Universidade do Estado do Rio de Janeiro

Centro de Ciências Sociais

Faculdade de Direito

Rodrigo Henrique Luiz Corrêa

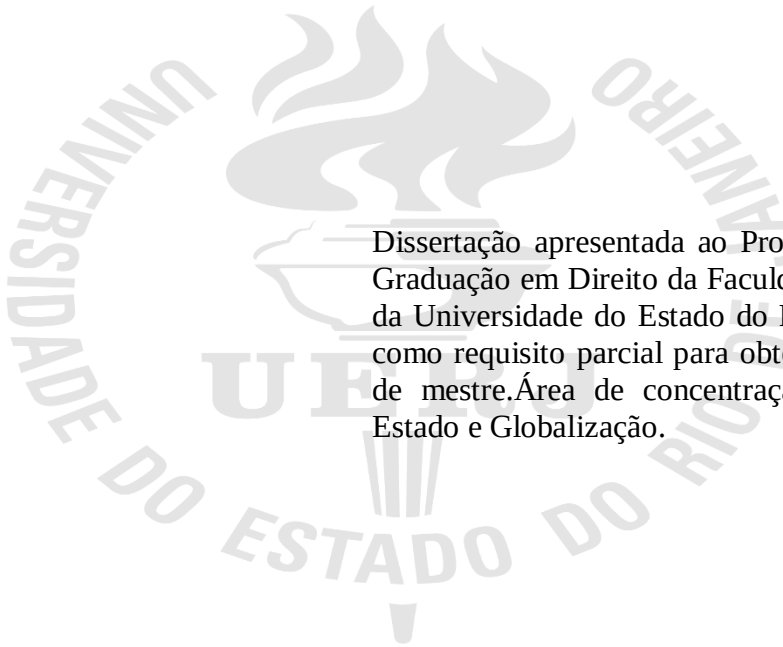
Big Data e Criptografia:
O Lugar do Direito Fundamental à Privacidade Diante das Novas Tecnologias da Informação e Comunicação

Rio de Janeiro

2018

Rodrigo Henrique Luiz Corrêa

Big Data e Criptografia:
O Lugar do Direito Fundamental à Privacidade Diante das Novas Tecnologias da Informação e Comunicação



Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade do Estado do Rio de Janeiro, como requisito parcial para obtenção do título de mestre.Área de concentração: Cidadania, Estado e Globalização.

Orientador: Rodrigo Brandão

Rio de Janeiro

2018

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/C

C824 Corrêa, Rodrigo Henrique Luiz.

Big data e criptografia: o lugar do direito fundamental à privacidade diante das novas tecnologias da informação e comunicação / Rodrigo Henrique Luiz Corrêa. - 2018.
318 f.
Orientador: Prof. Dr. Rodrigo Brandão.

Dissertação (Mestrado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito.

1.Privacidade - Teses. 2.Direitos fundamentais –Teses. 3.Criptografia– Teses. I.Brandão, Rodrigo. II. Universidade do Estado do Rio de Janeiro. Faculdade de Direito. III. Título.

CDU 342.7

Bibliotecária: Marcela Rodrigues de Souza CRB7/5906

_____ _____

Assinatura Data

Rodrigo Henrique Luiz Corrêa

Big Data e Criptografia:
O Lugar do Direito Fundamental à Privacidade Diante das Novas Tecnologias da Informação e Comunicação

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade do Estado do Rio de Janeiro, como requisito parcial para obtenção do título de mestre. Área de concentração: Cidadania, Estado e Globalização.

Data de aprovação: 21 de maio de 2018.

Banca Examinadora:

_____

Prof. Dr. Rodrigo Brandão (Orientador)

Faculdade de Direito - UERJ

_____

Prof. Dr. Carlos Affonso Pereira de Souza

Faculdade de Direito - UERJ

_____

Prof. Dr. Diego Werneck Arguelhes

Fundação Getúlio Vargas - RJ

DEDICATÓRIA

À Thais cujo amor me faz acreditar que vale a pena ter algo pelo qual se lutar.

A Henrique que me fez descobrir em um sorriso o privilégio da paternidade.

À Mara, pelo exemplo de tenacidade e apoio desde os meus primeiros dias de vida.

A José que nos disse até breve, não sem antes deixar seu exemplo de integridade e dedicação.

AGRADECIMENTOS

O ambiente efervescente, de profusão de ideias arrojadas e composto por homens e mulheres públicos notáveis, tem inspirado cada vez mais jovens a ingressarem no programa de Pós Graduação em Direito da UERJ (PPGD-UERJ). No meu caso, ainda durante a graduação na Faculdade Nacional de Direito, acalentava o sonho de ingressar em uma das linhas de pesquisa mais concorridas do país. Todavia, o cotidiano das aulas mostrou que o programa vai além de manter um nome respeitado pela excelência do trabalho acadêmico de seus membros. O PPGD da UERJ é feito de pessoas admiráveis – professores, corpo administrativo e alunos - que acreditam na educação pública de qualidade, no acesso democrático aos bens e serviços públicos, no papel libertador do ensino, na autonomia do indivíduo, mas também no reconhecimento e valorização de sua identidade política, social, econômica, religiosa e de gênero. A valorização do pluralismo, da livre circulação de ideias, da redução das desigualdades socioeconômicas vai aos poucos abrindo as portas para que os abismos existentes sejam superados e seja possível construir uma sociedade fluminense mais justa e solidária. A gratificante experiência no estágio docente me fez perceber que, a despeito de tudo, a Uerj resiste!

A realização do sonho de ingressar no programa permitiu a este mestrando o contato com figuras extraordinárias, dignas de agradecimento e admiração, cujas ideias repercutem no direito público pátrio e estrangeiro e tanto orgulham o programa. Agradeço a Luís Roberto Barroso que, antes de ministro da mais alta corte do país, com longa trajetória na advocacia pública, é professor Livre-docente pela UERJ, cujo exemplo de retidão, humildade e competência o coloca como exemplo a ser seguido. A Jane Reis que, além de ter me honrado, participando da banca de concurso para ingresso na Procuradoria do Município, me permitiu participar de frutíferas reflexões sobre interpretação constitucional e a atual situação político-institucional que atravessa o país. A Daniel Sarmento, por compartilhar de sua inegável competência acadêmica e por escolher, em sua gloriosa trajetória profissional, os melhores combates, na promoção de direitos fundamentais de quem sequer possui direito a ter direitos. A Ana Paula de Barcellos cujos encontros no grupo de pesquisa me permitiram reflexões sobre políticas de proteção à privacidade que contribuíram sobremaneira para o aperfeiçoamento deste trabalho. A Alexandre Aragão cuja generosidade e inteligência nos proporcionaram momentos únicos no grupo de pesquisa institucional sobre infraestrutura.

A Carlos Affonso de Souza, grata surpresa que o programa me concedeu, permitindo a perfeita interlocução entre o Direito Público e o Direito Privado, cujo profundo conhecimento da área de tecnologia e a generosidade de sempre me permitiram alcançar outro patamar no conhecimento dos desafios trazidos ao direito pelas novas tecnologias. Os seminários, bem como as conversas travadas no ITS Rio, sem dúvida, me propiciaram um manancial de conhecimento, deixando claro que o direito não pode se fechar em si mesmo, mas deve se lançar a resolver os conflitos da sociedade contemporânea. Agradeço sobretudo pelas orientações durante o processo de qualificação e as valiosas contribuições na estruturação deste trabalho.

Nos idos de 2009, ainda no fim da graduação e quando me dedicava à preparação para concursos públicos, tive a honra de ser aluno de Rodrigo Brandão e ali percebi que havia algo de novo e substancial em sua abordagem do Direito Constitucional. A profundidade de sua abordagem permitia a seus alunos irem muito além do trivial, a construir suas próprias reflexões de maneira qualificada. Por uma grata surpresa da vida, me foi permitido concretizar essa profunda admiração, através do ingresso nos quadros da Procuradoria Geral do Município do Rio de Janeiro, na qual descobri que, além de uma vida acadêmica admirável, Rodrigo também é dos mais destacados advogados públicos que a cidade poderia ter. Por fim, no Programa de Pós Graduação me foi concedida a honra de ter sido por ele orientado durante o mestrado, o que também me permitiu conhecer, além do colega admirável, a pessoa generosa - e não menos exigente - humana e competente que envidou todos os esforços para que este trabalho seguisse nos trilhos e, se isto não aconteceu, o foi em razão do orientando.

Aos diletos amigos que o programa me permitiu fazer, de diferentes origens e experiências profissionais, os quais muito enriqueceram meu modo de ver o direito, a saber, Luisa Lacerda, Caroline Tauk, Júlio Araújo, Eduardo Lasmar. Um agradecimento especial a Matheus Escossia, amigo de promissor futuro na vida acadêmica, que dedicou seu tempo a contribuir com o aperfeiçoamento deste trabalho. Também a André Farah que, além de combatente promotor de justiça e querido amigo, muito contribuiu com suas reflexões para este trabalho, durante e após as aulas de Regulação da Internet e Marco Civil da Internet, trocando as apreensões comuns e brindando o programa com excelente dissertação sobre novas tecnologias e liberdade de expressão. A proximidade existente entre os temas não o impediu de ser generoso a ponto de compartilhar os conhecimentos obtidos e reflexões alcançadas.

Enfim, a todos que, direta ou indiretamente, contribuíram para a conclusão deste trabalho, meus sinceros agradecimentos.

EPÍGRAFE

"Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety".

Benjamin Franklin

RESUMO

CORRÊA, Rodrigo Henrique Luiz. **Big Data e Criptografia:** o Lugar do Direito Fundamental à Privacidade Diante das Novas Tecnologias da Informação e Comunicação.2018**.**318f. Dissertação (Mestrado em Direito Público) – Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

O objeto deste trabalho é investigar o impacto das novas tecnologias de informação e comunicação sobre o direito à fundamental à privacidade. Para tanto, se investigará a concepção contemporânea de privacidade, a partir da comparação entre as culturas estadunidense e europeia de privacidade. A análise das novas tecnologias de informação e comunicação será feita mediante a abordagem de dois fenômenos tecnológicos recentes: *big data* e criptografia. O *big data* será abordado tendo em conta as repercussões da vigilância estatal e privada sobre os direitos individuais, bem como serão apresentadas as alternativas para a proteção de dados pessoais. A criptografia será investigada enquanto instrumento de proteção à privacidade e outros direitos fundamentais, bem como enquanto escudo contra a vigilância estatal, investigando especialmente as soluções para o conflito entre criptografia ponta a ponta e o direito à segurança pública.

Palavras-chaves:Privacidade. Direitos fundamentais. Cultura europeia de privacidade. Cultura americana de privacidade. Normas internacionais sobre privacidade. Big data. Dados pessoais. Vigilância. Criptografia. Privacidade diferencial. Direitos fundamentais. Segurança pública.

ABSTRACT

CORRÊA, Rodrigo Henrique Luiz. **Big Data and Cryptography**: the Place of Fundamental Right to Privacy in the Face of New Technologies of Information and Communication.2018.318 f.Dissertação (Mestrado em Direito Público) – Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

The purpose of this paper is to investigate the impact of new information and communication technologies on the fundamental right to privacy. To do so, we will investigate the contemporary conception of privacy, from the comparison between the American and European cultures of privacy. The analysis of the new information and communication technologies will be made through the approach of two recent technological phenomena: big data and cryptography. The big date will be addressed taking into account the repercussions of state and private surveillance on individual rights, as well as alternatives for the protection of personal data will be presented. Encryption will be investigated as an instrument for protecting privacy and other fundamental rights, as well as as a shield against state surveillance, especially investigating solutions to the conflict between end-to-end encryption and the right to public safety.

Keywords: Privacy. Fundamental rights. European privacy culture. American culture of privacy. International standards on privacy. Big data. Personal data. Surveillance. Cryptography. Differential privacy. Fundamental rights. Public safety.

SUMÁRIO

INTRODUÇÃO E OBJETIVOS

A privacidade, enquanto direito fundamental em espécie, tem apresentado um conteúdo variado ao longo da história. Nas sociedades feudais, não havia a concepção de um espaço privado do indivíduo ou da família, mantendo-se assim, inclusive, durante o fim da Idade Média, período durante o qual as corporações de ofício eram espaços coletivizados, com pouca ou nenhuma privacidade[1]. Deste modo, as condições econômicas que propiciaram a ascensão da classe burguesa também permitiram que a intimidade fosse ainda um privilégio de poucos, alterando-se a estrutura social feudal anterior.

Com efeito, a construção doutrinária da privacidade em sua fase embrionária esteve atrelada à inviolabilidade da casa e da vida familiar, sendo, portanto, um direito desfrutado apenas pelos que detinham a faculdade de uso e gozo de um imóvel, ou seja, um privilégio exclusivo usufruído inicialmente pela nobreza e, posteriormente, pela classe burguesa[2].

Com a ascensão da burguesia, a privacidade passou a ser uma preocupação específica dessa classe[3], apenas quanto aos seus aspectos patrimoniais, no momento inicial - ou seja, direitos asseguradores da inviolabilidade da propriedade -, para, posteriormente, resguardar os hábitos, opiniões e manifestações no âmbito da casa, enquanto local privado inviolável pelo Estado. Por outro lado, a imprensa da segunda metade século XIX, desejosa em noticiar em

---

[1] Para Stefano Rodotà, "o nascimento da privacidade pode ser historicamente associado à desagregação da sociedade feudal, na qual os indivíduos eram todos ligados por uma complexa série de relações que se refletiam na sua própria vida cotidiana: o isolamento era privilégio de pouquíssimos eleitos ou daqueles que, por necessidade ou opção viviam distantes - místicos ou monges, pastores ou bandidos". RODOTÀ, Stefano. **A vida na sociedade da vigilância** - a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 26.

[2] Para Danilo Doneda, o caráter excessivamente individualista da privacidade em sua chamada "era de ouro", que ocorreu na segunda metade do século XIX, fez com que inicialmente se constituísse em um direito subjetivo de poucos privilegiados, que possuíam alguma projeção social e econômica. Aos poucos, com o advento do estado de bem-estar social, a evolução tecnológica e o adensamento da classe trabalhadora, a relação entre indivíduos e Estado passou a ser mais intensa em todo o tecido social, o que avultou no aumento da demanda por privacidade de membros não integrantes da elite econômica ou social, ainda que coletivamente. (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 12-13).

[3] Há quem conteste o caráter eminentemente burguês da origem do direito à privacidade. Edoardo Giannotti, em negação a ideia que o "eventual caráter burguês da proteção da intimidade é discutível, quando lembramos que a legislação soviética reconhece esse direito a nível constitucional, como será visto adiante", GIANNOTTI, Edoardo. **A tutela constitucional da intimidade**. Rio de Janeiro: Forense, 1987, p. 12. Em que pese correta a constatação da proteção à privacidade no regime soviético, é questionável se em tais regimes de economia planificada havia liberdade suficiente para se demandar do Estado esta proteção, haja vista que o controle da informação é essencial em regimes deste modelo. Ademais, a identificação da privacidade com as demandas de uma elite econômica e/ou social não se restringe à classe burguesa, mas também é encontrada na cultura francesa como direito pleiteado pela nobreza e pela classe artística. Todavia, essa identificação elitista é meramente inicial e, à medida da inserção do restante da população nas relações de consumo e com o uso abrangente de banco de dados, passam a ser potenciais vítimas potenciais de violações da privacidade qualquer cidadão que trave relações no âmbito da sociedade.

suas colunas sociais detalhes da vida privada dos indivíduos de alguma projeção, tornou a burguesia de então apreensiva quanto ao registro e divulgação de hábitos e atitudes adotadas no âmbito familiar ou mesmo em relação à publicidade da relação de bens que constituía seu patrimônio.

No direito norte-americano, este incômodo culminou com a construção doutrinária de um direito à privacidade autônomo em relação à propriedade - ainda que fortemente baseado nos institutos típicos da propriedade material e imaterial -, cuja violação possibilitaria ao seu titular a reparação pecuniária ou mesmo a interdição preventiva da divulgação não autorizada de fatos da vida privada. Por outro lado, no direito continental europeu, data-se do século XVIII a preocupação com o direito de imagem dos membros da alta sociedade, a ponto de se proibir a venda de obras de arte que retratavam pessoas de poder aquisitivo em cenas de nudez ou em seu leito de morte, não sendo raro que membros da nobreza ou da alta burguesia fossem autores de demandas com vistas a resguardar a própria privacidade.

Noticia-se como o artigo histórico mais importante sobre o tema o escrito em 1890 pelos advogados Samuel Warren e Louis Brandeis[4], que definiram o direito à privacidade como o direito de ser deixado só (*right to be let alone*), no que se conceituava a privacidade, basicamente, como o direito de não ter fatos inerentes à vida privada e familiar registrados e publicados sem autorização do titular.

Desde a publicação do artigo histórico até os dias atuais, o panorama e os desafios impostos à privacidade mudaram sobremaneira. A evolução das tecnologias de informação e comunicação fez com que os sistemas de armazenamento e processamento de dados se tornassem praticamente ilimitados, com capacidade para processar um volume de dados sem precedentes. Aliado a esse instrumental, no contexto da guerra ao terror, após os atentados de 11 de setembro de 2001, surgiram denúncias de vigilância em massa e irrestrita de cidadãos, governos e empresas, por parte de agências norte-americanas de inteligência.

Nesta perspectiva, as novas tecnologias comunicativas foram também acompanhadas de um grande incremento de sensores e da capacidade de coleta e processamento de dados. Portanto, fenômenos como a vigilância pública e privada foram viabilizados pela capacidade de processamento massivo de dados, conhecida por *big data*. Uma das formas de resistência à vigilância e de proteção à privacidade é a criptografia.

---

[4] WARREN, Samuel; BRANDEIS Louis. The right to privacy, **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.

Com efeito, no atual estágio de evolução tecnológica, nos parece inadequado tratar a privacidade através do binômio *recolhimento e divulgação*, enquanto escolhas opostas e excludentes. Não nos parece ser mais uma opção a exigência de privacidade enquanto reclusão ou mesmo que se demande que a coleta e processamento de dados para os mais variados fins seja abolida.

Não se é mais possível uma reclusão absoluta, vez que a vida contemporânea exige um grau mínimo de interação e exposição. Por outro lado, não se mostra sustentável - embora a evolução tecnológica cada vez mais demonstre sua possibilidade - a completa transparência do ser humano, sob argumento dos imperativos de segurança da sociedade. O ponto ótimo deste conflito e a interação mútua do binômio está entre os objetos deste trabalho.

A coleta e processamento de grande volume de dados é característica da sociedade da informação e, no atual cenário evolutivo, não se pode imaginar que impedir essa coleta seja uma solução. Logo, há que se discutir o novo lugar da privacidade e os seus contornos diante das novas tecnologias e do advento do *big data*. Não que isto signifique se render aos ditames tecnológicos ou mesmo atestar o fim da privacidade[5], abrindo mão por completo de qualquer salvaguarda, mas de compreender que a privacidade contemporânea não lida com os mesmos desafios de outrora, exigindo-se o seu reposicionamento.

Desta forma, mostra-se até de certo modo utópico e ineficaz exigir a observância de um direito a ser deixado só no contexto de uma sociedade hiperconectada. Faz-se necessário que haja uma concepção mais adequada e contemporânea de privacidade, pois, ainda que a preservação da reclusão familiar seja o símbolo clássico deste direito, na era da informação, mesmo que o sujeito esteja só em sua esfera de reclusão pode ser objeto de monitoramento, classificação e interceptação.

Atualmente, não é pouco frequentemente que navegadores e aplicativos realizem a coleta e processamento de hábitos de pesquisa, de consumo, de deslocamento, formando-se um perfil involuntário do indivíduo para fins comerciais ou investigativos, mesmo que o usuário não perceba ou consinta expressamente. Há autores que vislumbram esse cenário de recolhimento massivo de dados como irreversível e até positivo para a evolução da sociedade, que contará com diagnósticos, sejam eles médicos, de consumo ou de tráfego mais amplos e completos[6]. Outros, porém, advertem sobre a possibilidade de essa coleta indiscriminada de

---

[5] WHITAKER, Reginald. **The End of Privacy**: How Total Surveillance Is Becoming a Reality. New York: Paw Prints, 2008.

[6] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. **Big Data**: A Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mffin Hartcourt, 2013.

dados viabilizar uma indevida vigilância em massa[7] por parte do Estado ou mesmo que o acesso a estes dados seja concedido a agentes privados interessados.

Neste mesmo contexto, avulta a importância da preservação e do tratamento de dados pessoais sensíveis, os quais, na sociedade da informação[8], tornam-se valiosas mercadorias[9], tanto para governos interessados no monitoramento social quanto para grandes corporações interessadas em monitorar e catalogar indivíduos-consumidores, potencializando sua parcela de mercado.

Pode-se afirmar que, com a expansão da rede mundial de computadores, além da personalidade física do indivíduo, com seus sentimentos, opiniões e hábitos afetos à própria privacidade, passou a ser objeto de preocupação jurídica o sujeito digital, cuja atividade, comunicação, preferências e opiniões na rede passam a ser objeto de monitoramento e catalogação[10].

Portanto, resguardar a privacidade da pessoa física não se mostra mais suficiente, passando a se falar em privacidade da pessoa digital, a partir da preservação do conjunto de informações sensíveis do indivíduo, constante dos variados e interligados sistemas de informação coletores de dados. Disto decorre a necessidade de haver uma legislação nacional que regulamente a coleta e o processamento de dados pessoais, a fim de que se defina qual modelo de proteção será adotado.

Na sociedade da informação, os indivíduos trocam um intenso fluxo de dados, sejam financeiros, afetivos ou de opinião. Logo, faz-se fundamental a proteção adequada da privacidade desses indivíduos, preservando seu espaço intangível, a despeito de pressões tanto das agências de investigação estatais como das corporações privadas.

---

[7] BAUMAN, Zygmunt. **Vigilância Líquida**. Diálogos com David Lyon. Zahar Editora, 2014.

[8] Sobre o conceito de sociedade da informação, conferir: LYON, David. Cyberespace: Beyond the Information Society? In: ARMITAGE, John Armitage; ROBERTS, Joanne (Eds.). **Living With Cyberspace**. New York: Bloomsbury Academic, 2002, p. 21-33.

[9] Para alguns, os dados são o novo petróleo. Vide THIRANI, Vasudha; GUPTA, Arvind. The value of data. **World Economic Forum**, set. 2017. Disponível em: <https://www.weforum.org/agenda/2017/09/the-value-of-data/>. Acesso em: 22 dez. 2017. Thirani e Gupta afirmam: "To discuss and resolve these issues, it is imperative to be cognizant about the value of data. In this age of hyper connected consumers, data is definitely the new age 'oil'" (em tradução livre: Para discutir e resolver esses problemas, é imperativo estar ciente sobre o valor dos dados. Nesta era de consumidores hiper conectados, os dados são definitivamente o novo "petróleo" da era).

Para outros, os dados possuem valor superior ao do petróleo, vide THE WORLD'S MOST valuable resource is no longer oil, but data. **The Economist**, may. 2017. Disponível em: <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>. Acesso em: 22 dez. 2017.

[10] SOLOVE, Daniel J. **The Digital Person**: Technology and Privacy in the information Age. New York: New York University Press, 2004.

O grande volume de dados, recolhido pelos mais diversos sensores - como aplicativos, dispositivos inteligentes, redes sociais, entre outros - associados a uma variedade sem precedentes destes dados - podendo-se hoje combinar dados que não possuiriam qualquer relação -, bem como uma elevada velocidade de processamento destes dados quase em tempo real foram fatores propícios ao advento do big data[11], ou seja, a coleta e o processamento massivo de dados, com vistas a extrair informações sobre hábitos, antecipar tendências ou mesmo decidir o destino de indivíduos com base na probabilidade que deste processamento se extrai[12].

Portanto, um dos temas que se pretende aprofundar é, diante dos evidentes benefícios que o *big data* pode trazer - tais como o aperfeiçoamento da educação, da medicina da agricultura de precisão, entre outros -, saber quais seus limites e contornos possíveis nas análises de probabilidade, sob pena de se estabelecer uma ditadura dos dados em que os algoritmos decidem a vida dos indivíduos, ceifando-lhes as oportunidades com base no comportamento de terceiros.

Neste mesmo contexto, a concreta possibilidade de vigilância irrestrita dos indivíduos fez surgir uma resistência cibernética a tais monitoramentos, a fim de se garantir a plenitude da liberdade de expressão, sem qualquer tipo de monitoramento ou controle governamental.

Entre outros instrumentos de resistência à vigilância estatal, está a criptografia, ou seja, a habilidade de codificar o conteúdo das comunicações para evitar interceptações e rastreamentos. A aplicabilidade da criptografia têm sido a mais ampla possível, seja na garantia da segurança do comércio eletrônico, na comunicação que envolva sigilo industrial ou profissional de grandes corporações, na intercomunicação bancária ou mesmo na criação de um modelo alternativo de transações financeiras com a criação das criptomoedas[13].

---

[11] Trata-se dos três V's que caracterizam o *big data* (da doutrina americana *volum*, *velocity* e *variety*) conforme se verá neste trabalho.

[12] Pode-se citar como caso emblemático, um condenado por se evadir da polícia de La Crosse, Wiscosin, nos Estados Unidos, cuja pena foi influenciada pela possibilidade de reincidência apontada por um algoritmo secreto que estabelece a escala Compas, utilizado pela justiça daquele estado na definição da propensão a reincidência de acordo com o risco calculado com base nas informações inseridas. Por óbvio que como todo e qualquer algoritmo se trabalha com o processamento de dados de outros presos para compor seus prognósticos de risco de reincidência. Voltaremos ao tema quando tratarmos de algoritmos. Vide: SMITH, Mitch. In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. **New York Times**, jun. 2016. Disponível em: <https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html>. Acesso em: 20 dez. 2017.

[13] "Criptomoeda é um tipo de moeda virtual que utiliza a criptografia para garantir mais segurança em transações financeiras na internet. Da mesma forma que a moeda tradicional possui números de série ou listras ocultas em seu interior para evitar falsificações, a criptomoeda também utiliza códigos que são muito difíceis de quebrar." PAVÃO, Samantha. Entenda o que é criptomoeda e saiba como usar. **PSafe Blog**, nov. 2017. Disponível em: <http://www.psafe.com/blog/o-que-criptomoeda/>. Acesso em: 17 dez. 2017.

Uma das aplicações mais recentes do recurso da criptografia se dá em aplicativos de troca de mensagens via web, tais como WhatsApp ou Telegram. Ambos os aplicativos citados possuem criptografia ponta a ponta, ou seja, o conteúdo das mensagens é cifrado, de maneira que somente emitente e destinatário possuem parte do código[14], que permite a visualização da mensagem, o que impossibilitaria[15] que o conteúdo das conversas fosse lido pelo gestor do aplicativo ou por terceiros[16].

Essas e outras funcionalidades dos referidos aplicativos - dentre as quais pode-se citar o não armazenamento de mensagens no servidor, a destruição do conteúdo das mensagens após a sua visualização ou até mesmo a verificação da identidade do usuário em duas etapas - fortalecem a garantia de privacidade dos usuários e, em tempos de vigilância e invasão de sistemas de informação, agrega maior valor de mercado às empresas que disponibilizem maiores mecanismos de segurança da informação.

Todavia, tais funcionalidades não são disponibilizadas sem nenhuma resistência. No que tange à criptografia ponta a ponta, não haveria a possibilidade de interceptação das mensagens. Esta inviolabilidade garantiria maior segurança ao usuário que teria a certeza de que, mesmo se quisesse, nem mesmo o gestor do aplicativo poderia acessar o conteúdo de suas mensagens.

Ocorre que há outros interesses constitucionais relevantes que, à primeira vista, são frustrados, em virtude da funcionalidade em pauta. Nesse sentido, não é possível afirmar que os milhões de usuários que utilizam o aplicativo o façam para atividades ilícitas. Seria o

---

[14] Sobre o uso de chave pública e chave privada em criptografia, vide FERNANDES, Carlos Henrique de; O.FILHO, Fernando Mario de. A Privacidade na Sociedade da Informação. **Rede Linux IME-USP**, nov. 2003.Disponível em: <https://www.linux.ime.usp.br/~carloshf/0302-mac339/fase1/>. Acesso em: 22 dez. 2017.

[15] Em que pese ser esta a informação oficial prestada pelo aplicativo às autoridades que determinam o fornecimento do conteúdo das conversas ou mesmo a sua interceptação, há profissionais que afirmem que a interceptação seria possível na hipótese de troca da chave da criptografia pelo aplicativa. A questão ainda é controvertida, sendo o seu esclarecimento um dos objetos da Audiência Pública convocada pelo Supremo Tribunal Federal na ADI 5527 e ADPF 403. Sobre a controvérsia do tema, veja-se: SCRIVANO, Roberta. 'Não é possível interceptar', afirma especialista sobre dados do WhatsApp'. **O Globo**, jul. 2016. Disponível em: <http://oglobo.globo.com/economia/nao-possivel-interceptar-afirma-especialista-sobre-dados-do-whatsapp-19750758>. Acesso em: 05 mar. 2017 ou EFE. 'WhatsApp tem vulnerabilidade que permite interceptar mensagens'. **Exame**, jan. 2017. Disponível em: <http://exame.abril.com.br/tecnologia/whatsapp-tem-vulnerabilidade-que-permite-interceptar-mensagens/>. Acesso em: 05 mar. 2017.

[16] Segundo os termos de uso de Telegram, todas as mensagens são criptografadas, mas apenas para os chamados chats secretos se garante haver criptografia ponta-a-ponta, ou seja, cliente a cliente e nos outros casos (chats privados e em grupo) se afirma haver a criptografia servidor-cliente. As informações estão disponíveis no próprio site do serviço: <https://telegram.org/faq/br#p-e-se-eu-for-mais-paranico-que-um-usurio-comum>. Acesso em: 18 fev. 2016.

No caso do WhatsApp, os termos de uso informam que a criptografia ponta-a-ponta é por padrão quando emitente e receptor estiverem utilizando uma versão do aplicativo que tenha sido lançada após o dia 2 de abril de 2016.

mesmo que extinguir estradas porque alguns veículos as usam para transportar drogas ou produtos de contrabando. Não se procurará neste trabalho a defesa de qualquer ausência de regulação. Pelo contrário, sabe-se que se contrapõe ao legítimo direito fundamental à privacidade do usuário o interesse da investigação criminal, na tutela da sociedade e na promoção da segurança pública.

Portanto, diante das novas tecnologias de informação e comunicação, o *big data*, enquanto processamento massivo de dados dos indivíduos, e a criptografia, enquanto instrumento de resistência à vigilância massiva, mostram-se como desafios contemporâneos do direito fundamental à privacidade, moldando-lhe o conteúdo e definindo seus novos limites.

As questões apresentadas não são triviais e estão longe de uma solução definitiva. O tema mostra-se relevante para o direito pátrio, em virtude da acelerada proliferação de aparelhos *smartphones*, os quais possibilitam o acesso a aplicativos que possuem criptografia, bem como pela relevância que os softwares de mensagens via web adquiriram, de forma a viabilizar, a custos mais baixos, a comunicação de grupos profissionais, a realização de negócios jurídicos, o tráfego de arquivos para todas as partes do mundo, bastando ter acesso à internet. Da mesma forma, esses mesmos aparelhos telefônicos, de múltiplas funcionalidades, permitem que a fabricante do aparelho, assim como outros aplicativos e redes sociais, coletem informações de hábito de trajeto, prática de atividades físicas, lugares de frequência, hábitos de consumo, assuntos de interesse, entre outros. O processamento destes dados combinados pode permitir o alcance de informações de extrema sensibilidade, tais como orientação política, informações sobre saúde, pessoas com quem se relaciona, entre outros, constituindo-se em informação de interesse tanto da vigilância estatal quanto de corporações privadas.

Portanto, para além do fato de a privacidade constituir direito fundamental, há, ainda, a necessidade de se estabelecer suas fronteiras em tempos de evolução tecnológica que permitem uma vigilância ilimitada do indivíduo. Ora, a coleta e tratamento de dados pode servir aos mais nobres fins, como é o caso de tornar mais eficiente uma política pública ou mesmo aperfeiçoar a segurança dos cidadãos. Todavia, o homem contemporâneo vive em rede e tem em seus dados quase a totalidade de sua personalidade, podendo-se falar em direitos da pessoa digital. Isto implica dizer que há fins menos nobres que poderão ser alcançados, tais como a perseguição e o monitoramento de indivíduos que possuam determinado posicionamento ideológico ou a exposição indevida e vexatória de fatos inerentes à intimidade.

O direito à privacidade está intimamente relacionado ao livre desenvolvimento da personalidade e, em última análise, à liberdade. Ora, não se trata de ter ou não algo a esconder[17], o que é uma premissa equivocada para a justificativa da vigilância indiscriminada. Pelo contrário, quem sabe que é ou pode estar vigiado não desempenha com a devida liberdade os atos que sua consciência indica. Por outro lado, não é o cidadão que deve justificar porque faz jus à preservação de sua privacidade, mas são os estados e corporações privadas que devem provar a pertinência, imprescindibilidade, finalidade específica e legitimidade da coleta e tratamento de dados do indivíduo, e isso deve estar ainda mais claro em tempos de vigilância massiva.

Impõe-se, portanto, o enfrentamento dos dilemas contemporâneos trazidos pelo direito à privacidade na era da tecnologia da informação. Se os equipamentos de fotografia causavam indignação nos advogados de Boston, em 1890, os recursos tecnológicos ilimitados dos dias atuais, que permitem as condições para o *big* data, de um lado, e a comunicação criptografada de outro, se utilizados sem parâmetro ético[18], tornariam o indivíduo um homem de vidro, absolutamente transparente nos seus segredos mais íntimos, vez que seus dados de consumo, afinidades, atividades *online*, deslocamentos, comunicações e afetos podem ser facilmente rastreáveis.

Cabe revisitar o direito à privacidade, sob a ótica da teoria dos direitos fundamentais, para situar sua amplitude e grau de proteção nos dias atuais, buscando um conceito exequível ante o inegável avanço tecnológico proporcionado pela tecnologia da informação que não deixe a descoberto ao indivíduo um espaço mínimo e intangível, essencial à sua dignidade, ao livre desenvolvimento da personalidade, infenso a intromissões indevidas.

Para tanto serão selecionados fenômenos tecnológicos recentes que mais se relacionam diretamente com a privacidade, quais sejam, o *big data* e a criptografia, para, a partir destes, dialogar com o lugar do direito fundamental à privacidade.

No primeiro capítulo, este trabalho se ocupará do percurso histórico do direito à privacidade no ocidente. Se realizará uma análise comparativa entre as principais culturas ocidentais de privacidade, a saber, dos Estados Unidos e Europa, apontando-se suas

---

[17]SOLOVE, Daniel J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. **San Diego Law Review**, v. 44, p. 745, 2007.

[18] Na obra Vigilância Líquida, Bauman, ao combater a diaforização, ou seja, o processo de distanciamento entre os agentes de vigilância e os dados pessoais processados, o que facilitaria a ausência de parâmetros éticos à vigilância, defende exatamente o contrário. O advento do uso ilimitado da tecnologia no processamento de dados não pode perder de vista o caráter ético deste processamento massivo. BAUMAN, Zygmunt. **Vigilância Líquida**. Diálogos com David Lyon. Rio de Janeiro: Zahar Editora, 2014.

divergências e semelhanças. Propor-se-á a abordagem que se entende adequada do conceito de privacidade a partir da verificação de sua adequação aos desafios contemporâneos.

No segundo capítulo, haverá um aprofundamento da compreensão do fenômeno do *big data*, a partir da apresentação do seu contexto, conceito e evolução. Serão abordadas as oportunidades decorrentes do *big data*, bem como os riscos de seu uso sem parâmetros éticos que podem limitar oportunidades, propiciar resultados discriminatórios e violar a privacidade dos indivíduos. Abordar-se-á, ainda, o fenômeno da vigilância, estatal e privada, que, se não é causado diretamente, é potencializado pelo processamento massivo de dados. Outro assunto importante relacionado ao *big data* é a proteção aos dados pessoais. Em consonância com o primeiro capítulo, será abordado o modelo de proteção aos dados pessoais nos Estados Unidos, Europa, bem como o atual estágio do tratado de compartilhamento e proteção de dados. Por fim, será brevemente apresentado o estágio da proteção de dados no Brasil e os desafios que são colocados a uma proteção suficiente.

No terceiro e derradeiro capítulo, será abordado o fenômeno da criptografia e sua relação com a proteção à privacidade, apresentando-se os formatos de encriptação, sua aplicabilidade e os riscos de sua utilização indevida. Tratar-se-á ainda acerca da juridicidade de um modelo de criptografia inquebrável e se de fato há um real conflito entre segurança publica e criptografia que justifique a limitação do direito à privacidade. Serão abordados, no mesmo capítulo, soluções propositivas, com vistas a proteger adequadamente a privacidade diante dos novos fenômenos tecnológicos, sem que essa proteção impeça que se desfrute dos avanços proporcionados pela tecnologia.

1 **ANÁLISE DA PRIVACIDADE NO DIREITO COMPARADO E NO DIREITO POSITIVO BRASILEIRO**

> Few values so fundamental to societys as privacy have been left so undefined in social teory or have been such vage and confused writing by social cientists.[19]
>
> *Alan Westin*

1.1 **Evolução e trajetória do conceito de privacidade no sistema norte-americano**

Como se sabe, em virtude da tradição da *common law*, a construção do direito norte-americano é essencialmente jurisprudencial. Isto significa dizer que o reconhecimento ou a consagração de determinado direito decorre, principalmente, da interpretação jurídica dada pelos tribunais, sobretudo os casos julgados pela Suprema Corte.

Curiosamente, no caso do direito à privacidade, sua construção foi inicialmente doutrinária, a partir de uma obra jurídica inaugural, e apenas décadas depois obteve seu reconhecimento na jurisprudência, não sem alguma resistência.

Desta forma, o direito à privacidade possui raízes teóricas no clássico artigo dos advogados Samuel D. Warren eLouis D. Brandeis, *The right to privacy*, publicado em 1890[20]. Diante do aparelhamento tecnológico pelo qual passava a imprensa de então, principalmente com a captação de imagens por fotografia instantânea e a avidez por noticiar fatos relacionados ao convívio privado, os autores motivaram a elaboração do artigo em nome da necessidade do ser humano à própria solidão[21].

Não que a proteção jurídica de alguns aspectos inerentes à privacidade não tivesse sido abordada anteriormente, mas o artigo é considerado divisivo, ao menos no direito norte-americano, por ter sido o primeiro a tratar a privacidade como direito autônomo e peculiar,

---

[19] Em livre tradução: "Poucos valores tão fundamentais para a sociedade quanto a privacidade foram deixados tão indefinidos na teoria social ou foram escritos de maneira vaga e confusa por cientistas sociais. WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 1967, p. 5.

[20] WARREN, Samuel D.; BRANDEIS, Louis D. Op. cit., publicado em 1890. Posteriormente, em 1916, Samuel Brandeis foi nomeado para a Suprema Corte dos Estados Unidos pelo Presidente Woodrow Wilson.

[21] Embora o artigo dê a entender que as motivações de sua elaboração decorram do assédio geral praticado pela imprensa sensacionalista, é mais crível a versão que Samuel Warren tenha motivações pessoais para a publicação. Isto porque, Warren, um advogado e abastado herdeiro de uma indústria de papel, casado com a filha do Senador Bayard, era membro de uma das famílias mais ricas de Boston do final do século XIX. Por esta razão, as recepções sociais realizadas pela esposa de Warren eram constantemente noticiadas pelas colunas sociais dos jornais de Boston, especialmente o Evening Gazette, que cobria estes eventos com detalhes pessoais e embaraçosos. Esta seria a razão de Warren ter proposto ao advogado Louis Brandeis, seu sócio, a elaboração do artigo. Esta versão dos fatos está disponível em PROSSER, William. Privacy. **California Law Review**, v 48, n. 3, p. 383-423, 1960.

distinto das manifestações do direito de propriedade e para além das hipóteses de calúnia e difamação.

Nesse sentido, o próprio texto cita[22] a obra do juiz Cooley[23] que tratara incidentalmente do direito a ser deixado só. Todavia, é mérito do artigo o fato de inaugurar a privacidade como um direito (*right to privacy*) e não apenas como um interesse individual, definindo alguns de seus contornos e diferenciando-o do direito de propriedade. É de se pontuar que a obra de Cooley, que tem por enfoque a responsabilidade civil extracontratual (*torts*), tratou, ainda que de forma tangencial, sobre o direito a ser deixado só apenas enquanto fundamento para a reparação civil. Todavia, o autor não aborda a privacidade como um direito autônomo por si, mas aponta uma relação de direitos do indivíduo cuja violação gera responsabilidade civil extracontratual[24].

Deste modo, a concepção do direito a ser deixado só foi amplificada e consagrada[25] no artigo de Warren e Brandeis cuja relevância se deve à criação de um direito à privacidade, que não possuía previsão expressa na Constituição norte-americana e sequer era tratado enquanto

---

[22] WARREN, Samuel D.; BRANDEIS, Louis D. Op. cit., p. 193.

[23] COOLEY, Thomas M. **A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract**. Chicago: Callaghan, 1879.

[24] O trecho a que a doutrina em geral faz referência para demonstrar ser um precedente à obra de Warren e Brandeis trata do direito à imunidade pessoal: *"Personal Immunity. The right to one's person may be said to be a right of complete immunity: to be let alone. The corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury. In this particular the duty goes beyond what is required in most cases; for usually an unexecuted purpose or an unsuccessful attempt is not noticed."* COOLEY, Thomas M. Op. cit., p. 29.

[25] Observe-se que, para Danilo Doneda, a menção a um *'direito a ser deixado só'*, como sendo a definição de privacidade Warren e Brandeis, não seria de todo exata. Isto porque no célebre artigo os autores em nenhum momento definem o *right to privacy*. A associação que recorrentemente é feita pela doutrina entre os autores e o *right to be let alone* seria em virtude de uma citação da obra do magistrado Thomas Cooley. Todavia, os autores não chegariam a afirmar que isto traduziria o conteúdo do direito à privacidade, ou seja, os autores trabalhariam a partir de uma perspectiva mais aberta de *privacy* (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 105-106). De fato, assiste parcial razão ao civilista, pois em nenhum momento os autores afirmam adotar para si o conceito de privacidade enquanto direito a ser deixado só. Ocorre que, pelo tom inflamado do artigo, diante da atitude que entendiam ofensiva da imprensa de então, ousa-se discordar parcialmente para afirmar que, se não está de todo correta a atribuição da definição aos autores, estes são responsáveis por popularizá-la e defini-la como ponto de partida para estabelecer suas conclusões ao final. Isto porque, nas passagens que faz referência ao *"rigth to be let alone",* embora tenham a honestidade de afirmar que não se trata de um conceito de sua autoria, os autores adotam o direito a ser deixado só como uma evolução decorrente de proteção à propriedade intangível do indivíduo. No primeiro parágrafo da obra afirma-se que aos poucos "o âmbito destes direitos foram se ampliando; e agora o direito à vida passou a significar o direito de aproveitar a vida, o direito de ser deixado em paz; o direito à liberdade assegura o exercício de extensas liberdades civis; e o termo "propriedade" foi ampliado para incluir todas as formas de domínio - intangível, assim como tangível". Logo, a nosso ver, em que pesem as verdadeiras afirmações do mestre civilista, a melhor conclusão é que, embora não tenham sido os autores da concepção do direito a ser deixado só, é certo que a publicação do artigo a popularizou e a disseminou nos tribunais e os autores, ao longo da obra não parecem discordar da definição, ao contrário, a utilizam como base a afirmar a existência de um direito autônomo à privacidade.

direito autônomo na jurisprudência[26]. Tanto é assim que, a partir do artigo, pouco a pouco, o direito à privacidade, ainda que para deixar de ser reconhecido, passa a ser tratado na jurisprudência daquele país, citando-se como exemplos inaugurais os casos *Schuyler v. Curtis* (1891) e *Marks v. Jaffa* (1893)[27].

Pontue-se que para muitos autores, à época da publicação do divisivo artigo, a ideia de um interesse a ser deixado só já fazia parte do pensamento jurídico norte-americano, tendo sido citado no caso *Wheaton v. Peters*, julgado pela Suprema Corte em 1834[28].

De acordo com o estudo em questão, os avanços tecnológicos intensos do fim do século XIX, principalmente os equipamentos de gravação de voz e de fotografia instantânea, tornaram o homem mais sensível à publicidade. Desta forma, solidão e privacidade passaram a ser essenciais ao indivíduo, vez que as invenções modernas tornaram mais fáceis o registro e a publicação não consentida de fatos privados, o que poderia lhe provocar dor e angústia.

O ponto de partida do texto é a proteção jurídica decorrente do direito de propriedade, incialmente restrita aos bens de natureza material, como os bens de direito real, e, posteriormente, aos de natureza imaterial, como a criação artística e literária. Neste sentido, a partir da análise da jurisprudência norte-americana, utiliza-se como argumento tanto a proteção dos direitos autorais para obras intelectuais que possuam valor econômico, quanto a legislação que impõe responsabilidades por calúnia e difamação.

Todavia, para os autores, estas legislações não seriam suficientes à proteção da privacidade, vez que a legislação de direitos autorais não protegeria obras que não possuem valor econômico, como uma carta a um amigo ou a mera divulgação de qualquer outra

---

[26] A doutrina faz referências ao caso *Wheaton v. Peters*, decidido pela Suprema Corte em 1834 que reconheceu o interesse individual de ser deixado só, mas não tratou da privacidade enquanto um direito, com reconhecimento da comunidade jurídica.

[27]No primeiro caso, julgado pela Corte de Nova Iorque tratava-se do direito de imagem de Mary Hamilton Shuyler, falecida, cujo sobrinho queria impedir a construção e exposição de sua estátua em um evento em Chicago que a relacionava com fato público com a qual a falecida não teria consentindo em vida. Invocando fundamento no artigo de Warren e Bradeis, a Corte de Nova Iorque acolheu o pedido, afirmando que a falecida tinha tido uma vida discreta e que sua exposição pública não era compatível com sua conduta em vida. Todavia, a decisão foi modificada pelo Tribunal de Apelação que entendeu irrelevante o desejo da falecida, vez que o direito à privacidade não teria sobrevivido à sua morte. Vide ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos. **Revista Brasileira de Direito Civil**, v. 3, p. 13, jan./mar 2015. No caso Marks v. Jaffa, também em Nova Iorque, um ator descobriu que um jornal local realizava concurso de popularidade com a sua fotografia, sem sua autorização. O Tribunal concedeu ao ator a ordem para que não utilizassem sua imagem. Entre os fundamentos da decisão, a Corte invocou o direito a ser deixado só ("The courts will in such cases secure to the individual what has been aptly termed the right "to be let alone").

[28]*Wheaton v. Peters*, 33 U.S. 591 (1834). O caso tratava de direitos autorais de um advogado que publicava obras a respeito dos julgados da Suprema Corte em face de outro autor que compilou e resumiu estas publicações, tornando-as acessíveis por um preço menor.

manifestação do pensamento. Da mesma forma, a proteção contra a calúnia e a difamação não seriam suficientes a inibir a indevida divulgação de fatos que, embora privados, sejam verdadeiros, vez que não seriam caluniosos ou difamadores. Ademais, somente pode ser tido como calúnia ou difamação manifestações que ofendam a reputação, ou seja, a imagem pública da qual goza o ofendido. Portanto, não contaria com proteção jurídica a mera violação de fatos inerentes à privacidade que não sejam tornados públicos, ou seja, não lhe afete a imagem pública. Desta forma, embora como valioso ponto de partida, o ordenamento jurídico de então não seria suficiente a proteger o indivíduo em relação à sua vida privada, sendo necessário admitir a existência de um direito à privacidade.

Na concepção dos autores, o direito à privacidade resguarda o direito do indivíduo não somente de estar sozinho, mas a ser deixado só, ou seja, é da necessidade humana que seus pensamentos, sentimentos e manifestações sejam preservadas do público em geral. Deste modo, caberia ao indivíduo definir a medida da publicidade de sua vida privada e familiar, de sua imagem, de seus registros de voz, de suas comunicações, de seu nome e de sua relação de bens.

A privacidade é resguardada inclusive em face de informações verdadeiras sobre o indivíduo, vez que sua violação se dá mesmo quando a invasão não é maliciosa e noticia a realidade dos fatos. O grande ponto de inflexão para caracterizar a violação à privacidade é o consentimento do indivíduo. Uma vez publicado o fato pelo próprio indivíduo ou consentido que o faça, deixa de haver a possibilidade da violação à privacidade[29].

O artigo datado de 1890 entende que a privacidade protege a divulgação de dados do indivíduo como fotografia ou imagem, além da fala, de escritos, da descrição de alguém, da sua relação de obras de arte ou da sua relação de bens ou patrimônio.

Assim, tendo como ponto de partida as legislações sobre propriedade artística e literária, bem como sobre calúnia e difamação, os autores propõem duas medidas possíveis à proteção da privacidade. Uma delas é a ação de responsabilidade civil por danos causados, que poderiam ser utilizadas para todos os casos de violação à privacidade, mesmo na ausência de danos especiais, para compensar a lesão a sentimentos, assim como nas ações de injúria e difamação. Outra solução proposta foi a obtenção de uma ordem judicial (*injunction*) para evitar que se viole a privacidade alheia.

O artigo foi escrito no início da estruturação da imprensa e dos equipamentos fotográficos e fonográficos. Hoje seria impossível imaginar qualquer alegação de violação à

[29] WARREN, Samuel D.; BRANDEIS, Louis D. Op. cit., p. 201.

privacidade em virtude da divulgação de fotografia ou gravação sonora em uma sociedade monitorada por câmeras, onde há equipamentos eletrônicos portáteis e imperceptíveis por todos os lados.

Ainda segundo o seminal trabalho, a proteção à privacidade não impede a publicação de matérias de interesse público ou geral[30], referentes a atos de pessoas notórias. Todavia, não é bastante para avaliar a licitude da publicação a classificação das pessoas, segundo suas atividades e notoriedade, como públicas ou privadas. Importa a classificação do ato ou fato em si, se de interesse público e geral ou não.

O artigo aponta também importante distinção em relação à privacidade de pessoas públicas que, em algum grau, renunciaram o direito de não sofrer nenhum escrutínio público. Não se trata de verificar, tão somente, a natureza da atividade do indivíduo - se pública ou privada. Características de natureza aparentemente privada, como é o caso de um defeito na fala, mostra-se indevido. Todavia, a informação sobre esta restrição pode ser relevante para um candidato a congressista. Com estes exemplos, se demonstra que a definição de fatos de interesse geral ou não se restringe tão somente à natureza do ato, se público ou privado. Não se trata apenas de verificar se se trata de pessoa pública ou privada, mas de observar as circunstâncias de cada caso a fim de determinar se aquela atividade a ser reportada, seja de pessoa pública ou privada, possui interesse geral[31]. Portanto, trata-se de parâmetro que até os dias atuais é utilizado, tamanha a importância do artigo[32].

Em síntese, o histórico artigo defende a privacidade como direito a ser deixado só, a não ter sua vida privada revirada e divulgada publicamente, não sendo a privacidade um mero interesse, mas um direito com conteúdo jurídico próprio. No entanto, embora o artigo afirme se distanciar do direito de propriedade quanto aos bens corpóreos, expressa uma lógica excessivamente individualista, de cunho patrimonial, e se restringe aos institutos típicos dos direitos intelectuais e artísticos, ou seja, ainda muito ligado aos aspectos patrimoniais decorrentes das manifestações culturais e artísticas do indivíduo.

Com alguma controvérsia, se reconhece que o artigo tenha inaugurado a concepção unitária e autônoma do direito à privacidade. Entretanto, não sem alguma razão, apontam os

---

[30] Ibidem, p. 214.

[31] Ibidem, p. 215.

[32] Embora seja de fácil compreensão o exemplo dado, não me parece que seja adequado aos dias atuais. Um defeito na fala não parece um claro impeditivo para acesso a cargos públicos eletivos, em uma sociedade cujo objetivo seja combater a discriminação. Contudo se concorda que há fatos de interesse público referente a postulantes de cargos públicos que não se exigiriam de pessoas comuns, tais como informações de patrimônio e renda, relações negociais, relações de amizade e até mesmo afetiva caso isto influencie a função pública.

críticos que a privacidade apresentada pelos autores seria de reconhecimento apenas incidental da privacidade decorrente de outros institutos, tais como o direito de propriedade, a proteção à propriedade intelectual, a quebra de contrato, a violação de confiança, entre outros. Ademais, afirma-se que o artigo parte de uma compreensão equivocada dos precedentes oriundos da jurisprudência norte-americana e inglesa para fundamentar a existência de um direito à privacidade[33].

Uma outra crítica à obra de Warren e Brandeis é que, a despeito de seu caráter inegavelmente inaugural no direito norte-americano, o texto está muito mais embebido na cultura europeia-continental de privacidade do que na estadunidense. Isto porque trabalha com valores estranhos à cultura de privacidade da sociedade americana, tais como os decorrentes de honra pessoal, dignidade e personalidade, valores estes cultuados, a título de exemplo, na tradição jurídica francesa e alemã.

Logo, em que pese reconheçam os autores as limitações do direito americano para proteger o indivíduo do mero insulto, o texto parte da cultura europeia de privacidade para construir sua concepção. Embora seja uma peça confeccionada para defender o direito à privacidade na ordem jurídica norte-americana, os autores flertam com a disposição de valores caros à cultura jurídica norte-americana como é o caso da liberdade de expressão. Com base na primeira emenda, a liberdade de imprensa é um dos valores mais cultuados na jurisprudência norte-americana, se sobrepondo, muitas vezes, à privacidade do indivíduo[34]. Portanto, em que pesem todas as ressalvas feitas pelo próprio artigo, a jurisprudência utilizada e o tom incisivo contra a liberdade de imprensa teriam sido, para alguns, o motivo da demora para sua completa aceitação nos tribunais estadunidenses[35].

A despeito das críticas apontadas, a obra possui caráter inegavelmente inaugural, sendo tamanha sua importância que seguiu influenciando a jurisprudência dos Estados Unidos até pelo menos a década de 1950 e é apontada doutrinariamente como obra fundante até os dias atuais.

---

[33] FESTAS, David de Oliveira. **Do conteúdo patrimonial do direito à imagem**. Coimbra: Coimbra, 2009, p. 156-157 *apud* ZANINI, Leonardo Estevam de Assis. Op. cit., p. 10.

[34] Um dos casos que demonstra isso e que no sistema jurídico europeu certamente teria outra solução foi a decisão da Suprema Corte dos Estados Unidos em *Cox Broadcasting Corp.* v. *Chon e em Florida Star v. B.J.F.*, nos quais se entendeu legal que a mídia publicasse o nome de vítimas de estupro, mesmo que no segundo caso a divulgação configurasse crime nos termos da respectiva lei estadual. Decerto que no direito europeu, a solução do caso seria contrária, haja vista a arraigada cultura de proteção à dignidade pessoal e à honra dos indivíduos.

[35] A crítica pode ser encontrada em WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, v. 113, p. 1202-1211, 2004.

