadãos brasileiros, é trazida à discussão e atesta, mais uma vez, a insuficiência da intervenção somente estatal em problema de dimensões que vão além da localização espaço-tempo. Ainda, a consideração da inexistência dos dados anônimos é explicada como situação de risco à proteção dos direitos humanos a que o Estado se dispõe, uma vez que a anonimização das informações é facilmente descartada como situação de segurança real.

Por fim, traça-se um exemplo que, desta vez, não pertencente ao Estado brasileiro, mas ao francês, por intermédio da Rede Tor, de como a estrutura da relação entre poder e política também é alvo de reconfiguração em resposta aos novos moldes sociais que, pela e com a *surveillance*, são refeitos.

Por conseguinte, finaliza-se a análise de como os limites do Estado são ultrapassados pelos mecanismos da sociedade em rede com a visualização de consequências que, apesar de ter começado a nível nacional com os instrumentos legais, recorre a um exemplo estrangeiro de estranhamento com a mudança – de

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

centralizado para difuso e dinâmico – de um dos elementos fundamentais ao Estado nacional: o poder.

Conclui-se, à vista dos argumentos trazidos, que a insuficiência do Estado e, assim, do direito, para lidar com situações de violação e abuso dos direitos humanos mediados pelas tecnologias da informação precisa de uma abordagem totalmente distinta da forma convencional de lidar com o mundo que, agora, além de interconectado, é pautado pelo paradigma da *surveillance*.

REFERÊNCIAS

BAUMAN, Z.; LYON, D. **Liquid Surveillance**: A Conversation. Cambridge: Polity, 2013. 152 p.

BENNET, C. J. et al. **Transparent Lives**: Surveillance in Canada. Edmonton: Athabasca University Press, 2014. 239 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.

BOLZAN DE MORAIS, J. L. **A subjetividade do tempo**: Uma perspectiva transdisciplinas do Direito e da Democracia. Porto Alegre: Livraria do Advogado, 1998. 124 p.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 24 abr. 2014.

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://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1449738&filename=REL+2/2016+CPICIBER+=%3E+RCP+10/2015. Acesso em: 4 maio 2018.

CASTELLS, M. **The rise of the network society**: The information age – economy, society and culture. 2. ed. Chichester: Willey-Blackwell, v. 1, 2010. 597 p.

CRAWFORD, Kate; BOYD, Danah. ***CRITICAL QUESTIONS FOR BIG DATA.*** *Provocations for a cultural, technological, and scholarly phenomenon*.2012. Pag. 662-679 Disponível em: https://www.tandfonline.com/doi/full/10.1080/1369118X.2012.678878

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

DE MONTJOYE, Y.-A. et al. ***Unique in the Shopping Mall:*** *On the Reidentifiability of Credit Card Metadata. Science, American Association for the Advancement of Science* – AAAS, v. 347, n. 6221, 29 jan. 2015, p. 536-539. Disponível em: http://dx.doi.org/10.1126/science.1256297. Acesso em: 23 jul. 2018.
FOUCAULT, M. **Vigiar e Punir**: história da violência nas prisões. 20. ed. Petrópolis: Vozes, 1999. 262 p.

GINSBERG, J. et al. ***Detecting influenza epidemics using search engine query data***. Nature, n. 457, 19 fev. 2009. p. 1012-1014. Disponível em: https://www.nature.com/articles/nature07634. Acesso em: 25 fev. 2018.

LYON, D. ***Surveillance Studies***: An Overview. Cambridge: Polity, 2007. 243 p.

NEW YORK TIMES. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 22 jul. 2018.

PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY. ***The darknet and online anonymity***. Houses of Parliament. London, 4 p. 2015.

ROCHA, L. S.; KING, M.; SCHWARTZ, G. **A verdade sobre a autopoiese no direito**. Porto Alegre: Livraria do Advogado, 2009. 148 p.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]