REVISTA ESMAT 17

QUESTÕES CONTROVERSAS ENVOLVENDO A TUTELA JURISDICIONAL PENAL E AS NOVAS TECNOLOGIAS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) BRASILEIRA: DATAVEILLANCE

CONTROVERSIAL ISSUES INVOLVING CRIMINAL JURISDICTION AND THE NEW TECHNOLOGIES UNDER THE BRAZILIAN GENERAL LAW OF DATA PROTECTION (DPL): DATAVEILLANCE

Víctor Minervino Quintiere

Víctor Minervino Quintiere é doutorando e mestre em Direito, no Instituto Brasiliense de Direito Público (IDP). Professor universitário do Centro Universitário de Brasília (UniCEUB). Membro do Instituto dos Advogados do Distrito Federal (IADF). Advogado.

RESUMO

O exercício da tutela jurisdicional penal, em tempos de inovação tecnológica, suscita dúvidas no mundo todo, cenário do qual o Brasil não se distancia. Dentre as inovações tecnológicas destaca-se o mecanismo de vigilância chamado *dataveillance*. No rol de princípios penais e processuais existentes, destaca-se a vedação à produção, pelo acusado, de provas contra si mesmo (*nemotenetur se detegere*). No campo legislativo brasileiro, destaque para a recém-criada Lei Geral de Proteção de Dados (LGPD) e sua não aplicabilidade na seara penal. A análise do conjunto de instrumentos e normas existentes no Brasil, em especial aquele relativo à proteção de dados, tornou possível a conclusão de que não garante ao Estado, mais especificamente na condição de titular da Jurisdição, eficiência no combate preventivo às violações aos direitos de personalidade do acusado, com destaque para aquele relativo à vedação contida no brocardo do *nemotenetur se detegere*, pela utilização de *dataveillance,* uma vez que o sistema normativo, além de não solucionar o problema, deve ser aprimorado.

PALAVRAS-CHAVE: Direito Processual Penal. Lei Geral de Proteção de Dados. Dataveillance. Nemo Tenetur se Detegere.

ABSTRACT

The exercise of criminal judicial protection, in times of technological innovation, raises doubts worldwide, a scenario from which Brazil does not distance itself. A mong the technological innovations is the surveillance mechanism called data-monitoring. In the list of existing criminal and procedural principles, its worth noting the prohibition on the production by the accused of evidence against himself (nemotenetur se detegere). In the Brazilian legislative field, the recently created General Law on Data Protection -

LGPD and its (non) applicability in criminal law are highlighted. The analysis of the set of instruments and norms existing in Brazil, especially the one related to data protection, made it possible to conclude that it does not guarantee the State, more specifically as a holder of the Jurisdiction, efficiency in the preventive fight against violations of the rights of personality of the accused, with emphasis on the one related to the fence contained in the nemotenetur se detegere, through the use of dataveillance since the normative system, besides not solving the problem must be improved.

Keywords: Criminal Procedural Law. General Data Protectionlaw. Dataveillance. Nemo Teneturse Detegere.

1 INTRODUÇÃO

Uma das perguntas que norteia a aplicação da tutela jurisdicional penal no Brasil é a seguinte: Se (e em que medida) o conjunto de instrumentos e normas existentes no Brasil, em especial aquele relativo à proteção de dados, garante ao Estado, mais especificamente na condição de titular da Jurisdição, eficiência no combate preventivo às violações aos direitos de personalidade do acusado, em especial aquele relativo à vedação contida no brocardo do *nemotenetur se detegere*, pela utilização de *dataveillance*, e em que medida o sistema normativo, além de solucionar, ou não, o problema, deve, ou não, ser aprimorado.

O presente trabalho, ciente do esforço que isso ensejará, realizará, por meio de metodologia multidisciplinar, o exame do *dataveillance* com conceitos não apenas de direito penal, tornando-se necessário, pelo ineditismo do tema, a busca de alicerces relativos aos direitos constitucional e civil.