A influência sobre a jurisprudência não foi imediata, mas paulatina. Iniciou-se a partir da publicação do artigo uma disputa entre as cortes, a fim de verificar se prevalecia o precedente estabelecido em *Roberson v. Rochester Folding box Co.*, julgado em 1902 pela Corte de Nova Iorque , que afirmou a inexistência de direito à privacidade no uso não autorizado de fotografia em propaganda[36], e o caso *Pavesich v. New England Life Insurance Co.*, que, como se verá a seguir, reconheceu o direito à privacidade do indivíduo retratado sem autorização em propaganda de seguro de vida, adotando as diretrizes do direito à privacidade estabelecidos por Warren e Brandeis. Ao longo desse período de consolidação jurisprudencial, o direito à privacidade teve sua afirmação favorecida pelo *Restatements Of Torts*[37] que previu expressamente o direito à privacidade em 1939.

Com alguma resistência inicial, as cortes passaram a reconhecer o direito à privacidade e repetir os fundamentos estabelecidos por Warren e Brandeis, em geral sob o pálio de institutos tradicionais, como o direito de propriedade. Fato é que o artigo é citado até os dias atuais como obra essencial sobre privacidade, em um tema sob atualização constante. É seu mérito, ainda, a criação de um direito autônomo de privacidade, ainda que inspirado no direito de propriedade que dele se difere. A publicação da obra inaugural, mesmo que sem a sistematicidade necessária e tendo por enfoque quase que absoluto o trabalho da imprensa, permitiu o lançamento das bases para se falar em privacidade no direito norte-americano.

Por fim, a obra foi de tamanha importância que seguiu influenciando quase que solitariamente a concepção norte-americana de privacidade até a sua revisão na década de 1960 por William Prosser.

1.1.1 A construção doutrinária de William Prosser

Na década de 1960, após ter sido alvo de muita controvérsia, a obra clássica sobre privacidade de Warren e Brandeis foi revisitada por William Prosser, professor da *California*

[36] *Roberson v. Rochester Folding box Co* (the flower of the Family) 1902171 N.Y. 538, 64 N.E. 442 (1902).Mais adiante, o caso será tratado com mais detalhes.

[37] *Restatements* são compilações de enunciados editados com base na jurisprudência norte-americana das mais variadas áreas do direito, realizadas desde 1923 pelo *American Law Institute*. Por se tratar de sistema da *commom law* a construção do direito norte-americano é essencialmente jurisprudencial e os juízes estão vinculados ao dever de observar os precedentes, em virtude do princípio do *stare decisis*. Por certo, que tais enunciados não constituem leis, nem possuem caráter vinculativos, mas por serem baseadas na jurisprudência possuem relevante valor doutrinário. Neste sentido foi editado o Restatement (First) of Torts, de 1939, seção 867 que reconhecia o direito subjetivo a quem sofresse irrazoável e séria invasão de privacidade. Vide, ainda, RICHARDS, Neil M.; SOLOVE, Daniel J. Prosser's Privacy Law: A Mixed Legacy. **California Law Review**, v. 98, n. 6, p. 1895, 2010.

School of Law (*Berkeley*) e, à época, uma das maiores autoridades em responsabilidade civil (*tort law*). A esta altura, existem pontos de vista favoráveis e contrários à concepção de privacidade formulada no clássico artigo de 1890. As críticas giram em torno do uso de um conceito único, o *right to privacy*, para abrigar variados atos ilícitos; contestam a definição da privacidade como direito a ser deixado só (*right to be let alone*), bem como afirmam a necessidade de substituição do conceito de *privacy* por outro mais adequado[38].

Prosser tem a obra de Warren e Brandeis como ponto de partida, mas admite que há inconsistências em alguns pontos, além de ausência de clareza e sistematização, vez que, embora haja o elemento comum de violação ao *right to be let alone*, há vários interesses tutelados de características distintas nas situações ali apresentadas, fazendo-se necessária a sistematização da matéria. A partir da análise da jurisprudência, a obra defende que os interesses protegidos pela privacidade não são unitários, apresentando variadas formas de violação. Portanto, a importância do autor, para além de apresentar uma nova concepção de privacidade, desde a obra de Warren e Brandeis, deve-se também à sistematização do conteúdo anteriormente produzido, bem como pela identificação do interesse jurídico tutelado em cada situação de violação à privacidade[39]. Longe de se tratar de uma obra revolucionária em relação à concepção anterior, a contribuição de Prosser vai no sentido de aperfeiçoar a concepção de privacidade de Warren e Brandeis, sistematizando suas diferentes manifestações, identificadas de acordo com o interesse jurídico tutelado.

A partir de seus conhecimentos sobre reponsabilidade civil, o autor estabelece quatro *torts* (atos ilícitos) através dos quais pode-se lesionar o direito à privacidade. Deste modo, consagrou-se no direito norte-americano os quatro testes que possibilitariam verificar se a conduta sob análise teria causado dano à privacidade passível de reparação, a saber: (i) invasão na esfera de privada da pessoa *(intrusion)*; (ii) divulgação pública de fatos privados embaraçosos acerca do indivíduo *(public disclousure of privact facts)*; (iii) exposição pública do indivíduo de forma desonrosa ou distorcida (*false light in the public eye*), o que se assemelha à difamação (*defamation*), mas para esta exige-se que a informação seja inverídica; e (iv) apropriação do nome ou de dados do indivíduo para proveito próprio (*appropriation*).

Quanto ao primeiro ilícito - da intrusão (*intrusion)* -, pode-se dizer que a invasão na esfera privada do indivíduo não ocorre apenas fisicamente, com o ingresso não autorizado no domicílio, local de trabalho ou quarto de hotel. Na concepção do autor norte-americano, a

[38] RIGAUX, François. **La protection de la vie privée et des autres biens de la personnalité**. Bruxelas: Bruylant, 1990, p. 272.

[39] ZANINI, Leonardo Estevam de Assis. Op. cit.,p. 20.

intrusão se caracteriza também pela interceptação ou gravação de conversas privadas ou mesmo por insistentes ligações telefônicas de agentes de cobrança para a residência ou local de trabalho[40], conduta capaz de causar intencional sofrimento mental. A invasão deve ser ofensiva ou deve ofender o chamado homem médio. Portanto, não configura invasão indevida, a retratação do indivíduo em locais de natureza pública, realizando atividades corriqueiras, mesmo que não autorizada a sua publicação.

O *tort* da intrusão visa resguardar o indivíduo do sofrimento psicológico decorrente do transtorno ou sofrimento causado pela indevida intromissão em sua esfera privada. Todavia, sequer é necessário que haja intenção de causar sofrimento psíquico ou estresse ao indivíduo[41].

Particularmente, neste trabalho, não se entende como violação à privacidade a mera intrusão sem que tenha acesso a informações de caráter privado, nos termos em que foi concebido. O que se quer dizer com isso é que a invasão de um local privado como o domicílio é, sim, uma violação à privacidade, bem como o é o acesso não autorizado ao conteúdo de comunicações da pessoa, sejam elas físicas ou eletrônicas. Todavia, por mais insistentes que possam parecer as ligações telefônicas ou mensagens eletrônicas para a realização de cobranças ou para a venda de produtos, não parece tratar-se de violação à privacidade, pelo fato de o agente no momento da ligação estar em seu repouso noturno ou nos limites do lar, vez que o agente de cobrança não capta qualquer informação pessoal sensível com uma mera ligação. Assim, embora haja conduta passível de responsabilidade civil, não é o caso de fundamentar essa violação com base na privacidade, já que o direito a ser deixado só é insuficiente a definir seu conteúdo.

O segundo teste, o *tort* da divulgação pública de fatos privados *(public disclousure of privact facts)* foi o principal motivo que levou Warren e Brandeis à publicação do artigo. Isso

---

[40] Cf. Duty v. General Finance Co., 154 Tex. 16, 273 S.W. 2d 64 (1954) *apud* PROSSER, William. Op. cit., p. 390. O caso foi julgado pela Suprema Corte de Ohio nos anos 1950. Guardando-se a diferença entre a amplitude do conceito de *right to privacy* norte-americano e a privacidade no Brasil, dificilmente seria reconhecida em nossa jurisprudência pátria a lesividade de conduta de cobrança de um débito, talvez nem nos Estados Unidos dos dias de hoje. A conduta fica entre o exercício legal do direito e a cobrança vexatória, cujo fundamento é muito mais a dignidade do consumidor que a sua privacidade, cuja previsão é expressa no art. 71 do Código de Defesa do Consumidor. Veja-se curioso caso de 2011 no qual empresa responsável pela recuperação de crédito foi proibida de cobrar créditos legítimos através da rede social Facebook, inclusive através de contatos do devedor, embora o financiamento tivesse sido contratado pela mesma rede social. Cf. VELOSO, Thássius. Justiça americana proíbe financeira de cobrar dívida pelo Facebook. **Tecno Blog**, 2011.Disponível em: <https://tecnoblog.net/59137/justica-americana-proibe-empresa-de-cobrar-conta-via-facebook/>. Acesso em: 22 jul. 2017.

[41] Trata-se de tradução livre do termo *mental distress* utilizado no seguinte trecho: "It appears obvious that the intersting protected by this branch of tort is primarily a mental one. It has been useful chiefly to fill in the gaps left by (...) the intencional inflinction of mental distress". PROSSER, William. Op. cit., p. 392.

porque, conforme já dito, em virtude da notoriedade da família Warren em Boston, o colunismo social fazia questão de viver no encalço da família e de publicar os detalhes mais íntimos ocorridos na casa dos Warren, o que provocou a revolta de um dos autores.

Por óbvio que não está coberta pela privacidade a divulgação de um fato que já é público ou que tenha manifesto interesse público, como a gravação de um testemunho ou de um julgamento - exceto os que estejam sob segredo de justiça - ou mesmo a informação de uma condenação criminal, que são fatos por si só de interesse público. A jurisprudência norte-americana dá tamanho prestígio à liberdade de imprensa em detrimento da privacidade que admite não somente a publicação de informações sobre a vítima de um crime, bem como a respeito de fatos privados de seus familiares, ou mesmo detalhes da orientação sexual de um cidadão que se tornou conhecido por evitar um atentado contra o Presidente dos Estados Unidos[42].

Todavia, a situação foi muito além da mera informação de interesse público em um caso que também é utilizado para discussões sobre direito ao esquecimento, que ficou conhecido como *Melvin v. Reid*, julgado na Califórnia em 1930. No caso, entendeu-se que a divulgação de fatos privados, ainda que de certa repercussão pública, como a absolvição em uma acusação de homicídio e o exercício da prostituição, referentes à própria história do indivíduo, era uma indevida violação de sua privacidade[43]. No julgamento, a violação da

---

[42] Refere-se aqui ao caso *Sipple v. Chronicle Publishing Co.*(1984), julgado pelo Tribunal de Apelação da Califórnia, no qual Sipple requeria uma a responsabilização civil de um periódico que tornou pública em uma de suas matérias a sua orientação sexual. O autor notabilizou-se por evitar que uma mulher cometesse um atentado com arma de fogo em face do Presidente Gerald R. Ford, por ocasião de sua passagem em 1975 pela cidade de São Francisco. Dada a notoriedade que adquiriu, o jornal publicou sua orientação sexual e os vínculos ativos com a militância gay de sua cidade. O autor, sentindo-se violado em sua privacidade, alegou ter passado por sofrimento e abandono de familiares pois em virtude da divulgação da informação privada. O Tribunal entendeu que o jornal estava no regular exercício de atividade de imprensa ao noticiar os fatos e trazer ao público informações de legítimo interesse público sobre o herói instantâneo, não havendo violação à privacidade na divulgação de matérias de interesse público, vez que protegida pela Primeira Emenda. Ademais, com base nos testes estabelecidos por Prosser, o Tribunal de Apelação entendeu que a divulgação dos fatos privados deve ser uma divulgação pública. Em segundo lugar, os fatos divulgados devem ser fatos privados e não públicos. Em terceiro lugar, a questão tornada pública deve ser uma que seria ofensiva e censurável para uma pessoa razoável de sensibilidades comuns. O Tribunal reconheceu ainda que, devido ao mandato supremo da proteção constitucional da liberdade de imprensa, mesmo uma invasão tortuosa de sua privacidade está isenta de responsabilidade se a publicação de fatos particulares for verdadeira e notável. A última proposição encontra apoio principalmente na seção 652D de *Restatement Second of Torts*, que prevê que "A pessoa que dá publicidade a uma questão relativa à vida privada de outra pessoa está sujeita à responsabilidade para a outra por invasão de sua privacidade, se a questão divulgada for de uma Tipo que (a) seria altamente ofensivo para uma pessoa razoável. Logo, o Tribunal entendeu que a orientação sexual do autor não era um fato privado, pois este se envolvia com a militância gay em vários atos específicos e revistas especializadas já haviam publicado a informação e, além do mais, o autor não negava responder a quem perguntasse sobre sua orientação sexual. Um resumo do caso está disponível em: <http://law.justia.com/cases/california/court-of-appeal/3d/154/1040.html>. Acesso em: 22 jul. 2017.

[43] Melvin v. Reid. Gabrielle Darley havia sido prostituta e acusada em 1918 de haver cometido homicídio em um julgamento de grande repercussão. Absolvida da acusação, deixou a prostituição e casou-se com Bernard

privacidade não se deu por se produzir um filme baseado em fatos reais, mas, sim, pela desnecessária divulgação do nome de uma de suas protagonistas e do seu atual paradeiro tantos anos após o seu julgamento e absolvição.

Um exemplo da divulgação pública de fatos privados dado por Prosser é o caso *Brents v. Morgan* do cobrador de Kentuchy que resolveu divulgar na janela de sua garagem a dívida que Morgan, seu vizinho, possuía e que não havia pago até então[44].

A terceira forma de violação é a exposição pública de forma distorcida (*false light in the public eye*), que se configura pela atribuição falsa ou não consentida de opinião, obra ou declaração ao indivíduo, que pode se configurar pela falsa atribuição de uma obra literária ou musical a um famoso escritor ou a falsa atribuição de assinatura de uma petição pública a uma personalidade, como até mesmo a utilização da imagem de uma personalidade para ilustrar um livro ou artigo com o qual não possui nenhuma conexão semântica[45].

A exposição pública distorcida não necessariamente se refere a um fato difamatório, basta que seja algo que incomode uma pessoa de sensibilidade razoável, sendo necessário apenas que haja uma distorção da realidade. Claro que erros menores, tais como datas e locais, bem como fatos de menor relevância ou que apenas ofenderiam pessoa de sensibilidade extrema não são ilícitos que podem ser responsabilizados por violação à privacidade.

O interesse jurídico protegido tanto na exposição pública de fatos privados quanto na exposição pública distorcida é a reputação do indivíduo e o sofrimento psicológico causado pela reputação ofendida, da mesma forma como ocorre com a difamação, com a exceção de que nesta última o fato atribuído é necessariamente não verdadeiro.

O quarto ilícito, a apropriação indevida de nome ou de imagem para proveito próprio (*appropiation*), está muito mais ligado ao direito de imagem e à exploração econômica do

---

Melvin, adotando seu sobrenome e passou a ter uma vida pacata, relacionando-se com amigos que não conheciam seu passado. Passados oito anos do julgamento, os réus na ação gravaram o filme *The Red Kimono* que contava toda a trajetória de Gabrielle, revelando seu nome de solteira, possibilitando a seus novos amigos conhecer parte de sua história que para ela era desonrosa. O marido de Gabrielle ingressou com ação que pedia reparação, vez que a mulher havia adotado outra trajetória de vida, passando a cuidar da família e havia há anos abandonado a prostituição e a divulgação de sua história havia lhe causado danos A condenação pela corte da California baseou-se no direito à felicidade da retratada que no caso estaria vinculada à não divulgação de fatos pretéritos. Entendeu-se desnecessária a divulgação do nome de Gabrielle para a produção do filme.

[44] Brents. v. Morgan, 221 Ky. 765, 299 S.W. 967 (1927). O anúncio trazia o valor da dívida de $ 49.67 cujo vencimento já havia ocorrido há tempos atrás. Afirmava ainda que o anúncio permaneceria enquanto o débito não fosse pago. Cf.PROSSER, William. Op. cit., p. 392.

[45] PROSSER, William. Op. cit., p. 399. Outros exemplos mencionados no artigo tratam do uso distorcido da imagem para ilustrar um artigo que trate de deliquência juvenil, tráfico de narcóticos, promiscuidade ou outras pautas de visibilidade negativa com as quais o individuo não possua nenhuma identificação. Pode ocorrer ainda com o indivíduo.

nome ou da imagem do indivíduo, de modo que o assunto foi melhor desenvolvido na doutrina norte-americana apenas posteriormente, ao se tratar do *right of publicity*, conforme se explicitará em tópico seguinte.

Na concepção de Prosser, a apropriação do nome ou da imagem do indivíduo, ocorre por seu uso desautorizado, em geral com fins econômicos, por trazer prestígio ou mesmo para ilustrar anúncio publicitário. Nesta última hipótese, há um claro intuito de obter vantagem econômica advinda do uso não autorizado da imagem. Outra hipótese formulada acerca da *appropriation* é utilização do nome de terceiro, se passando por este, para obter crédito ou informação confidencial.

O caso mais ilustrativo do ilícito da apropriação da imagem ou nome é o *Roberson v. Rochester Folding box Co.*, também conhecido como *The flour of the Family*, julgado em 1902 pela Corte de Apelação de Nova Iorque. Tratava-se do uso da fotografia de uma jovem sem o seu consentimento em uma propaganda de farinha acompanhada da legenda *"The flour of the family"*. A corte de Nova Iorque, embora por maioria apertada de quatro votos a três, entendeu que não existia direito à privacidade a ser tutelado e que o autor não teria proteção contra esta conduta[46]. Os fundamentos da decisão foram a falta de precedente, o caráter puramente mental da lesão, a dificuldade de se estabelecer a distinção entre natureza pública e privada e a indevida restrição à liberdade de imprensa e liberdade de expressão, rejeitando-se as alegações baseadas na construção doutrinária de Warren e Brandeis.

Vale observar que tanto na invasão (*intrusion*) quando na exposição pública (*disclosure*) faz-se necessária para sua configuração a indevida violação de algo secreto, reservado ou privado pertencente ao indivíduo. Já a divulgação distorcida (*false light*) e a apropriação da imagem (*appropriation*) não exigem este requisito. A publicidade deixa de ser requisito obrigatório apenas na invasão, exigindo-se sua ocorrência para os outros casos. Não que a intromissão não possa ser tornada pública – e geralmente o é –, mas a mera violação do âmbito privado do individuo já permite a responsabilização. Da mesma forma, apenas a apropriação exige vantagem por parte do agente que se apropria, não sendo necessária nas outras três situações.

Prosser ressalta também que o direito à privacidade possui natureza pessoal, não podendo ser transmitida as pretensões dele decorrentes a terceiros, nem se estende aos

[46]*Roberson v. Rochester Folding box Co* (the flower of the Family) 1902171 N.Y. 538, 64 N.E. 442 (1902). Disponível em: <https://casetext.com/case/roberson-v-rochester-folding-box-co-1>. Acesso em: 22 jul. 2017. O julgado teve forte reação da opinião publica e da comunidade jurídica, o que impulsionou o Legislativo de Nova Iorque a criar um estatuto que proibia a utilização do nome, retrato, figura de qualquer pessoa com propósitos publicitários ou comerciais. Depois esta previsão passou a integrar a lei de direitos civis de novaiorquina 1921.

membros da família. Diferente dos direitos reais, a proteção da privacidade não pode ser pleiteada depois da morte, pois é direito exclusivo do indivíduo. Da mesma forma, pessoas jurídicas não podem invocar direito à privacidade para resguardar, por exemplo, o direito ao nome. Embora possuam direitos sobre nome e imagem, os fundamentos jurídicos podem ser apenas outros que não a privacidade, como, por exemplo, a vedação da concorrência desleal[47].

De tudo que se expressou até o presente momento, tanto na construção doutrinária de Warren e Brandeis como nos quatro ilícitos sistematizados por Prosser, pode-se perceber que sob a denominação de *"rigth to privacy"* ou do *"rigth to be let alone"* há muito mais variadas proteções que aquelas comumente admitida no âmbito de proteção do direito à privacidade no Brasil, embora se negue que a concepção de Warren e Brandeis reflita de fato a cultura norte-americana de privacidade.

Em geral, os *torts* estabelecidos por Prosser no direito pátrio estariam protegidos por fundamentos outros tais como o direito de imagem, os crimes de calúnia, injúria ou difamação ou até mesmo a genérica reparação do dano moral. Isto não significa que o direito norte-americano proteja mais ou menos a privacidade que o direito brasileiro, apenas que os fundamentos invocados são distintos, utilizando-se aqui uma aplicação muito mais restritiva. Por essa razão, alguns autores preferem, por precisão metodológica, utilizar o termo *privacy* ao se referir ao tratamento da questão no direito norte-americano, vez que esta concepção não corresponderia exatamente ao direito à privacidade no direito brasileiro.

De fato, verifica-se no *right to privacy* uma pretensão muito maior de proteger as manifestações do direito da personalidade, não encontrando uma tradução precisa no ordenamento jurídico brasileiro, especialmente de acordo com o contorno dado pela Constituição brasileira. Todavia, considerando que o objetivo neste trabalho é uma análise comparativa das diferentes formas de proteção a aspectos inerentes à privacidade, se optará pela utilização do mesmo termo, a despeito da advertência de possuírem conteúdos distintos[48].

Neste sentido, é mais que natural que o conteúdo jurídico da privacidade, cujo conceito é envolto em controvérsias, varie no espaço e no tempo no que tange ao seu objeto e

---

[47] PROSSER, William. Op. cit., p. 408-409.

[48] Em sentido diverso, observa Leonardo Zanini que "já de início, que o termo privacy não pode ser confundido com a privacidade da língua portuguesa. De fato, deflui tanto do artigo de Warren e Brandeis como das primeiras decisões sobre a matéria que o privacy assumiu, desde o início, vocação para ampla tutela dos valores da personalidade, não se limitando apenas à tutela da privacidade (FESTAS, David de Oliveira. **Do conteúdo patrimonial do direito à imagem**: Contributo para um Estudo do seu Aproveitamento Consentido e Inter Vivos. Coimbra: Coimbra Editora, 2009, p. 32). Desse modo, considerando a dificuldade na tradução do termo, que não se confunde com a privacidade e nem com os direitos da personalidade, preferimos utilizar nesse trabalho, para não incorrermos em nenhuma imprecisão, a expressão em inglês.

grau de proteção, até porque o conteúdo jurídico da privacidade é definido pela construção social no âmbito de determinada cultura. Não é por outra razão que a privacidade no direito norte-americano se preocupa com aspectos distintos e em intensidade diversa da concepção de privacidade continental europeia, muito influenciado pelos valores tidos como importantes em cada cultura[49].

Por certo que, assim como a obra de Warren e Brandeis sofre críticas, a sistematização do direito à privacidade de Prosser recebe algumas objeções. Uma delas é a própria proteção da privacidade por meio de *torts*, ou seja, por meio do estabelecimento de hipóteses de atos ilícitos passíveis de responsabilização civil. Para Harry Kalven[50] só faz sentido proteger a privacidade por meio da responsabilidade civil no caso da apropriação indevida de imagem por meio de vantagem (*appropriation*), não sendo adequada esta proteção nas outras três hipóteses.

Outra crítica contundente, formulada por Edward Bloustein, é que a classificação de Prosser, ao dividir a privacidade em grupos, contraria a proposta de Warren e Brandeis de que o desenvolvimento do *right to privacy* fosse autônomo sem que se valesse de figuras jurídicas tradicionais como a honra e a propriedade[51].

A crítica afirma ainda que, ao definir o bem jurídico protegido em cada um dos *torts*, Prosser recorre a categorias que remetem às antigas instituições jurídicas, contrariando a natureza original e unitária do direito à privacidade, propostas por Warren e Brandeis. Para Bloustein, a privacidade protege um bem jurídico único, a dignidade humana, que perpassaria o direito público e o direito privado, abrangendo o direito como um todo, inclusive as normas de direito processual penal. O bem jurídico a ser resguardado pela privacidade é único e decorre da necessidade de preservar a dignidade e individualidade do ser humano, de modo que a privacidade abrangeria não apenas o sistema da *commom law*, mas ambos os sistemas jurídicos. Argumenta ainda que legislações mais recentes que regulamentam o sistema eletrônico de vigilância proíbem a realização de interceptações telefônicas, o que demonstra que há uma tutela da privacidade distinta da responsabilização civil proposta por Prosser[52].

---

[49] A respeito desta discussão, vide WHITMAN, James Q. Op. cit., p. 1151.

[50] KALVEN JR., Harry. Privacy in Tort Law - Were Warren and Brandeis Wrong? **Law and Contemporary Problems**, v. 31, p. 326-341, 1966.

[51] BLOUSTEIN, Edward J. Privacy as an aspect of human dignity: an answer to dean Prosser. **New York University Law Review**, v. 39, p. 962, 1964 *apud* ZANINI *op cit*, p. 22.

[52] ZANINI, Leonardo Estevam de Assis. Op. cit.,p. 22.

Em que pesem a contundência das críticas da concepção de Bloustein, mais vinculada à dignidade humana, essa vertente acabou não prevalecendo no direito norte-americano. Os quatro testes da privacidade se incorporaram à jurisprudência norte-americana, tendo sido adotada inclusive pelo *Second Restatement of Law* de 1977[53] em uma seção própria do documento.

Outrossim, a concepção de Bloustein, ao recorrer à dignidade humana, mostra uma aproximação muito maior com a cultura jurídica de privacidade europeia, para a qual os conceitos de honra pessoal, dignidade e personalidade são mais cultuados que os valores da liberdade norte-americana, especialmente a liberdade de expressão.

1.1.2 *Right of publicity* e *right to privacy*

Ao longo da aplicação do direito à privacidade, nas bases em que foi construído no artigo de Warren e Brandeis, verificou-se a dificuldade em adaptar o instituto aos interesses patrimoniais dos indivíduos cuja imagem fosse utilizada com fins econômicos. Isto porque a privacidade, consoante concebida, era pessoal e intransmissível, pleiteável apenas pelo titular do direito. Esta situação restou evidente no caso *Haelan Laboratories Inc v. Topps Chewing Gum Inc*.[54], julgado pelo 2º Circuito de Nova Iorque, em 1953. O laboratório *Haelen* havia celebrado vários contratos com jogadores profissionais de baseball, obtendo direito de explorar com exclusividade a imagem dos atletas, além de nome e elementos biográficos para a venda de seus produtos. Da mesma forma, o concorrente *Topps Chewing Gum*, sabendo do contrato, procurou os atletas e obteve a mesma autorização, da qual fez uso, motivo pelo qual foi demandada pela primeira contratante. Em sua defesa, a demandada alegou que o contrato com a demandante não tinha o condão de transferi-la o direito à privacidade, já que este é de

---

[53] *Restatement of the Law, Second, Torts, 652. The American Law Institute*. Trata-se da Seção 652, cujos itens são os seguintes:

652B Intrusion Upon Seclusion: One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

652C Appropriation of Name or Likeness: One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.

652D Publicity Given to Private Life: One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

[54] *Haelan Laboratories, Inc. v. Topps Chewing Gum*, Inc, 202 F.2d 866 (2d Cir. 1953). Disponível em: <http://law.justia.com/cases/federal/appellate-courts/F2/202/866/216744/>. Acesso em: 22 jul. 2017.

natureza pessoal e intransferível. Alegou, ainda, que o contrato não tinha nenhuma cláusula que transferisse algum direito de propriedade.

De fato, a Corte reconheceu que, pela sua intransmissibilidade e caráter não patrimonial, não faria parte do conteúdo do direito à privacidade a divulgação pública da própria imagem, vez que a privacidade iria no sentido contrário. Portanto, o efeito do primeiro contrato era tão somente isentar a empresa contratante de responsabilidade, e não alienar a ela a própria privacidade dos atletas. Todavia, havendo naquele contrato cláusula de exclusividade e, sabendo a segunda contratante desta cláusula, induziu o atleta a contratar também consigo, o que causou a violação o primeiro contrato.

Desta forma, a corte entendeu que, independentemente do direito pessoal à privacidade, há um direito autônomo, de caráter patrimonial, que permite ao titular da imagem o aproveitamento econômico exclusivo de sua notoriedade, que poderia ser chamado de *right of publicity*. Este direito não colidiria com o direito à privacidade, pois não feriria a honra e os sentimentos do titular, especialmente se tratando de uma personalidade pública, a qual pode dispor livremente sobre o aproveitamento de sua imagem, mediante retribuição pecuniária.

Pode-se perceber, portanto, que, em oposição ao direito pessoal e intransferível da privacidade (*privacy*), a Corte entendeu existente um direito autônomo, de caráter patrimonial e transferível, chamado de *right of publicity*[55]. Logo, a criação do direito à publicidade, embora tenha se originado de uma discussão acerca da privacidade, representa o total rompimento com a noção de um direito intransferível, de caráter não patrimonial, que apenas era reparado por meio de ação de responsabilidade civil.

Em linhas gerais, o direito à publicidade, consagrado no julgado citado, pode ser definido como o direito exclusivo do indivíduo à exploração comercial da própria identidade, possuindo caráter patrimonial, sendo inclusive transmissível após a morte, conforme prevaleceu na maioria da doutrina. O instituto é visto como uma espécie do gênero

---

[55] Destaca-se do julgado o seguinte trecho: “With regard to such situations, we must consider defendant's contention that none of plaintiff's contracts created more than a release of liability, because a man has no legal interest in the publication of his picture other than his right of privacy, i. e., a personal and non-assignable right not to have his feelings hurt by such a publication.

A majority of this court rejects this contention. We think that, in addition to and independent of that right of privacy (which in New York derives from statute), a man has a right in the publicity value of his photograph, i. e., the right to grant the exclusive privilege of publishing his picture, and that such a grant may validly be made "in gross," i. e., without an accompanying transfer of a business or of anything else. Whether it be labelled a "property" right is immaterial; for here, as often elsewhere, the tag "property" simply symbolizes the fact that courts enforce a claim which has pecuniary worth”.

concorrência desleal, vez que garante ao titular o direito exclusivo à exploração da identidade[56].

De maneira geral, as normas dos estados norte-americanos elencam entre os elementos do direito de publicidade o nome, a imagem e a semelhança, ou seja, elementos que constituam a própria identidade do indivíduo, os quais possam ser explorados comercialmente. Todavia, tais elementos podem variar de estado para estado. De acordo com o estatuto de Indiana, o *right of publicity* refere-se aos interesses patrimoniais inerentes ao nome, voz, assinatura, fotografia, imagem, semelhança, aparência distintiva, gestos ou maneirismos de um indivíduo[57].

Após o precedente de Nova Iorque, o direito de publicidade contou com a adesão e com a rejeição dos tribunais. Mostram-se especialmente interessantes os casos nos quais se utilizou elementos da identidade do indivíduo que não necessariamente o seu nome ou imagem, mas alguma outra semelhança que permitia identificá-lo ou até mesmo o ponto característico de sua notoriedade. Assim foi com *Midler v. Ford Motor Co.*849 F.2d 460 (9º Cir. 1989) e *Waits v. Frito-Lay, Inc.* 978 F.2d 1093 (9º Cir. 1992). Em ambos os casos, as celebridades envolvidas (Bette Midler e Tom Waits) recusaram-se a conferir suas próprias vozes aos jingles publicitários para os fabricantes em questão. A solução encontrada pelos anunciantes foi contratar artistas capazes de imitar a voz e o estilo das personalidades. Por haver a clara apropriação de uma semelhança de personalidade pública, constituinte de sua identidade, ou seja, a voz e o estilo comunicativo, ainda que por imitação, houve a condenação dos anunciantes com base no direito de publicidade. Isto porque a utilização de imitação da voz de personalidade pública é hábil a induzir os consumidores a erro, fazendo-os acreditar que a pessoa notória utiliza ou chancela o produto ou serviço propagandeado.

Situação semelhante ocorreu em um anúncio futurista no qual a Samsung utilizou um robô com toda caracterização da apresentadora Vanna White no cenário do programa "Roda da Fortuna", para demonstrar que, no futuro, os aparelhos de gravação de vídeo seriam fundamentais. Na propaganda, pela caracterização do robô e do cenário, era possível identificá-lo com a famosa apresentadora, de modo que se entendeu que houve apropriação de sua imagem sem lhe ter sido franqueado o respectivo aproveitamento econômico (*White v. Samsung Electronics America, Inc.*)[58]. Da mesma forma, foi reconhecido o direito à

[56] FESTAS, David de Oliveira. Op. cit.,p. 10.

[57] A BRIEF HISTORY of the Right of Publicity. **Right of Publicity**, [s.d.]. Disponível em: <http://rightofpublicity.com/brief-history-of-rop>. Acesso em: 22 jul. 2017.

[58] 971 F.2d 1395 (9º Cir. 1992).

reparação, sob a ótica do direito de publicidade, na utilização de imagem de veículo personalizado de conhecido atleta de automobilismo, sem, contudo, se mostrar o seu rosto, dando a entender que estaria de acordo com a qualidade do produto anunciado[59] ou mesmo no caso em que o bordão de abertura dito por apresentador de conhecido programa televisivo (*Here's Jhonny!*) foi utilizado como nome de banheiros sanitários portáteis[60]. Em ambas as situações, embora não se tenha colocado a voz ou imagem das celebridades envolvidas, a sua identificação e associação direta foram claramente possíveis. Tanto o foi que permitiu o aproveitamento de elementos característicos da personalidade pública para promover o produto anunciado[61].

Apenas em 1977, o *right of publicity* contou com o reconhecimento perante a Suprema Corte dos Estados Unidos, no caso *Zacchini v. Scripps - Howard Broadcasting Company*, quando se admitiu a existência de interesse econômico na transmissão pela televisão da apresentação de "homem-bala", a qual ocorreu sem a autorização do artista[62]. Portanto, dado o direito de publicidade do artista, a Suprema Corte reconheceu ao autor direitos patrimoniais sobre a transmissão integral de sua apresentação, não sendo oponível, no caso, o privilégio da imprensa em noticiar os fatos. Isto porque o julgado reconheceu que a transmissão televisiva da íntegra de seu espetáculo desestimularia os espectadores a pagarem pela performance ao vivo. Ademais, se afirmou que a finalidade do direito de publicidade se aproxima ao de uma patente ou de um *copyright*, na medida em que se protegem os frutos de uma atividade individual que não se relaciona com a ofensa a sentimentos ou à reputação do indivíduo.

A partir do reconhecimento pela Suprema Corte, o *right of publicity* passou a ser reconhecido pela jurisprudência dos tribunais do país[63]. Da mesma forma, os estados americanos passaram a reconhecê-lo em suas legislações, com algumas variações quanto aos

---

[59]*Motschenbacher v. RJ Reynolds Tobacco Co.* (498 F.2d 921, 9th Cir. 1974).

[60]*Carson v. Here's Johnny Portable Toilets* (698 F.2d 831, 6th Cir. 1983).

[61] Uma série de outros casos notáveis de direito de publicidade, desde 1905 aos dias atuais na jurisprudência norte-americana pode ser encontrado em A BRIEF HISTORY... Op. cit.

[62]*Zacchini v. Scripps-Howard Broadcasting* Co. 433 U.S. 562 (1977).

[63] Pode-se afirmar que tão abrangente foi a adoção do *rigth of publicity* que passou a integrar um tópico específico do *Restatement (Third) Of Unfair Competition*, editado pelo *American Law Institute*, contando com três parágrafos que tratam respectivamente da apropriação, do aproveitamento comercial de elementos da identidade do indivíduo, do seu uso para fins comerciais e as medidas que podem ser tomadas. Perceba-se que o compilado de enunciados que trata do direito de publicidade não integra os capítulos referentes ao direito de privacidade ou da responsabilidade civil em razão da violação dos direitos pessoais, mas integra as normas de concorrência desleal, no capítulo que trata da apropriação de valores comerciais, o que demonstra a absoluta separação entre as concepções do *right to privacy* e *right of publicity*, tratando-os em campos jurídicos distintos. AMERICAN LAW INSTITUTE. Restatement (Third) of Unfair Competition. **Masaryk University**, 2009. Disponível em: <https://is.muni.cz/th/169953/pravf_m/Extract_III.pdf>. Acesso em: 22 jul. 2017.

seus elementos e extensão[64], tal como o direito à exploração econômica dos aspectos inerentes à identidade[65]. Portanto, o direito de imagem naquele ordenamento passou a compreender um modelo dualista, no qual os valores pessoais são tutelados pelo *right to privacy* e os interesses patrimoniais são tutelados pelo *right of publicity*.

Embora a distinção doutrinária apresente relativa clareza, a dificuldade que emerge do modelo é a identificação da ocorrência do *rigth to privacy* ou do *right of publicity*. Isto porque, conforme vimos, na concepção norte-americana, o direito de publicidade nada mais é que uma exceção ao direito de privacidade, haja vista sua característica patrimonial, de modo que a uma mesma situação pode ser caso de tratamento sob a ótica da privacidade ou da publicidade, a depender da qualidade do agente, das circunstâncias, da transmissibilidade do direito.

Um dos critérios distintivos é o comportamento anterior do titular do direito, isto é, caso se trate de uma pessoa de grande notoriedade, que explorou economicamente aspectos inerentes à sua identidade, tais como imagem, registro de voz, biografia, entre outros, certamente se estará diante de um *right of publicity* a ser tratado e reparado nestes termos. Da mesma forma, caso o titular do direito consinta com a exibição de sua imagem, desde que aufira os ganhos econômicos dela decorrentes ou mesmo quando escolha o veículo ou o periódico no qual permite veicular sua imagem, tratar-se-á também do *right of publicity*. Por outro lado, caso se trate de pessoa anônima, que não exerce profissão que envolva a exibição pública ou em algum momento tenha aferido ganhos com a exploração da própria imagem, nem tenha dado nenhum consentimento neste sentido, estão presentes todos os elementos para que a questão seja tratada pela ótica do direito à privacidade[66].

---

[64] Consoante já citado neste trabalho, o Estado da Louisiana foi além da tríade de elementos do direito de publicidade geralmente adotada (nome, imagem e semelhança). Por outro lado, a legislação do Estado de Nova Iorque não reconhece até os dias atuais a extensão do direito de publicidade para além da morte do indivíduo, sendo esta posição cada vez mais minoritária. Esta posição minoritária tende a ser revertida, haja vista as repetidas tentativas do legislativo daquele país em implementar a fruição do direito de privacidade após a morte. Há variações ainda no que tange ao prazo de extensão dos direitos de exploração comercial da imagem para além da morte. Por exemplo, o Estado do Tennessee reconhece o direito por 10 anos após a morte, Virgínia por 20 anos. Florida há 40 anos, Kentucky, Nevada e Texas há 50 anos, Califórnia por 70 anos e Washington por 75 anos. Indiana concede reconhecimento pelo Direito de Publicidade por 100 anos após a morte da personalidade Oklahoma, ao mesmo tempo que oferece um reconhecimento semelhante de 100 anos como Indiana, limita a provisão de retorno para 50 anos. A BRIEF HISTORY… Op. cit.

[65] Ao todo, vinte e dois estados reconhecem o direito de publicidade em alguma capacidade através de legislações. São eles: Alabama, Arizona, Califórnia, Flórida, Havaí, Illinois, Indiana, Kentucky, Massachusetts, Nebraska, Nevada, Nova York, Ohio, Oklahoma, Pensilvânia, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington e Wisconsin. Ademais trinta e oito estados também possuem algum tipo de precedente jurisprudencial a respeito. A BRIEF HISTORY… Op. cit.

[66] RIGAUX, François. **La protection de la vie privée et des autres biens de la personnalité**. Bruxelas: Bruylant, 1990, p. 407 *apud* ZANINI, Leonardo Estevam de Assis. Op. cit.,p. 19.

Por esta razão, passou a ser critério distintivo geral da jurisprudência norte-americana a verificação se o nome ou imagem utilizada é de pessoa célebre, o que determinaria o tratamento sob ponto de vista do *right of publicity*. Do contrário, caso se trate de pessoa desconhecida, o tratamento deve ocorrer pelo *right of privacy*[67].

Outra distinção importante é a transmissibilidade do direito. O *right of publicity,* por ser considerado um direito de natureza patrimonial, referente à exclusividade na exploração comercial da própria identidade, admitiria a sua cessão contratual ou transmissão hereditária, à exceção de estados cuja legislação expressamente não as permitem. Contudo, no caso do *right to privacy*, trata-se de direito pessoal, de caráter não patrimonial, ligado a valores existenciais do ser humano, de modo que não se admite sua cessão, tampouco sua transmissão hereditária.

Tais critérios distintivos apenas orientam o caminho a ser seguido, mas estão longe de se tratar de um modelo seguro de categorização do *right to privacy* ou do *right of publicity*, vez que persiste a dificuldade de sua aplicação concreta, pois ambos os direitos são violados pela indevida apropriação da imagem do indivíduo, o que compõe um dos testes da privacidade definido por William Prosser. Ora, não seria incomum que um anônimo qualquer aspirante a celebridade quisesse que fotos suas fossem exibidas e divulgadas, mas não quisesse que fosse feito por determinado veículo, mas por outro. Se o veículo indesejado, sem saber da intenção do aspirante utilizasse tais fotos para publicidade não autorizada, não se sabe ao certo o tratamento a ser dado à matéria. Isto porque o titular do direito de imagem não se sentiria moralmente ofendido pela exploração econômica de sua figura – afinal é disso que as celebridades vivem, apenas se opondo ao veículo específico que a explorou, o que faria concluir tratar-se do *right of publicity*. Ao mesmo tempo trata-se de pessoa anônima sem nenhuma situação que lhe traga notoriedade, o que faria concluir que se trata do *right of privacy*. Logo, em situações limites, apenas a subjetividade do indivíduo poderia definir tratar-se de um caso ou outro, o que deixa clara a dificuldade da matéria.

Não se quer aqui criar um falso problema, mas, diante do *leading case* em *Haelen*, pode-se afirmar que a jurisprudência norte-americana criou o *right of publicity* como uma forma de viabilizar juridicamente a exploração econômica da imagem por parte de atletas e outras pessoas notórias e com o intuito de manter intacto o arcabouço teórico clássico do direito de privacidade. Isto, de alguma forma, criou um modelo dual em que as situações não estão pré-definidas. Deste modo, recorrer à qualidade do agente não parece ser um critério

[67] ZANINI, Leonardo Estevam de Assis. Op. cit., p. 19.

totalmente seguro quando se pensa no caso do "homem-bala" que, mesmo não sendo uma celebridade, teve seu caso tratado sob a ótica do *right of publicity*.

Talvez o equívoco da doutrina norte-americana seja tratar o direito de exploração econômica da imagem sob a ótica da privacidade, quando não há situação que exponha qualquer aspecto da vida privada[68]. Ora, parece difícil vislumbrar alguma questão de privacidade na exploração econômica da figura do indivíduo, tenha ele notoriedade ou não. Muito tempo se passou do caso *The flower of the family* para se dizer que a retratação pública de uma fotografia com fins publicitários, que não expõe nenhum aspecto íntimo ou nenhuma situação embaraçosa, tenha alguma repercussão na esfera de privacidade. Ora, pode-se até discutir a reparação pela exploração não autorizada da figura com base no direito de imagem, ou até mesmo em virtude do dano de natureza moral causado. Mas a mera divulgação da imagem sem que essa imagem exponha a intimidade ou seja de qualquer modo vexatória, pois captada em espaço público e sem qualquer possibilidade de se criar um juízo negativo a respeito, não parece se relacionar com a privacidade de quem quer que seja, anônimo ou não.

Diferente disso é retratar membros de uma minoria estigmatizada, que optaram por manter sua identidade nas sombras, por medo de retaliações profissionais ou físicas, como seria o caso de um homossexual ser fotografado em um ambiente de acesso específico ao público da comunidade gay ou mesmo a publicação da fotografia de um político ou celebridade em estado moribundo, agonizando em seu leito de morte. Nestes casos, não se pode negar que haveria uma estrita relação do uso da imagem com o *privacy* do indivíduo de maneira relevante a ser protegida sob a ótica da privacidade.

Como antes já dito, a abrangência do *right of privacy* norte-americano é muito mais ampla que a privacidade no direito brasileiro, abrangendo uma gama de aspectos que seriam inerentes ao catálogo de direitos da personalidade, ou seja, direitos que seriam pessoais, intransmissíveis e irrenunciáveis.

Além de a abordagem brasileira da privacidade ser muito mais restrita, o tratamento sobre a ótica dos direitos da personalidade dado pelo ordenamento jurídico brasileiro harmoniza plenamente sua natureza intransmissível e irrenunciável e, por outro lado, entende

[68] Embora aqui se aponte incongruência da doutrina norte-americana, em geral, a doutrina europeia de privacidade também trata o direito de imagem sob a ótica da privacidade, ao estabelecer que compete ao indivíduo a autonomia sobre a exibição pública da própria imagem, enquanto aspecto de sua dignidade.

que o titular do direito possui direito à autorização da exploração comercial de seus direitos da personalidade, desde que essa cessão de direitos seja específica e temporária[69].

Da mesma forma, a legitimação para reclamação de perdas e danos se transfere aos herdeiros. Portanto, resta claro que o direito brasileiro aborda a questão de forma mais simples, admitindo a cessão parcial e temporária de direitos da personalidade, bem como seu aproveitamento econômico e sua transmissibilidade. Por óbvio, o que se cede ou transfere – nunca se renuncia – são os efeitos patrimoniais decorrentes da exploração comercial de determinado direito da personalidade. Deste modo, não foi preciso a construção de uma categoria autônoma da privacidade, sob a ótica da concorrência desleal para permitir a exclusividade do aproveitamento econômico da própria imagem, como ocorreu nos Estados Unidos.

1.1.3 A evolução jurisprudencial norte-americana sobre privacidade

Para melhor compreensão da concepção norte-americana de privacidade, além dos casos aqui já apresentados, faz-se necessária a análise dos casos mais importantes acerca do direito à privacidade naquele país, com a ressalva sempre necessária de que a privacidade no direito norte-americano tem abrangência muito mais ampla que no Brasil, vez que se estende para outros direitos da personalidade, tais como a imagem e o nome.

Inicialmente, remete-se aqui aos casos inaugurais da discussão de privacidade, *Schuyler v. Curtis* (1891) e *Marks v. Jaffa* (1893), que tratavam, basicamente, do direito de imagem[70] enquanto aspecto da privacidade. Ambos representam o início das discussões jurisprudenciais do direito à privacidade, sendo que no primeiro caso deixou-se de reconhecer

---

[69] Prevê o Código Civil Brasileiro: Art. 11. "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

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

(...)

Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial.

Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome.

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais".

[70] Faz-se referência à nota de rodapé nº27, que trata em detalhes de ambos os casos, abordados no tópico 1.1.

o direito à privacidade do indivíduo para além da morte, pleiteado por seu sobrinho, por entender que sua natureza é de direito pessoal; já no segundo, concedeu-se razão ao requerente, proibindo-se a utilização de sua imagem em concurso de popularidade.

Solução distinta foi a adotada em caso já citado que adquiriu maior relevância, tendo ficado conhecido como *The flower of the family*, em virtude da utilização de imagem não autorizada de jovem solteira para retratar publicidade de farinha[71], tendo se negado o reconhecimento de que haveria um direito à privacidade a ser protegido.

Em *Pavesich v. New England Life Ins. Co.*, julgado em 1905, aqui já abordado, reconheceu-se a violação à privacidade por utilizar-se a imagem do indivíduo em propaganda de apólice de seguro sem a sua autorização. Logo, este último caso reverteu a jurisprudência do caso *Roberson*, ao reconhecer o direito à privacidade do retratado, o que passou a ser um parâmetro a ser seguido pelos outros tribunais durante a primeira metade do século XX.

Fato é que estes casos apresentados como exemplos da discussão do conceito clássico de privacidade na jurisprudência americana apresentam-se muito ligados antes à defesa de valores patrimoniais que à proteção de valores existenciais. Após os casos citados, a jurisprudência norte-americana praticamente estagnou-se até o fim da primeira metade do século XX, deixando-se de atualizar os parâmetros estabelecidos na doutrina de Warren e Brandeis, principalmente em virtude da dificuldade de abordar a privacidade dissociada de institutos clássicos, tais como a proteção da honra e da propriedade[72].

O que demonstra a citada estagnação da doutrina da privacidade é o caso *Olmstead v. United States*[73], julgado pela Suprema Corte em 1928. O autor Roy Olmstead questionava a violação à sua privacidade, vez que o FBI realizou escutas telefônicas dele e de outras pessoas, que teriam transportado e vendido bebidas alcoólicas em violação à lei nacional. No entanto, o tribunal decidiu que as escutas telefônicas, as quais eram o principal meio de prova, não tinham sido feitas com invasão da propriedade privada, já que os cabos telefônicos interceptados se localizavam na rua, em áreas próximas da casa e do escritório investigados.

Portanto, prevaleceu a tese de que a escuta telefônica não poderia ser considerada busca nos termos que é vedado pela Constituição, pois não teria havido invasão física do domicílio, já que a interceptação teria sido realizada nos cabos externos à residência do investigado. Nesta concepção, tais interceptações não teriam violado a Quarta Emenda da

---

[71] Trata-se do caso*Roberson v. Rochester Folding box Co* (the flower of the Family) 1902171 N.Y. 538, 64 N.E. 442 (1902), tratado no tópico anterior.

[72] ZANINI, Leonardo Estevam de Assis. Op. cit.

[73]*Olmstead v. United States*. 277 U.S. 438, 48 S. Ct. 564, 72 L. Ed. 944 (1928).

Constituição americana[74], que garante a inviolabilidade da pessoa, da sua casa, de seus documentos e dos seus bens contra a realização de buscas e apreensões ilegítimas.

Vê-se, contudo, que esta interpretação literal dada à quarta emenda, diante da clara violação de privacidade é criticável por inúmeros ângulos, vez que não se precisa ingressar no recinto físico para se violar de forma clandestina o ambiente doméstico protegido pela Constituição. Ora, não faz sentido proteger a residência de buscas e invasões ilegais se o que se quer resguardar são os registros de atos, falas e escritos que acontecem na sacralidade do lar. Portanto, se por outro meio se pode atingir a privacidade protegida por tal sacralidade que não seja o ingresso físico, este outro meio também constitui violação da privacidade.

Tanto é assim que, em que pese o entendimento da Suprema Corte dos Estados Unidos, o juiz Brandeis, coautor do artigo de 1890, apresentou voto em sentido contrário, defendendo a aplicação liberal da Quarta Emenda, no sentido de que a sua previsão protege o indivíduo contra qualquer violação injustificada da privacidade, seja qual for o meio utilizado. E, como o governo não obteve um mandado de busca antes da realização da interceptação, para o juiz, a medida perpetrada contrariava a Constituição, vez que essa protege os cidadãos não apenas nos aspectos materiais, mas também em suas crenças, pensamentos, emoções e sensações.

O caso *Olmestead* deixou clara a resistência da Suprema Corte em aplicar o direito à privacidade em matéria de produção de prova processual penal, adotando-se uma interpretação literal e pouco protetiva. Por esta razão, na mesma linha, deixou de ser reconhecida pela Suprema Corte a ocorrência de violação à privacidade *Goldman v. United States*, julgado em 1942[75], uma vez que a conversa do acusado foi gravada por microfone instalado na parede do apartamento vizinho, não tendo ocorrido invasão física[76].

---

[74] A Quarta Emenda possui por inspiração a noção de que a casa é o castelo inviolável do homem, protegendo o indivíduo de buscas irrazoáveis em sua propriedade. O texto da Quarta Emenda é seguinte: "**Amendment IV.** The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.".

[75] *Goldman v. United States*, 316 U.S. 129 (1942).

[76] O posicionamento foi mais uma vez confirmado no caso *On Lee v. United States* (343 U.S. 747), em 1952, quando o tribunal admitiu as provas colhidas pela escuta de conversações entre o autor da ação e um agente infiltrado, que portava um microfone. O mesmo também ocorreu em em *Silvermann v. United State*s (365 U.S. 505) de 1961, que, seguindo o precedente inaugurado no caso Olmstead, apenas condenou a utilização de microfones pelo fato de ter ocorrido invasão de propriedade.

Apenas no caso *Griswold v. Connecticut*[77], decido em 1965, a Suprema Corte dos Estados Unidos passa a reverter o precedente que estabeleceu no caso *Olmstead*, reconhecendo a privacidade no âmbito constitucional.

Em apertada síntese, o estado de Connecticut editou lei que tornou ilegal o uso ou a distribuição de medicamentos anticoncepcionais. A aplicação da lei resultou na condenação do médico, Dr. Lee Buxton, que havia prescrito os contraceptivos a uma mulher casada, tendo sido condenada também Estelle Griswold, diretora executiva da clínica de paternidade planejada onde o referido médico trabalhava.

Na Suprema Corte dos Estados Unidos, o juiz William Douglas redigiu o voto do caso *Griswoldv. Connecticut*, que se tornou célebre, no qual declarou-se a inconstitucionalidade da lei. O fundamento da inconstitucionalidade foi a existência de um direito geral de privacidade, que decorreria da aplicação das seguintes emendas à Constituição dos Estados Unidos: a primeira emenda, que garante a liberdade de expressão; a terceira, que prevê a restrição ao aquartelamento de soldados em casas particulares; a quarta, que proíbe busca e apreensões ilícitas; a quinta, que protege o cidadão contra a autoincriminação e a nona, que declara que os direitos não especificados na Declaração de Direitos são também protegidos por ela.

A decisão ainda destacou o caráter sagrado do leito marital e o respeito que merece a intimidade do casal, considerando, por conseguinte, inadmissível que a polícia pudesse estender suas investigações ao quarto do casal ("*the sacred precincts of marital bedrooms*")[78].

Portanto, a importância do caso *Griswold v. Connecticut* deve-se ao reconhecimento constitucional do *right of privacy*, que, apesar de não ser expressamente mencionado pela Constituição, poderia ser inferido a partir de uma interpretação da declaração de direitos.

O caso *Katz v. United States*[79], julgado em 1967, confirmou a superação do precedente de *Olmstead*, uma vez que se reconheceu a violação de privacidade injustificada, em virtude de a interceptação telefônica ter sido realidade em conversas mantidas em uma cabine telefônica. Embora não se tratasse de violação a algum bem material, tampouco de se estar no âmbito da sacralidade do lar, entendeu-se que, ao ingressar em uma cabine telefônica e fechar

[77]*Griswold v. Connecticut* (381 U.S. 479 (1965).

[78] Posteriormente, inspirado no caso Griswold, a Suprema Corte julgou o caso Em *Eisenstadt v. Baird*, 405 US 438 (1972), invalidando uma lei que proíbe a distribuição de contraceptivos a pessoas não casadas. O caso foi decidido sob a Cláusula de Igualdade de Proteção. O Tribunal estendeu o direito de privacidade do casal quanto ao uso de contraceptivo também ao indivíduo, sob o argumento de que o direito à privacidade em questão é o direito do *indivíduo*, casado ou solteiro, estar livre de invasão governamental injustificada em questões tão fundamentais de uma pessoa, como a decisão de suportar ou gerar uma criança.

[79]*Katz v. United States* (389 U.S. 347 (1967).

sua porta, haveria uma expectativa razoável de privacidade, de modo que a interceptação violou a previsão da Quarta Emenda, que protege pessoas, e não lugares.

Do mesmo modo, em 1969, no caso *Stanley v. Georgia*[80] reafirmou-se o precedente estabelecido no caso Griswold, ao se declarar ilegal busca e apreensão na casa do autor, embora munido de mandado, mas que havia sido deferido para levantamento de provas sobre agenciamento de apostas. No cumprimento do mandado, foram encontrados, fortuitamente, vídeos obscenos, o que violaria a legislação da Geórgia e resultou na condenação de Stanley por posse de material obsceno. No âmbito da Suprema Corte, embora o caso tratasse também da primeira emenda, que garante ao indivíduo a liberdade de expressão, entendeu-se também que teria havido violação à Quarta Emenda, uma vez que a busca foi realizada sem estar coberta pelo mandado respectivo, que apenas determinava a investigação sobre agenciamento, o que levou à absolvição de Stanley.

Outro caso memorável em matéria de privacidade foi o histórico julgamento da Suprema Corte norte-americana no caso *Roe v. Wade*, em 1973, no qual se permitiu o aborto por livre escolha da mulher até o momento em que o feto não tenha vida extrauterina viável, permitindo-se que o Estado proibisse o aborto apenas após a fase de viabilidade extrauterina[81]. No caso, a autora questionava a Lei do estado do Texas, que apenas permitia o aborto em caso de risco de vida à saúde da mulher.

A Suprema Corte entendeu que a decisão quanto à continuidade ou não da gestação era matéria afeta à privacidade da mulher, permitindo-se que esta decisão fosse tomada exclusivamente pela gestante até o primeiro trimestre da gestação, não cabendo ingerência estatal para proibir sua realização neste período. Nesta decisão, consolidou-se o que ficou conhecido como marco dos trimestres, inaugurado pelo caso *Roe*, no qual se permitiu a livre interrupção da gestação pela mulher no primeiro trimestre; a possibilidade de os estados regularem o procedimento médico para permitir a interrupção no segundo semestre, sem que pudessem limitar o direito de escolha da mulher e, no terceiro trimestre, quando há proximidade com a possibilidade de vida extrauterina do feto, permitiu que leis estaduais pudessem restringir o aborto, exceto no caso de risco à vida ou à saúde da mulher.

Posteriormente, em *Casey v. Planned Parenthood* (1992), a Suprema Corte dos Estados Unidos dispensou a necessidade de comunicação prévia ao marido antes da realização

---

[80] *Stanley v. Georgia*. 394 U.S. 557 (1969).

[81] *Roe v. Wade*, 410 U.S. 113 (January 22, 1973) 410 U.S. 113.

do abortamento, reafirmando tratar-se de decisão de exclusiva consideração da gestante, no recinto inviolável de sua privacidade.

Pode-se citar, ainda, o caso *Lawrence v. Texas*[82], julgado pela Suprema Corte em 2003. A lei texana condenava criminalmente relações sexuais entre pessoas do mesmo sexo. A polícia texana, ao atender uma denúncia de uso de arma, adentrou ao apartamento de John Geddes Lawrence, que mantinha relações sexuais com outro homem no momento da diligência. Ambos foram presos com base na lei texana. A Suprema Corte reafirmou os precedentes firmados em *Griswold*, no sentido da sacralidade do leito matrimonial, para concluir que a relação homoafetiva entre dois adultos diz respeito a sua própria privacidade e exercício de liberdade, não cabendo ao Estado a realização de intromissões nesta esfera privada.

Por fim, para além dos casos históricos, diante das novas tecnologias da informação e comunicação, há casos mais instigantes que demonstram que a privacidade do indivíduo vai muito além dos limites físicos do lar e que um aparelho de *smartphone* pode dizer mais sobre o indivíduo que uma busca em seus pertences.

Isso ficou claro no caso *Riley v. California*[83], julgado pela Suprema Corte dos Estados Unidos em junho de 2014. Em síntese, *Riley* foi parado em 2009 pela polícia de San Diego por estar com o registro do veículo vencido. Descobriu-se ainda uma arma de fogo escondida no capô do veículo, motivo pelo qual Riley foi preso. Foram realizados exames de balística que ligavam a arma apreendida a um homicídio relacionado a gangues ocorridos em agosto daquele ano. Além do exame de balística, a polícia vasculhou o celular que Riley portava sem mandado judicial e descobriu informações (fotos, vídeos e mensagens) que o ligavam à gangue de Lincoln Park, tendo sido indiciado pelo crime ocorrido em agosto, bem como pela associação ao grupo criminoso.

Para efetuar a busca no *smartphone*, a polícia se baseou na jurisprudência consolidada desde 1969 no caso *Chimel v. California*[84], no qual a Suprema Corte entendeu que, na prisão de um suspeito, os policiais poderiam, sem mandado judicial, promover busca pessoal, ou seja, poderiam revistar o suspeito e realizar busca nas adjacências do local em que se encontrava o suspeito. Segundo o julgado, a polícia poderia revistar tudo aquilo que, no

---

[82]*Lawrence v. Texas* 539 U.S. 558 (2003).

[83]*Riley v. California*, 573 U.S.(2014). Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>. Acesso em: 18 nov. 2017.

[84]*Chimel v. California*, 395 U.S. 752 (1969). Disponível em: <https://supreme.justia.com/cases/federal/us/395/752/case.html>. Acesso em: 18 nov. 2017.

momento da prisão, estivesse ao alcance do suspeito, pois isso garantiria a proteção da evidência material e a segurança dos policiais. A possibilidade de revista do suspeito e tudo que estivesse ao seu alcance é conhecida como *SITA doctrine - search incident to a lawful arrest* (em tradução livre, busca incidental na realização de uma prisão legal) ou *Chimel rule*. A doutrina CITA, a bem da verdade, admite a busca fortuita de provas no momento da realização da prisão. O precedente, portanto, de certo modo, excepcionava a quarta emenda, na medida em que permitia buscas pessoais sem mandado judicial.

Todavia, contrariando a doutrina consolidada há mais de quatro décadas, a Suprema Corte dos Estados Unidos entendeu que a busca de aparelho *smartphone* sem mandado judicial era medida ilegal, determinando o desentranhamento desta prova dos autos, vez que violaria a quarta emenda. Tal caso deixa evidente que a privacidade nos dias atuais está diante de novas fronteiras, não mais físicas, mas virtuais. Os aparatos tecnológicos, tal como os *smartphones* atualmente utilizados, podem informar muito mais sobre o indivíduo que ele mesmo, vez que possuem um grande volume dos mais variados dados de um indivíduo identificável. A pessoa digital mostra-se muito mais rastreável e transparente que a pessoa física, seus bens, domicílio e local de trabalho, de modo que a busca em um dispositivo que concentra uma gama de variada informação sobre o indivíduo é e deve ser matéria de reserva de jurisdição, haja vista a especial relevância que estes dados possuem para o direito fundamental à privacidade do indivíduo[85].

Decerto que há outros memoráveis casos em matéria de privacidade oriundos da jurisprudência norte-americana. Ocorre que o conjunto de casos até agora citados neste tópico, bem como outros já analisados incidentalmente, permitem traçar um panorama. Inicialmente muito vinculada a aspectos tradicionais, como o direito de imagem, e a questões patrimoniais, pode-se dizer que a jurisprudência norte-americana foi se moldando para proteger o valor liberdade, muito cultuado naquele país de cultura liberal.

Em geral, os casos tratam da liberdade do indivíduo para tomar as próprias decisões, desembaraçado de qualquer ingerência estatal, ou mesmo da importância que se dá ao exercício da liberdade de expressão e, mais especificamente, à liberdade de imprensa, sendo a

[85] No mesmo sentido, a Suprema Corte norte-americana julgou o caso *United States v. Wurie*. Brian Wurie foi preso por suspeita de tráfico de drogas. Com vistas a fortalecer as evidências do crime, durante a prisão, os agentes acessaram o aparelho do preso e identificaram o contato identificado como "my house" (minha casa). Com o número do telefone, identificaram o local daquela linha telefônica. De posse de um mandado, fizeram busca na casa e encontraram 215 gramas de cocaína crack, quatro sacos de maconha, parafernália de drogas, dinheiro, arma de fogo e munição. A Suprema Corte, nos moldes decididos no caso Riley, entendeu que a busca no celular do preso sem mandado judicial, é ilegal. Disponível em: <https://harvardlawreview.org/wp-content/uploads/pdfs/vol127_united_states_v_wurie.pdf>. Acesso em: 20 dez. 2017.

imprensa livre um dos valores mais caros à cultura norte-americana, conforme se verá no tópico a seguir.

1.1.4 Diferenças entre a cultura de privacidade europeia e norte-americana

Sabe-se que o grau de proteção de privacidade de determinado ordenamento jurídico é o reflexo da cultura de privacidade da sociedade, de modo que compreender a privacidade em certo país ou continente é, antes, compreender a sua cultura e os motivos pelos quais determinados interesses são mais ou menos relevantes a ponto de serem protegidos pela legislação de privacidade. Por se tratar de conceito fortemente influenciado pelo elemento cultural, o conteúdo da privacidade varia no espaço e no tempo, além de ser comumente fluido e variável[86].

A importância de se realizar um panorama sobre a cultura de privacidade norte-americana para após contrastá-la com a cultura europeia é formular um panorama preciso do direito comparado, a partir das duas principais culturas ocidentais, a fim de se verificar em que ponto se situa a cultura brasileira de privacidade e se há um conceito adequado e possível de privacidade adaptado à cultura brasileira.

Inicialmente, é preciso observar que há diferenças relevantes entre a cultura europeia e norte-americana de privacidade. Tanto é assim que o clássico texto de Warren e Brandeis foi criticado por incorporar elementos excessivamente continentais, apelando a conceitos como honra pessoal e personalidade, os quais não são integrantes da cultura jurídica norte-americana.

Para além das diferenças típicas entre o sistema jurídico da *commom law* e sua vinculação aos precedentes e o sistema da *civil law*, há situações fáticas específicas nas quais se mostra a diferença de cultura de privacidade entre os Estados Unidos e a Europa, embora façam parte do ocidente. Para ficar em alguns exemplos, um indivíduo europeu não veria problemas em uma lei que submetesse a escolha do nome de seus filhos à autorização estatal, o que seria manifestamente absurdo à noção de liberdade do americano médio. Da mesma forma, as leis europeias sobre proteção de crédito, mais especificamente a francesa e a alemã, apenas permitem que se informe a situação de crédito do indivíduo em caso de insolvência ou de informação de débito, efetuando-se um controle rigoroso do compartilhamento dos bancos de dados que gerenciam essas informações. Para o europeu médio, ser perguntado sobre o

[86] WHITMAN, James Q. Op. cit., p. 1153.

próprio salário pode soar ofensivo ou dizer abertamente o quanto ganha pode violar as regras de etiqueta, segundo os padrões continentais.

No entanto, o americano convive bem com a possibilidade de rastreamento e compartilhamento de seu perfil de crédito, de seu histórico de consumo e do uso destes dados para direcionar a cada consumidor produtos personalizados, o que aumentaria a eficiência dos mercados e traria ganhos decorrentes do barateamento dos produtos e serviços, vez que se gastaria bem menos com publicidade, quando a tecnologia pudesse aproximar fornecedor e consumidor. Por outro lado, para o europeu, suas informações de consumo e de crédito são elementos caros a sua privacidade[87], de modo que o compartilhamento amplo pode comprometer a autonomia decisória do indivíduo sobre a imagem que quer apresentar de si mesmo.

As diferenças apenas pontuadas não possuem o condão de classificar esta ou aquela cultura de mais ou menos protetiva da privacidade, apenas trata-se de diferentes prioridades condicionadas pelos valores sociais e jurídicos de determinada sociedade.

O ponto de toque da cultura norte-americana de privacidade é que sua concepção de privacidade se manifesta como um aspecto da liberdade. Significa dizer que, para os americanos, o direito à privacidade é orientado pelo exercício da liberdade, especialmente da liberdade em face do Estado. Portanto, conceitualmente, o direito de privacidade americano se mantém o mesmo desde o século XVIII, enquanto direito de liberdade contra as intrusões estatais no lar do indivíduo[88].

Para o ponto de vista americano, o primeiro perigo é a violação da sacralidade dos lares a ser perpetrada pelos agentes do governo, de acordo com a jurisprudência predominante na Suprema Corte. Portanto, o bem a ser resguardado na privacidade é a soberania do indivíduo no limite de seus muros e o inimigo que colocaria essa soberania em risco seria o Estado. O lar é visto como um castelo onde o indivíduo exerce sua soberania privada, livre de qualquer ingerência estatal.

Esse raciocínio é tão arraigado na cultura norte-americana que no caso *Boyd v. United States*[89], julgado em 1886, a Suprema Corte entendeu que a busca e apreensão de documentos fiscais realizada no domicílio do autor para produzir prova contra o próprio indivíduo era

---

[87] Ibidem, p. 1156.

[88] Tratando da origem do direito à privacidade norte-americana, confira-se ROSEN, Jeffrey. **The Unwanted Gaze**: The destruction of privacy in America. New York: Vintage Books Edition, 2000 *apud* WHITMAN, James Q. Op. cit.

[89] *Boyd v. United States*, 116 U.S. 616 (1886).

irrazoável, nos termos do que prevê a Quarta Emenda à Constituição, pois as atuações do Estado devem observar a sacralidade do lar de um homem. A Corte invocou como argumento o célebre caso de John Entick[90], um dissidente político britânico cujos documentos foram apreendidos. A Corte britânica condenou a apreensão em 1765 e o julgado inspirou a edição da Carta de Direitos americana.

A ideia de soberania particular nos limites do castelo privado que é o domicílio permeia toda a reflexão norte-americana sobre privacidade, de modo que estar nos limites do domicílio confere proteção ao indivíduo em virtude da expectativa razoável de privacidade dentro de tais limites. Essa foi a noção concebida ao final do século XVIII, com a edição da Quarta Emenda. Para os americanos, a privacidade é o direito contra buscas e apreensões ilegais, vez que é senhor em sua própria casa. Tanto é assim que há quem defenda que a origem da história do direito à privacidade no país ocorre com o caso *Boyd* e não com o artigo de Warren e Brandeis, que apenas surgiu quatro anos depois como um eco das ideias europeia de privacidade. Em suma, o pensamento americano tende a ver a casa como primeira defesa e o estado como primeiro inimigo[91]. Portanto, diferente da cultura europeia, não é a mídia ou os excessos do livre mercado que são vistos como inimigos da privacidade, mas o Estado é o opositor a ser combatido.

Com base na noção de que a casa deve ser o símbolo máximo de privacidade, na cultura jurídica americana, desenvolveu-se o critério da expectativa razoável de privacidade. Significa dizer que a expectativa máxima de privacidade ocorrerá no âmbito do lar, ou seja, para o americano, à medida em que ele se afasta ambiente sagrado do lar, se enfraquecem as expectativas de privacidade[92]. Ressalte-se que o sentido de casa tem sido estendido para além da literalidade, contando com a mesma proteção em escritórios ou até mesmo cabines telefônicas[93].

Tanto é assim que a Suprema Corte reconheceu, que, no caso do consultório de um médico no interior de um hospital estadual, a expectativa de privacidade nas buscas realizadas

[90] Entick v. Carrington [1765] EWHC KB J98 95 ER 807

[91] WHITMAN, James Q. Op. cit, p. 1215.

[92] Ibidem, p. 1194.

[93] *Katz v. United States* (389 U.S. 347 (1967), tratado no tópico 1.1.3.

pelo superior hierárquico, nos documentos do subordinado são mais limitadas,por questões de "realidades operacionais", mas o consultório também protegido pela Quarta Emenda.[94].

Outro caso em que a Suprema Corte foi *Vernonia School District v. Acton*, julgado em 1995[95], no qual se concluiu que os atletas do ensino médio têm uma menor expectativa de privacidade do que o público em geral, uma vez que têm por costume se trocar na frente de outros atletas em vestuários coletivos e as condições de realização do exame não são muito diferentes das condições de utilização de um banheiro público. Portanto, neste caso, atletas estudantis teriam uma menor expectativa de privacidade. Ademais, o legítimo interesse do Estado no teste aleatório de drogas seria válido, uma vez que sua realização atende um interesse convincente nos sistemas públicos para impedir o uso de drogas.

O critério da expectativa razoável mostra-se bastante presente na jurisprudência norte-americana da privacidade, diminuindo-se a expectativa na medida em que o indivíduo se distancia do ambiente de reclusão. Isto mostra uma diferença com a cultura europeia de privacidade, pois mesmo em caso de nudez em ambiente público, como se verá a seguir, o europeu demanda o controle sobre a retratação de sua imagem, ainda que esteja no espaço público.

Desta forma, não resta dúvidas que a cultura americana de privacidade gravita em torno do valor liberdade e, entre todos os valores liberais, a liberdade de imprensa é o mais relevante, de modo que, na jurisprudência norte-americana, tende a prevalecer a liberdade de imprensa diante de eventual alegação da dignidade do indivíduo, permitindo-se inclusive, como já se viu, a divulgação da identidade de vítimas de estupro[96].

Da mesma forma, diferentemente do sistema jurídico europeu, não há uma proteção do indivíduo contra si mesmo no que tange à exposição da própria dignidade. Como se viu aqui, o *right of publicity* não permite fazer juízo de valor sobre o conteúdo do que será explorado economicamente. Logo, o interesse americano no direito de publicidade é o interesse em questões patrimoniais, não em honra ou dignidade[97]. Tanto é assim que permanecem separadas as noções de *right to privacy* e de *right of publicity*.

---

[94] Trata-se do caso *O'Connor v. Ortega*, 480 U.S. 709, julgado pela Suprema Corte em (1987), em que embora não se tenha chegado a uma conclusão no caso, se afirmou que a proteção da Quarta Emenda que garante expectativa razoável de privacidade no local de trabalho deve ser harmonizada com as realidades operacionais.

[95]*Vernonia School District v. Acto*n, julgado em 1995, 515 US 646 (1995).

[96] Faz-se referência à nota de rodapé nº 21 onde se tratou do caso *Cox Broadcasting Corp.* v. *Chon* e *Florida Star v. B.J.F.*, nos quais se entendeu ser legal que a mídia publicasse o nome de vítimas de estupro.

[97] WHITMAN, James Q. Op. cit.,p. 1210.

Exemplo disso é o julgamento do caso *Here's Jhonny*[98], no qual se utilizou um jargão do apresentador Johnny Carson, para ilustrar uma marca de toaletes portáteis. Restou claro no julgamento que não se tratava de uma questão de direitos à privacidade contra humilhação ou constrangimento, mas apenas de interesses patrimoniais, a saber, a exploração comercial da identidade do apresentador.

Em apertada conclusão, a cultura americana de privacidade fortemente influenciada pelo valor liberdade, especialmente a liberdade de imprensa e as condições de liberdade necessárias ao exercício do livre mercado, tem por fundamental a sacralidade do lar como fortaleza, a proteger a privacidade do indivíduo. Diferente da cultura europeia, o livre mercado e a imprensa não são vistos como inimigos prioritários da privacidade. Por outro lado, a Quarta Emenda, fortemente prestigiada na jurisprudência norte-americana, protege o indivíduo de buscas arbitrárias por parte do Estado, o qual a cultura americana vê como inimigo maior.

1.2 **Cultura continental-europeia de privacidade: as diferenças do modelo americano**

Pode parecer pouco didático iniciar o estudo sobre o direito à privacidade no sistema europeu com o tratamento da cultura de privacidade, enquanto no estudo do direito norte-americano se iniciou pela trajetória histórica, jurisprudencial para apenas ao final se tratar da cultura de privacidade norte-americana.

No estudo do continente europeu, inicia-se pelas peculiaridades culturais europeias, justamente para ressaltar os contrastes com a cultura norte-americana. O tratamento dado por determinado ordenamento jurídico nada mais é que um reflexo dos valores legais e sociais prevalentes em uma sociedade. Significa dizer que a proteção jurídica à privacidade, como acontece com as outras matérias, são um reflexo das convenções sociais e valores consolidados em determinada cultura.

Não que as diferenças sejam relevantes a ponto de se concluir que determinada cultura proteja mais ou menos a privacidade. Pelo contrário, as diferenças são relativas, ou seja, em maior ou menor intensidade, sem que se admitam generalizações. Pode ser inclusive que por razões culturais distintas se chegue ao mesmo resultado, embora o ponto de partida seja diferente.

---

[98] Faz-se referência à nota de rodapé nº 47, na qual se tratou do caso *Carson v. Here's Johnny Portable Toilets* (698 F.2d 831, 6th Cir. 1983).

A diferença mais perceptível entre o sistema americano e europeu é que, enquanto a concepção americana de privacidade orbita em torno dos valores da liberdade, a concepção continental europeia de privacidade tem seu centro na dignidade. A proteção europeia da privacidade é, sobretudo, uma forma de proteger o direito ao respeito e dignidade pessoal do indivíduo. A privacidade europeia tem por foco a proteção à imagem, ao nome e à reputação do indivíduo e protege sua autodeterminação informativa, ou seja, o direito de controlar a gama de informações levantadas sobre o indivíduo[99]. O objetivo das leis continentais de privacidade é proteger o indivíduo da vergonha e humilhação públicas e da perda de sua dignidade. Esta é a razão de atribuir ao próprio indivíduo a autonomia informacional para definir de que forma será moldada sua face pública. A privacidade europeia é parte de uma proteção jurídica maior do respeito interpessoal, dispensado a todos nas relações entre si.

Diferentemente da cultura norte-americana, o primeiro inimigo da privacidade na cultura europeia é o que se chama de excessos da imprensa livre. Significa dizer que, na concepção europeia, a mídia divulga as mais variadas informações sobre o indivíduo, colocando em risco sua dignidade pública[100]. Outro inimigo eleito da privacidade na cultura continental são os danos causados pelo livre mercado. Portanto, enquanto os americanos vislumbram a liberdade de comprar e vender apenas por seu aspecto positivo, a cultura europeia aborda um caráter predatório que pode transformar a dignidade em mercadoria e colocar em risco a honra dos indivíduos. Aliás, a história da privacidade europeia está muito relacionada à resistência a dois valores caros à cultura americana: a liberdade de expressão, materializada nos órgãos de comunicação social, e a propriedade privada, da forma como distribuída pelas regras do livre mercado.

Neste trabalho, à semelhança da obra aqui citada de James Whitman, serão adotados como exemplo da cultura de privacidade europeia a trajetória da França e Alemanha, por serem os dois países mais representativos dos valores europeus de privacidade.

Questiona-se a razão pela qual os níveis de exigência de privacidade da legislação europeia aparentam ser superiores aos norte-americanos. Uma resposta mais fácil e que conta com ampla adesão é que os horrores do nazismo fizeram florescer no pós II Guerra legislações mais protetivas da dignidade humana, entre elas a legislação sobre privacidade. Portanto, a dignidade dos dias atuais nada mais é que uma resposta à indignidade propiciada

[99] WHITMAN, James Q. Op. cit.,p. 1161.

[100] Ibidem, p. 1161.

pelos traumas causados pelas violações do nazismo. Essa resposta conta, inclusive, com a adesão de americanos[101].

Não há dúvidas de que a explicação, carregada de drama e comoção pelos extremismos do regime nazifascista, é sedutora. Todavia, a reação ao nazismo não se mostra uma resposta suficiente a explicar a densa cultura de privacidade verificada nos dias atuais. Talvez a reação às graves violações da Alemanha nazista seja parte da explicação e de fato tenha posicionado a dignidade humana no centro do sistema jurídico. Contudo, a cultura europeia de privacidade é, em muito, anterior ao pós-guerra, havendo notícia de legislações e sentenças sobre direito à privacidade no século XVIII e até mesmo XVII.

A cultura de privacidade atual decorre do desenvolvimento ao longo de dois séculos e meio da privacidade das sociedades aristocráticas e monárquicas das quais a França de Luís XIV era o modelo, ou seja, a privacidade era um direito pleiteado e usufruído pela nobreza, pelas famílias de *status* elevado na sociedade, na defesa de sua honra pessoal diante das cortes do continente[102]. O que se pode dizer é que o resultado desta maturação de séculos passou a constituir a cultura europeia de privacidade e as normas que eram de exclusividade do extrato social superior se estenderam a toda a população. Com o advento da modernidade, deixou de ser aceitável que apenas alguns grupos pudessem gozar de proteção jurídica para a sua dignidade. Desta forma, por exemplo, regras especiais de tratamento da nobreza quando recolhida ao cárcere passaram a ser o parâmetro de respeito à dignidade de qualquer preso[103].

Por outro lado, em que pese a omissão dos manuais jurídicos a respeito, pode-se afirmar que durante o nazismohavia proteção à privacidade. Todavia, tratava-se de proteção parcial e discriminatória, ou seja, apenas àqueles entendidos como dignos e superiores pela doutrina do regime fascista, uma vez que a promessa do regime era dar o mesmo grau de dignidade a todos os membros da raça dita superior. Pode parecer contraditório, mas o que ocorreu durante o regime fascista foi que algumas instituições jurídicas experimentaram relevante desenvolvimento e consolidação durante a atuação de Hitler, de modo que este

---

[101] KAGAN, Robert. **Of Paradise and Power**: America and Europe in the new world order. New York: Vintage Books Edition, 2003, p. 58-62 *apud* WHITMAN, James W. Op. cit.,p. 1165.

[102] WHITMAN, James Q. Op. cit.,p. 1166.

[103] No século XVIII, havia diferença de tratamento entre a nobreza e os não nobres quando condenados. Pessoas de status elevados quando condenadas à pena de morte eram decapitadas, um procedimento indolor e mais digno, se é que pode ser feita esta comparação, que os outros membros da sociedade que eram condenados ao enforcamento. Da mesma forma, quando condenados à prisão, nobres eram acomodados em confortáveis apartamentos, enquanto o restante da população se submetia à degradante escravidão penal. Nos dois séculos posteriores à Revolução Francesa, as normas que eram privilégio de apenas parte privilegiada da sociedade passaram a se estender a todos os presos e condenados.

período foi também parte de uma continuidade histórica de extensão da proteção da honra a todos os escalões da sociedade continental. Conduto, há que se ressalvar que, naquele período, a proteção à dignidade era seletiva e discriminatória[104].

Algumas normas continentais proporcionam a exata noção acerca da cultura de privacidade europeia e sua consolidação secular. Exemplo disso são as normas continentais sobre perfil de crédito *(credit reporting)*. Falar de salário ou patrimônio na cultura francesa é contrário às regras de etiqueta daquele país. Culturalmente, somente se revelava o patrimônio de alguém se estivesse insolvente ou quebrado[105].

Essa lógica influenciou decisivamente a legislação europeia sobre relatório de crédito. O mesmo ocorreu sobre a lei acerca de relatório de crédito. Na Franca, o relatório de crédito do consumidor apenas pode ser fornecido por fontes oficiais estatais e apenas é fornecido nos casos de pessoas que estejam experimentando sérias dificuldades financeiras. Portanto, tais relatórios apenas informam a lista de pessoas com comprovado risco de crédito. Qualquer coisa além disso, para a cultura francesa, é indevida intrusão na vida financeira. Na Alemanha, embora o país seja menos rigoroso com relatórios de crédito, o cadastro é feito por empresas de cobrança, as *Schufas*, e não pelo Estado. Todavia, para acesso a este cadastro é necessária autorização expressa do titular como também para compartilhar seu conteúdo, já que os acessos ficam registrados[106]. Aqui vale a máxima de privacidade europeia que permite ao indivíduo o amplo controle das informações de caráter pessoal, enquanto meio de controle da própria imagem pública[107].

Para os europeus, ter acesso ao compilado de hábitos de consumo de pessoas solventes é uma exposição perigosa da vida privada. Ainda que os relatórios amplos de crédito tornem as trocas de mercado mais eficientes e as pessoas mais ricas, consumidores precisam mais do que crédito e eficiência. Precisam de dignidade. Norte-americanos são muito mais propensos a soluções de autorregulação e à proteção de dados baseada nas soluções do mercado.

---

[104] WHITMAN, James Q. Op. cit.,p. 1166.

[105] Conforme observado neste trabalho, a proteção jurídica de privacidade de determinada sociedade, reflete suas convenções sociais, cultura e até mesmo regras de etiqueta. As normas sobre perfil de crédito é mais um resultado da longa consolidação da privacidade na Europa. Observe-se que na Europa, historicamente, por uma questão de etiqueta, assuntos financeiros não são tratados publicamente, a não ser que seja absolutamente necessário. Na França, por exemplo, até pouco tempo atrás revelar o salário de alguém constituía hipótese *per se* de violação de privacidade. Embora não seja mais violação por si só, a lei francesa de privacidade lista entre os assuntos passíveis de violação de privacidade os referentes à saúde, amor sexo e ganhos.

[106] Apenas a título comparativo.

[107] WHITMAN, James Q. Op. cit.,p. 1191.

Outra diferença é o tratamento dado à privacidade de pessoas notáveis ou atividades realizadas em público, como se pode observar com a comparação entre o já analisado caso *Sipple v. Chronicle Publishing Co.* (1984), julgado nos Estados Unidos, e o caso *Hauch*, ocorrido na França. É preciso lembrar que, para a cultura norte-americana, a proteção da privacidade se dá de acordo com a expectativa razoável de privacidade, que é mais intensa no interior do lar ou de outros ambientes de natureza privada. Significa dizer que os atos realizados em ambiente público não estariam, a princípio, protegidos pela privacidade por não haver expectativa razoável de privacidade nestas situações, à exceção dos casos do direito de publicidade, pois o que se resguarda aqui é o aproveitamento econômico da exploração da imagem, e não a revelação de um fato privado desconhecido.

Pois bem. Em ambos os casos estava envolvida a divulgação pública da orientação sexual minoritária do retratado. O americano do caso *Sipple*, que havia ficado famoso por evitar o assassinato do Presidente Ford, teve sua orientação sexual divulgada e entendeu-se não haver, no caso, violação de privacidade, mas apenas o exercício da liberdade de imprensa, ao trazer ao público informações de alguém que havia se tornado notório. No caso francês, o indivíduo foi fotografado na Parada do Orgulho Gay de Paris, tendo esta imagem ilustrado uma reportagem. A jurisprudência francesa entendeu que a publicação violaria a sua privacidade, deferindo ao retratado o direito de impedi-la[108]. Isto porque entendeu-se que o fato de revelar sua orientação a um público restrito, a saber, a comunidade gay de Paris presente na Parada do Orgulho Gay, não implica perder a proteção de sua privacidade em relação a todo grande público que tem acesso ao noticiário. Ressalte-se que um dos fundamentos para se permitir a divulgação da orientação sexual no caso *Sipple* foi o fato de o herói instantâneo haver se envolvido em causas específicas e frequentar lugares típicos da comunidade gay.

Em relação ao direito de imagem, em ambos os sistemas jurídicos se permite a cessão dos direitos de imagem, mesmo em casos de nudez. No direito norte-americano, o *right of publicity* não impõe limite de conteúdos para a exploração do direito de imagem, assim como no direito europeu. Todavia, em se tratando de exposição em situação de indignidade, no direito europeu se admite a revogação dessa cessão de direitos quando a retratação, mesmo que consentida, ofenda a dignidade pessoal do titular.

É de se ver que a própria consagração do direito de exclusividade de decidir, por si só, sobre a própria imagem nu contrasta claramente com o prestígio que a cultura americana dá à

[108] CA Paris, le ch, June 14, 1985, D. 1986 inf. Rap. 50, note R. Lindom.

liberdade de imprensa, vez que a sua tarefa de noticiar permitiria a divulgação destas imagens sem nenhuma dúvida.

No caso europeu, em regra, se permite o controle da própria imagem em caso de nudez mesmo que seja captada em público, enquanto no direito norte-americano, permite-se, em geral, a livre divulgação de imagens de pessoas nuas na imprensa, sob o pálio da liberdade de expressão.

As ações referentes à divulgação de nudez pública na Alemanha[109] tem consagrado a ideia de que pessoas nuas tem o direito de controlar sua imagem pública e que o controle da imagem do corpo nu pertence exclusivamente ao seu dono. Na concepção alemã, tirar toda a roupa, mesmo em um local público não significa que se tenha renunciado à privacidade.

Pode-se entender que no direito continental em geral não é o fato de a nudez que é refutada, mas o de a própria pessoa controlar sob que circunstâncias as pessoas serão vistas nuas, ou seja, cabe exclusivamente ao indivíduo controlar a reprodução de sua figura nua, com base no direito à imagem.

No caso alemão de um homem nu em Englischer Garten, apenas foi mantida a publicação porque as genitálias do homem não foram expostas com base na máxima de que pessoas nuas tem o direito de controlar sua imagem pública, assim como as pessoas vestidas fazem. Segundo as boas maneiras alemãs, uma pessoa nua em público tem o direito de não ser encarada[110].

Trata-se, portanto, de uma espécie de nudez pública privada, ou seja, embora adotada em local público, contaria com a proteção da privacidade. Isso seria inconcebível para os americanos. Como visto neste trabalho, no caso *Vernonia School District 47J v. Acton*, a Suprema Corte, em 1995, entendeu possível obrigar atletas do ensino médio a serem compulsoriamente submetidos ao teste antidoping. Um dos argumentos foi de que atletas comumente tomavam banhos coletivos nus o que mostraria que eles teriam reduzido sua expectativa de privacidade, de modo que colher a urina para um teste não seria uma grande violação. A cultura americana resguarda a privacidade na lógica da proteção às quatro paredes do lar, de modo que se o indivíduo se mostra fora destes limites, abandona a proteção da casa e diminui sua expectativa de privacidade. Logo, a atitude do indivíduo influencia diretamente a aferição da expectativa de privacidade com a qual ele pode contar. Em outras palavras, se realiza um ato em público não deve ter nenhuma ou quase nenhuma expectativa de

[109] Em um caso houve a negativa de direito de imagem de quem praticava nudez em publico, em virtude de a genitália do retratado não ter sido exposto.

[110] WHITMAN, James Q. Op. cit., p. 1201.

privacidade. Por outro lado, para os europeus, mais especificamente para os alemães, o fato de se apresentar nu a um público restrito nada diz a respeito do restante da população, de modo que é passível de responsabilização a divulgação de fotografia na qual se possa identificar o indivíduo.

Estas comparações evidenciam bem a diferença entre tratar a privacidade como um aspecto da liberdade ou como um aspecto da dignidade. A lógica da expectativa razoável de privacidade da jurisprudência norte-americana se choca com a exclusividade do indivíduo em controlar sua imagem pública e, portanto, qualquer retratação que, de algum modo, o desabone ou que ofenda sua honra pessoal pode ser proibida.

O direito americano não impede nenhuma comercialização da imagem por mais humilhante que ela seja. Já o direito europeu entende que a venda da imagem de nudez do indivíduo é sempre anulável, protegendo o indivíduo de momentos de tolices da juventude, por exemplo.

1.2.1 O desenvolvimento da privacidade na França

Na França, a privacidade sempre foi uma preocupação dos membros das famílias de *status* elevado[111]. Todavia, é com o advento da modernidade, inaugurada pela Revolução Francesa, que se inicia a aspiração de proteger a privacidade para todos os cidadãos, independente da posição social que ocupe[112]. O advento da imprensa livre é um fator impulsionador da proteção da privacidade francesa, vez que os franceses, assim como europeus em geral, mostram-se apreensivos quanto aos riscos que a imprensa livre poderia simbolizar à preservação da vida privada, sob o viés da honra pessoal. Logo, a proteção constitucional da liberdade de imprensa veio acompanhada de proteção constitucional contra calúnias e insultos que ofendessem a vida privada[113].

Data do período da Restauração, no qual se aperfeiçoou a liberdade de imprensa, após o primeiro período napoleônico, a frase do filósofo e símbolo do liberalismo francês, Pierre-

---

[111] Mesmo antes da Revolução Francesa, famílias de status elevado sempre fizeram questão de proteger a própria privacidade. A título de exemplo, a nobreza francesa por vários séculos resistiu e lutou contra a obrigação de registrar as hipotecas sobre as suas propriedades, vez que isso poderia expor sua situação patrimonial publicamente.

[112] A Constituição revolucionária de 1791 trazia a proteção da honra do indivíduo contra calúnias que violassem a vida privada do indivíduo. Constituition du 3 septembre 1791, tit III, ch. V, art. 17 ("Les calomnies et injuries contre quelques persones que ce soit relatives aux actions de leus vie privée, seront punies sur leur poursuit").

[113] WHITMAN, James Q. Op. cit.,1173.

Paul Royer-Collard, o qual, mesmo defendendo a liberalização da imprensa, advertiu da necessidade de que a vida privada deve ser murada, o que se tornou um jargão na cultura europeia de privacidade[114]. Embora a afirmação de Royer-Collard tenha sido contundente, não se produziu uma legislação específica protegendo a honra pessoal, o que não significa dizer que a honra não era protegida. Para os franceses, costumava-se dizer que a honra deveria ser mais protegida que a própria vida[115]. Era culturalmente corrente que ataques à honra pessoal eram protegidos através do duelo direto[116].

Ao longo do tempo, enfraqueceu-se a cultura do duelo e passou-se a recorrer aos tribunais para a defesa da privacidade. O direito de privacidade concebido como o direito à própria imagem consagrou-se ao longo do século XIX, podendo-se citar casos em que se reafirmou esta concepção, como a retratação de celebridades ou pessoas notórias em seu leito de morte[117].

Na França, há o clássico caso de madame Moitessier de 1877, que, seguindo a moda da época, encomendou uma pintura na qual foi retratada nua[118]. Ocorre que, após a sua morte, o artista ofereceu sua foto à venda e foi processado pelo viúvo de Moitissier. O Tribunal

---

[114] O seguinte trecho dá a exata noção do que significa a proteção que se deve dar a vida privada, embora admitamos que atualmente o rigor em blindar totalmente a vida privada soe utópico na era da tecnologia de informação, em que pese seu valor doutrinário e histórico: "Si la notion de vie privée n'apparaît pas dans les termes de la loi, elle a été présentée dans la discussion, notamment dans un célèbre discours de Royer-Collard du 27 avril 1819. Pour mieux justifier l'admission de l'exception de vérité uniquement pour faits relatifs aux fonctions, Royer-Collard dit nettement qu'il « n'est pas permis de dire la vérité sur la vie privée ». C'est alors le célèbre passage de ce discours, « voilà donc la vie privée murée, et si je puis me servir de cette expression, elle est déclarée invisible, elle est renfermée dans l'intérieur des maisons ». La suite de l'argumentation est moins souvent citée : admettant cette protection de la vie privée comme un postulat, Royer-Collard se demande si la vie publique doit être murée de la même manière : il juge insoutenable l'idée que la « puissance publique » appartienne aux fonctionnaires (qui y verraient leur domaine, leur champ à labourer comme ils leur plairaient) et au contraire indispensable que la société connaisse la vérité sur les actions des agents de l'autorité (il ne faut pas attendre un délai pour rendre possible l'histoire, « il est dans les besoins de la nation que l'histoire commence pour nous chaque jour ») et de toutes les « personnes publiques » qui « sortent de la vie privée » et ne peuvent réclamer le « privilège » de l'absence d'exception de vérité, comme par exemple les députés". ARCHIVES PARLEMENTAIRES, 2e série, tome XXIV, p. 71-73, 27 avril 1819. Disponível em: <https://droitcultures.revues.org/3073#ftn17>. Acesso em: 22 jul. 2017.

[115] WHITMAN, James Q. Op. cit., 1174.

[116] Um caso que emblemático em que isso ocorreu foi o da duquesa de Berry. A duquesa era uma ativista política e objetivava que seu filho assumisse o trono. Após estar presa em 1833, constatou-se a sua gravidez mesmo estando viúva há alguns anos, o que a expôs a comentários maliciosos. A duquesa contou com a solidariedade de alguns e com o desprezo de outros, o que ocasionou inclusive um duelo entre o General Bugeaud que matou um membro da Câmara dos Deputados. Veja WHITMAN, James Q. Op. cit.,p. 1174, nota de rodapé 101.

[117] A título de exemplo, retratou-se em seu leito de morte uma famosa atriz dramática que ficou conhecida por sua beleza. Entendeu-se que a retratação violava o direito à própria imagem. (PATAILLE, J. Sargent c. Defonds, Trib. Civ. Seine. **Annales de la proprieté industrielle artistique et littéraile**, n. 1860, nov. 1859, *apud,* WHITMAN, James Q. Op. cit.,p. 1175).

[118] A bem da verdade, as senhoras daquela sociedade desejavam serem retratadas nuas, mas não aceitavam posar nuas diante do pintor, de modo que este contratava modelos e fazia montagens colocando sobre os corpos os rostos das clientes. Tratava-se de uma prática artística de luxo ser retratado nu.

entendeu que o autor tinha direito à privacidade, o que impunha limites ao direito de propriedade artística do pintor. Estabeleceu-se o princípio de que o indivíduo tem o direito sagrado e inalienável sobre si mesmo e, consequentemente, sobre a reprodução da sua imagem[119]. Esta lógica orientou o julgamento dos casos posteriores referentes ao direito de imagem.

Cite-se, ainda, o caso do pai do escritor Alexandre Dumas, que pousou voluntariamente para fotos obscenas para a época, em trajes íntimos, ao lado de uma famosa atriz com a qual se relacionava, em trajes seminus, e havia consentido em ceder onerosamente os direitos sobre a fotografia[120]. Pressionado pela família, resolveu processar o fotógrafo que havia adquirido os direitos. Todavia, a corte entendeu que, mesmo que o titular do direito tivesse consentido na publicação de fotos que lhe causem constrangimento, esse consentimento poderia ser revogado. Afirmou-se, ainda, que a mera publicação destas fotos pode fazer o indivíduo notar que "ele esqueceu de ter cuidado com a própria dignidade e lembrar que a vida privada deve ser murada no interesse do próprio indivíduo e também no interesse da boa moral"[121]. A corte definiu que a privacidade prevalece sobre os direitos de propriedade quando há imagens de lascívia envolvida, uma vez que a privacidade não seria uma *commodity* que pode ser simplesmente vendida. Qualquer venda neste sentido - de pessoa que tenha esquecido de resguardar sua dignidade - deve ser passível de anulação.

O julgado é criticável por variados ângulo e esta valorização da dignidade em detrimento da liberdade de mercado e do direito de propriedade se mostra incompatível com a cultura americana de privacidade e com o *right of publicity*. Embora se trate de caso julgado muito antes do tratamento da privacidade em solo americano, talvez nos dias atuais a solução fosse outra, fazendo-se a ressalva de se tratar do membro da família de um conhecido escritor. Ainda assim, para os padrões da época, a decisão de resguardar o indivíduo de seus próprios atos, adotados sem qualquer vício de vontade, mostra-se de algum modo paternalista até para os padrões ocidentais da época. Todavia, a decisão passou a constar como parâmetro de resolução de conflitos sobre direito de imagem envolvendo nudez na França o que deixa claro que, diferente da América, no embate entre liberdade de imprensa e dignidade, esta última tende a prevalecer.

---

[119] WHITMAN, James Q. Op. cit.,p. 1177.

[120] Ibidem, p. 1175-1176.

[121] Tradução livre. Dumas c. Lébert, CA Paris, May 25, 1867, 13 A.P.I.A.L. 247 (1867).

Pode parecer contraditório o aspecto moralista da jurisprudência francesa ao permitir a proibição de divulgação de fotos de nudez com a qual se consentiu, em uma sociedade cujo ambiente cultural parisiense é conhecido por sua liberalização sexual, o que só reforça a afirmação que, em matéria de privacidade, cabe ao indivíduo a definição da própria imagem pública.

1.2.2 O desenvolvimento da privacidade na Alemanha

No caso da Alemanha, a proteção à privacidade iniciou-se apenas no fim do século XIX. Não havia, naquele país, o ambiente propício das artes e da nudez, tanto nas pinturas quando na moda. Diferentemente da cultura francesa que herdou da privacidade pré moderna a proteção à honra pessoal dos nobres, o pensamento germânico deve ser entendido como uma tentativa de criar uma teoria alternativa à concepção de liberdade inglesa[122].

Não somente à privacidade, mas a toda cultura jurídica alemã se assenta na personalidade do indivíduo. Trata-se de um conceito denso que assenta raízes nas filosofias kantianas e hegeliana. A personalidade é entendida como um direito da liberdade, ou seja, do livre desenvolvimento das potencialidades da pessoa humana de forma autorresponsável. O raciocínio anglo-americano de liberdade pensa a privacidade sob a ótica da liberdade contra o arbítrio estatal e esta liberdade se consolida a partir da distribuição da propriedade de acordo com as regras do livre mercado. Por outro lado, para a cultura europeia e, especificamente, germânica, o Estado não é visto como um inimigo da privacidade. A personalidade não é abordada como necessária ao exercício das liberdades econômicas ou em face do Estado, mas contra qualquer ideia de determinismo do ser humano. É o exercício do livre-arbítrio e o desenvolvimento das potencialidades do ser humano que caracterizam a personalidade[123].

Assim como não é correto dizer que a cultura norte-americana não resguarda a dignidade do indivíduo em sua privacidade, não se pode dizer que a privacidade europeia continental não respeite ou desprestigie o exercício das liberdades econômicas. Toda generalização neste campo é incompleta. O que se pode afirmar com certeza é que a cultura europeia de privacidade é muito mais simpática ao exercício de uma regulação estatal do mercado e da liberdade de imprensa, haja vista que o Estado não é visto como algoz da liberdade.

---

[122] WHITMAN, James Q. Op. cit., *p.* 1180.

[123] Ibidem., p. 1182.

Partindo-se da filosofia neokantiana que aborda a tensão entre livre arbítrio e determinismo, compreende-se a teoria da personalidade como uma teoria da liberdade do indivíduo, de modo que a privacidade para os alemães é parte da livre autorrealização[124].

Além dos casos aqui já citados de proibição da retratação de nudez em público enquanto manifestação do direito de controlar a própria imagem pública, cite-se o caso de proibição de distribuição da foto de Otto won Bismarck em seu leito de morte, que influenciou a inclusão, em 1907, de normas de proteção à imagem como parte de um esquema que regulava os direitos dos profissionais de arte. Ademais, no Código Civil alemão de 1900 foram incluídas proteções contra a apropriação do nome e do direito de crédito do indivíduo, além de previsões de proteção da vida, do corpo, da saúde e da liberdade[125].

Em que pese não poder se falar em cultura mais ou menos protetiva da privacidade, pode-se perceber a diferença de fundamentos e objeto de preocupação da cultura de privacidade europeia continental e norte-americana.

A importância desta compreensão orientará a investigação da possibilidade em se definir o conteúdo jurídico da cultura de privacidade brasileira, a partir da verificação das influências recebidas e dos modos culturais aqui consagrados.

Diferentemente do que se possa pensar, a cultura brasileira apresenta incongruências e contradições que não a permitem identificá-la nem com o sistema europeu, nem com sistema norte-americano. Isto porque o país que exibe corpos seminus no carnaval durante as folias carnavalescas, também apresenta um viés extremamente conservador no que tange à liberdade de orientação sexual, tendo sido objeto de intensa disputa a possibilidade de união civil entre pessoas do mesmo sexo. Deste modo, apenas em 2011 o Supremo Tribunal Federal enfrentou a questão, conferindo reconhecimento das uniões homoafetivas, não sem alguma insistente resistência do legislativo[126].

Da mesma forma, embora de maioria ainda cristã católica e tendo a laicidade estatal reafirmada no texto constitucional, não se pode dizer com certeza que haja uma cultura de laicidade ou mesmo que se permita às mulheres a autodeterminação quanto ao exercício do direito sobre o próprio corpo para a prática do aborto, quando a atual legislatura visa restringir as possibilidades de interrupção voluntária da gravidez. É certo que há uma distorção da

---

[124] Ibidem.

[125] Vide §§ 12; 824, par. 1; 823, par. 1 do Código Civil Alemão de 1900.

[126] BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 4277-DF*. Tribunal Pleno. Relator Ministro Ayres Britto. Julg. 05 mai. 2011. ***DJe***13 out. 2011; BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 132-RJ*. Tribunal Pleno. Relator. Min. Ayres Britto. Julg. 05 mai. 2011. ***DJe*** 13 out. 2011.

representatividade popular no legislativo, mas também é certo que os poucos avanços que se obteve na autonomia e dignidade da mulher ocorreram pela jurisprudência corajosa e progressista da Suprema Corte, ao permitir a interrupção da gestação do feto anencefálico[127].

Portanto, a cultura de praias e os corpos expostos no verão durante o carnaval ocultam um conservadorismo que pouco zelam pela autonomia e dignidade da pessoa humana nos aspectos inerentes à privacidade, podendo-se arriscar que, embora previstas algumas garantias constitucionais e legais em matéria de privacidade, o caldo cultural que condiciona a jurisprudência brasileira estaria a alguma distância dos patamares norte-americanos e europeus. Por uma questão de justiça, há que se apontar que, em geral, a jurisprudência dos tribunais superiores pátrios costuma ser mais progressista e arrojada que os tribunais ordinários. Todavia, ainda há muito o que evoluir na cultura jurídica de privacidade brasileira.

1.3**Direito à Privacidade: Breves Apontamentos sobre a Construção Doutrinária**

Cumpre, neste item, analisar as principais construções doutrinárias acerca da privacidade construídas até aqui. Com efeito, é inegável a natureza de direito fundamental do direito à privacidade. Não só por sua localização topográfica no elenco de direitos e garantias fundamentais na Constituição brasileira[128], mas pela própria natureza do direito em si. Não satisfeito em prever de forma ampla a proteção da intimidade e da vida privada que, como se verá são âmbitos de proteção da privacidade, o constituinte de 1988 desceu a minúcias necessárias e no mesmo catálogo protegeu o espaço físico privado (a casa), bem como as comunicações telefônicas, telegráficas e de dados.

Isto porque, como já dito, ninguém que é vigiado e tem seus hábitos e atitudes mais íntimas tornadas públicas indevidamente pode dizer que possui plena autonomia para desenvolver a própria personalidade. Disto se dizer que a privacidade é condição essencial à

---

[127] BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 54*. Tribunal Pleno. Relator Min. Marco Aurélio. Julg. 12 abr. 2012. ***DJe*** 29 abr. 2013.

[128]Art. 5º "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;".

liberdade e ao exercício da democracia[129]. Classicamente, a privacidade garante ao indivíduo um espaço intangível ao escrutínio público, onde a exposição de fatos privados que digam respeito apenas ao indivíduo somente possam ser compartilhados mediante consentimento, distinguindo-se as esferas do espaço público e privado.

Em outras palavras, a privacidade possui também caráter instrumental, na medida em que a proteção de certas ações do indivíduo do escrutínio público o permitem ser com mais liberdade quem de fato deseja ser[130], fortalecendo seus vínculos familiares, afetivos, sexuais e ideológicos, sem que suas escolhas sejam objeto de ridicularização ou exposição públicas.

Com efeito, esse caráter instrumental da privacidade, na visão de Alan Westin, revela suas quatro funções básicas: a garantia da autonomia pessoal, do relaxamento emocional, da autoavaliação e da proteção às comunicações privadas[131]. A mais interessante destas funções é a garantida da autonomia pessoal, ou seja, é fundamento das sociedades democráticas a crença no indivíduo e a preservação desta individualidade. A preservação da individualidade como já dito é essencial à proteção da autonomia privada, vez que quem não possui seu espaço intangível de pensamentos, opiniões e atitudes preservado não poderá manifestar com a devida liberdade a pessoa que é[132].

Nesta linha, a privacidade, enquanto direito fundamental, relaciona-se diretamente à dignidade humana, especialmente em relação aos seus elementos de autonomia[133] e valor

---

[129] WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 1967.

[130] "When we protect privacy, we protect against disruptive to certain activities. A privacy invasion interferes with the integrity of certain activities and even destroys or inhibits some activities". Em tradução livre: "Quando protegemos a privacidade, protegemos contra o rompimento de algumas atividades. A invasão de privacidade interfere na integridade da realização de certas atividades e até mesmo a destrói ou inibe seu exercício" SOLOVE, Daniel J. Conceptualizing Privacy. In: CANNATACI, Joseph A. (Ed.). **The Individual and Privacy**. V. I. London and New York: Routledge, 2015.

[131] O que foi livremente traduzido como relaxamento emocional (*emotional release*) diz respeito ao estresse psicológico causado pela necessidade de desempenhar variados papeis sociais, cumprindo normas sociais e de etiqueta que na visão do autor aprisionam o indivíduo e em seu espaço de intimidade o indivíduo pode ser quem ele realmente é. A autoavaliação é o momento no qual o indivíduo precisa realizar um inventário moral de si mesmo, refletir autonomamente sobre suas próprias questões sem intromissões de terceiros, o que somente seria permitido com a garantia da privacidade. Por fim, a proteção às comunicações privadas permite ao indivíduo dizer realmente o que pensa e sente e desenvolver sua personalidade, sem a preocupação de estar sendo julgado. WESTIN, Alan. Op. cit., p. 25-56. Particularmente, discorda-se parcialmente do elemento *emotional release*. De fato, o ser humano é pressionado pelos papeis sociais que desempenha. Todavia, com a vida mais intermediada eletronicamente pelas redes sociais, os diferentes papeis desempenhados são integrados em um só, mostrando-se de certo modo inviável viver através de diferentes personagens. Deste modo, sem ignorar a necessidade de um relaxamento emocional, o âmbito privado foi por muito tempo o escudo para perpetramento de abusos e relações de subordinação sem interferências externas, de modo que não é nesse sentido que deve ser interpretado este elemento da privacidade.

[132] WESTIN, Alan. Op. cit., p. 28.

[133] Com vistas a dar à dignidade humana um sentido mínimo universalízável, *aplicável a qualquer ser humano, onde quer que se encontre*, Luís Roberto Barroso elenca três conteúdos essenciais da dignidade. São eles: valor

intrínseco[134]. Ora, se a pessoa humana tem valor por si só e constitui um fim em si mesmo, não podendo ser instrumentalizada para fins coletivos, a garantia de sua privacidade previne tais instrumentalizações, ao preservar um espaço decisório mínimo ao indivíduo no que tange aos seus afetos, hábitos, vínculos pessoais, visão política e procedimentos médicos que digam respeito à própria pessoa, independentemente de aspirações coletivas.

É sempre difícil conceituar a privacidade, pois, como já visto, o conceito de privacidade é variável ao longo do tempo e é fortemente influenciado pela cultura em determinada sociedade[135]. Para Westin, a privacidade é uma reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como, onde e em que extensão a informação sobre si é transmitida a outros[136].

Westin, que alertava sobre o risco decorrente do advento das tecnologias de informação e com a vigilância estatal e seus impactos no regime democrático deve ser reconhecido pela abordagem visionária de sua obra. Todavia, em que pese a transmissão de dados pessoais merecer preocupação, assim como suas implicações na noção de privacidade, o conceito de privacidade sofre modulagens causadas pela própria alteração das relações sociais, principalmente após o crescimento das relações intermediadas eletronicamente. Conforme se verá, no contexto de processamento massivo de dados que caracteriza o *big data*, talvez não seja mais possível, pelas circunstâncias fáticas, se exigir o consentimento para cada compartilhamento de dado realizado, haja vista que o grande valor atribuído aos

---

intrínseco, autonomia e valor social da pessoa humana. A autonomia é o elemento ético da dignidade, ligado à razão e ao exercício da própria vontade. A dignidade enquanto autonomia envolve tanto a capacidade de autodeterminação, ligada à autonomia privada, ou seja, de decidir o próprio rumo e desenvolver livremente sua personalidade, bem como a autonomia pública, ligado ao exercício da participação política no processo democrático. O autor inclui ainda o mínimo existencial como elemento essencial ao exercício das autonomias privadas e públicas. BARROSO, Luís Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo - natureza jurídica, conteúdos mínimos e critérios de aplicação. In: _____. **O novo direito constitucional brasileiro**: contribuições para a construção teórica e prática da jurisdição constitucional no Brasil. Belo Horizonte: Fórum, 2013,p. 307-313.