2 CONTEXTUALIZANDO A PROTEÇÃO AOS DIREITOS DO ACUSADO NO SISTEMA PENAL BRASILEIRO

Antes, contudo, de esmiuçar a pergunta feita acima, até mesmo para que os direitos da personalidade (objeto dessa reflexão) sejam mais bem compreendidos, oportuno esclarecer a diferença entre termos que, na prática, podem gerar confusão, quais sejam: direitos humanos, direitos fundamentais e direitos da personalidade.

Direitos humanos são "os direitos da pessoa humana, enquanto indivíduo e cidadão, que são inalienáveis, imprescritíveis, irrenunciáveis, com eficácia erga omnes, e que têm origem nos denominados direitos naturais, podendo identificarem-se como direitos transindividuais, coletivos e difusos. São inerentes à pessoa e devem ser respeitados e implementados pelo Estado" (FARIAS, 2005, p.157).

Direitos fundamentais, em que pese à sua fundamentação estar intimamente ligada aos Direitos humanos, dizem respeito aos direitos básicos individuais, sociais, políticos e jurídicos previstos na Constituição de determinado Estado (QUINTIERE, 2015).

Direitos da personalidade, de acordo com Nelson Rosenvald, "são situações jurídicas existenciais que tutelam os atributos essenciais do ser humano e o livre desenvolvimento da vida em relação" (ROSENVALD, 2017).

Nesse sentido, o referido autor complementa asseverando que tais direitos pertencem à terceira via do direito civil, cujo objeto são os próprios atributos existenciais da pessoa, dentre outros modos de ser.

Os três conceitos acima nos permitem concluir, preliminarmente, o seguinte: i) direitos da personalidade dizem respeito à órbita privada; ii) direitos fundamentais possuem normatividade, estão na Constituição e são vinculantes; e iii) enquanto todo direito da personalidade é um direito fundamental, nem todo direito fundamental é direito da personalidade.

Especificamente sobre os direitos da personalidade relacionados ao acusado, objeto inicial deste estudo, é possível visualizar que a pessoa do acusado, no sistema penal brasileiro, não é obrigada a produzir prova contra si mesmo.

Trata-se, em suma, da aplicação do princípio do "*nemotenetur se detegere*"[1]. Historicamente[2], enquanto no Código de Hamurabi, o acusado poderia ser ouvido sob juramento, em especial quando não existisse outra prova testemunhal ou documental, mesmo diante da ausência de previsão formal de interrogatório.

No Egito, o interrogatório era possibilitado, perante os chamados tribunais ordinários, em instrução complementar, valendo o destaque para o emprego de tortura a partir do uso da roda e golpes de bastão, havendo submissão ao juramento.

Já o direito Hebreu partia de lógica distinta quando comparada, por exemplo, ao sistema egípcio. O interrogatório do acusado era admitido sem, contudo, juramento como regra. O juramento apenas era admitido para a prova de inocência.

No que diz respeito às civilizações clássicas, com destaque para a Grécia, a tortura era vista como ferramenta para a obtenção não apenas da confissão, como também da delação dos cúmplices.

Atualmente, o princípio em foco pode ser extraído, para além da incorporação ao direito interno do Pacto Internacional dos Direitos Civis e Políticos e da Convenção Americana sobre Direitos Humanos, no âmbito constitucional, a partir do disposto no art. 5º, LXIII (direito ao silêncio), LIV, LV e LVII, respectivamente, como correlacionado às próprias garantias do devido processo legal, da ampla defesa, mais especificamente na vertente da autodefesa, e da presunção de inocência.

Sobre referido ponto, importante destacar que os princípios constitucionais servem como instrumentos ordenadores e dirigentes de ações tanto do legislador como

---

[1] Referido princípio é expresso, não raro, dos seguintes modos: *nemoteneturedere contra se, nemoteneturdetegereturpitudinem suam e nemotestis contra se ipsum.*

[2] Relato histórico baseado na seguinte obra de Maria Elizabeth Queijo: O direito de não produzir prova contra si mesmo: o princípio nemotenetur se detegere e suas decorrências no processo penal. Ed. – São Paulo: Saraiva, 2012. ISBN 978-85-02-17158-9.

dos legislados. Por isso, ganha relevo analisar se a Lei Geral de Proteção de Dados, com sua atual redação, serve, ou não, para referido fim (FISCHER, 2016)[3].