[134] Ainda segundo Luís Roberto Barroso, o valor intrínseco da pessoa humana, enquanto elemento ontológico da dignidade, é ligado a natureza do ser, ao que é comum e inerente a todos os seres humanos, independente das circunstâncias pessoais de cada um. Da dignidade enquanto valor intrínseco decorrem dois postulados, um deles de ordem antiutilitarista - derivado do imperativo categórico kantiano - segundo o qual o homem é um fim em si mesmo e não um meio para a realização de metas coletivas ou projetos sociais de outros; o outro postulado, de ordem antiautoritária assenta-se na ideia de que o Estado existe para o indivíduo e não o contrário. BARROSO, Luís Roberto. Op. cit., p. 307 a 313.

[135] O exemplo dado por James Whitman para ilustrar essa variação são as ruínas de Éfeso, que possuíam latrinas coletivas no espaço público, o que demonstra que para aquela cultura, o hábito de usar o toalhete não era aspecto inerente à noção de privacidade ou a privacidade é uma noção burguesa datada que floresceu no final do século XIX que não era cultuada na história antiga. WHITMAN, James Q. Op. cit., p. 1154.

[136] Tradução livre do trecho: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". WESTIN, Alan. Op. cit., p. 5.

dados não é o seu valor de face, mas sua utilização secundária, em finalidades que não poderiam ter sido previstas inicialmente.

Pode-se citar, ainda, a doutrina francesa que enumera oito temas como abrangidos pelo conceito de vida privada, que são: vida sentimental, conjugal e familiar, além do direito ao nome, à saúde - incluindo informações sobre a causa da morte -, eventos familiares, emoções, lazer, opiniões políticas, filosóficas e religiosas, além de patrimônio[137].

Quando se trata a privacidade com a utilização de termos distintos, tais como vida privada ou intimidade, surge a indagação se há diferenças entre estes termos e se há uma proteção jurídica diferenciada para cada uma dessas esferas, não sendo incomum a categorização doutrinária dos graus de privacidade de acordo com a esfera envolvida[138]. O próprio texto constitucional, em seu artigo 5º, inciso X, diferencia a proteção contra a inviolabilidade da intimidade e da vida privada[139], distinção essa que deriva da construção alemã dos círculos de privacidade.

A doutrina alemã desenvolveu, no século XX, a teoria dos círculos concêntricos, segundo a qual haveria níveis diferentes de proteção à privacidade, partindo-se do círculo mais externo, de menor proteção, ao mais interno, cuja proteção é mais reforçada. A teoria das esferas que mais teve recepção no Brasil comportaria basicamente três círculos

---

[137] Ana Paula de Barcellos se baseia na obra de HURTAUD, M. H. La protection de la vie privé- note sur l'article 9 du Code Civil, 1997,para traçar o panorama da privacidade no direito francês.BARCELLOS, Ana Paula de. Intimidade e pessoas notórias. Liberdades de expressão e informação e biografias. Conflito entre direitos fundamentais. Ponderação, caso concreto e acesso à justiça. Tutelas específica e indenizatória. **Migalhas**, 2014, p. 5. Disponível em: <http://www.migalhas.com.br/arquivos/2014/5/art20140522-01.pdf>. Acesso em: 20 dez. 2017.

[138] Para abordagem do direito à privacidade neste tópico, baseamos este artigo nas pesquisas de BARCELLOS, Ana Paula de. Intimidade e pessoas notórias. Liberdades de expressão e informação e biografias. Conflito entre direitos fundamentais. Ponderação, caso concreto e acesso à justiça. Tutelas específica e indenizatória. **Migalhas**, 2014. Disponível em: <http://www.migalhas.com.br/arquivos/2014/5/art20140522-01.pdf>. Acesso em: 20 dez. 2017.

[139] Para Paulo José da Costa Junior, a diferença entre vida privada e intimidade constitui-se basicamente no grau de interesse protegido, de acordo com a modalidade de agressão. A vida privada seria agredida com a mera invasão, uma intromissão não autorizada. A outra violação possível ocorreria com a indevida divulgação dos fatos privados. Para o autor não haveria distinção substancial entre vida privada e intimidade, apenas formas distintas de violação a um interesse protegido podendo-se denominar ambos os interesses de direito à intimidade, sendo as duas manifestações momentos distintos do mesmo direito, mas sem qualquer distinção de conteúdo. (COSTA JR., Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Editora Revista dos Tribunais, 1995, p. 32-35). Particularmente discordando da visão do autor e nos alinhamos ao texto constitucional que entende serem diferentes as tutelas da vida privada e da intimidade, a considerar que o constituinte não teria utilizado dois termos distintos no mesmo dispositivo para tratar do mesmo direito. Embora sejam aspectos decorrentes do direito fundamental à privacidade, intimidade e vida privada são diferenciáveis e tutelam interesses diversos, sendo adequada a teoria alemã dos círculos concêntricos.

concêntricos[140], e, quanto mais internos os círculos, maior o nível de proteção oferecido, a saber, vida privada, intimidade e segredo.

Com efeito, a esfera privada seria representada pelo círculo mais externo e neste círculo estariam os comportamentos e acontecimentos que o indivíduo não deseja que se tornem de domínio público, tais como informações patrimoniais, financeiras e fiscais, bem como o registro das comunicações. Esse círculo inclui as relações interpessoais com familiares, amigos, conhecidos e colegas de trabalho[141]. O âmbito de proteção da esfera privada ou vida privada é concebido em oposição à esfera pública, esta última caracterizada por comportamentos e informações acessíveis licitamente a toda coletividade, adotadas no espaço público[142].

No círculo intermediárioestaria a intimidade, que seria o espaço próprio dos sigilos familiar, profissional, doméstico e do conteúdo das comunicações. O terceiro e mais interno círculo, o segredo, comportaria as informações e relações mais íntimas do indivíduo sobre seu corpo, sua vida sexual e relações afetivas próximas[143].

Mais recentemente, tendo em vista a complexidade das relações humanas na chamada sociedade de informação, a doutrina tem observado a ampliação dos objetos próprios do direito de privacidade, passando-se a tratar da privacidade de dados sobre o indivíduo, principalmente na internet, protegendo-se não só a pessoa física, mas a pessoa digital[144]. Neste sentido, recorre-se novamente ao magistério de Stefano Rodotá, para quem a privacidade se constitui no direito à autonomia informativa de controlar os próprios dados[145]. Para tanto, deveria ser observado o necessário consentimento do indivíduo para coleta e

---

[140] Paulo José da Costa Júnior adota a teoria tríplice das esferas, baseado em Henkel (HENKEL, *Der Strafchutz des Privatebens gegen Indiskretion, in Verhandlungen des 42. Deutschen Juristentages.* – em tradução livre O direito penal da vida privada contra a indiscrição, nas negociações do 42º dia dos advogados alemães. Dusseldorf*:* 1957 *apud* COSTA JR., Paulo José da. Op cit, p. 36). Todavia, a concepção também alemã de Mans Heinrich Maass, apresenta em sua obra seis esferas gradativas de proteção à privacidade, quais sejam, esfera íntima; esfera própria; esfera de confiança, esfera privada, esfera social e esfera pública. A parte de entender inadequado incluir a esfera pública entre as esferas de proteção à privacidade, o próprio autor da concepção restringe sua classificação para as esferas íntimas e privadas, em oposição à esfera pública. Não é objeto deste trabalho revisitar a teoria alemão dos círculos concêntricos, fazendo-se apenas este adendo para fins de registro. Fato é que a divisão tripartite é a que mais contou com adeptos na doutrina brasileira (GIANNOTTI, Edoardo. Op. cit., p. 26).

[141] Ibidem.

[142] COSTA JR., Paulo José da. Op cit, p. 36.

[143] Ibidem, p. 32-35; FROTA, Hidemberg Alves da. A proteção da vida privada, da intimidade e do segredo no direito brasileiro e comparado. **Revista Jurídica da UNIJUS**, v. 29, n. 11, p. 79, 2006.

[144] SOLOVE, Daniel J. **The Digital Person**:… Op. cit.

[145] RODOTÁ, Stefano. Op. cit., p. 59.

tratamento destes dados, bem como a observância da finalidade para a qual os dados foram fornecidos, entre alguns princípios que protegem os dados pessoais.

Todavia, para o autor, a ótica da proteção à privacidade na sociedade de vigilância não se dá sob o aspecto individualista, o que seria ineficiente no contexto do processamento massivo de dados. Não se pode manter a privacidade aprisionada à sua origem patrimonial, que assenta raízes na doutrina norte-americana, como se a privacidade fosse mais um elemento do patrimônio privado do indivíduo. A tutela individuada da privacidade enfraquece seu poder reivindicatório, especialmente diante de poderosas corporações globais privadas. Logo, o que se propõe é que também se observe a dimensão coletiva da proteção à privacidade, com vistas a torná-la mais eficiente. Mecanismos individualizados de proteção de dados não estão devidamente preparados para os desafios do processamento coletivizado e massivo de dados[146].

Já verificamos neste trabalho que é do direito americano a consagração da teoria dos quatro testes da privacidade, desenvolvidas por William Prosser e amplamente tratados em tópico anterior[147]. Mesmo se considerando as variações da noção de privacidade em decorrência das diversidades culturais e temporais, persiste a dificuldade em se definir um conceito confortável de privacidade. Isto porque a privacidade engloba multifárias manifestações, o que dificulta a definição de um denominador comum a todas essas hipóteses[148]. Ao se afirmar que se teve violada a privacidade, pode se estar falando do direito às informações sobre a própria saúde, o direito de não ser perturbado em seu recolhimento, o controle sobre os dados pessoais, a liberdade de não ser objeto de vigilância ou de buscas sem razão legal que o justifique, entre outros.

Esses múltiplos interesses fazem da privacidade um conceito difícil de se definir por sua natureza vaga e evasiva[149] que pode englobar vários interesses e ao mesmo tempo não significar nada. Para Robert Post, a privacidade é um valor complexo, envolvido em dimensões contraditórias e concorrentes, com vários e distintos significados, o que dificulta a elaboração de um conceito útil que abranja todas as suas hipóteses[150].

---

[146] Ibidem, p. 37.

[147] Vide item 1.1.2. Os quatro testes são: (i) de intrusão na reclusão ou solidão do indivíduo ou em seus assuntos privados; (ii) exposição pública de fatos privados embaraçosos acerca do indivíduo; (iii) exposição pública do indivíduo de forma distorcida; e (iv) apropriação do nome ou de dados do indivíduo para proveito próprio.

[148] SOLOVE, Daniel J. Conceptualizing Privacy. Op. cit.

[149] MILLER, Arthur. Assault on privacy, 1972,p. 25 *apud* SOLOVE, Daniel J. Op. cit.

[150] "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether in can be usefully addressed at all." POST,

A dificuldade em definir um conceito abstrato, abrangente e que expresse um denominador mínimo da privacidade se demonstra nas concepções mais consagradas, de modo que não se pode dizer que a privacidade possa ser suficientemente definida como o direito a ser deixado só, especialmente na sociedade da informação, não sendo este suficiente a explicitar em que hipóteses pode-se exigir ser deixado só.

Outra concepção, a privacidade como segredo, pode apresentar falhas, na medida em que determinadas informações, mesmo que alguma vez divulgada, continuam constituindo elementos da privacidade, além de desconsiderar que há uma diferença entre assuntos de natureza privada e secreta[151]. Mais adequado seria adotar a noção de graus de privacidade, vez que há informações que, por sua própria natureza, merecem uma proteção maior que outras mais corriqueiras. Exigir segredo total e absoluto para tudo que diga respeito à privacidade, além de ineficaz pode ser pouco factível.

Diante dessas dificuldades, há autores que preferem abordar a definição de privacidade não por meio de conceitos abstratos e parciais, mas defini-la através de suas classificações, de sua taxonomia. É o caso de Daniel Solove para quem a vagueza da concepção da privacidade é melhor definida de baixo para cima, dos casos concretos para a abstração[152]. Não que qualquer conceito, que contenha a pretensão de englobar o ponto comum de variadas situações, não tenha algum grau de abstração. Todavia, no caso do autor, o caminho é o inverso. Propõe-se ainda que se abandone o modo tradicional se elaborar uma concepção com base nas semelhanças, uma vez que a privacidade consiste em situações muito diferentes, mas relacionadas[153].

Desta forma, a conceituação da privacidade através do modelo taxonómico divide as formas de violação da privacidade em quatro grandes grupos, quais sejam: (i) coleta de informações, que inclui vigilância e interrogatório; (ii) processamento de informações, que inclui agregação, identificação, falha de segurança, uso secundário e exclusão; (iii) disseminação de informações que pode ocorrer através da quebra de confidencialidade, da

---

Robert C. The Concepts of Privacy. **Georgetown Law Journal**, v. 89, p. 2087, 1967 *apud* SOLOVE, Daniel J. Op. cit.

[151] SOLOVE, Daniel J. Conceptualizing Privacy. Op. cit.

[152] Além da generalidade e do método de não buscar características comuns, outros critérios também utilizados pelo autor são: a variabilidade – ou seja, a consideração das variações da privacidade em cada cultura, evitando-se a elaboração de um conceito contingencial e o foco, o que significa desvendar a complexidade da privacidade, evitando-se um conceito difuso e discordante. O foco se dá antes nos problemas da privacidade do que na busca do seu conceito. SOLOVE, Daniel J. Conceptualizing Privacy Op. cit.,p. 14-15.

[153] Ibidem, p. 9.

divulgação, da exposição, da facilitação do acesso, da chantagem, da apropriação ou da distorção; e (iv) invasão que pode ocorrer através da intrusão ou da interferência decisional[154].

Não obstante reconhecer a devida importância da classificação taxonômica de Solove e sua abordagem concreta das questões da privacidade, sua obra não se diferencia substancialmente de outras obras que abordam os problemas contemporâneos da privacidade, especialmente no ambiente digital. De fato, a ambiguidade que caracteriza o conteúdo múltiplo e variado do que venha a ser privacidade, sendo um verdadeiro conceito guarda-chuva que alberga as mais diversas hipóteses de proteção, dificulta qualquer tentativa de conceituá-la. Todavia, qualquer definição, por mais analítica que seja, será sempre contingencial, historicamente localizada e parcial.

Ainda assim, com todas essas limitações faz-se necessária uma sistematização do conceito de privacidade através de seus elementos comuns, a despeito de todas as limitações e falibilidades que esta tentativa pode enfrentar. A noção geral do que significa determinado direito, facilita a definição do seu âmbito de proteção, orienta legisladores na criação de leis, bem como governantes na sua conduta, tanto abstendo-se de violar quaisquer de seus aspectos, bem como na implementação de prestações positivas que promovam o direito.

Deste modo, a despeito da importância de se ter em mente a resolução das questões concretas da privacidade, não é menos importante um conceito que consiga aglutinar essas questões relevantes cuja compreensão seja razoavelmente alcançada. Não se pode negar que, assim como o conceito de determinado direito sofre mutações impulsionados justamente pelas questões que visa resolver, tais questões são melhores resolvidas se estudadas de forma que sejam englobadas por uma linha mestra que apresente seus pontos comuns, consolidadas em uma definição que seja abstrata o suficiente para fazer se compreender do que se trata determinado direito.

Neste trabalho, defende-se como melhor abordagem de privacidade a teoria cuja gênese se dá no direito jurisprudencial norte-americano, consagrada no caso *Katz v. United States*[155], que define a privacidade a ser protegida como aquela que envolve uma expectativa razoável de privacidade, ou seja, deve-se verificar, no caso concreto, se as circunstâncias e as normas sociais propiciavam ao indivíduo uma expectativa razoável de privacidade. Neste sentido, em regra, não se pode invocar a privacidade para manter em segredo ato realizado em

---

[154] Não cabe aqui entrar nos pormenores da teoria de Daniel Solove, vez que este é o cerne de sua obra e é desenvolvido por todo um capítulo. Para mais detalhes, vide SOLOVE, Daniel J. Conceptualizing Privacy. Op. cit., p. 101-170.

[155] *Katz v. United States* (389 U.S. 347 (1967), tratado no tópico 1.1.3.

praça pública, assim como não se pode negar privacidade aos atos cometidos na esfera íntima do leito conjugal.

A concepção pode parecer casuística e subjetivista, na medida que outorga ao indivíduo a expectativa da própria privacidade. Mas não é exatamente isso que se deseja defender. Defende-se que a expectativa de privacidade seja uma construção intersubjetiva, ou seja, o que razoavelmente pode-se conceber como inerente ao direito fundamental à privacidade em determinado o contexto histórico e geográfico, sem que se perca de vista os elementos da dignidade da pessoa humana, entre os quais o seu valor intrínseco e autonomia[156].

Não se trata, portanto, de defender um âmbito de proteção formal do direito à privacidade, ou seja, proteger tudo que a pessoa decide excluir do conhecimento alheio. Trata-se de adotar a expectativa razoável de privacidade como um conceito material, ou seja, o âmbito de proteção do direito fundamental à privacidade inclui toda informaçãoque, de acordo com as *pautas sociais vigentes*[157], é entendida como indisponível ao interesse do Estado ou curiosidade de terceiros.

A concepção de privacidade, a partir da expectativa razoável de privacidade aqui defendida, não se vincularia aos limites físicos do conceito jurídico de domicílio, mas se relacionaria com a expectativa média de privacidade em determinada cultura. Por exemplo, pode ser que o brasileiro tenha menos expectativa de privacidade em uma praia que um alemão que resolva praticar nudismo coletivo em parques públicos, para protestar por determinada causa.

A concepção proposta será construída também a partir do princípio da proporcionalidade, de modo que, o âmbito de proteção à privacidade será definido, no caso concreto, quando estiver em conflito com outros direitos fundamentais ou interesses constitucionais.

Conforme se vê, muito se evoluiu da concepção de privacidade tão somente enquanto direito a ser deixado só, ou seja, direito a não ser escrutinado em sua reclusão, conforme pregado por Warren e Brandeis.

---

[156] Embora tenha se optado pela definição de dignidade humana elaborada pelo professor Luís Roberto Barroso neste tópico, apenas para fins de justificar e concepção que se entende mais adequada de privacidade, deve-se noticiar que Daniel Sarmento apresenta uma relação mais ampla de elementos integrantes da dignidade humana, quais sejam: valor intrínseco da pessoa, igualdade, autonomia, mínimo existencial e reconhecimento. Vide SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetória e metodologia. Belo Horizonte: Fórum, 2016, p. 92.

[157] O termo é cunhado por Ingo Sarlet. SARLET, Ingo; MARINONI, Luiz Guilherme; MITIDIERO, Daniel *et al*. Curso de Direito Constitucional. 5. ed. rev. e atual. São Paulo: Saraiva, 2016. *p.* 446

Apontadas de forma breve as premissas básicas do direito à privacidade, cabe prosseguir na análise concreta da legislação nacional e estrangeira acerca do tema.

1.3.1 Marco legal da privacidade: dos tratados internacionais à Constituição brasileira

A privacidade conta com a proteção de inúmeros tratados de direitos humanos, bem como de constituições, como é o exemplo da Constituição brasileira de 1988.

A Declaração Universal dos Direitos Humanos, da Organização das Nações Unidas, de 1948, prevê em seu artigo XII o direito à privacidade em sua concepção mais clássica[158]. Isso porque a concepção clássica do direito à privacidade a identifica com o direito a ser deixado só, ao direito a estar em sua reclusão sem ser devassado de forma injustificada. Deste modo, a vida privada do indivíduo identifica-se com as atividades realizadas no âmbito do lar, espaço privado por excelência, no sigilo das comunicações, bem como pela inviolabilidade da honra e da reputação, predicados esses que podem ser arranhados caso haja uma indevida exposição da vida privada do indivíduo.

Por óbvio que o conceito de privacidade se sofisticou ao longo do tempo[159] e a complexidade da vida moderna não mais permite uma proteção absoluta à inviolabilidade das atividades no âmbito familiar. Isto porque mesmo nas atividades que à primeira vista seriam inerentes à vida privada pode haver algum interesse público. Isto ocorre, por exemplo, no caso em que um conhecido político tem por padrinho de casamento um empresário que coincidentemente é agraciado com benesses estatais por decisão do referido político. Ora, embora as relações afetivas e familiares sejam o núcleo definidor da intimidade do indivíduo, aspetos da vida íntima do indivíduo que tenham evidente repercussão na sua atividade pública[160] contam com a legítima necessidade de informação da sociedade.

---

[158] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Artigo XII: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

[159] Embora se possa afirmar que os argumentos acerca da inviolabilidade da privacidade tenham se sofisticado, no clássico artigo de Warren e Brandeis, os autores faziam a ressalva que as informações de interesse público não estariam protegidas pela privacidade, podendo-se destacar o seguinte trecho: "Há pessoas que podem razoavelmente reivindicar como um direito, a proteção em face da notoriedade ocasionada por ter sido vítima da iniciativa jornalística. Há outros que, em variados graus, renunciaram o direito de viver suas vidas protegidos da observação pública" (tradução livre) WARREN, Samuel; BRANDEIS, Louis. Op. cit., p. 193 e ss.

[160] "É certo que, dependendo de suas opções pessoais, o âmbito de proteção da intimidade e da vida privada de um indivíduo será menor que o dos outros (…) Nem tudo na vida desses indivíduos está relacionado à atividade que lhes dá notoriedade e não se trata de uma troca: os proveitos da fama em troca de seus segredos mais íntimos". BARCELLOS, Ana Paula de. Op. cit., p. 12.

Desta forma, não se trata da mera e vil curiosidade - a existência de curiosidade por si só não pode ser fundamento à violação da privacidade, tampouco o fato de não ter nada a esconder[161]. Trata-se, por outro lado, de inegável vínculo entre as atividades de âmbito privado e familiar e as de natureza pública.

No sistema europeu, a legislação de proteção à privacidade é difundida em inúmeros documentos, apresentando interessante gradação evolutiva. Um exemplo disso é a Carta de Direitos Fundamentais da União Europeia, que elenca entre as liberdades o respeito pela vida privada e familiar, bem como ao domicílio e às comunicações[162].

Verifica-se que a mesma carta, em artigos diferentes, regulamenta a proteção de dados pessoais. Isso coloca em oposição dois aspectos marcadamente inerentes à privacidade. De um lado, o artigo 7º traz a proteção à privacidade enquanto sua concepção clássica, a saber, o respeito à vida privada e familiar ao domicílio e às comunicações.

Tecnicamente, consoante visto anteriormente, de acordo com a teoria dos círculos concêntricos, respeito à vida privada seria o âmbito mais externo de proteção à privacidade e englobaria as relações patrimoniais, financeiras e fiscais do indivíduo, bem como o registro das comunicações. Já a vida familiar, o domicílio e as comunicações estariam no círculo intermediário de proteção à privacidade, a não ser no que tange às relações de afeto ou sexual mais íntimas que estariam no círculo mais interior da privacidade denominado segredo[163].

Além dos elementos clássicos do direito à privacidade desde sua consagração, o artigo 8º da Carta de Direitos Fundamentais europeia vai além e busca proteger a pessoa digital, ou seja, o conjunto de dados que são coletados rotineiramente sobre o indivíduo na sociedade da informação. Esta proteção à privacidade na esfera digital garante a chamada autonomia informativa, ou seja, a liberdade de controlar o conteúdo dos próprios dados[164].

---

[161] SOLOVE, Daniel J. **Nothing to Hide**: The false tradeoff between privacy and security. New Haven: Yale University Press, 2013.

[162]CAPÍTULO II LIBERDADES

Artigo 6º - Direito à liberdade e à segurança. Todas as pessoas têm direito à liberdade e à segurança.

Artigo 7º - Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8º - Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[163] BARCELLOS, Ana Paula de. Op. cit.

[164] RODOTÁ, Stefano. Op. cit., p. 59.

Inicialmente, o primeiro item do art. 8º garante a proteção geral aos dados pessoais. Em seguida o segundo item do artigo é mais específico ao trazer diretrizes a serem seguidas no tratamento de dados. Primeiro, o dispositivo impõe um "tratamento leal", ou seja, a observância de parâmetros éticos, da fidedignidade e veracidade da informação no tratamento desses dados. Aqui se aplica o princípio da *correção* na coleta e tratamento das informações, bem como o princípio da *exatidão* dos dados coletados, elencados por Stefano Rodotà entre os princípios gerais da disciplina jurídica da proteção de dados[165].

O item impõe, ainda, que esses dados sejam utilizados para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Portanto, este mesmo dispositivo abrange outros princípios aplicáveis à proteção de dados, qual seja, o da *finalidade*, ou seja, a coleta de dados deve ter finalidade específica.Ainda de acordo com esse princípio, a finalidade da coleta de dados deve poder ser conhecida antes que ocorra a coleta. O princípio da finalidade se especifica no princípio da *pertinência*, que nada mais é que a correta relação entre os dados colhidos e a finalidade perseguida. Desdobra-se também no princípio da *utilização não abusiva* que pode ser definido como a relação existente entre a utilização dos dados e a finalidade para a qual foram colhidos. Um último e não menos importante desdobramento do princípio da finalidade é o princípio do *direito ao esquecimento*[166], que consiste na eliminação ou na transformação em dados anônimos das informações que não são mais necessárias.

Caso não haja o consentimento do indivíduo, o dispositivo prevê que a coleta deve ocorrer para outro fundamento legítimo previsto em lei. Portanto, trata-se de relevante reserva legal a proteger o direito à privacidade, vez que, ao se excepcionar o consentimento do indivíduo na coleta de dados, não poderá a Administração ou o agente por si só recolhê-los, invocando princípios que entende aplicáveis. Será imprescindível a intermediação do Poder Legislativo para definir as hipóteses específicas em que se admitirá a coleta de dados, a despeito de não haver consentimento do indivíduo.

Pode-se indagar se a ausência de consentimento incluiria apenas os casos com os quais o indivíduo não consentiu ou abarcaria também aqueles nos quais o indivíduo expressamente se recusou a fornecer determinado dado.

---

[165] Ibidem.

[166] Acerca do direito ao esquecimento no debate Brasil, veja-se: SARMENTO, Daniel. Liberdades comunicativas e "Direito ao Esquecimento" na ordem constitucional brasileira. **Revista Brasileira de Direito Civil**, v. 7, p. 190-232, jan./mar. 2016.

Ora, trazendo o debate para o ordenamento jurídico brasileiro, sabe-se que a Constituição da República elenca entre os direitos e garantias fundamentais a proteção à intimidade e à vida privada em seu art. 5º, inciso X. Sabe-se também que qualquer renúncia a direito fundamental deve ser expressa e específica[167]. Logo, no caso em que não há recusa expressa, o indivíduo conta com proteção jurídica, vez que a renúncia a direito fundamental não se presume.

Por certo que a Carta de Direitos Fundamentais da Europa juridicamente não se aplica ao Brasil. Todavia se mostra como importante parâmetro a exigência de lei formal para a relativização da ausência de consentimento. No caso do Brasil, por exemplo, não havendo lei que regulamente a coleta de dados em caso de ausência de consentimento, a questão se resolverá pela aplicação direta do direito fundamental à privacidade. Não resta dúvida que a cláusula que garante o respeito à intimidade e a vida privada tem como seu corolário lógico a necessidade de consentimento do indivíduo para a coleta de dados. Do mesmo modo, exceções à exigência de consentimento ou mesmo a recusa expressa apenas podem ser relativizadas caso haja outro valor constitucional igualmente relevante a prevalecer na ponderação do caso concreto. Em outras palavras, ainda que o legislador brasileiro pretenda regulamentar as hipóteses de coleta de dados sem consentimento, apenas a poderá fazer nas hipóteses em que houver outro valor constitucional relevante de igual importância.

O item 2 do artigo 8º da carta europeia prevê, ainda, o direito de acesso de dados e a possibilidade de retificação. Esta previsão é muito semelhante ao *habeas data* previsto na Constituição brasileira (art. 5º, LXIX). O direito de acesso individual ao conteúdo das informações que lhe digam respeito é importante instrumento a garantir a autonomia informacional do indivíduo, de forma que este pode exigir que os bancos de dados tenham informações corretas e contextualizadas a seu respeito. Não basta a proteção ao sigilo e privacidade desses dados, mas deve-se garantir ao indivíduo a possibilidade de seu conhecimento, esclarecimento e retificação. Ressalta-se neste ponto, para além do aspecto negativo da proteção a privacidade, o aspecto positivo de sua proteção, ou seja, a pretensão em face do Estado ou do gestor do banco de dados a que seja franqueado o acesso, bem como

[167] Sobre o tema da renúncia a direitos fundamentais, vide: MARTEL, Letícia de Campos Velho. Indisponibilidade de Direitos Fundamentais: Conceito lacônico, consequências duvidosas. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coords.). **Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica. Rio de Janeiro: Lumen Juris, 2011, p. 75-112.

retificação das informações equivocadas. Trata-se do princípio do *acesso individual*, também elencado por Stefano Rodotà[168].

Por fim, o terceiro item prevê a fiscalização destas regras por parte de autoridade independente. A previsão é salutar, na medida em que indica um terceiro árbitro não interessado, que fiscalizará a atuação de mercados e estados no tratamento de dados, a fim de que a privacidade não se torne uma mercadoria, tampouco um instrumento de perseguição na mão de algum autoritário de ocasião.

Da mesma forma, pode-se apontar o Tratado que estabelece uma Constituição para a Europa[169], que possui as mesmas disposições previstas na Carta de Direitos Fundamentais da União Europeia.

No mesmo sistema,o Regulamento (UE) 2016/679 do Parlamento Europeu[170] e do Conselho, de 27 de abril de 2016, que trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados que revogou a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). O referido regulamento encontra-se em vigor desde abril de 2016 e sua aplicabilidade se dará a partir de maio de 2018.

O Regulamento traz em seu artigo 4ºas definições, entre elas o de tratamento de dados[171], o de consentimento[172], violação de dados[173]. Dentre os conceitos do Regulamento, destaca-se o conceito de dado pessoal:

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa

---

[168] RODOTÁ, Stefano. Op. cit. p. 59.

[169] Disponível em: <https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf>. Acesso em: 20 fev. 2017.

[170] Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/. Acesso em 20/02/2018.

[171]«Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

[172]«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

[173] «Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

> singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

O que se extrai dos trechos destacados é que a definição de dados pessoais não se preocupa com o dado em si, com sua relevância ou mesmo a banalidade de seu conteúdo. Qualquer informação relativa a uma pessoa identificada ou identificável é dado pessoal e assim deve ser protegido. A construção conceitual é positiva na medida em que não deixa ao arbítrio subjetivo das autoridades a definição do que é ou não dado pessoal protegido pela privacidade. Na vida contemporânea, o indivíduo deixa rastro de suas atividades mais rotineiras, seja o trajeto até uma reunião em um aplicativo de trânsito, os sites em que se cadastrou para obter informações, o local onde efetuou o pagamento de seu almoço, quais transportes públicos fez uso e em quais locais parou, enfim, todos esses dados, a princípio não são desabonadores. Todavia, tais dados podem ser sensíveis, vez que, se tratados de forma integrada, podem expor o indivíduo ao escrutínio público e revelar inclinações políticas, relações afetivas, preferências de consumo, entre outras.

Ademais, assim como nas legislações em geral, a definição ampla do conceito de tratamento de dados para incluir qualquer operação efetuada sobre dados pessoais desde a coleta e até mesmo a sua destruição, passando pelo seu armazenamento, consulta ou utilização, faz com que o indivíduo esteja mais protegido de qualquer ingerência sem que o gestor do dado possa alegar irresponsabilidade pelo tratamento indevido.

Se por um lado o conceito ampliado de dados pessoais amplia o conjunto de dados que devem ser protegidos, enquanto proteção material à privacidade, o conceito ampliado de tratamento destes dados traz uma garantia instrumental de que qualquer operação sobre estes dados, seja uma mera consulta ou um remanejamento, contará com a proteção dispensada aos dados pessoais, com a necessidade de uma autoridade independente, da observância de regras de segurança, dos princípios gerais aplicáveis aos dados pessoais, entre outros.

O Regulamento traz ainda os princípios aplicáveis ao tratamento de dos pessoais (art. 5º), as condições de licitude de tratamento dos dados (art. 6º), os requisitos para o consentimento livre e explícito (art. 7º), as condições de tratamento dos dados pessoais sensíveis (art. 9º), o direito de acesso aos dados por seu titular (art. 15), bem como o direito de se opor de forma justificada ao tratamento de dados que lhe digam respeito em algumas situações, alegando razões legítimas (art. 18).

Da mesma forma, o Conselho da Europa editou a Convenção nº 108 que trata da Convenção para a proteção ao tratamento automatizado de dados pessoais, de 14 maio 1981, que traz disposições semelhantes, cuja principal preocupação àquela época era o tratamento automatizado de dados.

No mesmo sentido, a Convenção Americana sobre Direitos Humanos, conhecida como Pacto de São José da Costa Rica, da qual o Brasil é signatário, possui cláusula que protege o direito à privacidade, relegando à lei o dever de proteger o indivíduo de ingerências em sua vida privada[174]. O dispositivo é muito semelhante à Declaração Universal dos Direitos Humanos da ONU.

Como se vê do dispositivo, o tratado protege o indivíduo de ingerências arbitrárias ou irrazoáveis, ou seja, buscas sem fundamento legítimo e que não observem a proporcionalidade da medida. O pacto em questão trabalha com elementos clássicos da privacidade, tais como a privacidade familiar, no âmbito do domicílio, o sigilo das correspondências e a proteção à honra e à reputação.

No Brasil, não bastassem os tratados internacionais dos quais faz parte, o direito à privacidade possui assento constitucional, reservando-se entre os direitos e garantias fundamentais três incisos que definem os limites gerais do direito à privacidade[175].

O inciso X do artigo 5º da Constituição é a sede da cláusula geral de privacidade, resguardando-se a intimidade, a vida privada, a honra e a imagem das pessoas, prevendo-se o direito à reparação em caso de dano. Os incisos seguintes tratam de aspectos mais concretos do direito à privacidade, tais como a inviolabilidade de domicílio, o sigilo de correspondência e de comunicações.

Ressalte-se que, tanto quanto à inviolabilidade do domicílio - admitida a exceção apenas para prestar socorro ou no caso de flagrante delito - quanto ao sigilo das comunicações telefônicas, sua violação apenas é admitida mediante reserva de jurisdição. Em outras

---

[174]Artigo 11. Proteção da honra e da dignidade. "1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas".

[175]Art. 5º "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (…) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;".

palavras, tamanha é a importância que o constituinte deu à projeção do direito à privacidade na garantia da inviolabilidade do domicílio e no sigilo das comunicações telefônicas[176] que apenas a autoridade investida de jurisdição pode determinar seu levantamento, desde que observadas as balizas legais.

Segundo o artigo 5º, XII, da Constituição da República[177], o conteúdo de toda e qualquer ligação telefônica é protegida por meio de reserva legal qualificada, ocorrendo sua violação apenas através de ordem fundamentada de autoridade judicial na forma da lei.

O referido dispositivo é didático ao definir que o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas é inviolável em regra.

Admite-se excepcionalmente, a violação do sigilo das comunicações telefônicas ("salvo, no último caso"), mas para tanto, o dispositivo constitucional estabelece três requisitos:

1. a existência de ordem judicial (cláusula de reserva de jurisdição);
2. que a ordem judicial ocorra nas hipóteses e na forma que a lei estabelecer (reserva legal qualificada);
3. que a finalidade da violação seja a investigação criminal ou instrução processual penal;

Neste sentido, o legislador ordinário editou a Lei nº 9.296/1996, Lei da Interceptação Telefônica, que regulamenta o inciso XII, parte final, do art. 5°, da Constituição Federal. Decerto que há outros dispositivos dentro e fora do catálogo dos direitos e garantias fundamentais que protegem o direito à privacidade na Constituição. Pode-se citar como exemplo o inciso LX do art. 5º, que prevê que a lei apenas pode limitar a publicidade dos atos processuais, caso seja para resguardar a intimidade das pessoas[178].

Com efeito, em um Estado Democrático de Direito, a regra é que todos os seus atos, inclusive os judiciais, sejam públicos, ou seja, estejam submetidos ao livre escrutínio popular,

---

[176] O Supremo Tribunal Federal admite que as Comissões Parlamentares de Inquérito determinem a quebra de sigilo telefônico, que envolve apenas o sigilo de dados e registros telefônicos, (vide BRASIL. Supremo Tribunal Federal. *Mandado de Segurança nº 24817*. Tribunal Pleno. Relator Min. Celso de Mello. Julg. 03 fev. 2005. ***DJe*** 05 nov. 2009), o que não se confunde com o sigilo da comunicação telefônica, vez que este envolve o seu conteúdo. Todavia, em relação à interceptação telefônica e à busca domiciliar, entende o Supremo Tribunal Federal tratar-se de matéria submetida à reserva de jurisdição, não sendo possível sua decretação pelas Comissões Parlamentares de Inquérito (vide BRASIL. Supremo Tribunal Federal. *Mandado de Segurança nº 23452/RJ*. Tribunal Pleno. Relator Min. Celso de Mello. Julg. 16 set. 1999. ***DJ*** 12 mai. 2000).

[177] Art. 5º. (...). "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;".

[178] Art. 5. (...). "LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;".

para o livre debate e crítica no âmbito da sociedade. Tanto é assim que a publicidade é princípio constitucional aplicável a toda a Administração Pública, conforme prevê o art. 37, *caput*, da Constituição[179].

Ocorre que há situações nas quais a intimidade dos envolvidos fica por demais evidente no processo e a publicidade dos atos processuais pode fragilizar ainda mais as partes diante da opinião de terceiros. Imagine-se, por exemplo, uma ação de guarda entre os pais de uma criança na qual há uma acusação de abuso psicológico ou sexual da criança envolvida ou mesmo uma ação em que se discute um crime de natureza sexual cometido no âmbito das relações familiares: não seria o estigma que a vítima será obrigada a carregar publicamente muito mais danoso que a restrição da publicidade dos atos judiciais nestes casos?

Portanto, o condicionamento da publicidade dos atos judiciais à proteção da intimidade das pessoas é uma ponderação entre a privacidade do indivíduo e o direito à informação já realizada pelo constituinte em prestígio ao direito fundamental insculpido no art. 5º, X da mesma Constituição.

Pelos mesmos fundamentos, o art. 93, inciso IX, da Constituição excepciona a regra da publicidade dos julgamentos no âmbito do Poder Judiciário, em nome da intimidade do interessado[180]. Em outra passagem, a Constituição determina que nenhum embaraço seja imposto à liberdade de informação jornalística, mas estabelece entre os limites que a atividade jornalística deve observar o previsto no artigo 5º, inciso X, que prevê a inviolabilidade da intimidade, vida privada, honra a imagem das pessoas[181]. Por fim, outro exemplo da mesma natureza diz respeito à previsão constitucional de criação de lei para definir as formas de participação do cidadão na administração pública, determinando que se regule especialmente o acesso dos usuários aos registros administrativos e aos atos do governo, impondo, no

---

[179] Art. 37. "A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:" (Redação dada pela Emenda Constitucional nº 19, de 1998).

[180] Art. 93. (...) IX todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;" (Redação dada pela Emenda Constitucional nº 45, de 2004).

[181] Art. 220. "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV. § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística".

entanto, que se observe a cláusula geral de privacidade prevista no art. 5º, inciso X, da Constituição[182].

1.3.2 Legislação brasileira infraconstitucional acerca do direito à privacidade: da Lei da Interceptação Telefônica ao Marco Civil da Internet

A legislação infraconstitucional brasileira é rica em exemplos de proteção à privacidade. Pode-se citar, por exemplo, a aqui já mencionada Lei nº 9.296/1996, Lei da interceptação telefônica, que regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal, que exige que a interceptação telefônica ocorra na forma da lei.

A lei traz normas específicas, tais como exigir a preservação do sigilo com o processamento do pedido de interceptação em autos apartados[183] e o descarte de parte que não interessar à produção probatória[184]. A lei prevê também que deve haver a existência de indícios razoáveis de autoria ou participação em crimes cuja punição máxima não seja a detenção. Outra exigência é que a prova a ser produzida pela interceptação telefônica seja imprescindível, não podendo ser produzida por outros meios[185].

A lei prevê ainda em seu art. 1º, parágrafo único[186], a possibilidade de interceptação do fluxo de dados. Há relevante controvérsia acerca da constitucionalidade do dispositivo[187], especialmente porque o texto constitucional (art. 5º, inciso XII) apenas excepciona a

---

[182] Art. 37. "(…) § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: (Redação dada pela Emenda Constitucional nº 19, de 1998) I - as reclamações relativas à prestação dos serviços públicos em geral, asseguradas a manutenção de serviços de atendimento ao usuário e a avaliação periódica, externa e interna, da qualidade dos serviços; (Incluído pela Emenda Constitucional nº 19, de 1998) II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;" (Incluído pela Emenda Constitucional nº 19, de 1998).

[183] Art. 8° "A interceptação de comunicação telefônica, 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".

[184] 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".

[185] Lei nº 9296/96, Art. 2° "Não será admitida a interceptação de comunicações telefônicas 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. 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".

[186] Art. 1º. "(…) Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática".

[187] Para compreender em resumo a controvérsia, veja: BANDEIRA, Gustavo. **A Interceptação do Fluxo de Comunicações por Sistemas de Informática e sua Constitucionalidade**. 2002. Trabalho apresentado como exigência final da disciplina Processo e Garantias Fundamentais. Mestrado em Direito, Rio de Janeiro, 2002.

possibilidade de interceptação telefônica. Em que pese toda a controvérsia, o texto legal, seja por atecnia ou omissão, apenas fala do fluxo de dados e não do conteúdo das comunicações, podendo-se qualificar o fluxo como o volume de dados transferidos de terminal a terminal e não do conteúdo da comunicação em si, embora esta questão sequer seja posta. De qualquer forma, entendendo-se que o dispositivo se refere ao conteúdo das comunicações por meios eletrônicos, serão necessárias todas as cautelas legais previstas na Lei nº 9.296/96, a fim de que esta interceptação seja legalmente adequada.

Outro exemplo é a Lei Complementar nº 105 de 2001, que regulamenta as hipóteses do sigilo bancário e define em que situações se permite o fornecimento de informações bancárias[188], como é o caso da comunicação interbancária para análise de crédito ou de informações fornecidas à Receita Federal para fins de verificação de pagamento de tributo. Admite-se também a comunicação às autoridades competentes a respeito da prática de ilícitos penais ou administrativos.

Pode-se citar, ainda, as disposições do Código Tributário Nacional que preveem a necessidade de preservação do sigilo fiscal por parte das autoridades fazendárias[189]. Os

---

[188]Lei Complementar nº 105/2001, Art. 1o "As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. (…) § 3o Não constitui violação do dever de sigilo: I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; III – o fornecimento das informações de que trata o § 2o do art. 11 da Lei no 9.311, de 24 de outubro de 1996; IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa; V – a revelação de informações sigilosas com o consentimento expresso dos interessados; VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2o, 3o, 4o, 5o, 6o, 7o e 9 desta Lei Complementar".

[189] Código Tributário Nacional, Art. 198. "Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades. (Redação dada pela Lcp nº 104, de 2001) § 1o Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes: (Redação dada pela Lcp nº 104, de 2001) I – requisição de autoridade judiciária no interesse da justiça; (Incluído pela Lcp nº 104, de 2001) II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa. (Incluído pela Lcp nº 104, de 2001) § 2o O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo. (Incluído pela Lcp nº 104, de 2001) § 3o Não é vedada a divulgação de informações relativas a: (Incluído pela Lcp nº 104, de 2001) I – representações fiscais para fins penais; (Incluído pela Lcp nº 104, de 2001) II – inscrições na Dívida Ativa da Fazenda Pública; (Incluído pela Lcp nº 104, de 2001) III – parcelamento ou moratória. (Incluído pela Lcp nº 104, de 2001).

Art. 199. A Fazenda Pública da União e as dos Estados, do Distrito Federal e dos Municípios prestar-se-ão mutuamente assistência para a fiscalização dos tributos respectivos e permuta de informações, na forma estabelecida, em caráter geral ou específico, por lei ou convênio. Parágrafo único. A Fazenda Pública da União,

dispositivos excepcionam o fornecimento de informações fiscais apenas por determinação da autoridade judiciária ou por pedido de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa.

O Supremo Tribunal Federal, em julgamento conjunto de ações direta de inconstitucionalidade em face dos artigos 5º e 6º da Lei Complementar 105 de 2001[190], entendeu que são constitucionais os dispositivos desta lei que permitem o compartilhamento de informações com as autoridades fiscais e tributárias, no caso da União, vez que esta observa os regulamentos previsto no Decretos nºs 3.749/2001 e 4.489/2009. O fundamento da decisão foi o fato de que ao direito à intimidade encontra, por outro lado, o dever de pagar tributos, conforme previsto Constituição[191]. Em relação aos Estados e Municípios, previu a possibilidade de compartilhamento de informações entre entes, desde que haja regulamento

---

na forma estabelecida em tratados, acordos ou convênios, poderá permutar informações com Estados estrangeiros no interesse da arrecadação e da fiscalização de tributos". (Incluído pela Lcp nº 104, de 2001)

[190] Art. 5º "O Poder Executivo disciplinará, inclusive quanto à periodicidade e aos limites de valor, os critérios segundo os quais as instituições financeiras informarão à administração tributária da União, as operações financeiras efetuadas pelos usuários de seus serviços. (Regulamento) (…)§ 2º As informações transferidas na forma do caput deste artigo restringir-se-ão a informes relacionados com a identificação dos titulares das operações e os montantes globais mensalmente movimentados, vedada a inserção de qualquer elemento que permita identificar a sua origem ou a natureza dos gastos a partir deles efetuados. § 3º Não se incluem entre as informações de que trata este artigo as operações financeiras efetuadas pelas administrações direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios. § 4º Recebidas as informações de que trata este artigo, se detectados indícios de falhas, incorreções ou omissões, ou de cometimento de ilícito fiscal, a autoridade interessada poderá requisitar as informações e os documentos de que necessitar, bem como realizar fiscalização ou auditoria para a adequada apuração dos fatos. § 5º As informações a que refere este artigo serão conservadas sob sigilo fiscal, na forma da legislação em vigor".

Art. 6º "As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade administrativa competente".

[191] Veja-se trecho da ementa que é bastante esclarecedor: "Ação direta de inconstitucionalidade. Julgamento conjunto das ADI nº 2.390, 2.386, 2.397 e 2.859. Normas federais relativas ao sigilo das operações de instituições financeiras. Decreto nº 4.545/2002. Exaurimento da eficácia. Perda parcial do objeto da ação direta nº 2.859. Expressão "do inquérito ou", constante no § 4º do art. 1º, da Lei Complementar nº 105/2001. Acesso ao sigilo bancário nos autos do inquérito policial. Possibilidade. Precedentes. Art. 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentadores. Ausência de quebra de sigilo e de ofensa a direito fundamental. Confluência entre os deveres do contribuinte (o dever fundamental de pagar tributos) e os deveres do Fisco (o dever de bem tributar e fiscalizar). Compromissos internacionais assumidos pelo Brasil em matéria de compartilhamento de informações bancárias. Art. 1º da Lei Complementar nº 104/2001. Ausência de quebra de sigilo. Art. 3º, § 3º, da LC 105/2001. Informações necessárias à defesa judicial da atuação do Fisco. Constitucionalidade dos preceitos impugnados. ADI nº 2.859. Ação que se conhece em parte e, na parte conhecida, é julgada improcedente. ADI nº 2.390, 2.386, 2.397. Ações conhecidas e julgadas improcedentes".

no ente e tal regulamento observe as balizas estabelecidas no Decreto nº 3.724/2001, exigindo-se que estes entes observem as seguintes medidas em seu regulamento:

> i) pertinência temática entre as informações bancárias requeridas na forma do art. 6º da LC nº 105/01 e o tributo objeto de cobrança no processo administrativo instaurado;
>
> ii) prévia notificação do contribuinte quanto à instauração do processo (leia-se, o contribuinte deverá ser notificado da existência do processo administrativo previamente à requisição das informações sobre sua movimentação financeira) e relativamente a todos os demais atos;
>
> iii) submissão do pedido de acesso a um superior hierárquico do agente fiscal requerente;
>
> iv) existência de sistemas eletrônicos de segurança que sejam certificados e com registro de acesso, de modo que torne possível identificar as pessoas que tiverem acesso aos dados sigilosos, inclusive para efeito de responsabilização na hipótese de abusos;
>
> v) estabelecimento de mecanismos efetivos de apuração e correção de desvios;
>
> vi) amplo acesso do contribuinte aos autos, garantindo-lhe a extração de cópias de quaisquer documentos e decisões, de maneira a permitir que possa exercer a todo tempo o controle jurisdicional dos atos da administração, segundo atualmente dispõe a Lei 9.784/1999[192].

As exigências elencadas no acórdão mencionado decerto dão mais garantias ao titular das informações bancárias e impede que dados sejam acessados por mera curiosidade ou com fins de perseguição e indevida exposição. É claro que o direito à privacidade, classicamente concebido como o direito à não divulgação de informações patrimoniais e de renda, atualmente não possui tão fortemente a mesma tônica. Isto quer dizer que, por mais que diga respeito à vida privada do indivíduo, informações acerca de rendimentos e bens, há por outro lado o correlato dever de informar corretamente ao fisco suas atividades financeiras, exclusivamente para fins de determinação da base de cálculo de tributos. Portanto, é bastante razoável que, havendo o estabelecimento de balizas seguras de regulamentação do compartilhamento das informações, tais informações sejam compartilhadas entre entes tributantes, desde que guardado o devido sigilo.

Por óbvio que isso se mostra relativamente preocupante quando o país tem 5.570 municípios e 26 estados da federação. Ocorre que a ocultação completa de informações financeiras e a exigência de reserva de jurisdição burocratiza sobremaneira a atividade arrecadatória e inviabiliza a própria existência do Estado. Ora, a própria legislação apenas

[192] Trechos extraídos do voto do Ministro Dias Toffoli, relator da ADI 2390/DF.

permite o compartilhamento de movimentações globais mensais e identificação do titular, sem se identificar a origem e destino dos recursos e sem se individualizar as movimentações[193].

Desta forma, preserva-se parte dessas informações sensíveis sem que se frustre na totalidade a finalidade do Estado de recolher tributos. Invocando a teoria dos círculos concêntricos, as informações sobre transações financeiras e relações negociais estão no círculo mais externo da privacidade, ou seja, naquele que conta com menor proteção.

Conforme consagrado na doutrina, é certo que nenhum direito fundamental possui caráter absoluto. Significa dizer que havendo direitos igualmente fundamentais em rota de colisão, não haverá a prevalência absoluta de um em detrimento da total inaplicabilidade de outro. Sabe-se que a técnica mais adequada é a ponderação entre estes direitos no caso concreto.

O dever constitucional de pagar tributos que decorre do Título VI, Capítulo I, da Constituição da República (artigos 145 a 162), uma vez que não se pode prever o poder de cobrar tributos pelos entes federativos, sem que estes entes possuam instrumentos mínimos de fiscalização. A vida moderna permite a aplicação de recursos nos mais variados investimentos, sejam no país ou no exterior, de forma que a capacidade contributiva, se torna cada vez menos visível fisicamente.

Ora, a decisão da Suprema Corte, declarando a constitucionalidade do dispositivo é uma ponderação entre o dever de pagar tributos e o direito à privacidade, ambos de estatura constitucional, adotadas todas as cautelas possíveis para que não se anule por completo a privacidade.

Outra lei brasileira importante acerca do direito à privacidade é o marco civil da internet, a Lei nº 12.965 de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A lei em questão afirma como um dos fundamentos da internet no Brasil a liberdade de expressão e, entre outros, elenca o livre desenvolvimento da personalidade e o exercício da

[193] Lei Complementar nº 105 de 2001. Art. 5º "(…) §2o As informações transferidas na forma do *caput* deste artigo restringir-se-ão a informes relacionados com a identificação dos titulares das operações e os montantes globais mensalmente movimentados, vedada a inserção de qualquer elemento que permita identificar a sua origem ou a natureza dos gastos a partir deles efetuados".

cidadania em meios digitais[194]. Ademais prevê entre os princípios norteadores no uso da internet a liberdade de expressão, a proteção à privacidade e a proteção aos dados pessoais[195].

Uma primeira leitura desta declaração de fundamentos e princípios faz concluir tratar-se de um marco legal compromissório, vez que estabelece na mesmo código princípios antagônicos, quais sejam, a liberdade de expressão e o direito à privacidade ou à preservação de dados pessoais. Todavia, ao longo do texto se verá a intenção de legislador em harmonizar ambos os direitos fundamentais.

Tanto é assim que o art. 8º da referida lei[196] afirma que a garantia da liberdade de expressão e a proteção à privacidade são condições ao pleno exercício de direito de acesso à internet, tornando nulas as cláusulas que violem estes princípios ou impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas ou nos contratos de adesão não ofereçam ao usuário a possibilidade de optar pelo foro brasileiro para solução de problemas decorrentes da prestação do serviço no Brasil.

O artigo 7º traz extenso catálogo de direitos e garantias dos usuários na internet visando garantir a preservação da privacidade da forma mais ampla possível[197]. Além da

---

[194] Art. 2º "A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: I - o reconhecimento da escala mundial da rede; II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;".

[195] Art. 3º "A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;".

[196] Art. 8º "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que: I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil".

[197] Art. 7º "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI - publicidade e clareza de eventuais políticas de uso dos

reafirmação da inviolabilidade da intimidade e da vida privada e sua proteção inclusive com a reparação moral ou material, prevê o sigilo do fluxo de comunicações, bem como do conteúdo das comunicações armazenadas. Tais sigilos apenas poderão ser quebrados por ordem judicial.

A previsão é salutar. Isto porque em que pese a Constituição prever em seu art. 5º, XII, a inviolabilidade de dados, o que no nosso entender incluiria o fluxo das comunicações, a doutrina tradicional entende que a preservação desse sigilo apenas estaria protegida se se tratar de dados que estariam sendo transmitidos, ou seja, a captação ilícita da transmissão. Para os dados estáticos, arquivados, não haveria a mesma proteção constitucional, cuja sede seria o artigo 5º, X, da Constituição. Para Luís Gustavo Grandinetti Castanho de Carvalho[198], em ambas as situações seria necessária a ordem judicial.

No entanto, para o autor, na hipótese, do art. 5º, inciso XII, a ordem judicial apenas poderia se basear em outro valor jurídico constitucional, não se podendo invocar razões de lei ordinária. Já no caso de proteção de dados pela cláusula geral prevista no art 5º, inciso X, dá a entender o autor que bastaria uma ordem judicial por se tratar de violação à intimidade, sem a necessidade de se invocar outro valor constitucional contraposto.

Ao que parece a distinção não possui razão de ser, senão vejamos. Ainda que se entenda que a sede de proteção da interceptação da transmissão de dados e da apreensão de dados seja distinta, ambas possuem sede constitucional e figuram no catálogo de direitos e garantias fundamentais. Diferentemente da interceptação telefônica, o texto constitucional não exige necessária intermediação legal para a interceptação de dados. A bem da verdade, o inciso XII do art. 5º apenas permitiria a interceptação das comunicações telefônicas, nos termos da lei.

Todavia, é pouco eficiente se sustentar que haveria plena vedação constitucional à interceptação da transmissão de dados. Ora, os hábitos de comunicação mudaram diante das novas tecnologias da última década, o que significa dizer que nos comunicamos mais por e-

---

provedores de conexão à internet e de aplicações de internet; XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet".

[198] A observação é de CARVALHO, Luiz Gustavo Grandinetti Castanho de. Direito à Privacidade. **Revista da EMERJ**, v.1, n. 2, p. 55, 1998 que, citando a obra Crime Organizado, expõe a opinião de seus autores da seguinte forma: "A rara doutrina sobre o assunto caminha no sentido de considerar que não estão compreendidos na proteção constitucional os dados armazenados ou estanques, ou melhor, os que não estão sendo transmitidos. A vedação, portanto, portanto, é para captação ilícita da transmissão. Os dados armazenados, segundo Geraldo Prado/William Douglas e Luiz Flávio Gomes, podem ser aprendidos como documentos em geral. Evidentemente, por também evocarem o direito de intimidade, como as cartas, sua apreensão depende de mandado judicial".

mail, aplicativos de mensagem do que pelo próprio telefone, de modo que, se no contexto da Constituição de 1988, o instrumento de comunicação por excelência era o telefone, hoje o meio mais utilizados são as mensagens trocadas em um grupos de e-mail ou aplicativos de mensagens instantâneas via web, vez que seria difícil sustentar a impossibilidade de qualquer interceptação desses meios.

O que se pode sustentar é a seguinte analogia: considerando que todos os sigilos, sejam de dados, sejam de comunicação têm por sede o art. 5º, inciso XII, para a quebra de sigilo de comunicação de dados deverá haver a ordem judicial prévia.

Em que pese o consagrado entendimento do Supremo Tribunal Federal de apenas exigir a ordem judicial específica e prévia para a interceptação de dados e não para a apreensão eventual de dados em um computador[199], defende-se que as novas fronteiras de privacidade na era da sociedade da informação devem ser mais eficazes, garantindo-se uma reserva de jurisdição mais efetiva no que tange ao sigilo das comunicações e fundamentada na necessidade específica de quebrar tal sigilo. Sabe-se que esta proposição encontrará

---

[199] BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 418416*. Tribunal Pleno. Relator Min. Sepúlveda Pertence. Julg. 10 mai. 2006. ***DJ*** 19 dez. 2006: "I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE 140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 - AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00). II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem "interessantes à investigação" que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a "Fiscalização do INSS" também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, "observado o sigilo imposto ao feito". IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal)".

resistência, haja vista que nenhum direito fundamental é absoluto e já é consagrado na doutrina que ordem judicial de busca e apreensão de computadores incluem a verificação dos dados ali registrados.

Fato é que não se pode ver diferença entre o conteúdo de uma comunicação interceptada durante a transmissão e o conteúdo de uma comunicação encontrada eventualmente no interior de um computador. Ora, ambas são conteúdos de comunicações protegidas pela Constituição cuja violação deve contar com ordem judicial específica e prévia. Não faz sentido a distinção entre os incisos X e XII do art. 5º da Constituição quando ambos possuem envergadura constitucional e a violação em ambos os casos se fará chegar ao conteúdo das comunicações.

Retornando ao marco civil da internet, a previsão do art. 7º, incisos II e III protegem não só o sigilo das comunicações privadas arquivadas como também o fluxo das comunicações, que somente pode ser quebrado por ordem judicial.

Com efeito, se o Marco Civil da Internet exige ordem judicial para a quebra de sigilo de comunicação privada arquivada, entende-se que toda comunicação privada arquivada - e, portanto, dado arquivado - conta com a proteção legal da ordem judicial. E mais: não faria sentido se exigir ordem judicial se esta ordem judicial não for prévia e específica. Isto significa dizer que para o acesso não autorizado a toda e qualquer comunicação privada - esteja ela armazenada em uma nuvem de um aplicativo de mensagens, em um provedor de e-mails, em um terminal físico ou em um computador apreendido - será sempre necessária ordem judicial fundamentada, específica e prévia. Não se pode admitir, na era da sociedade de informação que, a pretexto de se investigar crimes cometidos por determinado agente, se apreendam todos os computadores de quem possua arquivadas essas mensagens, mediante ordem judicial genérica e se viole a privacidade de todos os usuários que possuem ali arquivadas suas conversas. Tampouco se pode imaginar ordem judicial que determine genericamente a busca e apreensão de todos os bens necessários à investigação e esta ordem fundamente o acesso a toda e qualquer comunicação do investigado com quaisquer pessoas e sob qualquer assunto, sem ordem judicial específica para tanto.

O fato de o Marco Civil da Internet em boa hora exigir ordem judicial para a quebra do sigilo dessas comunicações não é mera perfumaria, pois já se exigia anteriormente, pelo próprio texto constitucional (art. 5º, inciso X e XII). Tal previsão específica deve ser interpretada como a exigência de ordem judicial específica para a violação de conteúdo de

toda e qualquer conversa, implicando na necessária revisão inclusive da jurisprudência consolidada pela E. Suprema Corte.

Outro ponto positivo do Marco Civil da Internet é o fato de também resguardar o sigilo do fluxo das comunicações. Atualmente, pode-se falar em pessoa digital, da qual grande parte de comunicações e atividades componham algum banco de dados. Desta forma, a informação acerca do fluxo de comunicações, ou seja, que portais visita com mais frequência, qual o volume de dados enviados e recebidos, quais os destinatários frequentes de suas comunicações, podem permitir o tratamento destes fluxos de tal maneira que se defina com precisão o perfil político ideológico, de identificação racial, de gênero, religiosa de afinidades afetivas e sexuais. Portanto, a indevida violação do fluxo de dados pode ser mais comprometedora e invasiva que a própria violação de domicílio, no qual podem ou não ser encontradas evidências físicas do indivíduo. Já as evidências de hábitos, costumes e afinidades do indivíduo na rede são muito mais transparentes e catalogáveis. Desta forma, defende-se igualmente que não bastaria a ordem judicial genérica de interceptação do fluxo de dados, mas da ordem judicial específica, devidamente fundamentada aduzindo as razões pelas quais a violação do fluxo de dados é essencial à investigação criminal. Tanto é assim que a própria Lei nº 9.296/96, em seu art. 1º, parágrafo único, já previa a interceptação dos fluxos de comunicação em sistemas de informática e telemáticos, com todas as cautelas previstas naquela lei.

O Marco Civil da Internet prevê ainda regras que regulamentam a guarda e o registro de conexão e acesso a aplicações de internet, bem como o de dados pessoais e o conteúdo de comunicações privadas, prevendo a necessidade de ordem judicial para que o provedor responsável pelo registro seja obrigado a disponibilizar estes registros de forma autônoma ou associados a dados pessoais ou a informações que possam contribuir para identificação do usuário ou terminal[200]. Prevê ainda, reiterando o art. 7º que o conteúdo das comunicações

[200] Art. 10. "A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o. § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o. § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais".

privadas apenas poderá ser disponibilizado mediante ordem judicial. A única exceção à ordem judicial é a possibilidade de acesso aos dados cadastrais do usuário por autoridades administrativas com competência legal para requisição e neste caso sem associação aos registros de acesso e conexão.

Os dispositivos apontados são importantes ao resguardar dados pessoais sensíveis. Fornecer registros de conexão que identifiquem ou permitam identificar o usuário ou terminal é indevida violação à privacidade dos usuários da rede, por isso a necessidade de ordem judicial.

Louvável também é o dever de transparência imposto aos responsáveis pela provisão de serviços de informar de forma clara as medidas e procedimentos de segurança e de sigilo, bem como de atender os padrões definidos em regulamento, ressalvando-se apenas a confidencialidade de seus segredos empresariais.

As normas citadas não são sem eficácia, uma vez que o art. 12[201] prevê sanções por inobservância dos artigos 10 e 11 que vão desde advertência e multa e até mesmo, no caso de prática de atos previstos no art. 11 da lei, pode ser aplicada a sanção de suspensão das atividades ou mesmo a proibição do exercício das atividades.

Ressalte-se que a lei apenas prevê as sanções de suspensão e proibição de atividades para as condutas narradas no art. 11 da mesma lei, a saber, quando nas operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, não se observar a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Portanto, apenas nas atividades mencionadas e se houver violação à lei brasileira ou aos direitos à privacidade e proteção de dados pessoais é que se admitirá tais sanções. Ocorre que a aplicação de tão gravosas sanções não pode ocorrer pela mera inobservância da legislação brasileira genericamente falando, embora uma das hipóteses de sanção seja a violação à legislação brasileira.

---

[201] Art. 12. "Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11. Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País".

Há que se fazer uma interpretação sistemática para que as violações à legislação brasileira sobre as quais fala o dispositivo sejam apenas aquelas previstas no próprio dispositivo, a saber, o dever de proteção à privacidade, à proteção de dados pessoais e aos sigilos das comunicações bem como o sigilo dos registros. Ainda assim, tal sanção, por ser de máxima gravosidade e restringir sobremaneira a livre iniciativa, insculpida no artigo 170 da Constituição, apenas se pode aplicar de forma proporcional quando as sanções menos graves não sejam eficazes na proteção ao direito. Pode ser que uma multa proporcional a 10% do faturamento já seja capaz de constranger o indivíduo à observância dos deveres legais.

Esses apontamentos são feitos em virtude de decisão judicial de maio de 2016, da lavra de juíza de direito da vara criminal de Duque de Caxias[202], determinou a suspensão do aplicativo em função do não fornecimento do conteúdo das mensagens, em cumprimento a decisão judicial anterior. A decisão fundamentou-se no artigo do 11 do Marco Civil da Internet. Todavia, conforme visto, este artigo apenas prevê sanção para as condutas ali narradas, o que não inclui o descumprimento de decisão judicial.

Ademais, ainda que se entendesse cabível a suspensão para todo e qualquer caso de descumprimento de decisão judicial se mostraria a decisão desproporcional, haja vista que o Marco Civil da Internet foi editado para proteger o usuário e não para inviabilizar o uso das funcionalidades da rede. Tanto é assim que a sanção mais gravosa no âmbito do marco civil é a suspensão das atividades. Ressalte-se que uma decisão desta natureza, ao tempo em que sanciona uma companhia, prejudica milhões de usuários do serviço que não possuem nenhuma relação com a conduta ilícita.

Com efeito, as decisões judiciais determinando a suspensão do aplicativo foram em virtude do não fornecimento de conteúdo das conversas por parte do aplicativo, alegando limitações técnicas. Todavia, os gestores dos aplicativos de mensagens instantâneas afirmam não poder acessar o conteúdo das mensagens por estarem protegidas por chaves de criptografia que nem o próprio aplicativo pode acessar.

Ora, sequer o marco civil da internet impõe como obrigação o registro e arquivamento do conteúdo das mensagens, impondo-se apenas a guarda temporária dos registros de acesso e ainda assim pelo prazo máximo de seis meses[203], salvo se houver solicitação de autoridade

---

[202] BRASIL. Poder Judiciário do Estado do Rio de Janeiro. 2ª Vara Criminal da Comarca de Duque de Caxias. *Inquérito Policial nº 062-00164/2016*. Juíza Daniela de Souza. Julg. 19 jul. 2016. Decisão disponível em: <http://www.migalhas.com.br/arquivos/2016/7/art20160719-03.pdf>. Acesso em: 20 fev. 2017.

[203] Art. 15. "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis)

administrativa ou Ministério Público para extensão do período de guarda. Logo, se não há obrigação legal em se manter arquivado o conteúdo da conversa, ainda que criptografado, como se exigir judicialmente, sob pena de suspensão das atividades este conteúdo?

Em suma, pode-se afirmar que foram positivos os parâmetros de proteção à privacidade trazidos pelo marco civil da internet. É correto também dizer que muito dos conceitos e dispositivos a ele incorporados foram inspirados no projeto de lei acerca da proteção de dados pessoais, ainda em tramitação perante o Poder Legislativo[204].

Ademais, mostra-se de suma importância o intuito da norma em tentar conciliar a liberdade de expressão do indivíduo e o respeito a sua privacidade e intimidade, direitos fundamentais que, ora estão em campos antagônicos, ora se mostram aliados, vez que a garantia da privacidade é instrumental da livre expressão sem constrangimentos.

---

meses, nos termos do regulamento. § 1o Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. § 2o A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13. § 3o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 4o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência".

[204] Veja-se o PL nº 5276/2016 que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, de autoria da então Presidente da República, apensado ao PL 4060/2012 que trata do mesmo tema, bem como ao PL 6291/2016, que altera o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de internet. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 20 fev. 2017.

2DESAFIOS DA PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO: BIG DATA E VIGILÂNCIA

> Data is to the information society what fuel was to the industrial economy: the critical resource powering the innovations that people rely on. Without a rich, vibrant supply of data and a robust market for services, the creativity and productiblity that are possible may be stified.[205]
>
> *Viktor Mayer-Schonberer e Kenneh Cukier*

Conforme abordado no capítulo anterior, embora a coleta, processamento e compartilhamento de dados pessoais e outras informações sejam objetos tratados seriamente pelos ordenamentos jurídicos transnacionais, estrangeiros e, recentemente, brasileiro, com a edição do Marco Civil da Internet, a vida contemporânea eletronicamente mediada parece constantemente desafiar o direito à privacidade.

Nesta nova ordem, indivíduos, grupos ou comunidades inteiras passam a ser inesgotáveis fontes produtoras de dados, recolhidos pelos mais variados sensores, os quais, se devidamente processados podem antecipar tendências de consumo, prevenir doenças, prever ou resolver desastres naturais, potencializar os resultados da agricultura, mas também podem expor inimigos políticos de regimes totalitários, revelar informações sensíveis não compartilhadas voluntariamente pelo indivíduo, viabilizar a adoção de práticas discriminatórias no acesso ao mercado de trabalho ou na oferta de produtos e serviços.

Nesse novo jogo de forças das potências corporativas passa a deter o poder aquele que possui a capacidade de coletar, armazenar e processar dados, transformando-os em mercadoria lucrativa. Tanto é assim que os gastos globais com propaganda na internet em 2016 estão em franca ascensão e, pela primeira vez desde 1995, superaram os realizados através da mídia televisiva, atingindo a marca de 200 bilhões de dólares[206]. Neste cenário, por mais democrático que o ambiente de internet possa parecer, a receita de propaganda na internet apenas do Google é da ordem de 35 bilhões superior, portanto, à soma de todos os outros concorrentes, seguido pelo Facebook cuja receita no último ano é metade da todas as

---

[205] Em livre tradução:"[Os] dados são para a sociedade da informação o que o combustível era para a economia industrial: o recurso crítico que impulsiona as inovações nas quais as pessoas dependem. Sem um rico e dinâmico fornecimento de dados e um mercado robusto de serviços, a criatividade e a produtividade possíveis podem ser fortalecidas".MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. **Big Data**: A Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mffin Hartcourt, 2013, p. 182.

[206] PERKINS, Kleiner. **Internet Trends 2017** – Code Conference, p. 14. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 20 dez. 2017.

outras companhias somadas, à exceção do Google[207]. Esta concentração de mercado apenas é apontada para demonstrar que não apenas os Estados devem ser uma preocupação no qua tange à privacidade no ambiente de internet, mas também corporações globais bilionárias cujos intuitos lucrativos podem não observar os parâmetros éticos e jurídicos necessários.

Por esta razão, diante da nova riqueza a ser explorada, cuja fonte, a princípio, é inesgotável, passa a ter importância avultada a atividade de intermediação de dados. O profissional especialista em determinado assunto ou mercado, cede lugar ao estatístico e ao analista de dados. Deve-se advertir, no entanto, que, por mais apurada e ampla que possa ser, a análise de *big data* não se baseia em uma relação necessariamente causal. Os dados não estabelecem a causa de determinado evento, apenas permitem que se estabeleçam análises relacionais do que pode ter sido a causa, amparado em estatísticas, passando, a partir da frequência de determinado evento, a projetar uma probabilidade futura, o que se convencionou chamar de análise preditiva[208].

Alerta-se para que o risco da fetichização dos dados não nos conduza ao cenário de governo ou ditadura dos dados[209], na qual os algoritmos decidem destinos e em que se decida o futuro com base em análises preditivas de probabilidade, bem como se limitem direitos, com base em comportamento de terceiros que, eventualmente, possam sugerir um provável comportamento futuro do indivíduo, desconsiderando por completo a autodeterminação humana.

O acesso facilitado a dispositivos móveis tais como *tablets* e *smartphones* potencializa ainda mais a produção dos mais variados dados, desde hábitos de trajeto adotados na rede de transporte público à rota adotada em veículos privados, dados de localização recolhidos por aplicativos, as opiniões sobre os mais variados temas nas redes sociais, os dados de saúde e atividade física inseridos em aplicativos do gênero, os metadados[210] de comunicações

---

[207] Ibidem, p. 15.

[208] "To be sure, subject-area experts won't die out. But their supremacy wil ebb. From now on, they must share the podium with big-data geeks, just as princely causation must share the limelight with humble correlation." MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit.,p. 143.

[209] Ibidem, p. 163.

[210] Metadados, de forma simplista, podem ser definidos como dados sobre dados, ou seja, é a informação que descreve o dado. O prefixo meta, que significa "além de" significa que os metadados permitem ir além do próprio dado ou informação em si, ou seja, esse tipo de informação é usado para classificar, organizar e pesquisar. Portanto, os metadados permitem a indexação, a classificação, ou mesmo a investigação do próprio conteúdo do dado sem que seja necessário acessá-lo. Os metadados permitem, extrair e consolidar dados de múltiplas fontes numa base de dados que possa ser consultada de várias maneiras pelos utilizadores identificando e integrando dados comuns de fontes varidas. Vide: O QUE SÃO metadados. **Metadados**, [s.d.]. Disponível em: <http://www.metadados.pt/oquesaometadados>. Acesso em: 11 jan. 2018. Para uma visão mais técnica do assunto, vide CAMPOS, Luiz Fernando de Barros. METADADOS DIGITAIS: revisão bibliográfica da evolução

privadas, como mensagens instantâneas e e-mails, além de vídeos, textos, imagens e outros conteúdos produzidos ao longo do dia.

Não é por outra razão que a produção destes dados tem crescido exponencialmente. Aliado a isso há um barateamento das tecnologias de armazenamento de dados, podendo-se citar como exemplo o *cloud computing*[211], que permitindo um armazenamento de dados sem precedentes. Por fim, outro fator importante é a capacidade de processamento destes dados, que ocorre praticamente em tempo real, quase que no exato momento em que o dado é gerado.

Este conjunto de fatores possibilitou o fenômeno que ficou conhecido por *big data*, que, em suma, é caracterizado pelo armazenamento e processamento de um grande e variado volume de dados, em uma velocidade sem precedentes que possibilita a tomada de decisões automatizadas. Tais decisões automatizadas são baseadas em algoritmos que, alimentados pelos dados, podem definir se um candidato é elegível a determinado posto de trabalho ou a uma bolsa em curso universitário, bem como se é seguro conceder a determinado consumidor uma linha de crédito.

Ocorre que a coleta e processamento massivo destes dados impõem desafios à privacidade. Há que se indagar que parâmetros foram observados na preservação do sigilo dos dados recolhidos, se houve coleta de dados sem consentimento de seu titular ou se os dados coletados podem agravar a esfera de direitos do indivíduo.

Conforme se verá, são inegáveis os benefícios advindos do uso do *big data* e a sua aplicação mostra-se irreversível. Qualquer empresa minimamente precavida desejará conhecer as futuras tendências, os desejos do consumidor e até mesmo alcançar da forma mais eficiente possível o seu público alvo. Da mesma forma, é interesse aos Estados, em um cenário de recursos sempre precários, a máxima eficiência de suas políticas públicas. Ocorre que, tanto empresas quanto Estados podem fazer uso desvirtuado da tecnologia, seja para discriminar consumidores ou aumentar de forma desleal sua margem de lucro, seja para implementar um programa de vigilância com vistas a neutralizar opositores políticos internos ou realizar atividades de espionagem e monitoramento de cidadãos de outros países.

---

e tendências por meio de categorias funcionais. **Enc. Bibli: R. Eletr. Bibliotecon. Ci. Inf.**, Florianópolis, n. 23, p. 16-46, 2007.

211 "Cloud computing ou computação em nuvem é a entrega da computação como um serviço ao invés de um produto, onde recursos compartilhados, software e informações são fornecidas, permitindo o acesso através de qualquer computador, tablet ou celular conectado à Internet" FERNANDES, Carol. O que é cloud computing. **TechTudo**, mar. 2012.Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/03/o-que-e-cloud-computing.html>. Acesso em: 20 dez. 2017.

Pode-se imaginar que os desafios apresentados pelo uso cada vez mais comum do *big data* apenas potencializam a ordem de grandeza do volume de dados que é coletado e processado e, para tanto, bastaria elevar os rigores do ordenamento jurídico com as situações de violação à privacidade. Todavia, mais que a alteração da ordem de grandeza - que é inegável, diante da ubiquidade dos sensores e diante do aumento exponencial da produção e coleta de dados -, há uma alteração qualitativa. O que altera o estado de coisas é o uso cada vez mais frequente, em virtude do *big data*, das análises preditivas, realizadas com base nas probabilidades estatísticas.

Decerto que nenhuma tecnologia por si só é boa ou ruim, mas o uso que é feito deste recurso pode se converter nos seus malefícios ou benefícios, ou seja, pode tanto contribuir para aperfeiçoar mecanismos de inclusão social e combate à discriminação ou pode aprofundar desigualdades[212]. Diante disso, a função essencial do ordenamento jurídico será a deestabelecer balizas para o legítimo e adequado uso do *big data* e o direito à privacidade será um dos termômetros a determinar se o uso dos dados ocorre de forma lícita ou ilícita.

2.1 ***Big data*: contexto, conceito e evolução**

Não é novidade que sempre foi interesse de corporações conhecer o conjunto de dados de seus consumidores ou potenciais consumidores, para orientar suas decisões e estratégias de mercado; bem como é interesse de ocupantes de poder a descrição mais precisa do perfil dos cidadãos pertencentes a determinado Estado, o que poderá orientar políticas públicas mais eficientes e menos custosas.

Ocorre que a ordem de grandeza destes dados muda substancialmente a partir das mais variadas fontes de coleta destes dados, que vai desde um *smartphone* ou um desktop, mas pode também se originar de dados de um dispositivo inteligente, como a *smart TV*, que, conectada à internet, transmite as preferências de programação e cataloga conteúdo adquirido[213]; o carro inteligente, que alerta sobre a necessidade de realizar revisão ou sobre

---

[212] FEDERAL TRADE COMISSION. **Big Data**: A tool for inclusion or exclusion? Understanding the issues. FTC Report, jan. 2016. Disponível em: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>. Acesso em: 18 dez. 2017.

[213] Poderia ser utilizado o termo "TV inteligente", mas não me parece adequado, haja vista que o termo estrangeiro já está consolidado nas práticas comerciais. Vide interessante trecho: "Um desenvolvedor de software baseado no Reino Unido disse na segunda-feira (18), em um post no seu blog, que a sua Smart TV estava compartilhando informações sobre quais canais ele estava assistindo com a LG por causa de uma opção chamada "coletar informações de assistir", ativada por padrão. Mas, mesmo depois de desligar o recurso, a TV continuou a compartilhar seus hábitos com a empresa, disse o desenvolvedor, que usa o pseudônimo on-line de DoctorBeet." CONSTANTIN, Lucian. LG admite que Smart TVs coletam dados sobre hábitos de usuários.

novo recall[214], além de solicitar socorro em caso de acidente[215], mas pode, por outro lado, armazenar e transmitir hábitos de trajeto e locais frequentados pelo motorista[216]. Soma-se a isto tudo a possibilidade de todos esses dispositivos inteligentes, permanentemente conectados à internet, serem alvo de *hackeamento* ou vigilância, de modo que as câmeras ou sensores de áudio presentes em alguns deles transmita em tempo real imagens do cômodo de uma casa, conversas privadas de um casal, segredos diplomáticos ou empresariais tratados em uma reunião, entre outros[217].

Essa grande base de dados se potencializa quando 3,4 bilhões de usuários[218] possuem acesso à internet, o que representa 46% da população mundial. No Brasil esse número supera cem milhões de usuários[219]. Este acesso é potencializado pelos cinco bilhões de aparelhos *smartphones*[220] que permitem conexão à internet. No caso do Brasil, a última medição chegou ao número de 198 milhões de aparelhos *smartphones*, além de 166 milhões de computadores, projetando-se atingir a marca de um computador por brasileiro em 2022[221].

IDGNow!, nov. 2013. Disponível em: <http://idgnow.com.br/internet/2013/11/25/lg-admite-que-smart-tvs-coletam-dados-sobre-habitos-de-usuarios/>. Acesso em: 20 dez. 2017.

[214]SISTEMA AVISA QUANDO carro precisa de manutenção. **Autoo**, jul. 2012. Disponível em: <https://www.autoo.com.br/sistema-avisa-quando-carro-precisa-de-manutencao/>. Acesso em: 20 dez. 2017.

[215] CALMON, Fernando. Ford lança sistema que chama o Samu em caso de acidente com o novo Ka. **Carros**, jul. 2014. Disponível em: <https://carros.uol.com.br/colunas/alta-roda/2014/07/29/ford-lanca-sistema-que-chama-o-samu-em-caso-de-acidente-com-o-novo-ka.htm>. Acesso em: 20 dez. 2017.

[216] Veja interessante declaração do vice-presidente de marketing e vendas da Ford, Jim Farley, em 2014: "Nós sabemos quais motoristas descumprem a lei, sabemos quando estão fazendo isso. Se há um GPS no seu carro, sabemos o que você faz, mas não fornecemos estes dados a ninguém". CONTESINI, Leonardo. GPS integrado pode coletar dados do motorista e do carro e enviá-los para as fabricantes. **Flatout**, jan. 2014. Disponível em: <https://www.flatout.com.br/gps-integrado-pode-coletar-dados-motorista-e-carro-e-envia-los-para-fabricantes/. Acesso em: 20 dez. 2017.

[217] BATISTA, Henrique Gomes. CIA controla celulares, PCs e até smart TVs, indica WikiLeaks. **O Globo**, mar. 2017. Disponível em: <https://oglobo.globo.com/mundo/cia-controla-celulares-pcs-ate-smart-tvs-indica-wikileaks-21025130>. Acesso em: 20 dez. 2017: "o site WikiLeaks divulgou na terça-feira 8.761 documentos que apontam o uso de softwares elaborados para invadir smartphones, computadores e até mesmo TVs conectadas à internet. Embora a CIA não tenha confirmado a autenticidade dos documentos, o vazamento aumenta as suspeitas de que a agência possa ter ultrapassado limites na vigilância sobre os cidadãos".

[218] PERKINS, Kleiner. Op. cit.

[219] GOMES, Helton Simões. Brasil supera marca de 100 milhões de internautas, diz IBGE. **G1**, São Paulo, nov. 2016. Dispnível em: <http://g1.globo.com/tecnologia/noticia/2016/11/brasil-supera-marca-de-100-milhoes-de-internautas-diz-ibge.html>.Acesso em: 20 dez. 2017.

[220] CHANG, Lulu. 5 billion people worldwide now have a mobile device, GSMA data shows. **Digital Trends**, jun. 2017. Disponível em: <https://www.digitaltrends.com/mobile/5-billion-mobile-users/?utm_source=feedly&utm_medium=webfeeds>. Acesso em: 20 dez. 2017.

[221] CAPELAS, Bruno. Até o fim de 2017, Brasil terá um smartphone por habitante, diz FGV. **Link Estadão**, abr. 2017. Disponível em: <http://link.estadao.com.br/noticias/gadget,ate-o-fim-de-2017-brasil-tera-um-smartphone-por-habitante-diz-pesquisa-da-fgv,70001744407>. Acesso em: 20 dez. 2017.

Todas esses fatores geram um volume de dados sem precedentes, de modo que produzimos, todos os dias, 2,5 quintilhões de bytes de dados, seja através de sensores que coletam dados de compra, tempo e deslocamento, seja através das mensagens, vídeos e imagens trocadas nas redes sociais, de modo que 90% dos dados existentes atualmente foram produzidos nos últimos dois anos[222].

Com efeito, o termo *big data* surgiu justamente em virtude da preocupação de astrônomos e geneticistas que, no início do século XXI, diante da impossibilidade de armazenar todos os dados disponíveis na memória dos computadores, se debruçavam a criar novos instrumentos para analisar estes imensos bancos de dados[223]. O grande diferencial do *big data* é a volumosa oferta de dados aliada ao barateamento das tecnologias de coleta, armazenamento e processamento de dados. Não se pode dizer que haja um conceito único do que seja *big data* utilizando-se, no mais das vezes, o mesmo termo para descrever diferentes situações, de modo que se afirma ser a expressão ampla, vaga, imprecisa e até mesmo criticada[224].

Contudo, compreender os traços comuns do fenômeno que se convencionou chamar de *big data* mostra-se deveras importante para perquirir os reflexos da sua aplicação sobre o direito à privacidade.Para o relator especial sobre direito à privacidade da Organização das Nações Unidas, Joseph Cannataci, big data "é o termo comumente usado para descrever o grande volume crescente de dados e as técnicas avançadas de análise usadas para pesquisar, correlacionar, analisar e disso extrair conclusões"[225]. No mesmo sentido, para Viktor Mayer-Schonberer e Kenneh Cukier, *big data* diz respeito a coisas que alguém pode fazer em larga escala que não podem ser feitam em escala menor para extrair novas ideias ou criar novas

---

[222] JACOBSON, Ralph. IBM. 2.5 quintillion bytes of data created every day. How does CPG & Retail manage it? **IBM**,abr. 2013. Disponível em:<https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/>. Acesso em: 20 dez. 2017.

[223] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 6.

[224] GOMES, Rodrigo Dias de Pinho Gomes. 2017. **Big data**: desafios à tutela da pessoa humana na sociedade da informação. Dissertação (Mestrado em Direito) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017.

[225] Tradução livre. Lê-se, no original: "Big data is the term commonly used to describe the large and increasing volume of data and the advanced analytic techniques used to search, correlate, analyse and draw conclusions from it. United Nations. Report of Special Rapporteur on the right to privacy (advanced United Version)". UNITED NATIONS. Report of the Special Rapporteur of the Human Rights Council on the right to privacy. A/72/43103, out 2017, p. 10. Disponível em: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>. Acesso em: 20 dez. 2017.

formas de valor, de modo que se modifiquem mercados, organizações, o relacionamento entre cidadão e governo, e outros[226].

O Instituto de Tecnologia & Sociedade do Rio apresenta uma concepção mais completa e compreensível do *big data*:

> [P]odemos dizer que Big Data é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores. Todas as ações e comunicações em plataformas digitais, como com telefones celulares, computadores ou mesmo transações de cartão de crédito e, mais recentemente, declarações de imposto de renda, ou ações que, em algum momento, são digitalizadas e assim transformadas em dados, como as câmeras de segurança associadas com software de reconhecimento facial ou de padrões, são passíveis de serem armazenadas, processadas, copiadas e distribuídas quase instantaneamente, possibilitando análises de dados que podem levar governos e empresas a tomar decisões supostamente melhor fundamentadas.[227]

Do cotejamento entre as duas concepções aqui trazidas, resta claro que um ponto comum na definição de *big data* é a elevada quantidade de dados, viabilizada pela difusão de dispositivos e sensores e o aparato tecnológico que permita o rápido processamento destes dados com vistas a resultados que possibilitem a solução de problemas, o aperfeiçoamento de produtos e serviços ou mesmo a prevenção de prováveis adversidades.

Uma descrição mais analítica do *big data* possui como ponto de partida as condições essenciais para a sua ocorrência, haja vista que somente através destes elementos foi possível gerenciar as novas bases de dados de proporções sem precedentes. Tais elementos ficaram conhecidos como os 3 Vs do *big data*[228], quais sejam, volume, variedade e velocidade.

O volume se refere ao tamanho da base de dados, consistente em terabytes ou pentabytes de dados[229], portanto, diz respeito à vasta quantidade de dados que pode ser reunida e analisada efetivamente. Os custos da coleta e do armazenamento de dados

---

[226] Tradução livre. Lê-se, no original: "big data refers to things one can do on a large scale that cannot be done on a smaller scale to extract new insights or create new forms of value, so that markets, organizations, the relationship between citizen and governments, and more" MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 6.

[227] INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. **Big Data no Sul Global**: Relatório sobre estudos de caso. Rio de Janeiro: ITS, 2016, p. 9. Disponível em: <https://itsrio.org/wp-content/uploads/2017 fev. ITS_Big-Data_PT-BR_v4.pdf>. Acesso em: 22 dez. 2017.

[228] Na verdade, há variações que apresentam 4 Vs, como é o caso do National Institute of Standards and Technology, vide NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Big Data Interoperability Framework**: Volume 1, Definitions. [s.l.]: NIST, 2015, p. 4. Disponível em: <https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf>. Acesso em: 20 dez. 2017.

[229] UNITED NATIONS. Op. cit., p. 2.

continuam a cair intensamente e a possibilidade de acessar inúmeras fontes de dados potencializa a base da dados da análise preditiva[230].

A velocidade se refere à rapidez com que companhias podem acumular, analisar e usar novos dados, praticamente em tempo real. A evolução tecnológica permite que companhias aproveitem o poder preditivo dos dados mais imediatamente que antes, algumas vezes instantaneamente[231]. Exemplos de dados em alta velocidade incluem dados de fluxo do clique que registra as atividades online dos usuários à medida que interagem com páginas da web, os dados GPS de dispositivos móveis, que acompanham a localização em tempo real, pois na verdade, um aplicativo de mapeamento móvel é essencialmente inútil se não pode identificar de forma imediata e precisa a localização do dispositivo e o processamento em tempo real é essencial para aplicativos utilizados para traçar rotas, por exemplo[232].

A variedade se refere aos diferentes tipos dos dados que passam a estar disponíveis para coleta, análise e processamento, comodados extremamente diferentes, nunca relacionados, que permitem inferir preferências do indivíduo para fins comerciais ou mesmo identificar indivíduos com propensões a ações criminosas. Desta forma, pode-se combinar dados de pagamento com dados de localização e trajeto para se concluir que determinadas pessoas se reuniram e realizaram negócios em determinado local.

A variedade de dados, portanto, se manifesta tanto por suas fontes quanto por seus formatos. Pode-se citar como exemplo os dados disponíveis na internet em geral; as mídias sociais; os aplicativos de aparelhos móveis; os registros e bancos de dados federal, estadual e municipal; os bancos de dados comerciais que agregam dados individuais de transações comerciais e registros públicos; dados de geolocalização; pesquisas; e documentos *offline* tradicionais, digitalizados pelo reconhecimento óptico de caracteres em eletrônicos.

Ademais, com o advento dos dispositivos e sensores mais habilitados para Internet, expande-se a capacidade para coletar dados de entidades físicas, incluindo sensores e identificação por chips de radiofrequência (RFID), como é o caso dos sistemas de bilhetagem eletrônica[233] dos modais de transporte público[234]. Os dados de localização pessoal podem vir

---

[230] FEDERAL TRADE COMISSION. Op. cit.

[231] EXECUTIVE OFFICE OF THE PRESIDENT. **Big data**: seizing opportunities, preserving values. Washington: The White House, 2014. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 18 dez. 2017. p. 5.

[232] Ibidem.

[233] GUERREIRO, Yan. você Sabia Que o Bilhete Único Utiliza a Tecnologia RFID?**RFID Brasil**, out. 2017. Disponível em: <https://rfidbrasil.com/blog/bilhete-unico-com-rfid/>. Acesso em: 05 jan. 2018.

de chips de GPS, triangulação de torre celular, de dispositivos móveis, mapeamento de redes sem fio e pagamentos em pessoa.

Esta base de dados será ainda mais expandida com a popularização ainda em curso de equipamentos que integram a chamada internet das coisas[235], cujos sensores serão novos coletores de dados que, conectados à internet, se comunicarão entre si sem qualquer intermediação humana. Portanto, os dados de consumo monitorados pela geladeira inteligente serão transmitidos ao supermercado, as manobras arriscadas nas quais se envolveu serão transmitidas pelo computador de bordo do veículo à concessionária ou seguradora, ou mesmo os dados de saúde serão transmitidos ao seu médico através dos monitores conectados à rede.

À medida que todos os meios de coleta de informação se integram à internet, expande-se a variedade do banco de dados disponíveis ao *big data*. Tal fato não é isento de preocupações, porque quanto maior a base de dados, mais difícil a segurança da anonimização destes dados, vez que a combinação dos diferentes tipos de dados é justamente o que possibilita desanonimizá-los. Nessa perspectiva, a expansão do volume e a variedade de dados, a partir da integração de diferentes bancos de dados, fontes e sensores, podem ocasionar a violação da privacidade de indivíduos, estimulando estigmatização, perseguição e até mesmo repressão estatal de dissidentes.

Há quem analise entre os elementos do *big data* um quarto ou quinto "V", enquanto elemento do *big data*, representado pela variabilidade (*variability)*[236],que se refere à variação tanto da taxa de fluxo de dados, causado por picos de fluxo de dados, quanto por variações no formato ou na composição. Outro elemento apontado é a veracidade *(veracity)*,que nada mais é que a preocupação com a integridade e precisão dos dados. Neste ponto, vale a máxima

---

[234]No âmbito do Município do Rio de Janeiro, desde 2000, a Lei nº 3.167 instituiu o sistema de bilhetagem eletrônica por radiofrequência nos serviços de transporte público de passageiros por ônibus, tendo o Decreto nº 19.936/2001 promovido a devida regulamentação.

[235] Do inglês, *Internet of Things*, A "Internet das coisas" é um termo usado para descrever a capacidade dos dispositivos se comunicarem uns com os outros, sem qualquer intermediação humana (comunicação máquina-máquina) usando sensores integrados que estão ligados por meio de conexão com fio e sem fio redes. Esses dispositivos podem incluir seu termostato, seu carro ou uma pílula que você engula e possibilite ao médico pode monitorar a saúde do seu aparelho digestivo. Estes dispositivos conectados usam a internet para transmitir, compilar e analisar dados. Para ficar em um exemplo hipotético de um futuro n, a geladeira inteligente poderá monitorar seu estoque de bebidas e solicitar via internet ao supermercado de sua preferência que bebidas faltantes devem ser entregues, debitando o supermercado o valor da compra no seu cartão cadastrado e "avisando" à geladeira que o produto foi comprado, informando a previsão de entrega. Da mesma forma, o computador de bordo do carro pode monitorar o quanto a condução de determinado motorista é cautelosa/perigosa e comunicar todos os dados de trajeto a uma base de dado das seguradoras que dará maiores ou menores descontos no valor de seguro de acordo com os locais pelos quais trafega e o tipo de condução que realiza.

[236]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Op. cit., p. 15.

"garbage in, garbage out"[237], ou seja, se o dado processado é incorreto, impreciso ou foi alterado, seu processamento não trará nenhuma utilidade, pois, como resultado do processamento, haverá também uma informação incorreta[238].

No nosso sentir, para fins didáticos, é preferível que se fique com a classificação tradicional que define o *big data* por seus três elementos principais.

Há quem afirme, ainda, que o *big data* é algo maior que o fenômeno tecnológico, tratando-se de um fenômeno cultural, tecnológico e acadêmico, que se assenta na interação entre: (i) tecnologia, caracterizada pela maximização do poder da computação e da precisão do algoritmo para reunir, analisar, relacionar e comparar grandes bancos de dados; (ii) análise, que significa extrair dos grandes bancos de dados padrões com o objetivo de alcançar resultados de cunho jurídico, econômico, social e técnico; (iii) mitológico, pelo qual o *big data* gera a crença generalizada de que amplos bancos de dados oferecem uma forma de inteligência superior e um conhecimento que pode gerar ideias que eram antes inalcançáveis, com o diferencial da veracidade, objetividade e precisão destes dados[239].

Este grande volume de dados que caracteriza o *big data* possui um ciclo de vida, ou seja, há um caminho a ser percorrido desde o dado tal como produzido até se tornar uma informação útil. O ciclo de vida do *big data* consiste em quatro fases[240]: (i) coleta, (ii) compilação e consolidação, (iii) mineração dos dados e análise e (iv) uso[241]. O ciclo de vida dos dados é, portanto, o conjunto de etapas em uma determinada aplicação que transforma dados brutos em conhecimento útil. No entanto, nem todo dado começa como *big data*. A bem da verdade podem ser coletados poucos bits de diferentes fontes e a integração destes dados pode gerar o *big data.*

A primeira fase do ciclo de vida do *big data* é a coleta de dados que pode ser definida como a etapa que reúne e armazena dados em seu formato original[242]. Esta fase mostra-se

---

[237] Tradução literal: lixo entra, lixo sai.

[238] Há outras características apontadas, tais como o valor da análise para quem processa o dado que deve ser superior àquele anterior ao processado; volatilidade, ou seja, a tendência de mudanças nas estruturas de dados ao longo do tempo e a validade (a adequação dos dados para o uso pretendido). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Op. Cit., p. 7.

[239] BOYD, Danah; CRAWFORD, Kate.Critical questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. **Information, Communication & Society**, v. 15, n. 5, p. 663, jun. 2012.

[240] Há uma classificação alternativa das quatro fases do ciclo do *big data* que pouco se diferencia na essência da apresentada. São as seguintes: coleta; preparação; análise e ação. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Op. cit., p. 4.

[241] FEDERAL TRADE COMISSION. Op. cit., p. 3.

[242]NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Op. Cit., p. 16.

essencial e quanto mais ampla e representativa a coleta melhor será o resultado do processamento. Para a realização da coleta, há tecnologias de rastreamento do usuário que cada vez mais desafiam a privacidade do indivíduo na rede.

Uma das tecnologias mais tradicionais de rastreamento são os *tracking cookies*[243], que consiste em um arquivo de texto simples, que armazena temporariamente no navegador os locais que o internauta está visitando na rede. A maioria dos sites armazena informações básicas, como endereços IP, preferências sobre idiomas, cores, entre outros. Os *cookies* permitem que essas informações armazenadas sejam distribuídas, compartilhadas e lidas em dois ou mais sites da Web não relacionados, com o objetivo de coletar informações, o que significa dizer que quando o internauta retorna ao site que armazenou cookies, o site poderá ler estas informações, o que possibilitará traçar um perfil específico daquele internauta. Seu objetivo é duplo – personalizar a navegação de acordo com suas preferências e ajudar os sites visitados (além de investidores e anunciantes) a conhecer melhor o internauta[244]. Por se tratar de uma das formas mais antigas de coletar dados, não se pode negar que a utilização dos *cookies* tem aperfeiçoado a qualidade da navegação, facilitando ao usuário localizar assuntos de seu interesse, mas isso não isenta o uso de *cookies* de preocupações quanto à violação da privacidade[245].

Em virtude de ser uma forma antiga de coleta, atualmente, navegadores e anti-vírus possibilitam configurações específicas que permitem o bloqueio da coleta por cookies. Outra forma de rastreamento alternativa é o *browser fingerprint* (ou *device fingerprint*)[246], que

---

[243]TRACKING COOKIE. **Symantec**, jul. 2014. Disponível em: <https://www.symantec.com/security_response/writeup.jsp?docid=2006-080217-3524-99&tabid=2>. Acesso em: 22 dez. 2017. Tracking cookie é uma forma específica de cookie, há outra forma de cookie, o orphan cookie que pode ser considerada inofensiva pois os dados armazenados no disco rígido não podem ser lidos pelo navegador.

[244] REDAÇÃO. O que são cookies? **Super Interessante**, out. 2016. Disponível: <https://super.abril.com.br/tecnologia/o-que-sao-cookies/>. Acesso em: 18 dez. 2017. O termo *cookie* (biscoito em inglês) é também uma gíria para "pessoa de um determinado tipo". Ou seja, uma figura ou estereótipo. E é exatamente essa a função dos cookies da internet: moldar um perfil determinado do usuário que ficam armazenados no seu computador. E há quase 20 anos causam polêmica por ameaçar a privacidade do internauta.

[245] "Em síntese: a tecnologia dos cookies não representa em si uma violação ao direito da privacidade. Todavia, a forma pela qual irá se estruturar a coleta, o armazenamento e a utilização das informações pessoais é que irá determinar a licitude, ou ilegalidade, da conduta do administrador do banco de dados.

Uma das utilizações que podem ser manejadas depois da coleta dos dados pessoais é a compilação de e-mails para a finalidade de envio de spams.". LEMOS, Ronaldo et al. Estudo sobre a regulamentação jurídica do spam no Brasil. Trabalho comissionado pelo Comitê Gestor da Internet no Brasil ao Centro de Tecnologia e Sociedade (CTS), da Escola de Direito do Rio de Janeiro/Fundação Getúlio Vargas, Fundação Getulio Vargas, Rio de Janeiro, 2007. Disponível em: <https://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 22 dez. 2017.

[246] "[F]ingerprinting é parte de um conjunto amplo de tecnologias e técnicas, também conhecidas como Device Intelligence, Machine Fingerprinting, Browser Fingerprinting, Web Fingerprinting ou Device Fingerprinting,

consiste na criação de uma impressão digital do navegador ou dispositivo, ou seja, trata-se da coleta de informação sobre um dispositivo de computação para efeitos de estabelecer uma identificação única do dispositivo ou usuário com base em informações do navegador do dispositivo, sistema operacional, versão do software, resolução de tela, plugins, entre outros.

As impressões digitais podem ser usadas para identificar total ou parcialmente usuários ou dispositivos individuais, mesmo quando os *cookies* estão desligados. Uma aplicação útil da impressão digital dos dispositivos é prevenir fraudes e roubos de identidade *online*[247], tanto é assim que algumas instituições bancárias[248] apenas permitem o acesso ao aplicativo do banco caso seja por meio de dispositivo cadastrado. Embora inegável a utilidade da impressão digital do dispositivo, a técnica traz sérias ameaças à privacidade. A uma porque, diferente dos *cookies*, a dificuldade de impedir a coleta é maior[249]. Ademais, possibilitando a identificação do dispositivo por meio de uma impressão única, será possível rastrear com precisão a atividade daquele dispositivo em específico na *web* e, se se tratar de um dispositivo de uso pessoal, será possível identificar o dispositivo e até mesmo o usuário.

Uma terceira forma de coleta, conhecida como *history sniffing*[250] (do literal, cheiro do histórico) consiste em explorar as vulnerabilidades do navegador da internet para investigar que sites o usuário visitou. Isto porque, em geral, os navegadores exibem em cores diferentes os sites visitados e aqueles que o usuário já clicou. Portanto, a exploração desta vulnerabilidade pode deixar exposto todo o histórico de navegação do usuário, informação que pode ser usada para aperfeiçoar a experiência do indivíduo[251] ou mesmo para

---

usadas para identificar (ou reidentificar) um usuário ou um dispositivo, através de um conjunto de configurações, atributos (tamanho da tela do dispositivo, versões de software instalado, entre muitos outros) e outras características observáveis durante comunicações." SARAIVA, Adriana R. et al. Device Fingerprinting: Conceitos e Técnicas, Exemplos e Contramedidas. Minicursos do XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Sociedade Brasileira de Computação, 2014. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0035.pdf>. Acesso em: 20 dez. 2017.

[247] Ibidem, p. 53.

[248] FRANCIS, Bob. User confidence takes a Net loss. **InfoWorld**, jul. 2005. Disponível em:<https://www.infoworld.com/article/2670085/security/user-confidence-takes-a-net-loss.html>. Acesso em: 20 dez. 2017.

[249] Diferente dos cookies, não é possível bloquear a prática do *device fingerprint* que utiliza Javascript. Todavia, é possível atenuá-la com algumas medidas, tais como o uso de navegadores mais populares, manter o sistema mais atualizado, navegar em modo privado, usar um serviço de VPN, entre outros. CRAIG, Cristina. Device Fingerprinting the tracking we can't avoid. **Nordvpn**, abr. 2017. Disponível em: <https://nordvpn.com/blog/device-fingerprinting-the-tracking-we-cant-avoid/>. Acesso em: 20 dez. 2017.

[250] BROOKMAN, Justin. Browser History Sniffing in the News. **Center for Democracy & Technology**, dez. 2010. Disponível em: <https://cdt.org/blog/browser-history-sniffing-in-the-news/>. Acesso em: 20 dez. 2017.

[251] "According to Albanesius, information collected via **history sniffing** could be used by organisations to track visits to competitor's sites, by advertisers to help construct detailed user profiles, and by criminals to launch

perseguições e exposições. Ressalte-se que o código utilizado para rastrear o histórico do navegador é utilizado de forma sorrateira, sem que o usuário perceba que esta informação está sendo recolhida.

Alguns responsáveis por navegadores, como o Chrome e Safari, afirmaram que as versões atualizadas dos seus navegadores não mais possuem a vulnerabilidade que permite o rastreamento do histórico[252]. Todavia, mesmo que o uso da prática seja algo superado, certamente serão criadas novas formas de obter o máximo de informações possíveis do usuário, seja de forma lícita ou ilícita, de modo que o ordenamento jurídico deve dar respostas claras e suficientes a resguardar a privacidade dos usuários quanto às práticas de rastreamento nas redes.

A fase posterior à coleta no ciclo de vida do *big data* é a compilação e consolidação[253] dos dados, que consiste na organização dos dados recolhidos e na transformação dos dados em estado bruto em um formato lapidado, pronto para a análise. A compilação é realizada por variados agentes, citando-se como exemplo empresas de anúncios *online*, mídias sociais, grandes bancos ou varejistas.

Neste ponto, uma categoria que se destaca são os *data brokers*[254] ou corretores de dados. São empresas cujo modelo de negócios é coletar informações de usuários e as revender ou compartilhar, bem como vender serviços de perfilamento e classificação do usuário. Os *data brokers* utilizam informações de diferentes fontes, estatais ou não, sejam sobre atividades *online*, tais como compras em websites e informações em redes sociais, ou *offline*, como cadastros preenchidos, aquisição de imóveis ou outros bens em lojas físicas. A

---

increasingly realistic phishing attacks." HISTORY SNIFFING. **Schott's Vocab**, jun. 2011. Disponível em: <https://schott.blogs.nytimes.com/2010/12/08/history-sniffing/>. Acesso em: 20 dez. 2017.

[252]WHAT YOU SHOULD Know About History Sniffing. **Krebs on Security**, dez. 2010. Disponível em:<https://krebsonsecurity.com/2010/12/what-you-should-know-about-history-sniffing/>. Acesso em: 20 dez. 2017.

[253] FEDERAL TRADE COMISSION. Op. cit., p. 4.

[254] Um relatório da *Federal Trade Comission* analisou a atividade de nove empresas *data brokers* nos Estados Unidos e concluiu que havia falta de transparência quando ao método utilizado para a coleta e combinação de dados, tendo havido recusa destas empresas em declinar quais eram suas fontes de dados e clientes. Veja-se algumas práticas de legalidade duvidosas dos data brokers, constantes do relatório: Data brokers combinam e analisam dados sobre consumidores para fazer inferências sobre eles, incluindo inferências potencialmente sensíveis; combinam dados online e offline para gerar anúncios para consumidores online. FEDERAL TRADE COMISSION. **Data Brokers**: A Call for Transparency and Accountability. FTC: [s.l.], p. 46. Disponível: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 20 dez. 2017.

combinação e compilação destas variadas informações permite que se construam perfis sobre usuários e se comercialize esse material[255].

A próxima etapa do ciclo do *big data* consiste na análise. As análises podem ser prescritivas, diagnósticas, descritiva e preditiva. Dentre estas, as análises mais relevantes são a descritiva e a preditiva. A primeira ocorre quando o objetivo é descobrir e catalogar padrões ou características que existem na base de dados. Trata-se de analisar os dados em tempo real para atribuir respostas aos problemas do presente. A segunda é realizada através da prática do *data mining*[256](‘mineração de’ dados’ ou ‘prospecção de dados’), que consiste no processo automatizado de extrair padrões úteis e consistentes de grandes bancos de dados[257], estabelecendo regras de associação ou sequências temporais, para detectar relacionamentos entre variáveis, com vistas a descobrir regras, identificar fatores e tendências. Na análise prescritiva, busca-se, a partir do estudo de casos, definir a consequência para cada ação realizada[258].

Por outro lado, a análise preditiva de dados consiste no modelo estatístico não apenas para descrever um cenário e compreender o presente, mas para prever um cenário futuro. Significa dizer que esse modelo utiliza os dados atuais, para, identificados certos padrões de comportamento, “prever” comportamentos futuros de pessoas com perfis semelhantes. Portanto, compras anteriores, buscas na internet, hábitos de consumo e preços pagos são

---

[255] Um exemplo que pode ser dado no contexto brasileiro é o grupo Serasa Experian, conhecido pela análise de crédito de consumidores, verifica-se sua atividade de *data broker* ao realizar os serviços abaixo listados, anunciados em seu website, utilizando ferramentas típicas de *big data*:

(i) Mosaic: O poder da segmentação de clientes ao seu alcance. Segmentação de dados baseada em técnicas analíticas e estatísticas. O Mosaic Brasil classifica a população brasileira em 11 grupos e 40 segmentos, considerando aspectos financeiros, geográficos, demográficos, de consumo, comportamento e estilo de vida.

(ii)*Clone Express*: Clone o perfil dos seus melhores clientes, por meio de modelagem estatística, para ações de prospecção.

(iii) *Digital Audience*: Trabalhe com uma base de dados offline e toda a expertise da Serasa Experian no mundo online, atingindo seus clientes no ambiente digital e procurando perfis semelhantes para melhorar sua campanha.

(iv) *Perfil Express*: Obtenha relatórios visualmente intuitivos para auxiliar na compreensão do perfil dos seus clientes, comparando-os ao mais completo banco de dados de marketing do país.

[256] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 4.

[257] “The most commonly accepted definition of “data mining” is the discovery of “models” for data. A “model,” however, can be one of several things.” (Em tradução livre: “A definição mais comum de "mineração de dados" é a descoberta de "modelos" para dados. Um "modelo", no entanto, pode ser uma das várias coisas”.) Os autores apresentam outros modelos de mineração de dados além da modelagem estatística, tais como leitura de máquina, a sumarização, extração de características, entre outros os quais não cabe aqui um maior aprofundamento por fugir do escopo deste trabalho. Vide LESKOVEC, Jure; MILLIWAY, Anand R.; ULLMAN, Jeffrey D. **Mining of Massive Datasets**. Disponível em: <http://infolab.stanford.edu/~ullman/mmds/book.pdf>. Acesso em: 08 jan. 2017.

[258] SAISSE, Renato. Big Data Contra o Crime: Efeito Minority Report. **Direito & TI**, Porto Alegre, v. 1, p. 5, 2017.

informações que, se devidamente processadas, podem antecipar um comportamento altamente provável do consumidor, dando vantagem competitiva a quem faz uso do modelo. Logo, a análise preditiva utiliza dados do modelo descritivo para gerar novos dados de comportamento, preditivos[259]. Em outras palavras, os modelos de análise descritivo e preditivo não são estanques, podendo o modelo descritivo servir de subsídio ao preditivo[260].

O termo prever é utilizado entre aspas porque por mais que haja probabilidades estatísticas de determinado comportamento ser adotado, a análise preditiva é tão somente um modelo estatístico, de probabilidade, de tendência, não se podendo desconsiderar a autodeterminação humanaenquanto elemento essencial da ação. Assemelha-se, portanto, à previsão do tempo que apenas aponta tendências com base em padrões anteriores. No caso do comportamento humano, há uma incerteza ainda maior que a meteorologia.