Referido autor, sobre o tema, destaca que "a Constituição, por ocupar função central no sistema vigente, irradia efeitos sobre o ordenamento infraconstitucional, que precisa ser devidamente harmonizado".

Portanto, a palavra-chave que pode ser associada ao princípio em análise é proteção. Desse termo, em especial diante do caráter preventivo a ele inerente, surgem as indagações vistas acima.

Ou seja, se (e em que medida) o conjunto de instrumentos e normas existentes no Brasil, em especial aquele relativo à proteção de dados, garante ao Estado, mais especificamente na condição de titular da Jurisdição, eficiência no combate preventivo às violações aos direitos de personalidade do acusado, em especial a vedação de produção contra si mesmo, pela utilização de *dataveillanc*e, e em que medida o sistema normativo, além de solucionar, ou não, o problema, deve, ou não, ser aprimorado.

Aqui, convida-se o leitor a, entendendo o contexto dos direitos da personalidade, alcançar a correlação necessária entre referido elemento, a Lei Geral de Proteção de Dados e o princípio do *nemotenetur se detegere*.

Sobre a proteção aos direitos da personalidade, no Brasil, diferentemente do que ocorre em Portugal[4], considera-se que a proteção aos direitos da personalidade se dá por uma cláusula geral implícita prevista no art. 11 do Código Civil Brasileiro, de 2002. Já o Código Penal brasileiro não aborda especificamente o tema.

Voltando aos enfoques dos direitos da personalidade associados à sua natureza jurídica, referidos direitos são vistos como direitos gerais da personalidade, ou seja, o foco passa a ser a análise da substância dos direitos da personalidade.

---

[3] Para aprofundamento do tema, recomenda-se a leitura das seguintes obras: FISCHER, Douglas. Delinquência Econômica e Estado Social e Democrático de Direito. 2006. Porto Alegre: Verbo Jurídico, p. 46; CANOTILHO, José Joaquim Gomes. Constituição Dirigente e Vinculação do Legislador. 2 ed. Coimbra: Coimbra Editora, 2001, p. 11; GARCÍA DE ENTERRIA, Eduardo. La Constitución como Norma y El Tribunal Constitucional. 3 ed. Madrid: Civitas, 2001, p. 63-4.

[4] Artigo 70º (**Tutela geral da personalidade**), do Código Civil Português: 1. A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.2. Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida. Sobre referido artigo, caso haja interesse no aprofundamento da jurisprudência de Portugal, sugere-se a leitura dos seguintes temas: O direito ao descanso e ao sossego na jurisprudência das Secções Cíveis do Supremo Tribunal de Justiça (Sumários de Acórdãos de 1997 a Março de 2016), e; A liberdade de expressão e informação e os direitos de personalidade na jurisprudência do Supremo Tribunal de Justiça (Sumários de acórdãos das Secções Cíveis e Criminais, de 2002 a Janeiro de 2015). Disponível em:<http://www.codigocivil.pt/>. Acesso em 16. março 2019.

Em outras palavras, os casos concretos devem ser analisados com base na premissa de que o ser humano é o autor da própria história. Nesse ponto, diferentemente do que ocorre na Alemanha[5], o Brasil não possui disposição expressa dispondo de maneira generalizada sobre direitos da personalidade.

No que diz respeito aos atributos dos direitos da personalidade, de acordo com Nelson Rosenvald, são direitos oponíveis a todos quanto à chamada eficácia negativa, ou seja, exige-se que outros não nos desconsiderem como pessoas.

Sobre a eficácia negativa dos direitos de personalidade, em especial a denominada tutela inibitória do ilícito, é possível concluir preliminarmente que a prevenção a ilícitos de ordem civil são possíveis a partir da leitura conjunta do art. 12 do Código Civil[6] em conjunto com o art. 497 do Código de Processo Civil[7].

A respeito dos direitos da personalidade em espécie, o direito à intimidade ganha especial destaque na era da informação, não apenas na área cível como, e principalmente, na esfera penal.