Conforme se verá a seguir, a grande crítica que sofre o modelo preditivo é que crença irrefletida nos dados pode propiciar modelos de negócios enviesados e discriminatórios. Um fator adicional a essas preocupações é o uso cada vez mais comum pelas autoridades de segurança pública e mesmo pelo judiciário estadunidense do policiamento preditivo (*predictive policing*) que determinam onde e quando deve ser feito o policiamento ou mesmo qual a tendência estatística de reincidência de determinado preso para concedê-lo progressão ou liberdade condicional[261].

A última etapa do ciclo do *big data* é o uso efetivo das análises realizadas. No contexto atual,os dados assumiram papel de ativo econômico altamente valioso, de forma que podem ser utilizados para os mais diversos propósitos. Não é incomum que um indivíduo que tenha adquirido determinado produto de luxo seja alvo de marketing direcionado de outros produtos e serviços para esse segmento de mercado. Mas não é só isso, a ubiquidade dos dados e a multiplicidade de sensores decorrentes da atual integração tecnológica provê dados dos mais variados tipos, oriundos das mais diversas fontes, de modo que um mesmo dado pode servir para orientar estratégias empresariais no mercado de consumo ou possibilitar o desenho de determinada política pública de saúde, antecipando o possível surto de determinada doença.

---

[259] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 5.

[260] Há quem identifica quatro modelos distintos de análise de dados e não apenas dois, quais sejam: preditiva, prescritiva, descritiva e diagnóstica. Vide: AS DIFERENÇAS ENTRE análise prescritiva, preditiva, descritiva e diagnóstica. **Blog Vert**, [s.d.]. Disponível em: <http://www.vert.com.br/blog-vert/as-diferencas-entre-analise-prescritiva-preditiva-descritiva-e-diagnostica/>. Acesso em: 20 dez. 2017.

[261] MAYER-SCHONBERER, Viktor, CUKIER, Kenneh. Op. cit., p. 161.

Desta forma, avulta a importância do uso secundário dos dados, sem o qual perde o sentido qualquer modelo de negócios baseado em *big data*. O potencial de efeitos positivos do processamento deste grande volume de dados apenas faz sentido se tais dados puderem ser integrados e aplicados em variadas finalidades.

O uso secundário de dados apresenta novos desafios ao estágio atual da concepção de proteção da privacidade de dados pessoais. Isto porque a concepção clássica da proteção de dados impõe a observância de uma série de princípios[262], concebida nos documentos transnacionais editados na década de 1980 do século passado, citando-se como exemplo a Convenção do Conselho da Europa, de janeiro de 1981, e a recomendação da OCDE, de setembro de 1980. Todavia, há que se pontuar que, desde a década de oitenta até os dias atuais, muitas evoluções ocorreram no que tange à utilização e otimização do uso dos dados, de modo que há que se adequar tais previsões à era do *big data*.

Cumpre, agora, analisar os benefícios e riscos trazidos pelo uso do *big data* e que medidas podem ser tomadas para potencializar os benefícios e neutralizar os possíveis riscos.

2.2 **Benefícios e Oportunidades decorrentes da utilização do *Big Data***

Inicialmente, é preciso dizer que todo e qualquer avanço tecnológico não é por si só bom ou ruim, o que vai depender do uso que se faça ou se permita fazer com determinada tecnologia. Os benefícios concretos decorrentes do *big data* são inúmeros. Alguns deles já puderam ser desfrutados, outros estão em vias de implantação.

Imagine um sistema que, a partir da localização de dois milhões de chips de telefone celular, pode antecipar o trajeto do movimento migratório de um grupo afetado por um terremoto no Haiti, possibilitando que organizações humanitárias e governamentais monitorem o movimento migratório e se desloquem em direção aos desalojados para prestar auxílio[263]; ou um hospital em Toronto cujo algoritmo pode prever risco de infecções e outras complicações em bebês prematuros, a partir do monitoramento de sua frequência cardíaca,

---

[262] Pode-se citar como entusiasta destes princípios Stefano Rodotá, para quem os princípios que devem ser observados na proteção de dados pessoais são: o princípio da correção dos dados; o princípio da exatidão dos dados coletados; o princípio da finalidade da coleta; princípio da publicidade; do acesso individual; e princípio da segurança lógica e física da proteção de dados.

[263] WORLD ECONOMIC FORUM. **Big Data, Big Impact**: New Possibilities for International Development. WEF: [s.e.], 2012. p. 3. Disponível em: <http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf>. Acesso em: 20 dez. 2017.

com até 24 horas de antecedência[264]; ou um sistema de monitoramento por satélite que informa ao motorista que vagas públicas de estacionamento estão disponíveis em sua localidade praticamente em tempo real, levando em conta os dados de localização celulares dos motoristas cadastrados e a legislação local sobre locais permitidos de estacionamento[265].

A própria funcionalidade dos aplicativos em geral tem se aperfeiçoado a partir do uso do *big data*. O Waze, aplicativo que traça rotas urbanas, ao indicar caminhos mais rápidos, baseia seus diagnósticos de tempo de trajeto nas informações inseridas pelos usuários quanto às condições de trânsito, acidentes, vias interditadas, condições climáticas entre outros. Ademais, o trajeto realizado com o aplicativo aberto é processado em tempo real para que se chegue à média de tempo estimado e se oriente o usuário e outros motoristas[266].

Da mesma forma, o *big data* permite que o Google aperfeiçoe seu motor de buscas, processando em tempo real as mais de três bilhões de buscas diárias[267] que estão sendo feitas por outros usuários, filtrando e adaptando as sugestões de busca para as especificidades do usuário[268]. A funcionalidade é constantemente aperfeiçoada pelas próprias buscas que são

---

[264] BOGART, Nicole. Research in big data analytics working to save lives of premature babies. **Global News**, jul. 2013. Disponível em: <https://globalnews.ca/news/696445/research-in-big-data-analytics-working-to-save-lives-of-premature-babies/>. Acesso em: 20 dez. 2017.

[265] "A companhia Inrix, que tem aproveitado o Big Data para gerenciar o congestionamento do tráfego, revelou um novo serviço que ajuda os motoristas a encontrar pontos de estacionamento abertos. O sistema analisa os dados históricos, as leis e regulamentos atuais, o tempo restante nos estacionamentos conectados à Internet. KANELLOS, Michael. A Big Data App That Helps You Find A Parking Spot. **Forbes**, jun. 2015. Disponível em: <https://www.forbes.com/sites/michaelkanellos/2015/06/03/a-big-data-app-that-helps-you-find-a-parking-spot/#4b23e23c43ba>. Acesso em: 20 dez. 2017. Veja-se interessante estudo a respeito: RUIJTER, Tom.**A big data view of on-street parking**. 2015. Thesis (Master in Computer Science) - Radboud University, Nijmegen, 2015.

[266] O valor agregado do big data é a possibilidade de processar em tempo real o dado de milhões de usuários, estimando-se que sejam 65 milhões em todo o mundo e três milhões na Grande São Paulo. Isso permite ao aplicativo ter em sua base de dados informações úteis ao poder público como o tráfego de veículos em determinado local e permite orientar as políticas públicas para tornar mais eficiente o tráfego. "O Waze usa as informações do seu percurso para calcular a velocidade média, encontrar erros e melhorar o traçado das vias, além de aprender os sentidos de condução e conversões. Você não precisa fazer nenhuma viagem especial com o Waze. Na verdade, o Waze funciona melhor nas suas rotas diárias". COMO O WAZE funciona? **Suporte do Google**, [s.d.]. Disponível em: <https://support.google.com/waze/answer/6078702?hl=pt-BR>. Acesso em: 20 dez. 2017.

[267] DIAS, Guilherme. Cerca de 100 bilhões de buscas são realizadas no Google mensalmente. **TecMundo**, abr. 2014. Disponível em: <https://www.tecmundo.com.br/google/53852-cerca-de-100-bilhoes-de-buscas-sao-realizadas-no-google-mensalmente.htm>. Acesso em: 20 dez. 2017.

[268]"As previsões de pesquisa aparecem com base em: termos que você está digitando; pesquisas relevantes que você fez no passado (se estiver conectado à sua Conta do Google e se a Atividade na Web e de apps estiver ativada); itens que outras pessoas estão pesquisando, incluindo matérias em alta, que são assuntos conhecidos na sua área e que mudam ao longo do dia. Essas matérias não têm relação com seu histórico de pesquisa. Para ver as Matérias em alta, acesse o Google Trends. Observação: as previsões não são a resposta para sua pesquisa. Elas também não são declarações de outras pessoas ou do Google sobre seus termos de pesquisa". Informações disponíveis na área de suporte do google. Disponivel em: <https://support.google.com/websearch/answer/106230?co=GENIE.Platform%3DAndroid&hl=pt-BR>. Acesso em: 21 dez. 2017.

feitas, o que faz com que o aplicativo processe diariamente bilhões de buscas para personalizar e tornar mais eficiente o serviço de cada usuário.

No entanto, há também expectativas frustradas trazidas pelo *big data*, em virtude de correlações equivocadas e promessas não cumpridas. Este foi o caso do *Google Flu Trend*. Criada em 2008, a funcionalidade prometia antecipar os surtos de gripe e dengue antes mesmo dos relatórios oficiais das autoridades de saúde. O dado alimentador do algoritmo que determinava a incidência da doença eram os termos de busca utilizados pelos usuários no site, que considerava buscas pelas doenças bem como pelos seus sintomas. Ocorre queposteriormente se comprovou que as estimativas eram equivocadas, tendo o programa se encerrado[269].

Isso porque a funcionalidade partia de uma correlação equivocada. A busca de determinado termo não pode fazer inferir que quem tenha realizado a busca esteja contaminado, uma vez que as pessoas buscam informações sobre determinadas doenças por diversas razões. Da mesma forma, um sintoma pode ocorrer em razão de várias doenças ou ser um fato isolado. A ferramenta sofreu intensas críticas[270], já que a correlação realizada não implicava necessariamente em uma relação de causalidade.

Com efeito, casos malsucedidos não invalidam o *big data* enquanto modelo altamente promissor, mas tão somente alertam que os dados podem muito, mas não podem tudo[271] e seuslimites e riscos devem ser levados em consideração em qualquer análise implementada.

Cumpre, agora, analisar algumas áreas nas quais o uso do *big data* possui o potencial de revolucionar de forma disruptiva, a saber, o setor de saúde e as ações humanitárias, bem como a promoção da diversidade e igualdade no acesso à educação, crédito e mercado de trabalho.

2.2.1 Benefícios no setor de saúde e nas ações humanitárias

[269] "Google Flu Trends e Google Dengue Trends não estão mais publicando estimativas atuais de gripe e dengue com base em padrões de busca. As estimativas históricas produzidas pela Google Flu Trends e Google Dengue Trends estão disponíveis abaixo. Ainda são dias adiantados para nowcasting e ferramentas similares para compreender a propagação de doenças como gripe e dengue - estamos entusiasmados por ver o que vem depois. Os grupos de pesquisa acadêmica interessados em trabalhar conosco devem preencher este formulário" (Tradução livre). Informações disponíveis em: <https://www.google.org/flutrends/about/>. Acesso em: 20 dez. 2017.

[270]LAZER, D. M. et al.The Parable of Google Flu: Traps in Big Data Analysis. **Science**, v. 343, n. 6176, p. 1203-1205, mar. 2014.

[271] LOHR, Steve. Google Flu Trends: The Limits of Big Data.**Bits**, mar. 2014. Disponível em: <https://bits.blogs.nytimes.com/2014/03/28/google-flu-trends-the-limits-of-big-data/>. Acesso em: 20 dez. 2017.

O uso do processamento de grandes bases de dados para ações humanitárias tem mostrado um elevado potencial ainda não explorando. Principalmente entre populações economicamente vulneráveis, nas quais a informação e o panorama em tempo real são escassos, haja vista a ausência de interesse econômico esses grupos.

Neste campo, o *big data* pode contribuir com a possibilidade de proporcionar um cuidado à saúde personalizado de acordo com as características do paciente. Embora, a conduta médica para cada doença seja relativamente padronizada, a reação de cada paciente à conduta adotada e sua propensão de adesão ao tratamento são variáveis. Neste sentido, o uso do *big data* na área médica tem sido útil para prever a expectativa de vida do paciente, a predisposição genética a determinadas doenças, a probabilidade de novas internações ou de aderência ao plano de tratamento[272]. Isso permite prever a propensão de um paciente ter um enfarto ou mesmo ingressar na emergência médica com crise asmática a partir de seus dados de consumo, possibilitando a intervenção prévia[273]. É possível acompanhar por meio de sensores todo o tratamento do paciente, inclusive saber qual o exato momento em que um paciente psiquiátrico ingeriu o medicamento recomendado[274], se faz o uso do fármaco na frequência correta e se sua resposta ao tratamento está adequada à expectativa. Somente em virtude de haver uma capacidade sem precedentes de processamento e armazenamento de dados, além da comunicação com milhares de sensores, permitem esse monitoramento, todas essas funcionalidades são possíveis.

Como visto, a análise preditiva será tanto mais precisa quanto maior e mais processada for sua base de dados. Isto possibilita economia de recursos com procedimentos padronizados que não funcionarão ou serão pouco eficientes com aquele paciente em específico,

---

[272] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 7.

[273] "A Carolinas HealthCare, que administra mais de 900 centros de atendimento, incluindo hospitais, lares de idosos, consultórios médicos e centros cirúrgicos, começou a conectar dados do consumidor em 2 milhões de pessoas em algoritmos destinados a identificar pacientes de alto risco para que os médicos possam intervir antes que eles ficar doente. A empresa compra os dados dos corretores que eliminam os registros públicos, as transações do programa de fidelização de lojas e as compras de cartões de crédito. (...) Para um paciente com asma, o hospital seria capaz de avaliar a probabilidade de chegar à sala de emergência, observando se ele reabasteceu seu medicamento para asma na farmácia, vem comprando cigarros no supermercado e vive em uma área com uma alta contagem de pólen". Tradução livre. PETTYPIECE, Shannon; ROBERTSON, Jordan. Hospitals are mining patients' credit card data to predict who will get sick. **InfoWars**, jul. 2014. Disponível em: <https://www.infowars.com/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick/>. Acesso em: 20 dez. 2018.

[274] CORREIA, Luis Fernando. Medicação com sensor que envia alerta sobre ingestão ao médico é aprovada nos EUA. **CBN**, nov. 2017. Disponível em: <http://cbn.globoradio.globo.com/media/audio/137863/medicacao-com-sensor-que-envia-alerta-sobre-ingest.htm>. Acesso em: 18 jan. 2017.

viabilizando a prática da medicina de precisão, elevando as taxas de êxito, ao adequar o tratamento à especificidade genética, ambiental e de estilo de vida do paciente[275].

A medicina de ponta tem cada vez mais ampliado o uso do *big data* para aperfeiçoar seus resultados. O hospital infantil de Toronto, aqui já citado, é capaz de adiantar o diagnóstico de infecção em bebês prematuros a partir do monitoramento de seus sinais vitais. Há também a iniciativa do Centro Médico da Universidade de Columbia, que analisa informações fisiológicas de pacientes com danos cerebrais, e possibilita uma análise proativa, uma vez que detectam as possíveis complicações nestes pacientes com 48 horas de antecedência em relação aos métodos tradicionais; por fim, um instituto de ortopedia na Itália está reduzindo os custos de tratamento a partir da análise avançada de dados familiares em doenças ósseas hereditárias, monitorando as variabilidades dentro dessas famílias, o que já permitiu uma redução de 30% nas internações e 60% nos exames de imagem[276].

Ademais, somente com o advento do *big data* é possível, por exemplo, processar o sequenciamento genético de milhões de pacientes e encontrar traços comuns e relações desse sequenciamento com o diagnóstico e evolução da doença, propiciando uma medicina de precisão e especializada para determinado paciente. Isto porque o sequenciamento de apenas uma pessoa produz 1 terabyte de dados[277], quantidade de armazenamento e processamento inviável antes do *big data*.

Outras ações de natureza humanitária, sejam na área da saúde quanto na da segurança alimentar, têm sido viabilizadas graças aos recursos tecnológicos proporcionados pelo *big data*. Um exemplo disso é o Global Puse[278], programa das Nações Unidas, que, em 2015, a partir da análise integrada dos prontuários, mediante processamento eletrônico, possibilitou a

---

[275] SHAYWITZ, David. New Diabetes Study Shows How Big Data Might Drive Precision Medicine. **Forbes**, out. 2015. Disponível em: <https://www.forbes.com/sites/davidshaywitz/2015/10/30/new-diabetes-study-shows-how-big-data-might-drive-precision-medicine/#63d1637e44b0>. Acesso em: 20 dez. 2017. Uma iniciativa do governo Estados Unidos, durante a gestão de Barack Obama, foi reunir dados médicos e genéticos de pelo menos um milhão de voluntários, extraídos de bases de dados de grandes redes para caracterizar novos subtipos de diabetes tipo 2 (T2D), o que permitiu a identificação de novos subtipos da doença e os sintomas associados a cada subtipo. Essas distinções podem exigir regimes de tratamento personalizados, em vez de uma abordagem única para T2D. Identification of type 2 diabetes subgroups through topological analysis of patient similarity. LI, Li et al. Identification of type 2 diabetes subgroups through topological analysis of patient similarity. **Science Translational Medicine**, v. 7, n. 311, p. 311 e ss., out. 2015.

[276] **DATA-DRIVEN HEALTHCARE organizations use big data analytics for big gains**. New York: IBM, 2013, p. 5.

[277] PRADO, Eduardo. Medicina personalizada: Big Data no combate ao Câncer [Parte 02]. **Saúde Business**, out. 2015. Disponível em: <http://saudebusiness.com/medicina-personalizada-big-data-no-combate-ao-cancer-parte-02/>. Acesso em: 20 dez. 2017

[278] Vide LUENGO-OROZ, Miguel. Big Data for Development in Action: The Global Pulse Project Series. **United Nations Global Pulse**, jul. 2015. Disponível em: <https://www.unglobalpulse.org/blog/big-data-development-action-global-pulse-project-series. Acesso em: 08 jan. 2017.

identificação de um surto de febre tifoide em Uganda[279], determinando os principais focos da doença e orientando a ação dos agentes de saúde. Outra possibilidade foi verificar a percepção pública de imunização na Indonésiaa partir das postagens publicadas no Twitter[280] ou mesmo o monitoramento das postagens do Facebook a fim de se verificar a percepção do público jovem sobre os métodos contraceptivos e prevenção de doenças sexualmente transmissível, visando, com esse diagnóstico, reduzir o alto índice de gravidez na adolescência[281], o que expressa, nos últimos dois casos, o grande potencial que ainda há nas redes sociais para aplicação do *big data*[282].

O monitoramento da localização de chips de telefone celular revela outro campo fértil aos benefícios do *big data*, tendo sido essencial para as ações humanitárias no terremoto que devastou o Haiti em 2010 e lhe trouxe um surto de cólera, vez que o processamento anônimo das localizações dos chips de telefone celular se aproximavam em muito dos fluxos migratórios dos grupos afetados após o desastre[283]. O mesmo foi possível no terremoto no Nepal em 2014[284], tendo sido viável, ainda, monitorar os movimentos migratórios decorrentes de mudanças climáticas em Bangladesh[285]. A relevância destas aplicações do *big* data deve-se ao fato de 22 milhões de pessoas ficarem desabrigadas em razão de desastres naturais desde 2008, o que corresponde a mais de 60 mil pessoas por dia[286].

---

[279] UN GLOBAL PULSE. Data Visualisation and Interactive Mapping to Support Response to Disease Outbreak. **Global Pulse ProjectSeries**, n. 20, 2015. Disponível em: <https://www.unglobalpulse.org/projects/mapping-infectious-diseases>. Acesso em: 20 dez. 2017.

[280] UN GLOBAL PULSE. Understanding Public Perceptions of Immunisation Using Social Media. **Global Pulse Project Series**, n. 19 2015. Disponível em: <http://www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Perception_Immunisation_2014_0.pdf>. Acesso em: 20 dez. 2017.

[281] UN GLOBAL PULSE. Analyzing Attitudes Towards Contraception & Teenage Pregnancy Using Social Data. **Global Pulse Project Series**, n. 8, 2014. Disponível em: <https://www.unglobalpulse.org/projects/UNFPA-social-data>. Acesos em: 20 dez. 2017.

[282] KLEIN, Gisiela Hasse; NETO, Pedro Guidi; TEZZA, Rafael. Big Data e mídias sociais: monitoramento das redes como ferramenta de gestão. **Saúde Soc. São Paulo**, v. 26, n. 1, p. 208-217, 2017.

[283]HAITI EARTHQUAKE 2010. **Flowminder**, [s.d.]. Disponível em: <http://www.flowminder.org/case-studies/haiti-earthquake-2010>. Acesso em: 20 dez. 2017.

[284]NEPAL EARTHQUAKE 2015. **Flowminder**, [s.d.]. Disponível em: <http://www.flowminder.org/case-studies/nepal-earthquake-2015>. Acesso em: 20 dez. 2017.

[285] MOBILE PHONE DATA to Understand Climate Change and Migration Patterns in Bangladesh. **Flowminder**, [s.d.]. Disponível em: <http://www.flowminder.org/case-studies/mobile-phone-data-to-understand-climate-change-and-migration-patterns-in-bangladesh>. Acesso em: 20 dez. 2017.

[286] GRANDELLE, Renato. Desastres naturais forçam migrações de 60 mil por dia. **O Globo**, out. 2015. Disponível em: <https://oglobo.globo.com/sociedade/sustentabilidade/desastres-naturais-forcam-migracoes-de-60-mil-por-dia-17680284>. Acesso em: 20 dez. 2017.

Do mesmo modo, o surto de Ebola na África ocidental foi adiantado em nove dias pela faculdade de Harvard, a partir da combinação de dados anonimizados de mensagens de voz e texto, de 150 mil aparelhos[287], bem como pela localização dos chips fornecidos por uma operadora de celular do Senegal[288].

Ações de segurança alimentar também podem ser mencionadas. Descobriu-se que há uma estreita relação entre a compra de crédito de chamada de telefone móvel com os tipos de alimentos consumidos por estas famílias. Portanto, localizando os compradores desses créditos, de acordo com a frequência e valores que os compram, identifica-se um consumo mais qualificado de alimentos[289], o que permite uma estimativa próxima da realidade acerca dos locais cuja insegurança alimentar seja mais severa. Outro exemplo é o monitoramento das informações postadas em redes sociais sobre o preço dos alimentos, especialmente em países nos quais o monitoramento de preços em tempo real não se mostra tão confiável[290].

Diante de todos os exemplos, resta claro que a utilização do *big data* tanto para a personalização do tratamento médico, quando para o aperfeiçoamento através do processamento massivo de informações médicas e mapeamento genético está em seu início, mostrando um potencial ilimitado para a redução de custos das despesas de saúde e a personalização de tratamentos que serão otimizados e eficientes, com o uso de sensores e informações transmitidas em tempo real, mostrando-se um modelo bem mais econômico que a visita clínica ao consultório[291], haja vista que os aplicativos de monitoramento da saúde

---

[287] WALL, Matthew. Ebola: Can big data analytics help contain its spread? **BBC News**, out. 2014. Disponível em: <http://www.bbc.com/news/business-29617831>. Acesso em: 20 dez. 2017.

[288] RICHARDS, David. The Ebola Crisis and Where Big Data Can Help.**Recode**, out. 2014. Disponível em: <https://www.recode.net/2014/10/24/11632210/the-ebola-crisis-and-where-big-data-can-help>. Acesso em: 20 dez. 2017.

[289] UN GLOBAL PULSE. Using Mobile Phone Data and Airtime Credit Purchases to Estimate Food Security. **Global Pulse Project Series**, n. 14, 2015. Disponível em: <http://www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Airtimecredit_Food_2015.pdf>. Acesso em: 20 dez. 2017.

[290] UN GLOBAL PULSE. Nowcasting Food prices in Indonesia using Social Media Signals. **Global Pulse Project Series**, n. 1, 2014. Disponível em: <https://www.unglobalpulse.org/projects/nowcasting-food-prices>. Acesso em: 20 dez. 2017.

[291] CASTRO, Daniel.Spring Privacy Series: Consumer Generated and Controlled Health Data. **Center for Data Innovation**, Project No. P145401, 2014. Disponível em: <https://www.ftc.gov/system/files/documents/public_comments/2014/06/00016-90408.pdf>. Acesso em: 10 jan. 2018: "Patient-generated health data is an enormously valuable resource. Patients can use mobile health technologies to collect health data more frequently, conveniently, and at a lower cost than could be done in a clinical setting. Not only does this give patients and their caregivers the ability to track health indicators in real time, it also creates a rich dataset for potential analysis." (p. 1)

nunca foram tão difundidos[292]. Pode-se, portanto, dizer que as iniciativas inovadoras na área da saúde serão guiadas pelo processamento massivo de dados que caracteriza o *big data*[293].

Do mesmo modo, o *big data* possibilita que as ações humanitárias sejam mais eficientes e possuam informação atualizada em tempo real, evitando aprofundamento de situações humanitárias graves como surtos de doenças, fome e desastre natural, que podem ocasionar periclitação à vida e à saúde de populações vulneráveis.

2.2.2 Benefícios na promoção da diversidade e da igualdade: educação, acesso ao crédito e emprego

O uso do *big data* nos setores de educação, emprego e acesso ao crédito possui um relevante papel no acesso isonômico e na promoção da diversidade nestes setores.

No setor de educação, as técnicas do *big data* se mostram úteis para identificar potenciais estudantes de turmas avançadas que não seriam selecionados com base nas recomendações dos professores[294]; para identificar alunos de baixa renda que estariam se candidatando a universidades abaixo do seu potencial e indicar faculdades de melhor qualidade nas quais teriam condições de ingressar[295].

Nessa perspectiva, a experiência de uma universidade no Estado do Arizona reduziu as taxas de evasão escolar em 56% e aumentou a taxa de aprovação em 10% com o uso de algoritmo que propicia uma aprendizagem personalizada, tendo em conta as características do aluno, ao utilizar seus interesses, hábitos de aprendizagem e desempenho passado para recomendar os cursos mais adequados ao seu perfil. Foi possível, ainda, prever um comportamento de risco de determinado aluno e propiciar a intervenção antecipada, reduzindo as taxas de evasão nas turmas introdutórias de matemática pela metade[296].

Da mesma forma, nos Estados Unidos, a análise de dados tem possibilitado demonstrar como certas práticas disciplinares no ambiente escolar, tais como as suspensões,

---

[292] Anualmente, os dados gerados pelo setor de saúde crescem 48% ao ano e os downloads de aplicativos de saúde em geral crescem a uma taxa de 15% ao ano. PERKINS, Kleiner. Op. cit., p. 297-300.

[293] **DATA-DRIVEN HEALTHCARE**, op. cit.

[294] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 6.

[295] CASTRO, Daniel. The rise of Data Poverty in America. **Center for Data Innovation**, set. 2014, p. 6. Disponível em: <http://www2.datainnovation.org/2014-data-poverty.pdf>. Acesso em: 10 jan. 2017.

[296] Ibidem.

tem tido uma maior incidência sobre alunos afroamericanos do que em estudantes brancos, o que explica, em parte, a larga discrepância das notas destes dois grupos na graduação[297].

No que tange aos serviços financeiros, há um vasto campo a ser explorado pelo *big data*. Nos Estados Unidos, 11% dos consumidores são *credit invisible,* ou seja, não possuem histórico de crédito suficiente para que o algoritmo de crédito possa pontuá-los. A falta de acesso ao crédito impacta de forma mais intensa os consumidores de baixa renda, na medida em que 30% desses consumidores de baixa renda são invisíveis ao sistema de classificação de crédito. Ademais, entre afroamericanos e latinos a percentagem de invisibilidade chega a 15%, contra 9% dos consumidores caucasianos. Da mesma forma, entre os consumidores que, embora não invisíveis, não conseguem nenhuma classificação de crédito (*unscorable*) estão 13% de afro-americanos, 12% de latinos em comparação a 7% de brancos[298].

As alternativas propostas para resolver essas disparidades passam pelo *big data*. No âmbito da concessão de crédito, o *big data* tem propiciado fontes alternativas de histórico de crédito para quem não possuía acesso ao crédito pelos meios tradicionais. As alternativas de classificação propõem quantificar a história educacional e dados de licenciatura profissional; bem como dados de bens dos quais é proprietário.

Não se pode ignorar que, todavia, a proposta de expandir as fontes e a base de dados utilizável pelos algoritmos de classificação de crédito desperta preocupação. Isto porque a expansão das fontes utilizadas para alimentar os algoritmos de classificação de crédito dificulta ainda mais o controle e a eventual correção de dados inexatos por parte de seu titular[299]. Outra razão é que a expansão dos dados utilizados a partir da multiplicação das fontes torna cada vez mais complexa a classificação de risco de crédito, dificultando que seja explicada de modo transparente ao titular dos dados que, em geral não possui expertise em compreender o peso dado a cada informação na determinação da classificação de crédito, o que dificulta, inclusive, sua contestação[300].

---

[297] BIG DATA: A TOOL FOR Fighting Discrimination and Empowering Groups. In: **Future Of Privacy Forum and Anti-Defamation League**, [s.l.], [s.d.], p. 9. Disponível em: <https://fpf.org/wp-content/uploads/Big-Data-A-Tool-for-Fighting-Discrimination-and-Empowering-Groups-Report1.pdf>. Acesso em: 10 jan. 2018.

[298] BREVOORT, Kenneth P.; GRIMM, Philipp; KAMBARA, Michelle. Data Point: Credit Invisibles. **CFPB Office of Research**, mai. 2015. Disponível em: <http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf>. Acesso em: 20 dez. 2017.

[299] Nos Estados Unidos, um estudo da *Federal Trade Comission* concluiu que 21% dos consumidores havia confirmado erro em pelo menos um dos três relatórios de agência de crédito. Vide: FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 5.

[300] EXECUTIVE OFFICE OF THE PRESIDENT. **Big Data**: A Report on Algorithmic Systems, Opportunity, and Civil Rights. The White House: Washington, 2016, p. 13

Outro campo no qual o *big data* tem muito a contribuir diz respeito aos critérios de recrutamento e seleção no mercado de trabalho. Não é de hoje que grandes companhias utilizam sistemas de algoritmos para leitura e seleção de currículos[301], haja vista que o processamento massivo de dados pode permitir que se encontre a pessoa com o melhor perfil para a vaga disponível. Há ainda outras razões de aplicabilidade do *big data.* Um processo seletivo nos moldes tradicionais pode levar dias ou semanas e, ainda assim, não selecionar o candidato mais adequado em razão de um sem número de fatores: a divulgação da vaga não possuiu o alcance adequado, os candidatos adequados resolveram não se candidatar, o próprio processo de recrutamento excluiu potenciais pleiteantes indevidamente, entre outros.

Aplicar o *big data* no processo de recrutamento e seleção implica utilizar a leitura e processamento de máquina para filtrar dados de potenciais candidatos adequados à vaga. Logo, o algoritmo adequado poderia processar milhões de perfis com os filtros adequados para selecionar candidatos, economizando-se tempo e recurso aplicado no modelo tradicional[302]. Por exemplo, o processamento de dados permite encontrar relação entre o número de redes sociais que o indivíduo possui e a possibilidade de permanência no emprego, em uma empresa na qual a rotatividade é um problema[303], ou mesmo se verificar que empregadas que possuem filhos pequenos possuem o dobro de propensão de deixar o trabalho e, a partir disso, estender o período de licença maternidade, com vistas a manter seus recursos humanos[304]; permite, ainda, selecionar um candidato com base em sua conduta e atitudes em um jogo online[305].

---

[301] O GLOBO. Big Data já substitui currículos na seleção de candidatos. **O Globo**, jul. 2014. Disponível em: <https://oglobo.globo.com/economia/emprego/big-data-ja-substitui-curriculos-na-selecao-de-candidatos-13225088>. Acesso em: 10 jan. 2018.

[302] Estima-se que, após o investimento da publicidade da oferta de vagas em sites especializados, que empresas americanas gastam em média quatro mil dólares por candidato com entrevista, agendamento e avaliação e que o mercado de recrutamento movimenta duzentos bilhões de dólares em todo o mundo. Cf. BERSIN, Josh. Google For Jobs: Potential To Disrupt The $200 Billion Recruiting Industry. **Forbes**, mai. 2017.Disponível em: <https://www.forbes.com/sites/joshbersin/2017/05/26/google-for-jobs-potential-to-disrupt-the-200-billion-recruiting-industry/#544c89f74d1f> . Acesso em: 08 jan. 2018.

[303] "Alguns resultados são surpreendentes: verificou-se que profissionais que participavam de uma ou duas redes sociais costumam ficar no emprego por mais tempo do que aqueles que estão em quatro ou mais redes sociais. Com isso, informa a reportagem, a Xerox cancelou o recrutamento em convenções de games. Um detalhe chamou a atenção: na maioria dos casos, a experiência anterior em um emprego semelhante não foi determinante para uma boa contratação". O GLOBO. Big Data já substitui... op. cit.

[304]O BIG DATA antecipa a morte do currículo. **Fabramires**, out. 2013. Disponível em: <https://fabramires.wordpress.com/2013/10/30/o-big-data-antecipa-a-morte-do-curriculo/>. Acesso em: 10 jan. 2018.

[305] Exemplo disso, é a utilizaçao do “wasabi waiter”, jogo que simula que o candidato é um atendente de restaurante japonês e possui a missão de preparar pratos conforme o humo do cliente. Todas as atitudes do candidato durante o jogo permitem verificar a critatividade, a cautela, a possibilidade de realizar múltiplas tarefas ou de se distrair facilmente. Uma ferramenta simples como essa, capaz de armazenar e processar os dados

A base de dados proporcionada pelo *big data* para recrutar recursos humanos é especialmente expandida pelas redes sociais das mais variadas, havendo, inclusive, uma rede social que se destina especificamente a conectar profissionais às oportunidades de trabalho[306].

Logo, é fora de dúvida que o *big data*seria capaz de realizar um processo seletivo menos subjetivo e enviesado. Isto porque, ao processar os dados objetivamente, partindo do pressuposto de que tais dados estejam corretos, pode-se evitar a forma subjetiva com que os processos de contratação e promoção tradicionais são conduzidos.

É muito comum perceber que os modelos tradicionais de recrutamento acabam por selecionar candidatos que possuem muitas semelhanças com o recrutador, impedindo que os processos seletivos promovam a diversidade[307]. Ainda que com boas intenções, recrutadores são tendentes a selecionar candidatos com nível de formação e afinidades profissionais semelhantes a eles próprios, quando não oriundos do mesmo círculo de amizades ou de relacionamento profissional.

Essa postura pode excluir da seleção variados perfis de candidatos que não correspondam ao esperado pelo recrutador e que, talvez, possuam as habilidades desejadas pela empresa contratante. A empresa Google, por exemplo, reconheceu que seu processo seletivo enfatizava demais a pontuação acadêmica dos candidatos e formulava questões nas entrevistas que somente candidatos de determinado tipo de formação poderiam responder. A constatação fez com que a empresa criasse um modelo de entrevista baseado em perguntas de cunho comportamental que envolviam a resolução de situações concretas, e não perguntas abstratas que apenas conseguia responder quem dominasse determinado tipo de conhecimento[308], impedindo que se selecionasse quem, efetivamente, possuía as habilidades que a vaga exigia.

---

de todos os candidatos que participaram da seleção através do jogo permite às empresas ao menos filtrarem os candidatos mais adequados a uma fase posterior, economizando recursos que seriam gastos em uma triagem preliminar. Uma das que utilizaram os serviços da empresa Knack que criou a seleção de candidatos através do jogo *wasabi waiter* é a Shell, gigante do ramo de petróleo. RAMPELL, Catherine. Your Next Job Application Could Involve a Video Game. **The New York Times Magazine**, jan. 2014. Disponível em:<https://www.nytimes.com/2014/01/26/magazine/your-next-job-application-could-involve-a-video-game.html>. Acesso em: 10 jan. 2018.

306 STORNI, Eduardo. LinkedIn: o que é e para que serve? **WSI**, mar. 2017. Disponível em: <https://wsidm.com.br/blog/linkedin-o-que-e-e-para-que-serve>. Acesso em: 10 jan. 2018.

307 Trata-se do chamado "like me" bias ou "affinity bias" que é a seleção enviesada por semelhança ou afinidade. Vide EXECUTIVE OFFICE OF THE PRESIDENT. Op. cit., p. 14.

308 AMERLAND, David. 3 Ways Big Data Changed Google's Hiring Process. **Forbes**, jan. 2014. Disponível em: <https://www.forbes.com/sites/netapp/2014 jan. 21/big-data-google-hiring-process/#2de787061452>. Acesso em: 08 jan. 2018.

Deste modo, a análise objetiva de dados orientada por algoritmos pode selecionar o candidato com a mesma ou maior precisão que os processos seletivos tradicionais, sem que haja os efeitos negativos do viés e da discriminação que, por vezes, permitem que alguns potenciais selecionados sequer participem.

Por outro lado, como qualquer produto do invento humano, o *big data* não está isento de cometer os mesmos erros que a processo seletivo tradicional. Pode ocorrer que a qualidade ou quantidade de dados utilizados para processamento seja insatisfatório como, por exemplo, na seleção de candidatos por meio de determinada rede social ou aplicativo.Somente alcançará os potenciais candidatos que possuem acesso à internet e que façam parte daquela rede social[309].

Preocupação também importante é com o critério que é construído o algoritmo que seleciona os candidatos. Se for atribuído excessivo peso às informações que nada tem a ver com a capacidade de trabalho ou mesmo o potencial do candidato, tais como a distância do local de trabalho, o gênero do empregado e o seu estado civil, o resultado do algoritmo acabará perpetuando as mesmas discriminações que ocorrem no processo seletivo tradicional[310].

Pode-se imaginar que, se determinado algoritmo leva em conta a idade em que um candidato passou a se interessar por informática como critério preditivo de seleção, fatalmente haverá mais homens que mulheres selecionadas, dando a entender que os homens têm mais afinidade com a área de computação, quando a verdadeira razão é o fato de meninos serem expostos mais cedo às tecnologias da computação que as meninas, muito por influência do meio ambiente social na definição de papéis[311].

Uma possibilidade trazida da analise preditiva é determinar, a partir da na'lise dos perfis dos líderes exitosos, que habilidades e trajetória percorreram para chegar até ali. Logo, o *big data* apresenta a possibilidade de analisar os perfis de sucesso para prever os candidatos que terão maior probabilidade de serem exitosos.

---

[309] EXECUTIVE OFFICE OF THE PRESIDENT. Op. cit., p. 7.

[310] Ibidem, p. 15.

[311] Talvez, para as crianças desta geração, caracterizada pela hiperconexão e pelo variado número de dispositivos de acesso à internet, essa não seja mais uma característica tão marcante. Mas o argumento demonstra com clareza como o algoritmo pode reproduzir e perpetuar um cenário de desigualdade de gênero. Cf. WHY MACHINES DISCRIMINATE—and How to Fix Them. **Sciency Friday**, nov. 2015. Disponível em: <https://www.sciencefriday.com/segments/why-machines-discriminate-and-how-to-fix-them/>. Acesso em: 08 jan. 2018.

Em suma, o processamento de dados ou o algoritmo por si sónão podem ser considerados discriminatórios, mas os critérios sobre os quais são construídos o algoritmo podem perpetuar um cenário de desigualdade, através da análise enviesada ou discriminatória.

Por fim, podem ser citadas inúmeras iniciativas que visam atenuar práticas discriminatórias no mercado de trabalho, através do uso de informações obtidas pelo *big data.* Pode-se citar a Google que, reconhecendo o baixo percentual de 17% de funcionárias mulheres na área de tecnologia da empresa, percebeu que as suas convenções para promoção de empregados acabam por favorecer os homens. Deste modo, a empresa tomou a iniciativa de encorajar as mulheres a se candidatarem às vagas de promoção e garantir que as candidatas a uma vaga de trabalho pudessem encontrar com uma funcionária mulher durante o processo seletivo, com quem ficará mais propensa a destacar suas conquistas profissionais e credenciais[312].

2.3**Ameaças do uso irrestrito do *big data***

O uso irrestrito do *big data* inspira preocupações em relação aos direitos fundamentais dos indivíduos envolvidos. O tema merece especial atenção no que tange à análise preditiva. Conforme visto no tópico anterior, a análise preditiva tem sido aplicada para restringir a possibilidade de escolhas e oportunidades, tais como o acesso a instituição de nível superior, a uma vaga de emprego, a uma determinada linha de crédito e até mesmo a imposição de condições de cumprimento de penas mais gravosas com base nos algoritmos.

É comum se dizer que os dados ou números não mentem ou que o resultado do *big data* é objetivo e imparcial. Todavia, a afirmação não é de todo verdadeira. O uso de algoritmos pode ocultar ou mesmo perpetuar práticas discriminatórias cuja complexidade de linguagem de programação e suas variáveis podem dificultar a percepção. Isso porque mesmo que baseado em algoritmos, pode-se utilizar dados que apenas representam a realidade parcialmente ou mesmo absorver critérios de julgamento enviesados e discriminatórios, a ponto de afirmarem que os algoritmos são apenas uma ilusão para ocultar vieses[313].

---

[312]Outro caso a ser citado é a Entelo Diversity, plataforma de recrutamento de candidatos que visa a promoção da diversidade da força de trabalho, através da capacitação dos recrutadores e da identificação de perfis variados e específicos. A ferramenta pode filtrar candidatos a partir dos critérios de gênero, raça e história militar e dividi-los em cinco categorias: feminino, afro-americano, asiático, hispânico e veterano. BIG DATA: A TOOL FOR… Op. cit., p. 2.

[313] CRAWFORD, Kate. The Hidden Biases in Big Data. **Harvard Business Review**, abr. 2013. Disponível em: <https://hbr.org/2013/04/the-hidden-biases-in-big-data>. Acesso em: 08 jan. 2018.

Com efeito, um algoritmo que não se atente para a reprodução da discriminação ou práticas enviesadas pode causar prejuízos concretos às minorias discriminadas. Por exemplo, o sistema de anúncios de publicidade online da Google apresentou ofertas de empregos de alta renda em uma frequência maior para homens que para mulheres[314]; verificou-se, ainda, que o Google AdSense apresentou uma maior frequência de sugestão de pesquisas de registros criminais para nomes de pessoas negras do que brancas[315]; pesquisa da Universidade de Washingtonconstatou que um estudo da Google Images para "CEO" produziu 11% de mulheres, embora 27% dos executivos dos Estados Unidos sejam mulheres[316].

Ao mesmo tempo que o big data pode contribuir para facilitar o acesso de indivíduos a oportunidades de educação, crédito e emprego, além de tornar estratégias empresariais mais eficientes, o processamento massivo de dados pode ser a ferramenta básica do vigilantismo estatal; da prática discriminatória empresarial; da violação da privacidade de consumidores e inimigos políticos dos estados; do exercício da justiça penal, com base em probabilidades, que perpetuarão estatísticas enviesadas. Todos esses desdobramentos inspiram preocupações, embora o potencial do *big data* ainda esteja sendo explorado muito embrionariamente, o que permite afirmar que todas essas preocupações podem se multiplicar.

2.3.1 Riscos do *big data* à privacidade

Os inúmeros avanços trazidos pelo*big data* esbarram no fato de que todos eles dependem, essencialmente, de uma matéria prima em comum: os dados.

Embora os dados utilizados estejam em estado bruto, ou seja, não processados, em sua maioria, podem se referir a pessoas identificadas ou identificáveis, de modo que se o motor processamento de dados são os algoritmos, o seu combustível é e sempre será os dados, em especial os dados pessoais, ainda que não identificados.

É preciso que se esclareça que nem todo dado coletado e processado é necessariamente dado pessoal. Por exemplo, os sensores que coletam dados para previsão do tempo utilizarão dados de velocidade do vento, temperatura, umidade do ar, entre outros, para

---

[314] MILLER, Claire Cain. When Algorithms Discriminate. **The New York Times**, jul. 2015. Dispon'vel em: <https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html>. Acesso em: 08 jan. 2018.

[315]SWEENEY, Latanya. Discrimination in Online Ad Delivery.**Harvard University**. Disponível em: <https://dataprivacylab.org/projects/onlineads/1071-1.pdf>. Acesso em: 08 jan. 2017.

[316] UNIVERSITY OF WASHINGTON. Who's a CEO? Google image results can shift gender biases. **EurekAlert!**, abr. 2015. Disponível em: <https://www.eurekalert.org/pub_releases/2015-04/uow-wac040915.php>. Acesso em: 08 jan. 2018.

construir sua análise preditiva de eventos climáticos. Todavia, não se pode negar que a ameaça à privacidade venha do processamento de dados pessoais sem a devida cautela.

Pode-se imaginar que, na era do *big data*, a privacidade esteja mais ameaçada tão somente em virtude do volume de dados que podem ser acessados e processados por máquinas de capacidades antes inimagináveis. Desta forma, para resolver tais problemas bastaria redobrar a atenção com a privacidade, editando-se legislações mais rígidas. Não que a atenção do ordenamento jurídico não seja necessária, mas esta é apenas parte do problema.

O grande desafio do *big data* não diz respeito ao volume da dados.Antes, reside no seu uso secundário e, para isso, o ordenamento jurídico ainda não possui respostas[317]. O uso secundário consiste em utilizar os dados coletados em finalidade diversa para a qual foram coletados. No contexto do *big data*, o que agrega valor é a integração dos dados de diferentes fontes referentes a um indivíduo, com o objetivo de traçar um perfil que permita catalogare categorizá-lo , permitindo, a partir daí, o recebimento de publicidade customizada ou mesmo a análise preditiva apta a adiantar comportamentos e tendências.

O uso secundário dos dados mostra a capacidade de reciclagem de dados e sua combinação com novos dados aptos a gerar análises cada vez mais precisas e completas. Portanto, na atual quadra tecnológica, o uso secundário de dados é um processo irrefreável, haja vista que dados se tornaram verdadeira mercadoria[318], sendo negociados entre corretores de dados e empresas, compartilhados entre empresas parceiras ou mesmo reaproveitados pela mesma empresa que os coletou com novos propósitos. Neste novo modelo, o indivíduo perde, de algum modo, o controle sobre o caminho que seus dados seguiram, vez que a utilização secundária não encontra limites.

Um argumento de defesa comum para o compartilhamento de dados é a sua anonimização, ou seja, a desvinculação dos dados do respectivo titular, tornando-os anônimos. Ainda assim, tais dados seriam de grande valia, pois permitiriam seu processamento para construir diagnósticos, correlações e tendências.

Todavia, a anonimização não garante suficientemente a privacidade, pois já se demonstrou que, ao se percorrer o caminho inverso do dado, é possível se identificar o seu real titular. Um concurso promovido pela Netflix[319],empresa de conteúdo de vídeo pela

---

[317] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. **Big Data**… Op. cit., p. 153

[318] GEARY, Brandon. Data Is The New Commodity. **Brand Quaterly**, [s.d.]. Disponível em: <http://www.brandquarterly.com/data-new-commodity>. Acesso em: 08 jan. 2018.

[319]NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets. **The University of Texas at Austin**, [s.d.]. Disponível em: <http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>. Acesso em: 08 jan. 2018.

internet, pretendia aperfeiçoar seu sistema de sugestão de vídeos. Para tanto, disponibilizou aos candidatos as preferências de filmes de forma anonimizada. A partir da combinação da preferência dessa forma, possibilitou a identificação específica de um cliente através da combinação da opinião deste cliente em outros sites.

Pode-se citar, ainda, o caso AOL, de 2006, que, publicamente, disponibilizou arquivos anonimizados de buscas realizadas em seu site, referentes a 20 milhões de buscas de 657 mil usuários, visando estimular boas ideias a partir destas buscas. Embora a anonimização substituísse o número do IP e o nome de usuário por um outro número identificativo, foi possível identificar o usuário[320].

Esses e outros exemplos[321] mais que demonstram que a anonimização de dados está longe de ser a garantia absoluta da privacidade do indivíduo na rede. Isto porque basta que haja uma combinação cruzada dos dados ditos anônimos com outros dados públicos identificáveis para que a anonimização seja afastada.

Para Paul Ohm, havendo uma quantidade suficiente de dados, a anonimização perfeita é praticamente impossível, pouco importando o empenho aplicado em anonimizar os dados. Deste modo, não faria sentido uma tentativa de banir a desanonimização por completo[322].

---

[320]O jornal The New York Times combinou buscas como "homem solteiro de sessenta anos", "paisagistas em Lilburn"; "chás que fazem bem pra saúde", "cachorro que destrói tudo" e "dedos entorpecidos" e associou à usuária de número 4417749, de nome Thelma Arnold, uma senhora de 62 anos, viúva, dona de três cães e moradora de Lilburn na Geórgia, que ficou estarrecida ao ter sido identificada pelo jornal The New York Times. Cf. BARBARO, Michael; ZELLER JR., Tom. A face is exposed for AOL searcher no. 4417749. **The New York Times**, ago. 2006. Disponível em: <http://www.nytimes.com/2006/08/09/technology/09aol.html>. Acesso em: 08 jan. 2018.

[321] Um concurso promovido pela empresa Kaggle, que disponibilizou dados anônimos de usuários de uma rede social e pela combinação com as conexões à rede social Flickr, permitiu identificar os titulares dos dados anonimizados do concurso através de padrões nestas conexões à rede social. Cf. LINK PREDICTION BY De-anonymization: How We Won the Kaggle Social Network Challenge.**33 Bits of Entropy**, mar. 2011. Disponível em: <https://33bits.wordpress.com/2011/03/09/link-prediction-by-de-anonymization-how-we-won-the-kaggle-social-network-challenge/>. Acesso em: 08 jan. 2018.

[322] "A reidentification ban is sure to fail, however, because it is impossible to enforce. How do you detect an act of reidentification?Reidentification can happen completely in the shadows. Imagine that Amazon.com anonymizes its customer purchase database and transmits it to a marketing firm. Imagine further that although the marketing firm promises not to reidentify people in Amazon's database, it could increase profits significantly by doing so. If the marketing firm breaks its promise and reidentifies, how will Amazon or anybody else ever know? The marketing firm can conduct the reidentification in secret, and gains in revenue may not be detectable to the vendor". Em radução livre: "Uma proibição de reidentificação certamente falhará, no entanto, porque é impossível aplicar. Como você detecta um ato de reidentificação? 281 A reidentificação pode acontecer completamente nas sombras. Imagine que a Amazon.com anonima seu banco de dados de compras de clientes e transmite para uma empresa de marketing. Imagine ainda que, embora a empresa de marketing prometa não reidentificar pessoas no banco de dados da Amazon, isso poderia aumentar significativamente os lucros ao fazê-lo. Se a empresa de marketing rompe sua promessa e reidentifica, como a Amazon ou qualquer outra pessoa saberão? A empresa de marketing pode realizar a reidentificação em segredo, e ganhos de receita podem não ser detectáveis para o fornecedor". OHM, Paul. Broken Promises of Privacy Responding to the Surprising Failure of Anonymization. **UCLA Law Review**, v. 57, p. 1758, 2010.

A desanonimização é viabilizada pelo *big data*, na medida em que apenas no cenário do *big data*é possível combinar dados de diferentes fontes sobre um mesmo usuário, facilitando sua identificação. Fato é que manter a anonimização como meio de proteção à privacidade, diante da captura de uma quantidade maior de dados e de uma combinação de dados mais variadas, é o grande desafio[323].

A preocupação é mais intensificada pelo fato de que não apenas os dados convencionais são desanonimizados, mas também os dados referentes às conexões de pessoas com outras, ou seja, seus contatos frequentes, o volume de dados trocados, entre outros[324].

Não se trata de negar da anonimização de dados, enquanto escudo na proteção da privacidade, de modo que deve continuar sendo uma obrigação para todas as empresas cujo modelo de negócios envolva gestão e compartilhamento de dados. O que não pode ocorrer é que a falsa sensação de segurança proporcionada pelos dados anônimos oculte o risco que a prática encerra e desonere empresas que trabalham com dados de tomar cautelas adicionais. Ademais, a relação com o titular de dados deve ser transparente, informando-se que mesmo com a anonimização há riscos de esses dados serem reidentificados.

No caso do direito brasileiro, entendemos que a ausência de anonimização de dados poderá colidir frontalmente com o direito ao anonimato, enquanto garantidor da liberdade de expressão. Em nosso entender, a despeito de o dispositivo constitucional prever, a princípio, a vedação ao anonimato[325], a previsão constitucional de liberdade de pensamento apenas veda o anonimato com o fim específico de coibir atividades ilícitas, ou seja, atividades que transbordem a liberdade de expressão e ofendam a honra de terceiros. Portanto, para as atividades lícitas, o anonimato continua sendo uma proteção à liberdade de pensamento, desde que não se cause dano a terceiro. Até porque, conforme visto, a anonimização de qualquer dado não impossibilita que se faça o seu caminho inverso e, de posse de outros dados, se permita a sua identificação.

Em síntese, a anonimização é importante, mas não suficiente. Há outras proteções à privacidade, tais como a obrigação de obter consentimento específico, ou seja, o consentimento informado do titular dos dados. Ocorre que, conforme se verá, quando se tratar de dado pessoal, o consentimento específico pode ser uma proteção excessiva e pouco efetiva. Se mostra excessiva na medida que o grande valor atribuído aos dados é a sua utilização

---

[323] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. Cit, p. 155.

[324] Ibidem.

[325] Art. 5º. "(...): V - é livre a manifestação do pensamento, sendo vedado o anonimato;".

secundária, o que esvaziaria por completo o valor secundário destes dados. Não faria sentido se exigir consentimento para uma finalidade que não se sabe qual ou para toda e qualquer finalidade possível, o que contaria com a negativa dos titulares.

Outra alternativa que não se mostra viável por si só seria o direito de retirada *(rigth to opt out)*. Isso porque já se demonstrou que o direito de retirada deixa rastros. Exemplo disso é o caso do *Google Street View* na Alemanha que, após protestos dos proprietários de imóveis, concordou em retirar as imagens de imóveis dos seus mapas. Ocorre que o fato de alguns imóveis aparecerem com a imagem borrada no aplicativo demonstrava que houve ali um pedido de exclusão, dando a entender a criminosos que aquele proprietário poderia ser um alvo lucrativo[326].

Conforme se vê, a era do *big data* traz desafios mais profundos e complexos à garantia da privacidade e os instrumentos disponíveis possuem cada qual suas limitações, não se podendo dizer que cada um individualmente considerado proteja adequadamente a privacidade, de modo que pode se pensar na utilização integrada dos modelos de proteção.

2.3.2 Risco do *big data* à promoção da diversidade e ao combate à discriminação

Ao longo deste trabalho, foi possível perceber inúmeras situações nas quais o uso do *big data* baseou-se em uma premissa discriminatória ou o resultado da sua utilização perpetuou ou criou uma situação discriminatória.

Não é demais dizer que a Constituição da República elenca entre seus objetivos fundamentais o combate à discriminação e a promoção do bem de todos sem preconceito de qualquer ordem[327]. Ademais, o mesmo texto constitucional prevê entre os direitos e garantias fundamentais a obrigação de combate quaisquer formas de discriminação, prevendo a inafiançabilidade e imprescritibilidade para o crime de racismo[328].

---

[326] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 154.

[327] Art. 3º "Constituem objetivos fundamentais da República Federativa do Brasil: I - construir uma sociedade livre, justa e solidária; II - garantir o desenvolvimento nacional; III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação".