Sobre o referido direito, vale destacar que, apesar de ser quase sempre considerado como sinônimo do direito à privacidade, tal constatação não pode ser utilizada para os fins do presente trabalho, uma vez que, nos termos da Constituição Federal Brasileira, de 1988, "o inciso X do art. 5º separa intimidade de outras manifestações da privacidade: vida privada, honra e imagem das pessoas" (SILVA, 2009, p. 206).

Nessa concepção, destaca-se que a privacidade deve ser vista sob uma perspectiva ampla, uma vez que "abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo" (OLIVEIRA, 1980, p. 50).

---

[5] Artigo 2 [Direitos de liberdade], da Lei Fundamental da Republica da Alemanha: (1) Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral. (2) Todos têm o direito à vida e à integridade física. A liberdade da pessoa é inviolável. Estes direitos só podem ser restringidos em virtude de lei. Disponível em:<https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso em: 16 março 2019.

[6] Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau. BRASIL. Código Civil. Disponivel em:< http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm >. Acesso em: 16 março 2019.

[7] Codigo de Processo Civil Brasileiro, Art. 497: Na ação que tenha por objeto a prestação de fazer ou de não fazer, o juiz, se procedente o pedido, concederá a tutela específica ou determinará providências que assegurem a obtenção de tutela pelo resultado prático equivalente. Parágrafo único. Para a concessão da tutela específica destinada a inibir a prática, a reiteração ou a continuação de um ilícito, ou a sua remoção, é irrelevante a demonstração da ocorrência de dano ou da existência de culpa ou dolo. Disponivel:<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm>. Acesso em 16 março 2019.

Diante de tal cenário, a privacidade reflete "o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito" (PEREIRA, 1980, p. 40).

Já a intimidade pode ser definida como sendo a "esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais" (DOTTI, 1980, p. 69).

Em caminho semelhante, tratando a intimidade como algo mais restrito dentro da privacidade, Adriano de Cupis define a intimidade como o modo de ser da pessoa que consiste na exclusão do conhecimento de outrem de quanto se refira à pessoa mesma (CUPIS, 1969, p. 115).

Diante dessas constatações, em especial aquelas relativas à evolução pela qual o Direito Civil passou a partir do fenômeno da despatrimonialização, perguntas específicas surgem, a saber: Como fica a autodeterminação informativa[8] da pessoa com o advento da *internet* e as práticas cada vez mais frequentes de obtenção de dados?

O ser humano, diante da inefetividade da proteção, em caráter preventivo, de seus direitos da personalidade, estaria, de fato, podendo utilizar-se do direito (garantia) a não produzir provas contra si mesmo? A evolução tecnológica é compatível com as garantias penais e processuais penais derivadas do Estado Democrático de Direito?

Mais do que isso, se o Homem, nas palavras de Pierre Teilhard de Chardin (1988), não é centro estático do Mundo, mas eixo e flecha da evolução, como fica a manutenção (e continuidade) desse papel perante o domínio de técnicas de obtenção e manipulação de dados nas mãos do Estado?

Como palavra-chave para elucidação, ainda que inicial, sobre todas as perguntas feitas até aqui, surge o chamado *dataveillance*. Antes, contudo, de explicar no que consiste referido mecanismo, oportuno contextualizar o surgimento da recente Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados (LGPD)).

3 NOVAS TECNOLOGIAS E O DATAVEILLANCE

A Lei Geral de Proteção de Dados foi responsável pela proteção de dados pessoais, bem como pela alteração da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

A proteção de dados tem relevo não apenas com a edição da referida norma, como também em outros Países. Na Europa, foi editado o *General Data Protection Regulation* (GDPR), o qual passou a ser obrigatório em 25 de maio de 2018 e aplicável a todos os países da União Europeia (UE)[9]. Já em solo norte-americano, foi

---

[8] O termo teve origem em caso julgado pelo Tribunal Constitucional Alemão, no ano de 1983, a respeito da Lei do Censo em que, após amplos debates, foi concedido aos cidadãos alemães o direito a autodeterminação informativa.