[328] Art. 5º "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais; XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;".

Como se sabe, uma das marcas do *big data* no âmbito corporativo é a possibilidade de identificar perfis e realizar a publicidade direcionada, com produtos personalizados. Todavia, a oferta de produtos baseada exclusivamente na decisão de algoritmos pode ocasionar situações indesejáveis, como a oferta de determinado produto ou serviço exclusivamente ao público-alvo determinado pelo algoritmo, excluindo potenciais consumidores unicamente porque não estariam naquela faixa de consumo. Portanto, o principal risco do *big data* para o combate à discriminação e promoção da diversidade é que decisões automatizadas e incontestáveis prejudiquem a margem decisória do indivíduo, impedindo-lhe acesso a determinado bem ou serviço.

A preocupação é intensificada pela falta de responsividade que o algoritmo pode significar, especialmente se se partir do pressuposto de que os dados processados são uma constatação em si mesmo e não reproduzem a mesma estrutura discriminatória presente na sociedade, mantendo ocultos os vieses sobre os quais os dados são tratados[329].

Os dois principais desafios do *big data* no combate à discriminação residem na falta de qualidade dos dados, incluindo sua precisão, completude e representatividade, bem como na tendência em admitir a correlação entre os dados como uma relação de causa e efeito[330].

No que diz respeito à falta de qualidade de dados, pode-se afirmar que se a base de dados é imprecisa, o resultado do processamento também o será (*garbage in, garbage out)*. Portanto, por mais bem elaborado que tenha sido construído o algoritmo, se os dados que o alimenta são imprecisos ou deturpados, a análise não trará nenhum resultado útil. Imagine-se um aplicativo de trânsito que se baseia apenas nas informações recolhidas de aparelhos smartphones de última geração. Certamente, embora apresente com precisão uma solução para seus usuários, o aplicativo melhor funcionará em áreas mais nobres ou nos centros urbanos, nos quais o número de usuários destes aparelhos é maior[331].

Uma demonstração de falta de qualidade dos dados é quando estes dados representam de forma não intencional a perpetuação de discriminações históricas pela falta de representatividade. Por exemplo, imagine-se uma empresa que desenhe um algoritmo que reproduza a sua cultura de contratação, pois acredita que os profissionais que tem recrutado são adequados ao objetivo. Imagine que esta mesma empresa, desde sua fundação, tem se caracterizado por contratar homens brancos, jovens e com formação em determinadas

---

[329] CRAWFORD, Kate. The Hidden Biases in Big Data. Op. cit.

[330] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 8.

[331] EXECUTIVE OFFICE OF THE PRESIDENT. Op. cit., p. 8.

áreas[332]. Ora, ao procurar perfis semelhantes ao seu quadro de funcionários, quando possui um quadro muito pouco representativo, o algoritmo perpetuará a ausência de diversidade, ainda que de modo não intencional. Da mesma forma, um algoritmo que pontue melhor profissionais oriundos de determinadas universidades e não de outras, poderá reproduzir uma seletividade e ausência de diversidade no mercado de trabalho, especialmente se o acesso às universidades escolhidas é restrito a alguns grupos sociais.

Além das variadas formas que podem expressar a falta de qualidade dos dados, há, ainda, a indevida conclusão de que a correlação entre dados expressa uma relação de causa e efeito. Em outras palavras, dados podem estar correlacionados e não dizerem absolutamente nada quanto ao binômio causa-consequência. O caso clássico que bem demonstra isso é o fato de nos dezoito dos últimos vinte anos de eleição presidencial nos Estados Unidos, se o time profissional de futebol americano de Washington DC ganhasse a sua última partida em casa, o partido que estava no poder garantia a reeleição; se o time perdesse seu último jogo em casa, o partido de oposição ganharia[333].

Esse exemplo demonstra com clareza que a correlação estatística não necessariamente está amparada em uma relação de causa e consequência. Um cuidado que se deve ter com o processamento dos dados é não adotar de antemão uma relação de causalidade entre fenômenos que não possuem nenhuma relação, embora estejam estatisticamente relacionados. Mais que isso, importante é não partir de uma probabilidade estatística para se adotar premissas discriminatórias, reproduzindo uma estrutura excludente.

Não se pode, portanto, ignorar o fato de que algoritmos possuem, por si só, uma carga valorativa, ou seja, os valores que são inseridos nos algoritmos, em geral, refletem premissas culturais dos engenheiros de software que desenharam o algoritmo, inserindo em forma de estrutura lógica suas opiniões pessoais[334]. Isso se manifesta nas informações que são exigidas por cada algoritmo, tais como local de residência, data de nascimento, histórico de empregos, histórico escolar para determinar se aquele indivíduo deve ser elegível ou não a uma linha de crédito.

Neste sentido, a lei estadunidense que trata do direito à igualdade de crédito e oportunidades (ECOA – *Equal Credit Opportunity Act*) proíbe a discriminação na concessão

---

[332] Ibidem, p. 8.

[333] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 9. Para outras relações espúrias, vide ALDRICH, John. Correlations Genuine and Spurious in Pearson and Yule. **Statistical Science**, v. 10, n. 4, p. 364-376, 1995.

[334] Ibidem, p. 13.

de crédito em virtude de características sensíveis, tais como raça, cor, religião, origem, sexo, estado civil, idade ou mesmo em virtude de receber qualquer auxílio público[335].

Há duas formas de violar a norma de igualdade na oportunidade de crédito: tratamento desigual ou impacto desigual[336].A situação de tratamento desigual ocorre quando duas pessoas são tratadas desigualmente em virtude de suas características sensíveis. Trata-se, portanto, de uma discriminação mais direta e evidente. Pode ocorrer, por exemplo, quando se deixa de conceder crédito a uma mãe solteira em virtude dessa natureza ou quando se concede condições de créditos mais favoráveis a pessoas solteiras em relação às casadas, orientado pelo fato de o algoritmo de crédito demonstrar a maior probabilidade de inadimplência por parte dos casados.

Já a modalidade discriminatória de impacto desigual ocorre quando determinada medida é aparentemente neutra em relação a todos os indivíduos, mas sua aplicação concreta pode produzir um efeito discriminatório. Imagine-se que determinada linha de crédito é concedida apenas a moradores de certa região da cidade, porque os dados revelam que estas são as regiões que contam com melhor adimplência. Ocorre que a concessão regionalizada terá um impacto desigual em regiões que não serão concedidas, o que pode impactar mais intensamente determinado grupo socioeconômico, racial ou religioso.

Tanto o impacto desigual quanto o tratamento desigual ocasionam consequências desastrosas aos indivíduos. Isso porque na era do *big data* cada vez mais decisões essenciais sobre a vida do indivíduo são tomadas ou influenciadas por algoritmos. Isso ocorre na oferta de emprego, de crédito, nas decisões sobre procedimentos para a saúde, na realização de políticas públicas, entre outros. Além da opacidade causada pela própria complexidade tecnológica, em geral, as decisões tomadas com base em algoritmo não permitem aos afetados contestarem seu conteúdo ou mesmo corrigirem premissas incorretas, ocasionando situações discriminatórias que reduzem oportunidades, em vez de ampliá-las.

Pode-se afirmar que o *big data* pode ser uma faca de dois gumes, na medida que pode ser capaz de promover a diversidade da força de trabalho, aumentar o acesso ao crédito para as populações mais vulneráveis e diminuir a evasão; por outro lado, pode perpetuar e intensificar a estrutura excludente da sociedade, se não aplicado com transparência, ética e a devida atenção à diversidade.

---

[335]CFPB CONSUMER LAWS AND REGULATIONS. Equal Credit Opportunity Act (ECOA). **CFPB**, jun. 2013. Disponível em: <http://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_ecoa-combined-june-2013.pdf>. Acesso em: 08 jan. 2018.

[336] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. iii.

2.3.3 Riscos da análise preditiva e seu uso no policiamento e nos sistemas de justiça

Conforme visto, a análise preditiva consiste na previsão de comportamentos futuros. Trata-se basicamente de minerar dados históricos e antecipar padrões ou alterações de padrões. Em suma, utiliza-se de inúmeras variáveis que possam estatisticamente precisar o que ocorrerá em um futuro próximo. Conforme pontuado, a análise preditiva do *big data* não apresenta a certeza absoluta do que irá acontecer, mas uma certeza estatística, provável, a depender de variáveis que podem ou não ser confirmadas, adicionando-se a isto certo grau de imprevisibilidade do fator humano.

A utilização da análise preditiva no policiamento tem muito a contribuir com um combate eficiente à criminalidade. Isto porque a determinação dos prováveis locais e horários dos crimes pode economizar recursos escassos e evitar desperdícios com o policiamento tradicional que apenas depende da discricionariedade do agente. No entanto, experiência tem mostrado que a discricionariedade policial não raramente envolve atuações discriminatórias que implicam em um desigual impacto sobre minorias estigmatizadas, tais como negros e pobres[337].

Portanto, em vez de a atuação policial eleger grupos sociais ou regiões preferenciais para aplicação do rigor legal, a promessa do *big data* é evitar o perfilamento, ou seja, a definição de um perfil preferencial para as abordagens policiais, o que em geral recai sobre grupos marginalizados, tais como negros e pessoas de baixa renda[338]. Em vez de definir grupos, a promessa do *big data* é poder prever crimes com maior precisão e orientar uma atuação policial mais individualizada, pontual, menos discriminatória e que não torne um perfil suspeito, mas atue profilaticamente, nas situações de alta probabilidade de conduta criminosa de indivíduos determinados[339].

A promessa parece tentadora, mas não ocorre sem riscos. Deve-se questionar qual o grau de privacidade será preciso se abrir mão em nome de se permitir um grau de vigilância que possibilite o correto funcionamento do policiamento preditivo. Ora, quanto maior a

---

[337] AYUSO, Silvia. Os hispânicos, vítimas silenciosas da violência policial nos EUA. **El País**, jul. 2016. Disponível em: <https://brasil.elpais.com/brasil/2016/07/17/internacional/1468715146_128605.html>. Acesso em: 08 jan. 2018.

[338] ANDREWS, Edmund. A new statistical test shows racial profiling in police traffic stops.**Stanford**, jun. 2016. Disponível em: <https://engineering.stanford.edu/magazine/article/new-statistical-test-shows-racial-profiling-police-traffic-stops>. Aceso em: 08 jan. 2018.

[339] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 161.

quantidade de dados, maior será a precisão do resultado do seu processamento. Resta saber que dados serão utilizados para alimentação do policiamento preditivo e o quanto violam a privacidade dos indivíduos envolvidos.

A análise preditiva tem sido aplicada com algum êxito no policiamento de algumas cidades estadunidenses. Um dos exemplos a serem citados é o programa chamado de *Blue CRUSH (Criminal Reduction Utilizing Statistical History*[340]), utilizado na cidade de Memphis, estado do Tenesse[341]. Basicamente, o programa utiliza os registros históricos de todas as ocorrências e, com o apoio de um software de análise preditiva da IBM(*International Business Machines*)[342], associado a um serviço de mapeamento geográfico, permite elaborar um mapa com os possíveis locais de novos crimes, com relativa precisão de local (um raio de alguns quarteirões) e horário (uma precisão de algumas horas durante o dia)[343]. Desde a implantação do programa em 2006, os crimes contra a propriedade e violentos foram reduzidos em 25%, enquanto a média de redução no país não chegou a 15%[344].

No caso de Memphis, a maioria dos crimes de rua se concentra nas regiões de alta pobreza, mas não significa que a criminalidade esteja presente em toda a periferia. Na verdade, há microrregiões dentro destes bairros que são pontos focais da criminalidade. Essa seria uma das vantagens da aplicação da análise preditiva para orientar o policiamento, pois evita a violência generalizada, tratando todo e qualquercidadão das regiões periféricas como um potencial suspeito. Logo, a vantagem da analise preditiva é reduzir a potencialidade de tratamentos discriminatórios, já que o policiamento se basearia na precisão estatística.

Em Nova York, com auxílio da Microsoft, foi lançado um mapa interativo, que permite geolocalizar os crimes cometidos desde 2012 na cidade. O mapa permite a filtragem por região e tipo de crime e pode ser acessado por cidadãos e autoridades[345]. O software é alimentado por dados das chamadas telefônicas para o 911[346], imagens de câmera de

---

[340] Em tradução livre: "Redução da criminalidade utilizando histórico estatístico".

[341] Atualmente, o sistema Blue CRUSH também é utilizado no policiamento da Inglaterra, Polônia e Israel. Vide HICKMAN, Leo. How Algorithms Rule the World. **The Guardian**, jul. 2013. Disponível em: <https://www.theguardian.com/science/2013/jul jan. how-algorithms-rule-world-nsa>. Acesso em: 11 jan. 2018.

[342]Trata-se de umaempresa estadunidense voltada para a área de informática cuja existência remonta ao século XIX.

[343] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 158.

[344] KATO, Rafael. Big Data contra o crime. **Exame**, abr. 2014. Disponível em: <https://exame.abril.com.br/tecnologia/big-data-contra-o-crime>. Acesso em: 11 jan. 2018.

[345] O mapa está disponível em: <https://maps.nyc.gov/crime/>. Acesso em: 10 jan. 2018.

[346] O 911 é número tradicional utilizado nos Estados Unidos para comunicar emergências das mais variadas. Segundo o site: "The 911 system was designed to provide a universal, easy-to-remember number for people to reach police, fire or emergency medical assistance from any phone in any location, without having to look up

segurança, além de reconhecer rostos, placas, radiação nuclear e é capaz de localizar o policial mais próximo da ocorrência[347].

Em Chicago, a utilização da tecnologia ShotSpotter permite identificar e localizar sons de tiros e, a partir disso, prever padrões de possíveis atividades criminais. A referida tecnologia é integrada a um mapa digital e associada à tecnologia *HunchLab* - a qual permite à polícia a tomar decisões de acordo com a análise massiva das informações sobre detenções, chamadas para o 911, atividades de gangues e outros dados policiais relevantes. Nos dois distritos nos quais a tecnologia foi implantada houve uma redução da criminalidade na ordem de 49% e 66%, respectivamente, contra 13% no restante do Estado[348].

Um projeto de pesquisa do Departamento de Segurança Nacional dos Estados Unidos chamado de FAST (Future Attribute Screening Technology[349]) afirma ser possível identificar potenciais terroristas através do monitoramento de seus sinais vitais, linguagem corporal e outros padrões psicológicos[350]. A ideia é que a vigilância destes aspectos poderia prever a intenção de causar dano do indivíduo com 70% de acerto[351]. Não se sabe ao certo o que se quer dizer com tendência a ser terrorista ou intenção de causar dano, tampouco que tipo de comportamento pode sinalizar ao algoritmo essa propensão.

---

specific phone numbers. Today, people communicate in ways that the designers of the original 911 system could not have envisioned: wireless phones, text and video messages, social media, Internet Protocol (IP)-enabled devices, and more". Em tradução livre: "O sistema 911 foi projetado para fornecer um número universal e fácil de lembrar para que as pessoas acessem assistência médica, incêndio ou assistência médica de emergência de qualquer telefone em qualquer local, sem ter que procurar números de telefone específicos. Hoje, as pessoas se comunicam de forma que os projetistas do sistema original do 911 não poderiam ter imaginado: telefones celulares, mensagens de texto e de vídeo, mídia social, dispositivos compatíveis com Internet Protocol (IP) e muito mais". ABOUT THE 911 Program. **911**, [s.d.]. Disponível em: <https://www.911.gov/about_national_911program.html>. Acesso em: 11 jan. 2018.

347 A tecnologia por trás do mapa é da Microsoft, que criou o *Domain Awareness System* (DAS), em tradução livre, Sistema de Conscientização de Domínio.

348 BOOTH, Alison. Minority Report in Chicago as police aim to stop crime before it happens. **Naked Security**, mai. 2017.Disponível em: <https://nakedsecurity.sophos.com/2017/05/10/minority-report-in-chicago-as-police-aim-to-stop-crime-before-it-happens/>. Acesso em: 18 jan. 2018.

349 Em tradução livre: "Tecnologia de triagem de atributos futuros".

350 Segundo o Departamento de Segurança Nacional dos Estados Unidos, FAST "combines cutting-edge behavioral and physiological science with deception detection theory and state-of-the-art sensor technologies. It is designed to be used at checkpoints to help security officers identify individuals for secondary screening". Em tradução livre: "FAST combina ciência comportamental e fisiológica de ponta com teoria de detecção de decepção e tecnologias de sensores de última geração. Ele é projetado para ser usado nos pontos de controle para ajudar os agentes de segurança a identificar indivíduos para seleção secundária". FUTURE ATTRIBUTE SCREENING Technology. **DHS Science and Technology Directorate**, nov. 2014. Disponível em: <https://www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST-508_0.pdf>. Acesso em: 10 jan. 2018.

351 MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 159.

Conforme se verá a seguir, é comum que o sujeito submetido à vigilância mais intensa possua um perfil específico, uma nacionalidade específica. Portanto, não é muito difícil que a vigilância descambe em atuações discriminatórias contra povos determinados, reproduzindo no algoritmo o estereótipo do senso comum. Por essa razão, é importante saber o quanto de pressupostos discriminatórios foram introduzidos no algoritmo que define e tendência a atos terroristas e seu desigual impacto sobre grupos marginalizados e sensíveis.

Outros exemplos de policiamento preditivo podem ser citados, tais como o PredPol (*Predictive Policing Software)* desenvolvido pelo departamento de polícia de Los Angeles e a Universidade da Califórnia em Los Angeles. Basicamente, o software se baseia nos variados modelos de comportamento criminal, a partir do tipo do crime, data, hora e local do crime para prever possíveis locais e horários dos crimes e geolocalizar os policiais nos locais previstos para novas ocorrências, antecipando-se ao fato[352].

No Brasil, o Estado de São Paulo adquiriu o Detecta[353], sistema de monitoramento criminal desenvolvido pela Microsoft em parceria com a prefeitura de Nova York. A proposta é que haja monitoramento de câmeras e a integração do maior banco de dados de informações policiais da América Latina. Estariam integrados ao sistema os bancos de dados das polícias civil e militar, do registro digital de ocorrências, do Instituto de Identificação,do Sistema Operacional da Polícia Militar (SIOPM-190),do Sistema de Fotos Criminais (Fotocrim), além de dados de veículos e de Carteira Nacional de Habilitação (CNH) do Detran. O sistema foi implantado com a promessa de realizar a análise de vídeo através da leitura de máquina, ou seja, sem intervenção humana poderia ser identificada de forma automática eventual conduta criminosa e emitir imediato alerta às forças policiais[354].

Com efeito, a aplicação do *big data* na área de segurança não se restringe ao planejamento e orientação do policiamento, se estendendo também para os sistemas de justiça e sua execução penal. Há casos de utilização do *big data* para verificar possibilidade de

---

[352] SAISSE, Renato. Op. cit., p. 7.

[353] DO PORTAL DO GOVERNO. Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. **Portal do Governo de São Paulo**, mai. 2017. Disponível em: <http://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em: 18 jan. 2018.

[354] Em que pese as promessas à época da implantação, a eficiência do programa tem sido questionada pelos órgãos de controle daquele ente da federação. RIBEIRO, Bruno; LEITE, Fabio. Após 2 anos, sistema Detecta da polícia não identifica crimes, diz TCE. **Estadão**, ago. 2016. Disponível em: <http://sao-paulo.estadao.com.br/noticias/geral,apos-2-anos-sistema-detecta-da-policia-nao-identifica-crimes-diz-tce,10000069080>. Acesso em: 18 jan. 2018.

concessão de liberdade condicional, para definir o valor da multa a ser paga ou mesmo para influenciar a extensão da pena privativa de liberdade.

Neste sentido, um projeto de pesquisa da Pensilvânia afirma conseguir prever se um condenado, após colocado em liberdade condicional, irá se envolver em um homicídio – seja enquanto autor ou vítima do crime[355]. O algoritmo usa as variáveis específicas de inúmeros casos, incluindo as razões anteriores para prisão, a data do primeiro crime cometido, bem como dados demográficos, socioeconômicos, de idade e de gênero[356]. Segundo o autor da pesquisa, é possível identificar um futuro assassino entre os candidatos à liberdade condicional com, no mínimo, 75% de precisão[357].

Ademais, tem se popularizado nos Estados Unidos a aplicação da análise preditiva para a definição de sentença. Pode-se citar o estado de Utah - cuja análise baseia-se nos chamados quatro grandes fatores[358]- fatores esses que orientam o magistrado na definição da pena e na concessão de liberdade condicional.

De mesma forma, o estado da Virgínia utiliza há mais de uma década sistema de pontuação de classificação de criminosos que surgiu como solução à crise orçamentária que não mais permitia a construção de novos presídios. De acordo com o modelo, há uma pontuação máxima de 71 pontos, que leva em conta fatores como idade em que se cometeu o delito, desemprego, fatores socioeconômicos, entre outros. Caso o acusado seja pontuado em até 35 pontos, haveria recomendação para a liberdade condicional. Caso a pontuação fosse superior, havia a recomendação para pena privativa de liberdade. Verificou-se que a utilização da sistemática implicou em um índice de reincidência 12% de quem obteve pontuação inferior a 35 pontos e de 38% de quem obteve pontuações mais altas. Em julho de 2004, o sistema foi atualizado para que a pontuação máxima para liberdade condicional fosse de 38 pontos[359].

---

[355] Sobre o trabalho de Richard Berk, veja-se: BERK, R.A. et al. Forecasting Murder within a Population of Probationers and Parolees: A High Stakes Application of Statistical Learning. **Journal of the Royal Statistics Society**, series A, n. 172, Part 1, p. 191–211, 2008.

[356]SOFTWARE ESTILO 'MINORITY Report' ajuda polícia a prever crimes. **Terra**, jan. 2013. Disponível em: <https://www.terra.com.br/noticias/mundo/estados-unidos/software-estilo-minority-report-ajuda-policia-a-prever-crimes,f957183d48a2c310VgnVCM5000009ccceb0aRCRD.html>. Acesso em: 10 jan. 2018.

[357] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 161.

[358] Em suma, os fatores se resumem a história de comportamento que prejudica a terceiros, padrões de personalidade anti-social, atitudes e crenças que favoreçam o crime e associação com colegas pró criminosos. O modelo pode ser encontrado em STATE OF UTAH. Adult Sentencing & Release Guidelines. **Utah Sentencing Comission**, 2015. Disponível em: <https://www.utah.gov/pmn/files/172049.pdf>. Acesso em: 10 jan. 2018.

[359] BAZELON, Emily. Sentencing by the Numbers.**The New York Times**, jan. 2005. Disponível em: <http://www.nytimes.com/2005 jan. 02/magazine/sentencing-by-the-numbers.html>. Acesso em: 18 jan. 2018.

Outra aplicação da análise preditiva ocorre na determinação da pena e na concessão do livramento condicional. Um caso emblemático ocorreu em Wisconsin. Em 2013, a polícia local prendeu um homem que dirigia um carro que havia sido usado em um tiroteio recente. O detido, Eric Loomis, se declarou culpado por resistir à prisão por utilizar veículo de terceiro sem consentimento do proprietário. Em sua sentença, o magistrado negou a liberdade condicional a Loomis e o condenou a 11 anos: seis anos de prisão e cinco anos de supervisão prolongada. O fundamento invocado para uma pena tão extensa foi o resultado do algoritmo de avaliação de risco de reincidência utilizado pelo estado de Wisconsin. Segundo o algoritmo, o condenado possuía um alto risco de reincidência.

A ferramenta de análise preditiva de risco utilizada chama-se COMPAS *(Correctional Offender Management Profiling for Alternative Sanctions*[360]) e é largamente utilizada nas justiças criminais estadunidenses. O algoritmo afirma ser capaz de analisar e prever o risco de reincidência criminal violenta e não violenta nos dois anos seguintes ao preenchimento do questionário, com base no histórico do acusado. Ocorre que se trata de algoritmo de propriedade da empresa Northpointe Inc que afirma que o código fonte do algoritmo constitui seu modelo de negócio, não podendo revelar detalhes do seu funcionamento[361].

Loomis recorreu ao Supremo Tribunal de Wisconsin, que manteve a sentença sob o argumento de que o *software* se baseou em informações constantes de um formulário, fornecidas pelo próprio acusado e em informações públicas, as quais o acusado teve a oportunidade de contraditar[362]. O acusado alegou não ter tido acesso ao devido processo legal, pois não possui conhecimento acerca dos critérios de pontuação do algoritmo para cada informação. Todavia, o tribunal entendeu que se tratava de algoritmo proprietário, cuja engenharia constituía segredo comercial da empresa responsável, não sendo direito do

[360] Em tradução livre: Gerenciamento Correccional de Perfis de Infratores para Sanções Alternativas.

[361] O Compas é um algoritmo desenvolvido por uma empresa privada, Northpointe Inc., que calcula a probabilidade de alguém cometer outro crime e sugere que tipo de supervisão um réu deve receber na prisão. Os resultados provêm de uma pesquisa do arguido e informações sobre sua conduta passada. As avaliações da Compas são um complemento baseado em dados para os relatórios escritos de apresentação elaborados por órgãos responsáveis pela aplicação da lei. Disponível em: SMITH, Mitch. In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. **The New York Times**, jun. 2016. Disponível em: <https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html>. Acesso em: 10 jan. 2018.

[362] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of Wisconsin. *State v. Lomis*. Disponível em: <http://caselaw.findlaw.com/wi-supreme-court/1742124.html>. Acesso em: 10 jan. 2018.

acusado o acesso aos critérios do algoritmo, mas apenas contestar as informações utilizadas[363].

Não se nega que o uso de um algoritmo como o COMPAS possa trazer um grau maior de objetividade na definição do perfil do acusado. Ocorre que a própria objetividade deste algoritmo sofre sérios questionamentos. Uma pesquisa implementada pela ProPublica[364], agência de jornalismo investigativo de Nova York, encontrou sérios vícios na análise de reincidência do algoritmo, especialmente em relação à etnia dos acusados. Após a análise do resultado de mais de 10.000 criminosos em *Broward County*, na Flórida, foram comparadas as taxas de reincidência previstas com as taxas que realmente ocorreram ao longo de um período de dois anos. Com o registro dos acusados no sistema prisional, o questionário COMPAS é alimentado e o software prevê vários resultados como o "risco de reincidência" e "risco de reincidência violenta".

A pesquisa concluiu que acusados negros eram classificados com um risco de reincidência muito maior do que acusados brancos e esses índices não se confirmavam na prática, na medida que os réus negros que não reincidiam eram classificados com risco duas vezes mais que os acusados brancos na mesma situação. Da mesma forma, acusados negros tinham chance duas vezes maior de serem classificados erroneamente com alto risco de reincidência em crimes violentos[365].

Por esta razão, o uso de algoritmos para definir sanção penal ou para conceder liberdade condicional tem sido fortemente contestado[366]. Isso porque em geral a análise preditiva não se baseia apenas na conduta do acusado ou em seus antecedentes. Para definir a

---

[363]KEHL, Danielle; GUO, Priscilla; KESSLER, Samuel. Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. **Harvard Law School**, jul. 2017, p. 19. Disponível em: <https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf?sequence=1>. Acesso em: 10 jan. 2018.

[364] ANDWIN, Julia et al. Machine Bias. **ProPublica**, mai. 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 10 jan. 2018.

[365] Segundo a pesquisa, os acusados negros costumavam estar em maior risco de reincidência do que realmente eram. Réus negros que não reincidiram foram quase duas vezes mais propensos a serem classificados erroneamente como um risco maior em relação às suas contrapartes brancas (45 por cento contra 23 por cento).Os réus brancos que cometeram novos crimes nos dois anos foram equivocadamente rotulados de baixo risco quase duas vezes mais vezes que os re-infratores negros (48% vs. 28%). Os acusados negros também tiveram duas vezes mais probabilidade de serem classificados erroneamente como sendo um risco maior de reincidência violenta. E os reincidentes violentos brancos foram 63 por cento mais propensos a ter sido classificados erroneamente como um baixo risco de reincidência violenta, em comparação com os negros. A análise de reincidência violenta também mostrou que os negros tinham 77% mais probabilidades de receberem pontuações de risco maiores do que os acusados brancos. LARSON, Jeff et al. How We Analyzed the COMPAS Recidivism Algorithm. **ProPublica**, mai. 2016. Disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Acesso em: 10 jan. 2018.

[366] SMITH, Mitch. Op. cit.

probabilidade de conduta futura assenta-se também no processamento massivo de dados de outros presos. Desta forma, a análise preditiva significa nada mais que apontar a provável conduta de um acusado com base na conduta adota por outros de perfil semelhante, o que desconsidera por completo a autonomia da vontade.

Outra objeção ao modelo preditivo na justiça criminal é a própria falta de transparência do algoritmo, os quais, em geral são adquiridos de companhias privadas e cujo código-fonte é protegido pelo sigilo comercial[367]. Os algoritmos fechados, protegidos pelo sigilo comercial, impedem conhecer a própria lógica de funcionamento do algoritmo, ou seja, dos critérios de ponderação de cada informação introduzida para definir a probabilidade de reincidência ou de não cumprimento das condições da liberdade condicional.

Mesmo naqueles casos que o algoritmo seja aberto, há a natural dificuldade decorrente da complexidade da linguagem de máquina, ou seja, os algoritmos trabalham com uma linguagem não acessível a todos, demandando conhecimento de profissional especializado. Isso pode significar a violação da garantia do contraditório e da ampla defesa, uma vez que, sem possuir expertise para conhecer os critérios do algoritmo, não poderia impugná-los de forma adequada.

Não se pode ignorar que a análise estatística da execução penal pode trazer valiosas contribuições, tais como a própria diminuição do encarceramento desnecessário ou mesmo a verificação da efetividade das sanções sob o ponto de vista da prevenção de novos crimes. O processamento de dados pode inclusive indicar a melhor direção das políticas públicas, prevenindo os riscos que geralmente levam à atividade criminosa, como vulnerabilidade social e econômica, evasão escolar, limitação de oportunidades, entre outros. A análise preditiva poderia ser um modelo mais eficiente e pontual de realizar a prevenção de atividades criminosas, alterando o rumo da história de jovens que ingressam na atividade criminosa em virtude dos mais variados fatores.

Todavia, a análise preditiva na área criminal não pode ser aplicada sem que se apresentem algumas preocupações com direitos fundamentais que são colocados em risco. É inevitável, neste ponto, a analogia por muitos feitas entre a análise preditiva e o filme de

---

[367] TASHEA, Jason. Courts are using AI to sentence criminals. That must stop now. **Wired**, abr. 2017. Disponível em: <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/>. Acesso em: 10 jan. 2018.

ficção científica *Minority Report*, lançado em 2002 cujos crimes eram evitados antes que ocorressem, em virtude de sua antecipação por três videntes[368].

Embora lançado em 2002, no gênero de ficção científica, a realidade em um futuro próximo cada vez mais se aproxima do filme. A diferença entre a aplicação da análise preditiva e o filme de ficção é que as previsões dos atos criminosos, em vez de serem realizadas por videntes, seriam determinadas por algoritmos. Isso expressa um risco ainda maior que a ficção, haja vista que há uma maior tendência a se acreditar no processamento de dados como uma atividade objetiva e imparcial, de confiabilidade superior à falibilidade humana.

A par das discussões típicas de direito penal que a detenção sem o cometimento de crime pode suscitar, há importantes discussões acerca da falibilidade da análise preditiva e os direitos fundamentais do acusado. Não é demais lembrar, algoritmos apresentam apenas uma probabilidade estatística e são construídos por seres humanos, dotados de seus preconceitos e vieses, os quais podem influenciar as correlações realizadas pelo algoritmo que não necessariamente são uma relação de causalidade.

Desta forma, reitera-se o caráter dúplice do *big data* também na análise preditiva. Ao mesmo tempo que apresenta o potencial de reduzir disparidades e subjetivismos aptos a prejudicar grupos sociais mais vulneráveis, pode ocasionar justamente o contrário, a saber, o aprofundamento das disparidades. Isto porque a base de dados que alimenta o *big data* são os fatos que ocorreram até então – tais como o número de crimes cometidos por região, classe social, faixa etária, etnia, entre outros. Ora, se o rigor da justiça criminal é mais duro com os mais vulneráveis, em virtude de uma série de fatores que vão desde o racismo à exclusão social, ao racismo estrutural, caso estes dados alimentem os algoritmos da análise preditiva, fatalmente o resultado do processamento irá reproduzir esse tratamento discriminatório.

Conforme já pontuado, tanto maior a quantidade de dados, mais precisa será a análise preditiva. Logo, o aperfeiçoamento da análise preditiva exige dados do próprio acusado, que podem ser dados públicos, obtidos nos mais variados bancos de dados governamentais ou de caráter público ou mesmo dados de natureza privada.

---

[368]No filme, que se passa em 2054, o departamento de Pré Crime se baseia na previsão coincidente de três videntes para evitar que crimes ocorram, prendendo o seu autor antes mesmo da prática do ato, tão somente baseado em sua intenção e iminência de fazê-lo. O filme é ambientado em uma sociedade amplamente monitorada, com tecnologia de vigilância que permite localizar qualquer indivíduo em qualquer lugar. Todavia, na previsão de um dos crimes, um dos três videntes prevê que determinado crime não ocorreria. Isso ocorre porque o policial do departamento de pré crime escolhe não praticar o crime a despeito da previsão, o que compromete toda a lógica sobre a qual se fundamenta a nova política criminal.

Ocorre que a vedação constitucional à não auto-incriminação[369], não permitiria o fornecimento forçado de tais informações. Isso porque, embora a informação sobre o histórico familiar, escolar ou de perfil sócio econômico não implique na condenação em si, tais informações poderão ser utilizadas para agravar a situação do eventual condenado. Portanto, fornecer dados para além dos necessários à qualificação e identificação, a exemplo do questionário COMPAS, pode implicar na extensão da pena ou mesmo na negativa de liberdade condicional, de acordo com o resultado da análise preditiva. Logo, se de algum modo o fornecimento das informações pode agravar a situação do indivíduo, fornecê-las compulsoriamente viola o direito à não auto-incriminação.

Não se ignora que a análise preditiva pode aperfeiçoar o processo de análise do histórico do acusado, fornecendo-se um resultado mais objetivo. Ocorre que condicionar o acesso aos eventuais benefícios do *big data* ao fornecimento de dados não é compatível com a não auto-incriminação. Tal fornecimento há de ser livre e voluntário, sem que a negativa implique em qualquer situação gravosa.

Do contrário, a análise preditiva pode comprometer a própria privacidade do indivíduo. Isto porque, ainda que sejam públicas as informações obtidas, reuni-las e processá-las pode constituir verdadeira varredura de informações sensíveis como círculos de amizade, relações afetivas, afinidades políticas ou ideológicas, expondo o indivíduo a um escrutínio desnecessário e que não se relaciona com o objeto da investigação criminal.

Na questão criminal a aplicação da análise preditiva é ainda mais delicada. Isto porque qualquer ato sancionatório exige a efetiva conduta humana ou sua omissão dolosa. No entanto, ao estender a pena de um acusado ou lhe negar o benefício da liberdade condicional com base nas probabilidades, está se agravando a situação jurídica de alguém com base em probabilidades obtidas a partir do comportamento de terceiros.

O processamento de dados, por mais objetivo que busque parecer, tem por combustível comportamentos anteriores e apenas antecipa tendências, não prevê fatos. Portanto é possível que alguém em situação de extrema vulnerabilidade, com histórico criminal extenso, ainda assim contrarie as previsões e adote outra conduta. Prejudicar a situação jurídica de alguém com base no comportamento de outrem contraria a garantia de

[369] A não autoincriminação encontra-se positivada no art. 5º, inciso, LXIII, da Constituição da República, que assim dispõe: "o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado".

que a pena não pode transcender a pessoa do acusado[370]. A garantia é uma via de mão dupla, não permitindo que qualquer sanção ao condenado alcance terceiros, mas que também os atos cometidos por terceiros não prejudiquem sua esfera de direitos. Pode violar ainda a pode violar a individualização da pena[371], caso se leve em conta atitudes de terceiros para apenar um acusado que não pode ter atribuído a si ato de outrem.

Não menos importante é o fato de haver uma limitação à garantia do devido processo legal[372], na medida em que o acesso ao código-fonte do algoritmo não é aberto ou mesmo quando aberto, sem que haja uma compreensão de seus critérios, dificulta o exercício do contraditório e ampla defesa. Não se pode dizer que haja efetivo exercício do contraditório e da ampla defesa se não há transparência do funcionamento do algoritmo.

Retornando à analogia com o filme *Minority Report*, a análise preditiva desconsidera a autonomia privada enquanto elemento da dignidade humana. Isto porque se a provável conduta do indivíduo é levada em consideração, desconsidera-se por completo sua liberdade de escolha, sua autonomia privada em adotar ou não a conduta prevista.

Atualmente a atividade preventiva nunca esteve tão valorizada na cultura ocidental, de modo que um dos pilares da sociedade contemporânea é a prevenção seja na área de saúde, patrimonial, ambiental, corporativa e porque não criminal. Decerto que as medidas preventivas em geral restringem a liberdade de escolha, mas costumam ser aceitas com relativa tranquilidade, sob o argumento de que seria um sacrifício apto a evitar um mal maior[373]. Logo, a análise preditiva vai ao encontro dos anseios por prevenção nos mais variados ramos, o que evidencia que a ficção não se encontra tão longe a realidade.

Com efeito, é tentador o bastante que, uma vez previsto o risco também haja uma demanda para que aquele risco não se concretize, ou seja, que haja a detenção antes mesmo da prática criminosa. Em uma sociedade assolada pelo medo, não seria incomum que se propusesse que, com base na probabilidade elevada de um indivíduo cometer um crime, não

---

[370] Nesse sentido, a Constituição Federal de 1988 prevê em seu art. 5º, inciso XLV que "nenhuma pena passará da pessoa do condenado, podendo a obrigação de reparar o dano e a decretação do perdimento de bens ser, nos termos da lei, estendidas aos sucessores e contra eles executadas, até o limite do valor do patrimônio transferido".

[371] De acordo com o art. 5º, inciso XLVI, da Constituição brasileira, "a lei regulará a individualização da pena e adotará, entre outras, as seguintes: a) privação ou restrição da liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão ou interdição de direitos".

[372] CRFB. Art. 5º (…):LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal;

[373] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 160.

ficássemos satisfeitos em apenas tomar medidas preventivas que evitassem o risco, mas também cedêssemos ao anseio de antecipar a punição, situação retratada na ficção[374].

Ressalte-se que as sociedades modernas construíram seus pilares sobre o estado de direito e a sanção estatal apenas se justifica após realização de ato previsto em lei como crime. A anterioridade da previsão legal para aplicação de sanção é pilar do direito sancionatório moderno, tanto é assim que a anterioridade da lei penal e sua irretroatividade são elencadas entre as garantias fundamentais[375].

Além disso, a aplicação de sanção tão somente com base na propensão do acusado viola outro pilar do estado democrático de direito que é a presunção de inocência[376]. Ninguém é presumidamente culpado, apenas formando-se a culpa após a condenação em sentença judicial transitada em julgado. Portanto, a aplicação de sanção com base tão somente na análise preditiva inverte a lógica da presunção de inocência e a exigência do devido processo legal substantivo. Além de impedir qualquer defesa que seja se um ato que não se cometeu, não permite que se presuma inocente até que haja segurança jurídica do cometimento da infração.

Ademais, a aplicação de sanção com base em análise preditiva desconsidera por completo a autonomia do indivíduo, utilizando-o antes para um fim coletivo do que um fim em si mesmo. Utilizar a análise de dados para punir alguém com base em propensões estatísticas ignora por completo a capacidade da pessoa humana de autonomamente fazer escolhas morais.

A aplicação da análise preditiva para definição de culpa ou de sanção terá o condão de substituir as escolhas morais dos indivíduos, tomadas a partir de sua concepção de bem, pelos cálculos algorítmicos. Isso contraria a lógica de ser responsável pelas próprias escolhas, substituindo-a por uma lógica paternalista que previne o indivíduo inclusive de escolhas não realizadas.

O risco é que, aos poucos as escolhas e, por conseguinte, as autonomias pública e privada serão substituídas pelas probabilidades futuras e as escolhas humanas serão cada vez mais coletivizadas, retirando do indivíduo qualquer resquício do que o define enquanto tal nas sociedades democráticas, o seu livre arbítrio. Portanto, punir um criminoso putativo, por um

---

[374] Ibidem, p. 159.

[375] Cf. o que prevê a Constituição Federal de 1988: Art. 5º. (...). XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal; XL - a lei penal não retroagirá, salvo para beneficiar o réu;".

[376] De acordo com o inciso LVII, do artigo 5º da Constituição Brasileira, "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória".

provável comportamento futuro, ainda que este cálculo seja o mais preciso possível, significará substituir a capacidade individual de fazer juízos morais pelas propensões de um algoritmo, cujo critério de cálculo é construído por outros seres humanos falíveis.

A análise preditiva tem muito a contribuir com a persecução penal. Todavia, essa contribuição não se dará na definição de culpa e aplicação de sanção sem que se rompam com pilares de modernidade. A centralidade que a dignidade humana assume nos ordenamentos jurídicos democráticos impede que se substitua a autonomia individual por probabilidades e propensões.

Deste modo, a análise preditiva deve observar a privacidade, a autonomia privada, o devido processo legal, a presunção de inocência e a isonomia.

De qualquer modo, a análise preditiva pode contribuir para orientar as políticas de segurança pública e prevenir os riscos sociais e fatores que levam à delinquência. No que tange à persecução penal, a análise preditiva pode contribuir para a ressocialização dos apenados, para aperfeiçoar a legislação, tornando-a mais eficaz, bem como para reduzir o encarceramento para as hipóteses estritamente necessária e elaborar medidas para prevenir a reincidência.

Todavia, a análise preditiva jamais pode ser utilizada para prejudicar a situação do acusado com base em provável comportamento futuro ou em comportamento estatístico de terceiro, o que implicaria em aniquilar a autonomia privada. Da mesma forma, o policiamento preditivo não pode perpetrar práticas discriminatórias[377], tampouco se utilizar de violação da privacidade para a base de dados da análise.

2.3.4 Consequências negativas do *big data*

As consequências negativas da aplicação do *big data* são as seguintes: (i) a negativa de oportunidades por engano baseada na atitude de terceiros (ii) preços diferenciados de bens e serviços para as comunidades de menor renda (iii) redução da capacidade de escolha do indivíduo, (iv) novas justificativas para práticas discriminatórias[378]

A redução de oportunidade por decisões baseada na atitude de terceiros refere-se ao próprio *modus operandi* do *big data*. Isto porque é da natureza da análise preditiva de grande volume de dados compilar comportamentos pretéritos e prever comportamentos futuros.

[377] FEDERAL TRADE COMISSION. **Big Data**:… op. cit., p. IV.

[378] Ibidem, p. 9-10.

Nesse sentido, o que pode ocorrer é que o indivíduo tenha uma vaga de emprego a si negada não com base em sua própria conduta, mas com base em probabilidade de comportamento baseada em atitudes de outros empregados. Da mesma forma, um consumidor pode ter seu pedido de crédito negado não com base em seu histórico de adimplência, mas com base na análise do histórico de crédito de outros clientes que compraram nos mesmos estabelecimentos do solicitanteHá inclusive notícia de que o algoritmo que determina a pontuação de crédito avaliar com um risco maior de inadimplência os clientes que tiveram despesas com aconselhamento matrimonial, terapia ou serviço de reparo de pneus, unicamente com base no histórico de outros consumidores que utilizaram os mesmos serviços[379]. É certo que esse modelo pode reduzir os riscos de crédito, tornando-o mais barato e acessível. Todavia, a redução de custos deve observar limites éticos e direitos fundamentais dos consumidores.

Outra consequência negativa é a possibilidade de criar ou reforçar disparidades. Ora, o algoritmo de busca de candidato que procura características parecidas com o corpo de funcionários de uma empresa com pouca diversidade, pode reforçar ainda mais a redução de oportunidades para grupos que não são os mais comumente procurados. Um outro exemplo é a publicidade direcionada. Ora, já se tratou neste trabalho de oportunidades de trabalho apenas apresentadas a homens de alta renda. Da mesma forma, a publicidade de crédito direcionada pode excluir populações de baixa renda que, embora tenha condições de arcar com o pagamento do empréstimo, sequer recebe a oferta, sendo excluído de antemão por não integrar o público-alvo.

Outra consequência negativa é a exposição de informação sensível a partir do processamento de dados. Exemplo disso é o fato de um estudo baseado no uso da função "curtir" do aplicativo facebook afirmar que pode determinar com 67% de precisão se o usuário está solteiro ou em um relacionamento; com mais de 60% se o usuário faz uso de cigarro, álcool ou drogas; com 88% a orientação sexual de um usuário do sexo masculino; com 82% se o indivíduo é cristão ou muçulmanoe 95% para precisar se o usuário é caucasiano ou afro-americano[380]. Isso demonstra que um conjunto de informações públicas básicas sobre o indivíduo, tais como os conteúdos para os quais apertou o botão "curtir" pode deixar à mostra informações de extremamente sensíveis, as quais talvez nem mesmo o indivíduo queira saber.

---

[379] Ibidem, p. 9.

[380] KOSINSK, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits & attributes are predictable from digital records of human behaviour.**PNAS**, v. 110, n. 5, p. 5802-5805, abr. 2013.

Por óbvio que tais informações podem aperfeiçoar as ferramentas de publicidade e permitir uma experiência mais personalizada. Por outro lado, a possibilidade de se saber com relativa precisão a orientação sexual do indivíduo[381] ou mesmo política[382] quando esta orientação é minoritária e estigmatizada pode expor indevidamente a privacidade, bem como possibilitar perseguições.

Outra consequência negativa associada ao *big data* é a possibilidade intensificação da política de preços diferenciados[383], apta a impactar com maior intensidade as populações de baixa renda.A diferenciação de preço por si só nada possui de ilegal, desde que não traga em si um tratamento desigual em relação a grupos minoritários. Todavia, o que pode ocorrer é impacto desigual quando a diferenciação afetar indiretamente características sensíveis, tais como cor, religião, origem, entre outros. A diferenciação de preços possui como guia a possibilidade de concorrência em determinado mercado e o risco daquele consumidor. Todavia, populações mais carentes[384], além de contarem com opções concorrenciais mais escassas podem ter os preços para compras mais elevados.Essa prática é melhor viabilizada com o *big data* que pode determinar de qual região é feita determinada busca, qual o nível de renda do comprador e qual o nível de concorrência a que terá acesso. Ocorre que esta personalização de preços impactará especialmente e mais intensamente grupos vulneráveis e mais sensíveis à variação de preços[385].

No Brasil, há notícia de ao menos um caso de diferenciação de preço, no qual se constatou que a empresa de turismo Decolar.com utilizava técnicas *geo-blocking* – bloqueio

---

[381] GREEN, Jon. Facebook knows you're gay before you do. **American Blog**, mar. 2013. Disponível em: <http://americablog.com/2013/03/facebook-might-know-youre-gay-before-you-do.html>. Acesso em: 10 jan. 2018.

[382] DATAINFORMED. They Know Who You're Voting For: How Big Data Redefines Political Campaigns' Microtargeting. Disponível em: <http://data-informed.com/they-know-who-youre-voting-for-how-big-data-redefines-political-campaigns-microtargeting/>. Acesso em: 18 dez. 2017.

[383] EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES. **Big Data And Differential Pricing**. Council of Economic Advisers: [s.l.], 2012, p. 4.Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf>. Acesso em: 08 jan. 2018.

[384] Nos Estados Unidos, Todavia, a loja Staples diferenciava preços de acordo com a localização do usuário. Isto porque há regiões em que há mais concorrência de lojas físicas que podem fazer frete ao preço online. Na prática isso desfavorece regiões com menos acessos a produtos e serviços e intensifica desigualdades, causando um impacto desproporcional sobre os mais vulneráveis. Não que isso constitua prática criminosa, mas deve haver transparência quanto à prática, a fim de que se possibilite a redução de seus impactos negativos. VALENTINO-DEVRIES, Jennifer; SINGER-VINE, Jeremy; SOLTANI, Ashkan. Websites Vary Prices, Deals Based on Users' Information. **The Wall Street Journal**, dez. 2012. Disponível em: <https://www.wsj.com/articles/SB10001424127887323777204578189391813881534>. Acesso em: 10 jan. 2018.

[385] Ibidem, p. 7.

da oferta com base na origem geográfica do consumidor - e de *geo-pricing* – precificação diferenciada da oferta também com base na geolocalização. A aplicação destas técnicas impedia que brasileiros tivessem acesso aos mesmos preços e ofertas de argentinos, que chagavam a pagar valores 30% menores em relação aos brasileiros.

Por fim, entre todos os efeitos negativos do *big data*, destaca-se apossibilidade de se viabilizar a criação de uma nova justificativa para práticas excludentes e discriminatórias. Conforme já apontado, um argumento comum a favor do *big data* é afirmar que as estatísticas ou os algoritmos são objetivos, ignorando-se que a própria engenharia do algoritmo pode estar viciada, perpetuando um cenário excludente na concessão de crédito e no acesso a oportunidades de emprego e educação[386].

2.4 **Dados como instrumento de vigilância massiva: o *big data* e a vigilância estatal**

Decerto que antes mesmo do advento do *big data*, a atividade de vigilância estatal em massa sempre existiu, seja por estratégia geopolítica, diplomática, para fins econômicos ou mesmo para neutralizar dissidentes. A própria origem da Quarta Emenda da Constituição estadunidense decorre da resistência dos então colonos do século XVIII em face das buscas irrazoáveis e gerais, realizadas em suas casas por autoridades da coroa britânica. Entendeu-se que a casa enquanto aspecto da privacidade apenas poderia ser objeto de busca razoável e específica, mediante mandado para tanto[387].

Da mesma forma, no início do século XX, o órgão precursor do FBI utilizava grampos, monitorava correspondências e utilizava informantes para neutralizar opositores às políticas nacionais. Não muito mais tarde, descobriu-se que o FBI na década de 1970 realizou investigação de espionagem doméstica que chegou a rotular mais de meio milhão de cidadãos

---

[386] FEDERAL TRADE COMISSION. **Big Data**..., op. cit., p. 10.

[387] FRIEDMAN, Barry; KERR, Orin. The Fourth Amendment. **Constitution Center**, [s.d.]. Disponível em: <https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv>. Acesso em: 10 jan. 2018:"The primary concerns of the generation that ratified the Fourth Amendment were “general warrants” and “writs of assistance.” Famous incidents on both sides of the Atlantic gave rise to placing the Fourth Amendment in the Constitution. In Britain, the Crown employed “general warrants” to go after political enemies, leading to the famous decisions in *Wilkes v. Wood* (1763) and *Entick v. Carrington*(1765). General warrants allowed the Crown’s messengers to search without any cause to believe someone had committed an offense. In those cases the judges decided that such warrants violated English common law. In the colonies the Crown used the writs of assistance—like general warrants, but often unbounded by time restraints—to search for goods on which taxes had not been paid. James Otis challenged the writs in a Boston court; though he lost, some such as John Adams attribute this legal battle as the spark that led to the Revolution. Both controversies led to the famous notion that a person’s home is their castle, not easily invaded by the government". Vide, ainda, HISTORY AND SCOPE of the Amendment. **Justia US Law**, [s.d.]. Disponível em: <https://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html>. Acesso em: 10 jan. 2018.

americanos como subversivos em potencial, estando entre os rotulados ativistas como Martin Luther King e o cantor John Lennon[388].

A relação entre banco de dados e vigilância também não se mostra como novidade. Há variados exemplos principalmente durante o último século. Pode-se citar a utilização dos dados do departamento censo dos Estados Unidos[389] para localizar os locais onde residiam nipo-americanos que seriam enviados aos dez campos de concentração criados em solo americano para confinamento, após os ataques à base de Pearl Harbor[390].

Da mesma forma, os amplos e abrangentes cadastros de cidadãos dos países baixos foram utilizados pelas forças nazistas para localizar judeus para os campos de concentração. Soma-se a isto o fato de que o número tatuado no braço dos judeus em campos de concentração correspondia àquele registrado nos cartões perfurados criados pela IBM como meio embrionário de armazenamento de dados, o que significa dizer que o processamento de dados de algum modo viabilizou - ou ao menos facilitou - o extermínio em larga escala, embora não se possa culpar a tecnologia pela aplicação que lhe é dada.

No Brasil, no período da ditadura militar iniciado em 1964, foram fichados cerca de 308 mil cidadãos sob a suspeita de serem contrários ao regime[391]. O candidato fichado, além da evidente perseguição e vigilância excessiva encontrava inúmeras dificuldades, entre elas a impossibilidade de conseguir emprego formal, sem contar o risco de sofrer prisão arbitrária para averiguação. Mais recentemente, no período democrático, veio a público uma operação conduzida pelo Exército Brasileiro destacou um de seus oficiais para se infiltrar entre manifestantes que organizavam protestos contra o governo[392].

Deste modo, sempre foi interesse de entes estatais e mesmo privados o controle das informações dos cidadãos nacionais e estrangeiros, seja legitima ou ilegitimamente. Ocorre que o *big data*traz um elemento adicional relevante, a saber, a possibilidade de coleta, análise

---

[388]GREENWALD, Glenn. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo americano. Tradução de: Fernanda Abreu. Rio de Janeiro: Sextante, 2014, p. 10 (ePub).

[389] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 151.

[390] OI, Mariko. As cicatrizes do confinamento de descendentes de japoneses nos EUA durante a 2ª Guerra. **BBC Brasil**, jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38440118>. Acesso em: 10 jan. 2018.

[391] VALENTE, Rubens. Ditadura "fichou" 308 mil, revelam arquivos do SNI. **Folha de São Paulo**, dez. 2008. Disponível em: <http://www1.folha.uol.com.br/fsp/brasil/fc1412200805.htm>. Acesso em: 08 jan. 2018.

[392] G1 SÃO PAULO. Deputado diz que Exército admitiu ter colocado militar em ato em SP nas Olimpíadas. **G1**, dez. 2016.Disponível em: <https://g1.globo.com/sao-paulo/noticia/exercito-admite-militar-infiltrado-em-ato-em-sp-nas-olimpiadas-diz-deputado.ghtml>. Acesso em: 10 jan. 2018.

e processamento massivo destes dados, integrando dados outrora desconexos que permitem constituir informações sensíveis sobre cada indivíduo.

Quando se trata de vigilância estatal, é comum se recorrer ao cenário distópico orwelliano[393], no qual o grande irmão observa a tudo e a todos através da mesma tela que realiza propagandas de um regime totalitário que não admite pensamentos dissidentes. O estado de vigilância ampla e constante por parte do estado não está longe de ser realidade em algumas situações.

Não significa dizer que big data e vigilância sejam termos que se confundem, até porque a vigilância existia muito antes do advento do *big data*. Todavia, não se pode negar que o *big data* potencializou a popularizou a vigilância, isto porque graças aos aparatos tecnológicos atuais é possível integrar dados de redes sociais, dados e metadados de comunicações eletrônicas, dados recolhidos por sensores de localização, permitindo o mais amplo acesso a dados integrados, bem como viabilizar a mineração destes dados aptos a localizar potenciais alvos, que antes poderiam passar despercebidos na multidão. A capacidade de armazenamento e processamento do *big data* faz a vigilância não eletrônica parecer artesanal.