[9] Comissão Européia. Proteção de dados. Disponível em:<https://ec.europa.eu/info/law/law-topic/data-protection_pt>. Acesso em: 7 jan. 2019.

editado o *California Consumer Privacy Act of 2018* (CCPA), aprovado em 28 de junho de 2018 (AB 375)[10].

Sobre o tema, é possível verificar que "a LGPD se inspira, em primeiro lugar, no conceito que ficou conhecido como o modelo europeu de proteção de dados336, amparado na Convenção do Conselho da Europa 108 de 1981, na Diretiva 46/95/CE e no Regulamento Geral de Proteção de Dados (Regulamento 2016/679)"[11].

O contexto no qual o projeto de lei sobre a proteção de dados foi aprovado pelo Poder Legislativo brasileiro foi decisivo para a respectiva tramitação célere. Como se não bastasse a aglutinação de outras propostas que há muito tempo vinham tramitando paralelamente sobre o tema (cuja atualidade é discutível), escândalos mundialmente famosos envolvendo a segurança de dados como o ocorrido na mídia social *Facebook*[12] também trouxeram visibilidade para o assunto.

De acordo com Danilo Doneda, é possível "identificar cinco eixos principais da Lei Geral de Proteção de Dados em torno dos quais a proteção do titular de dados se articula: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes".

É possível visualizar, a partir desse rol, que, em princípio, a Lei Geral de Proteção de Dados seria aplicável à jurisdição penal no que diz respeito à unidade e generalidade de sua aplicação, ou seja, a Lei Geral de Proteção de Dados possui características de uma Lei Geral[13].

---

[10] Californians for ConsumerPrivacy (ed.).Disponível em:<https://www.caprivacy.org/>. Acesso em: 7 jan. 2019.

[11] DONEDA, Danilo; SCHERTEL, Laura Mendes. Um perfil da nova Lei Geral de Proteção de Dados brasileira. In: BELLI, Luca;

[12] Sobre o tema, Andrew Burt descreve o episódio da seguinte forma "News ofFacebook'sexposureof tens ofmillionsofuseraccountsto data firm Cambridge Analyticabroke in March— a scandalthatwasonlycompoundedbyrecent newsthatthe tech giantsharedeven more private data throughhiddenagreementswithothercompanies". BURT, Andrew. Privacyandcybersecurity Are Converging. Here´sWhyThatMatters for People and for Companies. Disponível em Harvard Business School:<https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies>. Acesso em: 7 jan. 2019.

[13] Sobre o tema, Doneda: "O primeiro eixo diz respeito ao âmbito de aplicação material da Lei, caracterizado pela generalidade e unidade: a Lei concentra-se na proteção dos dados do cidadão, independentemente de quem realiza o seu tratamento, aplicando-se, assim, tanto aos setores privado e público, sem distinção da modalidade de tratamento de dados (art. 3o). O seu âmbito de aplicação abrange também o tratamento de dados realizado na Internet, seja por sua concepção de Lei geral, seja por disposição expressa de seu art. 1o. Essas são características fundamentais em uma Lei geral, que permitem a segurança do cidadão quanto aos seus direitos independentemente da modalidade de tratamento de dados e quem o realize, bem como proporciona isonomia entre os diversos entes que tratam dados, o que facilita o seu fluxo e utilização legítimos".

Essa aplicabilidade potencial, entretanto, não é concretizada quando da análise do art. 4º que expressamente dispõe não ser aplicável o diploma normativo em análise nas atividades de investigação e repressão de infrações penais.

Um dos grandes problemas da norma começa quando, além do art. 4º, o intérprete passa a analisar o art. 33, III, que dispõe que a transferência internacional de dados pessoais somente é permitida quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional.

Ou seja, ao mesmo tempo em que a lei não é aplicável no âmbito das investigações criminais nacionais, discorre sobre eventual cooperação internacional entre autoridades alienígenas com a brasileira.

Após o estudo de uma das palavras-chave do presente estudo (proteção de dados), será possível responder se, ao dispor sobre a matéria dessa forma, teria a Lei Geral de Proteção de Dados agido corretamente ou se foi perdida uma importante oportunidade de regulamentação do tema.

No estudo da vigilância propriamente dita, palavra intimamente ligada à proteção de dados e ao fenômeno da *dataveillanc*e, as análises de Jeremy Bentham[14]e Michel Foucault[15]serviram de modelo padrão.

O surgimento de novas tecnologias e as conseqüências quanto ao armazenamento e ao processamento de dados serviu de mola propulsora para o aumento exponencial de estudos tanto sobre metadados[16]como sobre a *surveillance*[17].

Dentro do estudo sobre vigilância, o modelo da *surveillance assemblage*s, proposto por Richard Ericson e Kevin Haggerty[18], dá ênfase aos fluxos discretos de dados, ou seja, "ao aspecto do *surveillanc*e que se convencionou chamar de *dataveillance*"[19].

---

[14] BENTHAM, Jeremy. The Works of Jeremy Bentham. Edinburgh: William Tait, 1843. v.4.

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

[16] Sobre o tema, Neto, Morais e Bezerra exemplificam o que seria um metadado: "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".

[17] Vigilância, ao traduzirmos literalmente o termo.

[18] ERICSON, Richard; HAGGERTY, Kevin. The surveillantassemblage. British JournalofSociology, London, v. 51, n. 4, p. 605-622, dez. 2000

[19] NETO, Elias Jacob de Menezes; MORAIS, José Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. 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. Rev.Bras.Polít.Públicas,Brasília,v.7, nº 3, 2017, p.184-198.

O seguinte experimento do *Center for Internet and Society*, realizado no âmbito da Escola de Direito da Universidade de Stanford, auxilia na visualização do que seria uma pesquisa envolvendo *dataveillance:*

> 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,e m vez de,simplesmente, terem um número, os pesquisadores poderiam ter o nome do destinatário da chamada telefônica[20].

A jurisprudência brasileira, representada pelos Tribunais Superiores, tem se debruçado sobre o acesso a dados e uso da tecnologia como instrumento de efetivação da tutela jurisdicional penal[21].

No que tange à proteção (e produção) dos dados à *cyber* segurança e à privacidade, Andrew Burt menciona, além da convergência que está diariamente ocorrendo entre referidas palavras-chave, o seguinte:

> And it was a world in which privacy and security were largely separate functions, where privacy took a back seat to the more tangible concerns over security. Today, however, the big gestrisk toour privacy and our security has become the threat of unintended inferences, due to the power of increasingly widespread machine learning techniques. Once we generate data, any one who possesses enough of it can be a threat, posing new dangers to both our privacy and our security.

Analisando o ordenamento jurídico brasileiro, desde a Constituição Federal, de 1988, passando pelos principais diplomas normativos infraconstitucionais (Código Penal, Código de Processo Penal e Lei nº 9.296, de 1998), é possível concluir que a

---

[20] MAYER, J.; MUTCHER, P. MetaPhone: The SensitivityofTelephoneMetadata. *Web Policy*, [S.l.], 12 mar. 2014.

[21] Exemplificativamente, na seara do direito penal, no Informativo nº 583, o STJ definiu que "sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no whatsapp presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante. STJ. 6ª Turma. RHC 51.531-RO, Rel. Min. Nefi Cordeiro, julgado em 19/4/2016 (Informativo nº 583 do STJ). Disponível em:<https://www.dizerodireito.com.br/2018/02/acesso-as-conversas-do-whatsapp-pela.html>. Acesso em: 7 jan. 2019.

Lei nº 9.296, de 1998, é a que mais se aproxima do tema, ao abordar interceptação de comunicações telefônicas.

Explicado o conceito de *dataveillance,* sua aplicabilidade na seara penal e sua importância para o desenvolvimento da jurisdição penal brasileira, oportuno responder aos questionamentos feitos no início deste trabalho.

4 CONCLUSÕES

A análise acima permite concluir (ainda que preliminarmente) que o conjunto de instrumentos e normas existentes no Brasil, em especial aquele relativo à proteção de dados, a Constituição Federal, de 1988, Código Penal, Código de Processo Penal, Lei nº 9.296, de 1998, e Lei Geral de Proteção de Dados não garantem ao Estado, mais especificamente na condição de titular da Jurisdição, condições mínimas no combate preventivo às violações aos direitos de autodeterminação informativa do réu, pela utilização de *dataveillance*, violando igualmente o princípio do *nemotenetur se detegere*.

Entretanto, ao mesmo tempo em que a regulamentação do *dataveillance* é recomendável, conforme será intentado ao final, o aparelhamento do Estado com mecanismos de efetivação da medida, em especial em caráter cautelar assim como já ocorre, exemplificativamente, com o sistema BacenJud, é recomendável para a garantia de proteção àquele que pleiteia, bem como de segurança jurídica àquele que se vê no polo passivo de tal medida.

A ponderação inicial que deve ser feita, portanto, diz respeito a uma modificação simples, entretanto, de impactos relevantes: alteração do teor do art. 4º da Lei Geral de Proteção de Dados para que referidos institutos sejam aplicáveis à investigação criminal, mantendo-se na integralidade o teor do art. 33, III, do mesmo diploma normativo.

A efetivação da *dataveillance* no cotidiano, caso realizada com fins ilícitos, poderá impactar na autodeterminação informativa da pessoa com o advento da *internet*, gerando, por exemplo, produção de provas contrárias ao acusado e sem o seu consentimento, gerando consequente proliferação de ataques virtuais baseados no discurso de ódio etc.

De outro modo, o *dataveillance* pode servir, desde que baseado nas regras da Constituição Federal, de 1988, Código Penal, Código de Processo Penal e Lei Geral de Proteção de Dados, de importante instrumento no combate, justamente, à vulneração ao direito de autodeterminação informativa, não devendo o acusado ser coagido a produzir provas contra si mesmo.

Nessa toada, o *dataveillance*, desde que regularmente implantado na cultura jurídica brasileira pelos motivos vistos acima, serve igualmente como instrumento compatível tanto com o garantismo penal, evitando-se abusos por parte do Estado e assegurando garantias ao réu de ordem formal e material.

Por fim, tendo consciência plena de que o debate está apenas no início, adaptando o pensamento de Pierre Teilhard de Chardin (1988), o *dataveillance*, não sendo centro estático do Mundo da Informação, serve de eixo e flecha na evolução do tratamento conferido aos dados.

REFERÊNCIAS

ALEMANHA. Lei Fundamental da Republica Federal da Alemanha. Disponível em:<https://www.btg-bestellservice.de/pdf/80208000.pdf>. Acesso em: 16.março.2019.

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

BRASIL. Código Civil. Disponivel em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm >. Acesso em: 16 mar. 2019.

BRASIL. Código de Processo Civil. Disponivel em:<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm>. Acesso em: 16 mar. 2019.

BURT, Andrew. Privacyandcybersecurity Are Converging. Here´sWhyThatMatters for People and for Companies. Disponível em Harvard Business School:<https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies>. Acesso em: 7 jan. 2019.

CHARDIN, Pierre Teilhard de Chardin. O fenômeno humano. Brazil. Editora CULTRIX, 1988.

CUPIS, Adriano de. "*Riservatezza e segretto (Diritto a). Novissimo Digesto Italiano*. Torino. UTET. 1969.

DONEDA, Danilo; SCHERTEL, Laura Mendes. Um perfil da nova Lei Geral de Proteção de Dados brasileira. In: BELLI, Luca; DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*, São Paulo. Ed. RT. 1980.

FARIAS, Cristiano Chaves de; NETTO, Felipe Braga. ROSENVALD, Nelson. Manual de Direito Civil. Salvador: JusPodivm, 2017.

FARIAS, Paulo. Água: bem jurídico econômico ou ecológico? Editora Brasília Jurídica. Brasília. 2005.

FISCHER, Douglas. Sobre a compatibilização da ampla defesa, do nemotenetur se detegere, da boa-fé objetiva, do devido processo legal (penal) em prazo razoável e da cooperação. In Coleção repercussões do novo CPC – Processo Penal. Coordenadores: Antonio do Passo Cabral, Eugênio Pacelli e Rogério Schietti Cruz. Editora JusPODIVM. 2016. P. 50.

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

ERICSON, Richard; HAGGERTY, Kevin. The surveillantassemblage. British JournalofSociology, London, v. 51, n. 4, p. 605-622, dez. 2000.

KANT, Immanuel. Crítica da Razão Pura. São Pulo: Martin Claret, 2003, p. 29.

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

NETO, Elias Jacob de Menezes; MORAIS, José Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. 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. Rev.Bras.Polít.Públicas,Brasília,v.7, nº 3, 2017, p.184-198.

OLIVEIRA, Fabiana Luci de SILVA, Virgínia Ferreira da. *Processos judiciais como fonte de dados poder e interpretação.* Sociologias. Disponível em:< http://www.scielo.br/pdf/soc/n13/23563.pdf>.

PEREIRA, J. Matos. *Direito de Informação*. Lisboa. Associação Portuguesa de Informática, edição do autor, 1980.

PORTUGAL. Código Civil. Disponível em:<http://www.codigocivil.pt/>. Acesso em 16 mar. 2019.

QUINTIERE, Víctor Minervino. INTIMIDADE VS LIBERDADE DE EXPRESSÃO – Os critérios axiológicos na Jurisdição Constitucional Brasileira. Belo Horizonte. Editora D´ Plácido. 2016.

ROSENVALD, Nelson. O direito civil em movimento: desafios contemporâneos. Salvador: JusPodivm, 2017.

SARLET, Ingo Wolfgang. O direito ao esquecimento na sociedade da informação. Porto Alegre: Livraria do Advogado, 2019.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo.* Malheiros Editores. 32ª edição. 2009. São Paulo.

VITA, Álvaro de. A tarefa prática da filosofia política em John Rawls. Lua nova, n. 25, 1992, p.5-24.

APÊNDICE A

A proposta de regulamentação do tema, no bojo da Lei Geral de Proteção de Dados, com enfoque especial na Lei nº 9.296, de 1998, é a seguinte:

Art. 1º A investigação de fluxo de dados discretos, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Art. 2° Não será admitida a investigação de fluxo de dados discretos quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

IV – o fato investigado constituir contravenção penal.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

Art. 3° A investigação de fluxo de dados discretos poderá ser determinada pelo juiz, excepcionalmente de ofício mediante fundamentação específica sob pena de responsabilidade funcional ou a requerimento:

I - da autoridade policial, na investigação criminal;

II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Art. 4° O pedido de investigação de fluxo de dados discretos conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.

§ 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a investigação, caso em que a concessão será condicionada à sua redução a termo.

§ 2° O juiz, no prazo máximo de setenta e duas horas, decidirá sobre o pedido.

Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.

Art. 6° Deferido o pedido, a autoridade policial conduzirá os procedimentos de investigação de fluxo de dados discretos, dando ciência ao Ministério Público, que poderá acompanhar a sua realização.

§ 1° No caso de a diligência possibilitar a gravação do fluxo de dados discretos, será determinada a sua transcrição.

§ 2° Cumprida a diligência, a autoridade policial encaminhará o resultado da interceptação ao juiz, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas.

§ 3° Recebidos esses elementos, o juiz determinará a providência do art. 8° , ciente o Ministério Público.
Art. 7° Para os procedimentos de investigação de fluxo de dados discretos de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.
Art. 8° A investigação de fluxo de dados discretos, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, preservando-se o sigilo das diligências, gravações e transcrições respectivas.
Parágrafo único. A apensação somente poderá ser realizada imediatamente antes do relatório da autoridade, quando se tratar de inquérito policial (Código de Processo Penal, art.10, § 1°) ou na conclusão do processo ao juiz para o despacho decorrente do disposto nos arts. 407, 502 ou 538 do Código de Processo Penal.
Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.
Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.
Art. 10. Constitui crime realizar investigação de fluxo de dados discretos, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
Pena: reclusão, de quatro a dez anos, e multa.

Recebido em: 18/05/2019
Aprovado em: 05/06/2019