Com efeito, os variados e milhares de sensores espalhados na vida online e offline podem recolher informações de localização, deslocamento, preferências de compras, hábitos diários, opiniões políticas, voluntariamente ou não. Tais sensores integrados à capacidade massiva de coleta, armazenamento e processamento de dados pode permitir a diagramação de um perfil completo do indivíduo que inclua não somente as informações voluntariamente fornecidas, mas também aqueles obtidas através de *tracking cookies* e outras técnicas de rastreamento digital vistas anteriormente.

Desta forma, avulta-se a importância do uso secundário dos dados que, utilizados para finalidade distinta da qual foi recolhida, constitui um mercado altamente rentável e fora de controle.

Conforme se colocou aqui neste trabalho, um dispositivo eletrônico, tal como uma televisão conectada à internet, um aparelho de telefone celular, um tablet ou notebook pode ser hackeado e transformado em equipamento de vigilância, ativando-se silenciosamente o microfone e câmera do dispositivo para transmitir em tempo real imagem e som de onde quer que esteja. Ora, se a vigilância na obra de ficção era permanente e permitia alguns pontos

[393] ORWELL, George. **1984**. Tradução de: Alexandre Hubner e Heloísa Jahn. São Paulo: Companhia das Letras, 2009.

cegos, os quais a câmera não alcançava[394], no cenário atual, parece não haver onde se esconder, diante do investimento cada vez maior por governos e entidades privadas em vigilância massiva.

No final de 2010 e em 2011, no Norte da África e Oriente Médio, houve o que ficou conhecido como Primavera Árabe, na qual milhões de pessoas ganharam as ruas espontaneamente e sem o auxílio de máquinas partidárias, para protestar contra regimes ditatoriais. As mobilizações em geral foram convocadas pelas redes sociais tais como Facebook, Youtuber e Twitter[395], plataformas que viabilizaram a mobilização das massas para os protestos. Posteriormente, descobriu-se que as ditaduras ameaçadas se armaram com um verdadeiro arsenal de equipamentos de vigilância, obtidas de empresas de tecnologia ocidentais[396].

Após os atentados de 11 de setembro, sob o argumento de combate ao terrorismo, inaugurou-se um verdadeiro mercado global de vigilância, que passou a movimentar mais de 5 bilhões de dólares por ano e envolve ao menos 36 empresas que fornecem tecnologia para varredura de computadores e celulares, interceptação em massa, produtos esses que são fornecidos tanto aos países democráticos do ocidente quanto a regimes autoritários[397].

A comercialização ampla de vigilância massiva desperta preocupação do sistema interamericano de proteção de direitos humanos, através Relatoria Especial para a Liberdade

---

[394] Ibidem, p. 16.

[395] DI FÁTIMA, Branco. Primavera Árabe: vigilância e controle na sociedade da informação. **Biblioteca online de ciências da comunicação**, [s.d.]. Disponível em: <http://www.bocc.ubi.pt/pag/fatima-branco-primavera-arabe-vigilancia-e-controle.pdf>. Acesso em: 11 jan. 2018.

[396]O regime de Assad na Síria contratou empresa de vigilância para rastrear pessoas; a polícia de Mubarak adquiriu equipamentos para quebrar a criptografia do Skype e interceptar chamadas de ativistas; na Líbia, jornalistas que visitaram um centro de monitoramento do governo em 2011 encontraram um grande aparato de vigilância da empresa francesa Amesys. Esse aparato inspecionava o tráfego de internet do principal provedor líbio, permitindo que se acessasse conteúdo de e-mails e se interceptasse chats, mapeando conexões entre suspeitos de serem dissidentes do regime. Ibidem.

[397]Em uma conferência sobre vigilância realizada próximo a Washington em 2011, fechada ao público geral, empresas prometiam soluções de vigilância para captura em massa ou direcionada para dezenas de milhares de conversas simultâneas de redes fixas ou móveis de telefonia; monitoramento de conteúdo da internet de celulares em tempo real; uso de *malware* para acessar dados que ficavam armazenados no celular e não eram transmitidos, driblando a criptografia dos aparelhos; o envio de falsas atualizações para instalação de spyware que induziu, por exemplo, que usuários as baixassem para aparelhos BlackBerry e permitiu que se monitorasse todas as comunicações, incluindo mensagens de texto, emails e o Blackberry Messenger; houve ainda a oferta de tecnologia de vigilância que explora vulnerabilidades não corrigidas em programas criados pela Microsoft Corp. e Apple Inc. DEVRIES-VALENTINO, Jennifer; ANGWIN, Julia; STECKLOW, Steve. Tecnologias de espionagem agora são vendidas no varejo. **The Wall Street Journal**, nov. 2011. Disponível em: <https://www.wsj.com/articles/SB10001424052970204531404577050803429174524>. Acesso em: 12 jan. 2018.

de Expressão da Comissão Interamericana de Direitos Humanos (CIDH)[398]. Houve o vazamento de cerca de 400 GB de dados em poder da empresa italiana *Hacking Team*, dedicada à venda do software de espionagem através do *Remote Control System* (Sistema de Controle Remoto, RCS por suas iniciais em inglês), de nomes *DaVinci* ou *Galileo*. Entre os dados coletados estariam contas, correios eletrônicos, dados fiscais, entre outros arquivos.

Com efeito, de acordo com a Declaração Conjunta sobre Programas de Vigilância e seu Impacto na Liberdade de Expressão, dos Relatores das Nações Unidas e da Organização dos Estados Americanos para liberdade de expressão[399], as tarefas de vigilância que restrinjam que impactem a liberdade de expressão devem ter sua realização pautada na lei, a qual deve se pautar por um fim legítimo, que deverá prever as hipóteses, o tempo de duração da medida e a autoridade competente para executar, supervisionar e autorizar a atividade.Ainda de acordo com o documento, caso se invoque razões de segurança nacional, a lei deve definir com clareza o critério para permitir a violação de comunicações e de dados pessoais. Ademais, as decisões de realizar tarefas de vigilância que impliquem na restrição à privacidade devem ser autorizadas por autoridades judiciais independentes, a quem incumbe o dever de declinar as razões pelas quais a medida é idônea para alcançar os fins buscados no caso concreto.

Não se pode dizer, contudo, que a vigilância estatal em massa seja uma atividade exclusiva de regimes totalitários. Em 2013, a Agência de Segurança Nacional (National Agency Security) dos Estados Unidos envolveu-se no maior escândalo de vigilância de todos os tempos, após Edward Snowden, ex funcionário da NSA (*National Security Agency*)[400], fornecer à imprensa comprovações da vigilância em massa praticada pela agência.

---

[398] Esse vazamento motivou relatório elaborado pela, exortando os estados a tomarem providências em razão de ter se contatado que vários estados integrantes do sistema interamericano teriam adquirido produtos da citada empresa de vigilância nos últimos anos. Segundo o relatório, o software de espionagem vendido pela empresa estaria desenhado para driblar a encriptação nos computadores e telefones celulares, o que permitiria subtrair dados, mensagens, chamadas e correios, conversações de voz através de VOIP e mensagem instantânea. Afirma o relatório ainda que, através do referido software seria possível a ativação remota de câmeras e microfones de dispositivos sem consentimento do usuário, transformando-os em equipamentos de vigilância. Consta ainda do relatório que, segundo o site da própria empresa, a coleta de evidência nos dispositivos monitorados é silenciosa e a transmissão dos dados coletados desde o dispositivo ao servidor do RCS é criptografada e não é rastejável. OEA. Comunicado de Imprensa R80/2015. **OEA**, jul. 2015. Disponível em: <http://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=998&lID=4>. Acesso em: 12 fev. 2018.

[399] OEA. Declaração Conjunta sobre Programas de Vigilância e seu Impacto na Liberdade de Expressão. **OEA**, jun. 2013. Disponível em:<http://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=926&lID=4>. Acesso em: 08 jan. 2018.

[400]Em tradução livre, Agência de Segurança Nacional. É a agência de segurança e inteligência dos Estados Unidos, criada em 4 de novembro de 1952, subordinada ao Departamento de Justiça daquele país.

Apenas para se ter noção da amplitude do monitoramento, no relatório do programa *Boundless Informant*, no mês de março de 2013, em apenas uma das unidades de NSA[401], contabilizou-se a coleta de dados de mais de três bilhões de chamadas telefônicas e e-mails, que haviam transitado no sistema de comunicações norte-americano. A nível global, coletou-se em período semelhante dados sobre 97 bilhões e-mails e 124 milhões de chamadas de comunicações em todo o mundo[402]. Ainda em 2012, em relatório secreto da NSA, celebrou-se a marca de um trilhão de comunicações processadas pelo programa SHELLTRUMPET que realiza inclusive a interceptação direta dos cabos de fibra óptica marítimos para alcançar esta marca de processamento praticamente em tempo real[403].

Essa assustadora e gigantesca rede de monitoramento de informações e vigilância em solo americano avultou-se depois dos atentados de 11 de setembro. Em 2008, ainda no governo Bush, foi editada uma emenda à lei de vigilância de 1978, que ficou conhecida como FISA - *Foreign Intelligence Surveillance Act*[404]. Em suma, a legislação[405]permite a algumas autoridades administrativas do país espionar, sem mandado judicial, comunicações eletrônicas entre estrangeiros e entre americanos e estrangeiros[406], como estratégia para combate ao terrorismo, o que consolidaria juridicamente uma prática já adotada desde os atentados de 2001[407].

Revelou-se ainda que a pedido do FBI, em 25 de abril de 2013, o tribunal secreto de vigilância estrangeira *(FISA - Foreign Intelligence Surveillance Court)* expediu ordem para

---

[401] Trata-se da Global Access Operations (Operações de Acesso Global, GAO na sigla em inglês).

[402] GREENWALD, Glenn. Op. cit., p. 73.

[403] Ibidem.

[404]Em tradução livre, Lei de Vigilância da Inteligência Externa.

[405] O texto da referida legislação encontra-se em: <https://www.congress.gov/bill/110th-congress/house-bill/6304>. Acesso em: 10 jan. 2018.

[406] Há quem entenda que a Lei patriótica de 2001, em vez de permitir a vigilância em massa visava trazer limites à atuação das agências de inteligência, consolidando a legislação anterior, mas também protegendo liberdades civis. Vide: KERR, Orin S. Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't. 97 **Northwestern University Law Review**, v, 97, n. 2, p. 607-674, 2003.

[407] RISEN, James; LICHTBLAUDEC, Eric. Bush Lets U.S. Spy on Callers Without Courts. **The New York Times**, dez. 2005. Disponível em: <http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>. Acesso em: 10 fev. 2018.Destaca-se o seguinte trecho: "Tradução livre: Meses depois dos ataques de 11 de setembro, o presidente Bush, secretamente, autorizou a Agência Nacional de Segurança a escutar a americanos e outros dentro dos Estados Unidos para procurar evidências de atividades terroristas sem os mandados aprovados pelo tribunal normalmente exigidos para espionagem doméstica, de acordo com funcionários do governo. (...) Sob um pedido presidencial assinado em 2002, a agência de inteligência monitorou as chamadas telefônicas internacionais e as mensagens internacionais de e-mails de centenas, talvez milhares, de pessoas nos Estados Unidos sem mandados nos últimos três anos, em um esforço para rastrear possíveis "sujos" números "ligados à Al Qaeda, disseram as autoridades. A agência, segundo eles, ainda busca mandados para monitorar comunicações inteiramente domésticas.

que a empresa Verizon, a maior companhia telefônica dos Estados Unidos – fornecesse os dados de registro[408] de ligações telefônicas milhões de usuários[409], atualizando diariamente os registros junto ao FBI durante três meses. Trata-se de vigilância em massa da população sem que necessariamente haver comprovação de qualquer envolvimento com atividade terrorista.

No mesmo ano, revelou-se que o PRISM[410], programa ultrassecreto da NSA, tinha a capacidade de acessar os provedores de grandes companhias privadas da internet para obter conteúdo de e-mail, bate-papo por vídeo e voz, vídeos, fotos, ligação através da tecnologia VOIP (voz sobre IP, utilizada pelo Skype, por exemplo) transferências de arquivos, detalhes de redes sociais entre outros. O documento obtido afirma que a coleta diretamente no servidor é feito com colaboração da companhias[411], tendo-se iniciado em 2009 com a Microsoft, tendo-se obtido a adesão da Apple em outubro de 2012.

Desta forma, o programa revela um outro estágio de violação à privacidade pela vigilância estatal. Isso porque, se a vigilância já se mostrava invasiva com o acesso aos registros de comunicações, o acesso direto aos provedores dos gigantes da internet não deixa sob ameaça a privacidade apenas os usuários norte-americanos, mas todo o mundo na medida em que as citadas companhias, embora sediadas nos Estados Unidos, possuem ampla penetração em centenas de países.

Não menos importante é a descoberta originada do mesmo escândalo que, embora as atividades de vigilância sempre se justificassem sob o pretexto de combate ao terrorismo, a bem da verdade, todo o arsenal de espionagem da NSA foi utilizado para a realização de espionagem com fins estritamente econômicos, atingindo em cheio as comunicações da Petrobrás[412] e Eletrobrás. Foram interceptadas também, comunicações confidenciais e

---

[408] Segundo o conteúdo da ordem, apenas deveriam ser fornecidos os metadados das comunicações tais como os números de ambas as partes dados de localização, duração da chamada, identificadores exclusivos e o tempo e a duração de todas as chamadas, não incluindo, portanto, o conteúdo da conversa não estaria incluído no mandado.

[409] GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. **The Guardian**, jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.Acesso em: 10 fev. 2018.

[410] GREENWALD, Gleen; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, jun. 2013. Disponível em:<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 10 fev. 2018.

[411] Segundo o documento revelado, a adesão da Microsoft teria ocorrido em novembro de 2007, seguido de Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, encerrando-se com adesão da Apple em 2012. O relatório é datado de 2013. Recorrendo a argumentos desencontrados, em geral todas as empresas negam que colaborem com a NSA para acesso direto e irrestrito aos seus servidores.

[412] Outras companhias do ramo petrolífero também foram atingidas podendo-se citar, além da escuta e interceptação de emails da Petrobras, de conferências econômicas na América Latina, de empresas de energia da Venezuela e do México. GREENWALD, Glenn. **Sem lugar para se esconder**... Op. cit., p. 117.

estratégicas do Ministério das Minas e Energia[413], por parte do Canadá[414], que é parceiro dos Estados Unidos[415] em ações de vigilância no programa Five-Eyes[416]. Ora, sequer a Presidente da República brasileira[417] e seus assessores mais próximos escaparam ao vigilantismo, tampouco a primeira-ministra da Alemanha, o que abriu uma crise diplomática entre os dois países e os Estados Unidos[418].

Outra preocupação digna de nota são os "Fusion Centers", sob a responsabilidade da NSA, que consistem em "pontos focais de áreas urbanas para o recebimento, análise, coleta e compartilhamento de informações relacionadas a ameaças entre o âmbito federal, estadual, local, tribal, territorial, além de parceiros do setor privado[419]". Os referidos despertam preocupações no que tange à privacidade, pois ao utilizar padrões de atividades ditas suspeitas *(SAR - Suspicious Activity Reporting)* e os critérios para definir quais seriam as atividades ditas suspeitas são vagos[420] e não observam um critério de proporcionalidade, ocasionando,

---

[413] O programa de espionagem Olympia era destinado a vigiar comunicações do Ministério das Minas e Energia Brasileiro, já que o setor é estratégico para empresas canadenses. Segundo documentos apresentados por Snowden, em conferência realizada em 2012, a CSEC (Organização de Serviços de Comunicações do Canadá) afirmou ter tido como alvo o Ministério das Minas e Energia do Brasil, agência responsável por regulamentar o setor de maior interesse para as empresas canadenses.

[414] G1. Ministério de Minas e Energia foi alvo de espionagem do Canadá. **G1**, out. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/10/ministerio-de-minas-e-energia-foi-alvo-de-espionagem-do-canada.html>. Acesso em: 10 fev. 2018.

[415] Documentos revelados por Snowden apontam que, em virtude da parceria do Programa Five-Eyes, há indícios de uma cooperação generalizada entre a CSEC do Canadá e a NSA, que inclui esforços do Canadá para criar postos de espionagem destinados a vigiar comunicações mundo afora a pedido da NSA e para o seu benefício, e a espionar parceiros comerciais de interesse para a agência norte-americana.

[416]O Tratado de Segurança UK-USA (*UK–USA Security Agreement*, em inglês), é um acordo que estabelece a integração de agências de inteligência de cinco países anglófonos com o propósito de compartilhar informações secretas. Integram o tratado a Austrália, o Canadá, a Nova Zelândia, o Reino Unido e os Estados Unidos da América, que em conjunto são denominados Os Cinco Olhos (*The Five Eyes*, em inglês). Vide, MAIEROVITCH, Wálter. Os "Cinco Olhos" e os cegos. **Carta Capital**, out. 2013. Disponível em: <https://www.cartacapital.com.br/revista/774/os-201ccinco-olhos201d-e-os-cegos-9894.html>. Acesso em: 10 fev. 2018.

[417] G1. Documentos da NSA apontam Dilma Rousseff como alvo de espionagem. **G1**, set. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html>.Acesso em: 10 fev. 2018.

[418] UCHOA, Pablo. Dilma usará discurso na ONU para criticar espionagem dos EUA. **BBC Brasil**, set. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/09/130923_dilma_onu_pu_dg>.Acesso em: 10 fev. 2018.

[419] Tradução livre de "Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners". STATE AND MAJOR Urban Area Fusion Centers. **Homeland Security**, [s.d.]. Disponível em: <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>. Acesso em: 10 jan. 2018.

[420] Segundo a Electronic Frontier Foundation, atitudes corriqueiras tais como tirar fotos ou vídeos de instalações, edifícios ou infra-estrutura ou demonstrar interesse incomum nessas instalações, profissionais (por exemplo, no caso de engenheiros) pode ser enquadrada como atividade suspeita. Os exemplos incluem a observação através

em alguns casos, uma atuação discriminatória com impacto desigual, com a criação de perfis de cidadãos sob investigação de determinadas religiões ou raças, já que 78% dos relatórios de atividades suspeitas recaíram sobre não brancos[421].

Atualmente, há 78 centros de integração reconhecidos nos Estados Unidos. Com efeito, tais centros inspiram preocupação por algumas razões: (i) o sigilo excessivo de suas ações, o que dificulta o controle de seus métodos, dada a ausência de transparência; (ii) por admitir a participação de entidades privadas, que podem ter atuação interessada e facilitar violações à privacidade dos investigados; (iii) por constituir um incentivo à mineração de dados, o que permite concluir que há coleta e processamento de dados em massa e não apenas sobre potenciais suspeitos; e o risco de utilização de repressão política, já que alguns centros têm monitorados movimentos acadêmicos, grupos de religião muçulmana e ativistas em geral[422]. Portanto, o risco maior é que os Fusion Centers se constituam na capilarização da vigilância estatal e que pratiquem tratamento enviesado e discriminatório de cidadãos, constituindo em instrumento de perseguição religiosa, racial e política.

De fato, do cidadão mais comum às mais altas autoridades dos estados, pode-se dizer que não há onde se esconder, diante do invasivo e constante aparato de vigilância utilizado por estados dos mais variados matizes ideológicos, sejam totalitários ou democráticos. As revelações apresentadas por Edward Snowden associadas aos documentos divulgados pelo siteWikiLeaks dão conta de que não há informação que não possa ser monitorada. Conforme se viu neste trabalho, agentes da CIA exploravam vulnerabilidades de aparelhos como telefones, tablets, computadores e até mesmo TVs conectadas à internet para ativar seus microfones e torná-los equipamentos de vigilância, mesmo quando aparentemente desligados[423].

---

de binóculos, a tomada de notas, a tentativa de medir distâncias etc. KAYYALI, Dia. Why Fusion Centers Matter: FAQ. **Electronic Frontier Foundation**, abr. 2014. Disponível em: <https://www.eff.org/deeplinks/2014/04/why-fusion-centers-matter-faq>.Acesso em: 10 jan. 2018.

[421] Ibidem.

[422] MORE ABOUT FUSION Centers. **American Civil Liberties Union**, [s.d]. Disponível em: <https://www.aclu.org/other/more-about-fusion-centers>. Acesso em: 10 jan. 2018.

[423] Na verdade, há notícia de 2006 que informa a realização pelo FBI de escuta telefônica através da ativação remota do microfone do telefone, para fins de investigação criminal. No caso concreto, houve autorização judicial diante da constatação de que por outros meios não seria possível a produção de provas contra os acusados. Vide: MCCULLAGH, Declan. FBI taps cell phone mic as eavesdropping tool.**CNET**, dez. 2006. Disponível em: <https://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/>. Acesso em: 18 jan. 2018.

Mostra-se suficientemente assustadora a capacidade dos meios de vigilância cibernética para preocupar qualquer um que utiliza a internet. A verdade é que grande parte da população atualmente possui a vida eletronicamente intermediada.

Em uma sociedade caracterizada pela modernidade líquida, a vigilância também se apresenta fluida, de modo que não há uma estrutura sólida da qual se possa ter certeza de seus limites, vez que os tentáculos da vigilância se espraiam para além das fronteiras nacionais. Enquanto a política, compreendida como meio democrático de acesso ao poder, é localizada nos limites geográficos do respectivo ente nacional, o poder é exercido globalmente. Deste modo, a vigilância apresenta-se transnacionalizada, alcançando cidadãos em diferentes territórios, situação na qual a política local não consegue se opor. É exemplo disso a segurança aeroportuária cuja lista de suspeitos pode ser determinada por uma autoridade que sequer pertence à burocracia daquele país, com base em banco de dados que sequer se sabe onde está localizado[424]. Portanto, enquanto os poderes políticos possuem fronteiras bem delimitadas, a vigilância não as conhece, espraiando-se por variados objetos e locais.

Nenhuma obra de ficção pode prever com exatidão o atual estágio de vigilância. O livro de George Orwell tinha por foco a vigilância estatal realizada através de telas de TV[425]. O panótico de Bentham[426] procurava estabelecer o modelo ideal de vigilância prisional que alcançasse todos os presos sem que estes soubessem em que direção o panótico estaria vigiando, obrigando-os a terem autodisciplina.

Ocorre que, nos tempos atuais, a vigilância antes de ser exclusivamente estatal é compartilhada com grandes corporações privadas. Equipamentos, técnicas e tecnologias de vigilância que antes se restringiam às agências nacionais de inteligência cada vez mais fazem parte do catálogo de produtos dos mercadores privados da indústria da vigilância que podem comercializá-los com os mais variados clientes.

---

[424]Até as fronteiras nacionais, antes geograficamente localizadas – ainda que de modo arbitrário –, agora aparecem, nos aeroportos, distantes das "bordas" territoriais, e, o que é mais significativo, em bases de dados que podem nem estar "no" país em questão.

Prosseguindo com o exemplo, a questão das fronteiras mutáveis, para muitos, é fonte de grande incerteza. É um momento de ansiedade passar pela segurança de um aeroporto sem saber exatamente em que jurisdição se está ou para onde irão seus dados pessoais, em especial quando se faz parte de uma população suspeita. E se você for desafortunado a ponto de ser detido ou descobrir que seu nome está numa lista de pessoas proibidas de voar, saber o que fazer é muitíssimo difícil. Além disso, é um desafio assustador realizar mudanças políticas que possam, por exemplo, tornar mais simples as viagens necessárias.

[425] ORWELL, George. Op. cit., p. 16.

[426]BENTHAM, Jeremy et. al. **O panóptico**. Tradução de: Guacira Lopes Louro, M. d. Magno, Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica Editora, 2008.

Da mesma forma, o poder que as grandes corporações globais de internet[427] possuem sobre a privacidade alheia superam em muito os poderes políticos locais, havendo a possibilidade de causar um dano muito maior à privacidade dos seus usuários em relação ao estado que pertence o cidadão. Logo, a vigilância que antes se encontrava concentrada nas mãos do estado, atualmente está em poder de variados agentes privados, de modo que não é possível pensar a vigilância apenas como atividade exclusivamente estatal.

Decerto que essa distribuição assimétrica dos meios de realização de vigilância, em razão do acesso às bases de dados, implica também uma distribuição de poder não necessariamente estatal[428]. Sendo os dados o novo petróleo, no sentido de ser o ativo mais valorizado de sua era, quem possui acesso a vastos bancos de dados possui o poder que disto decorre.

Diferentemente do panótico de Bentham, o agente da vigilância sequer está ao alcance físico do vigiado, estando para além das fronteiras nacionais e a sua vigilância não se restringe às prisões e aos presos, mas alcança um número indiscriminado de pessoas, mesmo que não realizem nenhuma atividade suspeita. Por essa razão pode-se nomear a vigilância atual de pós-panóptica, vez que não encontra limites geográficos nos sistemas prisionais nem se restringe a um público em específico[429].

A vigilância contemporânea embora não se destine a presos, possui um público preferencial. Uma das consequências da vigilância em massa é a coleta, análise e classificação das pessoas vigidas, dividindo-as em perfis[430]. Portanto, a categorização social é consequência e objetivo fim da vigilância, já que uma vez categorizados, podem ser definidos os perfis indesejados por quem vigia, seja sob argumento de combate ao terrorismo ou mesmo para perseguir dissidentes políticos. As ações de vigilância envolvem a análise de máquina por meio de algoritmo, o que faz parecer que o alvo da ação seja aleatório de acordo com os critérios estatísticos e de software. Todavia, os resultados da categorização apresentam-se homogêneos, sempre recaindo sobre um determinado perfil racial ou religioso. Não é por outra razão que coincidentemente árabes e muçulmanos parecem estar sujeitos a um controle

---

[427]ROOSENDAAL, Arnold. Facebook Tracks and Traces Everyone: Like This! **Tilburg Law School Legal Studies**, Research Paper Series No. 03, p. 1-10, 2011.

[428] PIMENTA, Ricardo M. Big Datae Controle da Informação na Era Digital: Tecnogênese de uma Memória a Serviço do Mercado e do Estado. **Tendências da Pesquisa Brasileira em Ciência da Informação**, v. 6, n. 2, p. 15, jul./dez. 2013.

[429] BAUMAN, Zygmunt. **Vigilância Líquida**. Diálogos com David Lyon. Zahar Editora: Rio de Janeiro, 2014, p. 40.

[430] BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **Revista FAMECOS**, Porto Alegre, v. 15, n. 36, p. 10-16, ago. 2008.

mais rigoroso nos aeroportos. Desta forma, categorização social constrói um sistema de distribuição de desvantagens cumulativas[431].

A justificativa para implementação de um programa de vigilância em massa sempre costuma ser a segurança dos próprios vigiados. Tanto é assim que os programas norte-americanos mais invasivos de monitoramento de comunicações em massa ocorreram no pós 11 de setembro, com o advento de normas que davam mais poderes às autoridades de inteligência, conforme visto. Há uma tendência estratégica de relacionar a segurança diretamente com a vigilância, como se a vigilância fosse condição essencial à sensação de segurança. Isso faz com que a aceitação dos programas de vigilância e mineração de dados tenha uma maior aceitação em relação à população em geral, como se fosse necessário renunciar parcela da privacidade que se tem em nome da segurança que se terá. Em uma sociedade de risco, tudo que não se quer perder é a segurança[432].

Um argumento muito comum a ser utilizado para justificar a adesão voluntária e dissipar resistências à vigilância é não ter nada e esconder. Significa dizer que apenas se oporiam às ações de vigilância quem possui esqueletos no armário, quem comete eventuais ilegalidades[433]. Ocorre que o argumento distorce a real discussão. A uma porque opor-se à vigilância irrazoável e sem critério não deve implicar em nenhuma presunção de culpa. Ora, a privacidade é direito fundamental do indivíduo contra o Estado de modo que cabe ao ente estatal justificar a razão pela qual viola, sem fundamento razoável, a privacidade dos cidadãos. Não se pode inverter a lógica transferindo ao cidadão, diante do imenso aparato tecnológico, a obrigação do ônus argumentativo.

Ademais, não há uma necessária oposição entre privacidade e segurança como se estes valores estivessem necessariamente de lados opostos da balança. Na verdade, esta abordagem mostra-se maniqueísta, vez que há insegurança também dos próprios cidadãos, quando não se sabe que informação será confidencial, diante do cenário de vigilância massiva.

Com efeito, se levado ao extremo o argumento de não ter nada a esconder, teríamos uma sociedade de homens transparentes, sem qualquer preservação do espaço essencial para reflexão e desenvolvimento da própria personalidade, haja vista todas as atitudes serem públicas, não havendo mais a invisibilidade e o anonimato. Em geral, quando se aceita facilmente o argumento de não ter nada a esconder, apenas se pensa pontualmente em que

---

[431] BAUMAN, Zygmunt. Op. cit., p. 14.

[432] Ibidem, p. 74.

[433]SOLOVE, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. **San Diego Law Review**, v. 44, p. 745, 2007.

tipo de informação se está permitindo desvelar em nome da suposta segurança. Não ter nada a esconder, não significa necessariamente ter a obrigação de mostrar.

No estado democrático de direito, cabe ao estado seguir as normas pré-estabelecidas e justificar sua atuação. Até porque a vigilância em massa apresenta algumas contradições insuperáveis. A primeira delas é o fato de, embora a justificativa da ação seja o combate ao crime e ao terrorismo, todos os cidadãos, inclusive aqueles que não possuem nenhuma relação com o terrorismo, sofrem varreduras eletrônicas. Portanto, a vigilância torna a todos suspeitos sob pretexto de neutralizar o suspeito, subvertendo a lógica.

Outra contradição que ocorre é que, enquanto cada vez mais se exige transparência dos cidadãos em nome de um suposto bem maior, vasculhando-se todos os aspectos de sua vida, a atividade da vigilância é cada vez menos transparente e não se submete a nenhuma *accountability*. Sob o argumento que a mineração de dados é atividade técnica, deixa-se de dar transparência aos critérios de funcionamento do algoritmo que seleciona atividades ditas suspeitas. Ademais, não há regras sobre a possibilidade de contestar os bancos dados que classifique o indivíduo negativamente, pois no contexto globalizado sequer se sabe a qual autoridade se reportar para retificar os registros[434]. Ora, a utilização do argumento de não ter nada a esconder é o primeiro passo para se fornecer uma delegação em branco para que se pratique o autoritarismo e perfeccionismo moral[435]

Além da falta de transparência, percebe-se uma ausência de parâmetros éticos da vigilância, da responsabilização ser humano diante de outrem. Pode-se citar dois confrontos entre ética e vigilância: a diaforização[436] – na qual sistemas e processos, sob o argumento de serem automatizados, se divorciam de qualquer consideração de caráter moral. Outro exemplo de confronto é a separação entre pessoas e as consequências de suas ações através da automatização. Isso porque a automatização permite cada vez mais que se tomem decisões à distância. Logo, um controle de fronteira que nega o acesso de pessoas em vulnerabilidade pode parecer desapaixonada e neutra, sob o argumento de que apenas se trata de automatização do processo. É como se a culpa por falta de ética fosse culpa da máquina e não de quem a opera.

---

[434] BAUMAN, Zygmunt. Op. cit., p. 13.

[435] PEREIRA, Jane Reis Gonçalves. Quem não deve teme apenas a injustiça. **Estado de Direitos**, set. 2012. Disponível em: <https://estadodedireitos.com/2012/09/03/quem-nao-deve-teme-apenas-a-injustica/>. Acesso em: 10 jan. 2018.

[436] Sobre o termo, vide nota de rodapé nº 18.

Todavia, a aparente neutralidade moral na mineração de dados na vigilância não se confirma na realidade. Na prática, a suposta neutralidade afeta oportunidades e escolhas existenciais dos indivíduos que possuam o perfil indesejado, vez que toda neutralidade milita a favor da manutenção do *status quo*, ou seja, na prática mantém as mesmas desvantagens para os grupos desfavorecidos.

De tudo que foi visto acerta da vigilância em massa e seus recursos e objetos de investigação praticamente ilimitados, resta questionar se, mesmo sob o argumento da ameaça do terrorismo, ou do crime organizado, em outros casos, seria juridicamente adequado um modelo de vigilância ampla, a fim de identificar possíveis ameaças.

Antes de tudo, deve ressaltar que, a despeito de consagrado no senso comum, a falácia do argumento de não ter nada a esconder não deve ser levada em conta, vez que a premissa ofende direitos fundamentais mais elementares, tais como a presunção da inocência, o devido processo legal e o próprio direito à privacidade. Admitir o argumento seria fazer prevalecer o vigilantismo estatal aprioristicamente, em uma espécie de hierarquização de interesses.

A justificativa da vigilância, sob argumento de que apenas são colhidos apenas metadados - ou seja, exclui-se o conteúdo da comunicação e apenas se coletam os seus dados secundários - além de ser questionado quanto a sua veracidade[437], é questionável ainda que a coleta de metadados seja de todo inofensiva à privacidade.

Nessa perspectiva, cabe repisar que o USA Patriotic Act, ou lei patriótrica[438], que entrou em vigor após os atentados de 11 de setembro, passou a permitir o recolhimento de metadados praticamente de maneira ilimitada[439]. Todavia, embora os metadados não se refiram ao conteúdo da comunicação, podem ser muito mais reveladores do que parecem. Isso porque definir a rede de comunicação do indivíduo, não se restringindo às pessoas com quem se comunica diretamente, mas também os contatos frequentes destes, pode rastrear contatos de um jornalista com a sua fonte, de uma rede de ativistas que protestam contra o governo ou mesmo de uma jovem que faz contato com uma clínica que realiza abortos. Isso apenas

---

[437] "Em termos bastante genéricos, a NSA coleta dois tipos de informação: conteúdo e metadados. "Conteúdo", nesta acepção, significa escutar de fato as chamadas telefônicas das pessoas, ler seus e-mails e chats, bem como ter acesso às suas ações na internet, como históricos de navegação e atividades de busca. A coleta de "metadados", por sua vez, envolve colher dados sobre essas comunicações. A NSA define isso como "informações sobre conteúdo (mas não o conteúdo em si)". GREENWALD, Glenn. Op. cit., p. 16.

[438] THE USA PATRIOT Act: Preserving Life and Liberty. **Department of Justice Website**, [s.d]. Disponível em: <https://www.justice.gov/archive/ll/highlights.htm>. Acesso em: 10 jan. 2018.

[439] REDAÇÃO ÉPOCA COM AGÊNCIA EFE. Casa Branca admite que monitora telefonemas de cidadãos americanos. **Época**, jun. 2013. Disponível em: <http://revistaepoca.globo.com//Mundo/noticia/2013/06/casa-branca-admite-que-monitora-telefonemas-de-cidadaos-americanos.html>. Acesso em: 21 jan. 2018.

demonstra que o monitoramento e processamento de metadados, associado a outras fontes de informação podem representar um alto risco à privacidade[440].

Não por outra razão o Marco Civil da Internet, além de proteger a inviolabilidade do sigilo das comunicações, prevê também a inviolabilidade sigilo do fluxo de suas comunicações pela internet, o que pode ser compreendido metadados. A referida lei apenas admite a quebra desse sigilo por ordem judicial[441]. Neste mesmo sentido, o artigo 10 da mesma lei obriga que os provedores de conexão possuem a obrigação de preservar a privacidade dos registros de conexão e de acesso a aplicativos, apenas podendo fornecê-los por ordem judicial[442].

Outrossim, não se mostra juridicamente adequado um modelo de vigilância estatal em massa determinado por autoridades administrativas, pois o texto constitucional é categórico ao definir as hipóteses nas quais se admite a quebra de sigilo telefônico, para o qual se exige ordem judicial, nas hipóteses e na forma que a lei estabelecer e para a fins de investigação criminal ou instrução processual penal[443]. Ainda que se faça uma interpretação evolutiva para se admitir a quebra de sigilo de dados, parece incontornável a reserva de jurisdição, uma vez

---

[440]"Os metadados de telefonia podem (...) revelar uma quantidade extraordinária de informações sobre nossos hábitos e conexões. Padrões de chamadas podem revelar quando estamos acordados e dormindo; nossa religião, caso alguém não costume usar o telefone no dia do sabá ou faça um grande número de ligações no dia de Natal; nossos hábitos profissionais e nossas aptidões sociais; quantos amigos nós temos, e até mesmo nossas afiliações civis e políticas". Em suma, escreve Felten, "a coleta em massa não apenas possibilita ao governo obter informações sobre mais pessoas como também lhe permite conhecer fatos novos e anteriormente privados que a simples coleta de informações sobre alguns indivíduos específicos não teria permitido". GREENWALD, Glenn. Op. Cit., p. 16-17.

[441] Art. 7º "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;".

[442] Art. 10. "A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. (...)

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros".

[443] Conforme o inciso XII do artigo 5º da Constituição Federal, "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

que a Constituição a exigiu para a única hipótese na qual se admitiu expressamente a quebra, devendo-se exigir com mais razão para as hipóteses que a Constituição sequer permitiu.

Com efeito, os dispositivos supracitados não fornecem fundamento jurídico para a vigilância em massa e irrestrita, ainda que sob o argumento emergencial de combate ao terrorismo ou ao crime organizado, uma vez que a medida inegavelmente atingirá terceiros que nenhuma relação possuem com a empreitada criminosa. Conforme se viu, a própria origem da concepção do direito à privacidade foram as buscas estatais genéricas e infundadas[444].

Logo, diante de todo o argumentado, entendemos que implementar vigilância em massa e irrestrita no Brasil além de violar princípios mais básicos do direito, violaria a Constituição da República, especialmente no que diz respeito à inviolabilidade de suas comunicações e à presunção de inocência. Desta forma, as ações de vigilância apenas poderiam ocorrer em sede de investigação criminal, regularmente instaurada em face de indivíduos sobre os quais houvesse razoável suspeita e ainda assim deveria se ponderar, sob a ótica da proporcionalidade, se no caso concreto o interesse da vigilância prevalece sobre a privacidade dos investigados.

Por fim, há que ressaltar que, em que pese esteja o direito fundamental à privacidade embora tradicionalmente relacionado a uma abstenção estatal[445], defende-se neste trabalho que há também um dever estatal de prestação jurídica[446], ou seja, cabe ao Estado criar a estrutura jurídica necessária à proteção da privacidade, especialmente em um contexto de vigilância estatal, transacional, assim como realizado por entes privados.

2.4.1 Vigilância estatal e sistema de crédito social chinês

[444] Embora não seja original, em variados cenários renasce a ideia de mandados de busca e apreensão genérico, que em geral facilitam enormemente o trabalho das forças policiais, mas por outro lado expõem a privacidade de um número indiscriminado de cidadãos que não se relacionam com a atividade criminosa, estimulando muito frequentemente um tratamento enviesado e discriminatório, direcionado aos destinatários de medida, muito embora devessem contar com a presunção de inocência. Veja-se: REDAÇÃO. Jungmann diz que mandado coletivo de busca e apreensão pode ser medida extra. **Isto É**, fev. 2018.Disponível em: <https://istoe.com.br/jungmann-diz-que-mandado-coletivo-de-busca-e-apreensao-pode-ser-medida-extra/>. Acesso em: 20 fev. 2018.

[445] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2008, p. 256.

[446] Sobre os direitos fundamentais de natureza prestacionais, em especial em relação à prestação jurídica, vide Ibidem, p. 257-258.

Está fora de dúvida que os programas de vigilância estatal têm alta propensão para se converterem em modelos totalitários, caso não tenham seus contornos pré-definidos em uma legislação democrática. Embora sempre se justifiquem as ações de inteligência e mesmo a vigilância em massa em virtude da ameaça de um inimigo externo, seja o terrorismo ou outro qualquer, fato é que a consciência da existência da vigilância estatal tem a consequência de domesticar corpos e mentes.

Com efeito, quem sabe que é vigiado não desempenha seus atos com a necessária liberdade pois tende a se conformar de acordo com os ditames da maioria. Mesmo estando em um local público, caso o indivíduo saiba que está sendo monitorado seja por áudios ou câmeras tenderá a adotar comportamentos autocensurados ou se inibirá[447], inclinando-se a se comportar como entende que desejam que o façam[448]. Nesta situação, perde-se o caráter instrumental da privacidade que consiste em resguardar um espaço intangível do indivíduo no qual ele possa desenvolver a própria personalidade.

A situação narrada está prestes a ocorrer na China, que visa implantar um projeto de crédito social. Segundo o projeto, todos os chineses serão classificados de acordo com a pontuação que o sistema lhe atribuir, tendo-se em conta as atitudes, o relacionamento interpessoal, o histórico de compras, o conteúdo das redes sociais, probabilidade de adimplemento de obrigações, entre vários outros, que servirão para pontuar.

De acordo com as informações coletadas, alguém poderá ser classificado como ocioso ou preguiçoso – e receber uma pontuação negativa - por adquirir um aparelho de videogame PlayStation ou um Xbox, ou mesmo poderá ser classificado como perdulário por concentrar gastos em bens supérfluos. Ocorre que possuir pontuações muito baixas fará o pontuado integrar listas negras que o impedirão de ter acesso a crédito, a comprar passagens aéreas, a alugar ou comprar imóveis, a se hospedar em hotéis de luxo ou até mesmo a matricular filhos em escolas particulares[449].

Com efeito, o sistema de crédito social chinês contará com auxílio substancial do *big data*, vez que a análise e o processamento das informações que comporão o rankeamento de indivíduos são dados captados na internet. Em que pese a grande dependência do *big data*, o

---

[447] SOLOVE, Daniel J. **Nothing to Hide**: The false tradeoff between privacy and security. New Haven & London: Yale University Press, 2011, p. 178.

[448] COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as a Object. **Stanford Law Review**, v. 52, p. 1373-1426, mai. 2000.

[449] HODGE, Mark. Real Black Mirror. **The Sun**, mar. 2018. Disponível em: <https://www.thesun.co.uk/news/5730910/china-social-credit-rating-blacklists-citizens/>. Acesso em: 10 mar. 2018.

sistema de crédito social produz por consequência um estado ideal da vigilância, haja vista que se poderá acompanhar cada passo do indivíduo e conformar suas atitudes de acordo com aquilo que o Estado entende como bom.

Para a cultura chinesa, a noção chinesa de crédito - ou *xinyong* - tem um significado que se relaciona com ideias morais de honestidade e confiança. Atualmente, existem até 30 projetos pilotos locais de crédito social, em grandes cidades como Xangai. Ao mesmo tempo, ao menos oito empresas privadas testam em conjunto diferentes de sistemas de pontuação de indivíduos. O projeto piloto de maior abrangência é o sistema *Sesame Credit*, de propriedade da Ant Financial, que se baseia em um algoritmo secreto para classificar seus usuários, pontuando-os entre 360 e 950 pontos[450]. Entre as facilidades disponíveis aos bem pontuados está a possibilidade de alugar veículos sem realizar depósito em garantia ou mesmo conseguir prioridade para a retirada de um visto europeu. Por outro lado, possuir amigos de baixa pontuação reduz a pontuação do próprio usuário.

As maiores preocupações em relação ao projeto é o fato de que o sistema de crédito social ainda piloto passará a ser obrigatório em 2020 e será gerido por duas empresas privadas que administram redes sociais, o que preocupa quanto à gestão e coleta destes dados que estarão em poder de entidades privadas. Ademais, qualquer usuário poderá verificar a pontuação de outra pessoa[451].

Não menos preocupante é o fato de que a manifestação de opiniões políticas, incluindo a manifestação de seus contatos poderá reduzir a pontuação do indivíduo, assim como a pouca visita aos pais idosos que moram distante e a infração à lei de trânsito reduzem mais ainda a pontuação do indivíduo. Não podemos ser inocentes a ponto de não cogitar que a pontuação negativa será sempre atribuída às opiniões de quem se opuser ao fechado regime chinês. Embora o caso não se trate de censura pura e simples, implicará em um esfriamento de qualquer debate ou discussão a respeito, o que é extremamente prejudicial à liberdade de expressão[452].

---

[450] HARRIS, John. The tyranny of algorithms is part of our lives: soon they could rate everything we do. **The Guardian**, mar. 2018. Disponível em: <https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data>. Acesso em: 10 mar. 2018.

[451] GOMES, Rodrigo Dias de Pinho Gomes. **Big data**: desafios à tutela da pessoa humana na sociedade da informação. Dissertação (Mestrado em Direito) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017, p. 47.

[452] Trata-se do que a doutrina estadunidense chama de *chilling effect*. Vide: SCHAUER, Frederick. Fear, Risk and the First Amendment: Unraveling the Chilling Effect. **Faculty Publications**, Paper 879, 1978.

Um dos objetivos da vigilância sempre foi conformar a conduta das pessoas ou para marginalizar os que se recusam a se adequaram. A categorização e estereotipia de indivíduos servem tão somente para definir como excluídos os indesejáveis, criando para estes um sistema de distribuição de desvantagens cumulativas[453].

Tal sistema será necessariamente excludente, na medida em que o acesso aos bens e serviços de modo facilitados ocorrerão apenas aos bens pontuados. O fato de ser pontuado em virtude da pontuação da própria rede de relacionamentos estimulará uma sociedade excludente e preconceituosa, na medida em que uma opinião ou atitude fora dos padrões esperados de umamigo influenciará a pontuação do usuário. Portanto, o sistema tornará cada vez mais difícil a vida de quem possui pontuação baixa, afetando negativamente sua esfera jurídica ou obrigando-se a atuar em conformidade com o desejado pelo Estado.

Em que pese o espanto que a iniciativa do perverso uso do *big data* possa causar, o rankeamento de pessoas para limitar-lhe oportunidades não é um privilégio do país oriental. Conforme já se viu aqui, a análise preditiva utiliza dados pretéritos de outros usuários[454] para limitar oportunidades, de modo alguém pode deixar de conseguir um empréstimo caso esteja se divorciando pode deixar de conseguir um emprego pela probabilidade de abandoná-lo com base no cálculo estatístico de terceiros[455].

Portanto, o sistema de crédito social chinês, embora afirme estar imbuído nobre objetivos de fortalecer a confiança das relações interpessoais, na prática significa montar um vasto laboratóriode vigilância, abrangendo um banco de dados de 1,3 bilhões de pessoas, no qual o *big data* encontra o *big brother* [456].

A sutileza do programa de vigilância para domesticar corpos e mentes é justamente a sua não sanção expressa, mas o estabelecimento de sanções premiais para quem se comporta de acordo com os princípios morais do regime, privilegiando os bem pontuados com acesso a bens e serviços e limitando a liberdade de contratar e circular daqueles que insistirem em não se adequar.

---

[453] BAUMAN, Zygmunt. Op. cit., p. 14.

[454] A rede social Facebook adquiriu patente de um produto no qual o crédito do usuário apenas é processado se os contatos daquele usuário possuírem a pontuação mínima exigida. EPSTEIN, Adam. Facebook's new patent lets lenders reject a loan based on your friends' credit scores—but don't freak out. **Quartz**, ago. 2015. Disponível em: <https://qz.com/472751/facebooks-new-patent-lets-lenders-reject-a-loan-based-on-your-friends-credit-scores-but-dont-freak-out/>. Acesso em: 10 jan. 2018.

[455] GIBBINS, Nicholas. How what's on your credit report can affect job applications. **Experian**, jan. 2015. Disponível em: <http://www.experian.co.uk/blogs/consumer-advice/credit-report-affect-job-application/>. Acesso em: 10 jan. 2018.

[456] CLOVER, Charles. China: When big data meets big brother. **Financial Times**, jan. 2016. Disponível em: <https://www.ft.com/content/b5b13a5e-b847-11e5-b151-8e15c9a029fb>. Acesso em: 18 mar. 2018.

O sistema proposto pelo governo chinês ofende direitos fundamentais básicos. Além de violar a privacidade dos usuários que terão sua pontuação exposta a todos e fatos inerentes à própria vida vasculhado por companhias privadas, mantar à disposição da vigilância estatal a possibilidade de perseguir dissidentes e prejudicar oponentes, sufocando opiniões.

Ademais, a iniciativa viola elementos constitutivos da dignidade humana. Viola a autonomia privada, pois sua capacidade de autodeterminação estará comprometida pela necessidade de alcançar uma boa pontuação; ademais, violará a autonomia pública do indivíduo, na medida em que suas opiniões políticas serão cerceadas ou lhe custarão uma vida mais difícil que a outros indivíduos de opinião diversa.

Mas o ponto mais relevante da violação à dignidade humana é ao elemento valor intrínseco, que deriva do imperativo categórico kantiano - segundo o qual o homem é um fim em si mesmo e não um meio para a realização de metas coletivas ou projetos sociais de outros; o outro postulado que decorre do valor intrínseco, é o de ordem antiautoritária assenta-se na ideia de que o Estado existe para o indivíduo e não o contrário[457]. Desta forma, o caráter utilitarista que permeia o sistema de crédito, ou seja, de servir a determinado critério de boa vida determinado por padrões morais de outrem, estimularia um perfeccionismo moral descabido.

Os perigos trazidos pela implementação de tal sistema servem de alerta aos países ocidentais e democráticos dos riscos de utilização do big data sem que se observem parâmetros éticos. Se o destino do indivíduo for integralmente traçado por algoritmos, combase em sua pontuação[458], teremos toda uma geração submetida à ditadura dos algoritmos[459].

2.5 **Dados como mercadoria: do uso do *big data* pelos agentes econômicos e a aplicação horizontal dos direitos fundamentais**

[457] BARROSO, Luís Roberto. A dignidade da pessoa humana... Op. cit., p. 307-313.

[458] HARRIS, John. The tyranny of algorithms is part of our lives: soon they could rate everything we do. **The Guardian**, mar. 2018. Disponível em: https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data>. Acesso em: 10 jan. 2018: "Credit scores already control our finances. With personal data being increasingly trawled, our politics and our friendships will be next". Em tradução livre: "A tirania dos algoritmos faz parte de nossas vidas: logo eles podem avaliar tudo o que fazemos. As pontuações de crédito já controlam nossas finanças. Com os dados pessoais cada vez mais tragados, nossa política e nossas amizades serão as próximas".

[459] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. **Big Data**…, Op. cit., cap. 8.

Consoante visto nos tópicos anteriores, programas de vigilância estatal despertam preocupação principalmente pelo efeito repressor que podem causar. Todavia, a prática do vigilantismo não é um privilégio de entidades estatais. A vigilância privada é uma realidade cada vez mais evidente, motivada pelos mais variados interesses econômicos, sejam eles a comercialização dos dados coletados, a agregação de valor dos sistemas de análise de mercado ou mesmo a expansão da fatia de mercado, com vistas à alcançar com maior precisão o público alvo de determinado serviço ou produto.

Na vigilância privada há certamente um interesse mercadológico, econômico. Todavia, esta vigilância não se dá de forma estanque. A vigilância privada somente acontece em parceria com as entidades governamentais. Simbioticamente, vigilâncias pública e privada se integram e se retroalimentam. Para corporações privadas é interessante que entidades governamentais sejam mais lenientes com a legislação sobre processamento e compartilhamento de dados pessoais. Por outro lado, é extremamente útil a governos uma postura mais colaborativa e menos rigorosa das entidades privadas, no que tange ao fornecimento de informações sobre usuários que possui em seus servidores[460]. Conforme visto anteriormente, o monitoramento massivo realizado pela NSA americana ocorreu com a colaboração das gigantes da internet e da telefonia.

Contudo, no caso da vigilância privada, há um fator adicional que não necessariamente aparece na vigilância estatal: a voluntariedade no fornecimento das informações. São os usuários que inserem seus dados voluntariamente nas plataformas sociais. É claro que se pode discutir o grau de voluntariedade, quando os termos de uso dos aplicativos são de adesão obrigatória para se conectar a determinada rede social, que exigem informações cada vez mais amplas e completas sobre o usuário[461].

Não se ignora que a inserção voluntária dos dados nas plataformas decorre de uma necessidade de integração social. Diferente de outras eras nas quais a invisibilidade e o anonimato eram garantias de preservação da privacidade, atualmente o compartilhamento passa a ser uma obrigação social.

---

[460] SCHNEIER, Bruce. The Public-Private Surveillance Partnership. **Bloomberg**, jul. 2013. Disponível em: <https://www.bloomberg.com/view/articles/2013-07-31/the-public-private-surveillance-partnership>. Acesso em: 10 jan. 2018.

[461] Segundo o Facebook, os critérios de sugestão de amizade seriam os seguintes: amigos em comum; participação no mesmo grupo do Facebook ou marcação na mesma foto; a rede do usuário (por exemplo, sua escola, universidade ou trabalho) e contatos carregados no aparelho. DE ONDE VÊM as sugestões de Pessoas que você talvez conheça? **Facebook**, [s.d.]. Disponível: <https://pt-br.facebook.com/help/163810437015615?helpref=faq_content>. Acesso em: 10 jan. 2018.

Com efeito, é possível arriscar que o temor da sociedade contemporânea não seja as consequências de exposição social, sem que se tenha preservado um espaço de sigilo, mas o contrário, o mal temido seja o esquecimento social, a irrelevância nas redes. Desta forma, o antídoto para a exclusão e o esquecimento passa a ser a exposição, a nudez social. No contexto da sociedade confessional[462] - na qual os confessionários são aparelhos portáteis que compartilham vídeos em tempo real, localização, opiniões, hábitos de consumo, entre outros – a palavra de ordem é a nudez social, destinando-se o objeto da confissão a um sem número de pessoas.

A dificuldade que emerge desse contexto é como conscientizar massas dos riscos à privacidade, se ainda estão impressionadas com as maravilhas da conectividade das mídias sociais e a exposição pública, onde cada pessoa comum se torna uma celebridade de si mesmo, testando a cada postagem a sua popularidade. Neste sentido, poderes públicos e organizações da sociedade civil têm a árdua missão de cobrar transparência destas plataformas acerca do uso que é feito com os dados dos usuários.

A vigilância privada não é apenas um formato de negócio na internet. Lamentavelmente é o modelo de negócios que triunfou e consolidou as grandes empresas do ramo. Deve-se conscientizar que as inúmeras funcionalidades, tais como aplicativos de deslocamento, motores de busca, servidores de e-mail, redes sociais profissionais, de fotos,possuem seus custos. Desta forma, se essas funcionalidades que inegavelmente facilitam a vida contemporânea são disponibilizadas aparentemente gratuitamente é porque o usuário é a própria mercadoria[463], ou melhor, o seu funcionamento apenas é garantido em virtude dos dados de consumo, localização, informações financeiras, contatos pessoais e profissionais dos próprios usuários. Significa dizer que a gratuidade dos serviços de internet nada mais são do que decorrente do lucro que as empresas de internet possuem a partir da diferença entre a receita obtida com a comercialização e processamento de dados de usuários e os custos de manutenção das funcionalidades[464].

---

[462] BAUMAN, Zygmunt. Op. cit., p. 14.

[463] SOLON, Olivia. You are Facebook's product, not customer. **Wired**, set. 2011. Disponível em: <http://www.wired.co.uk/article/doug-rushkoff-hello-etsy>. Acesso em: 18 fev. 2018.

[464] Nesse estudo, há análise do efeito comportamental diante da oferta de serviços ditos gratuitos ou a custo zero, o que tende a aumentar a adesão a esses serviços. Vide: SHAMPAN'ER, Kristina; ARIELY, Dan. Zero as a special price: The true value of free products. **MIT**, [s.d]. Disponível em: <http://web.mit.edu/ariely/www/MIT/Papers/zero.pdf>. Acesso em: 10 jan. 2018.

Não é por outra razão que a receita do Google ultrapassou a marca histórica dos 100 bilhões no último ano[465]. Neste ponto, se não há um custo da mercadoria, ou seja, se os serviços do Google são supostamente gratuitos[466] aos usuários, isso ocorre porque a mercadoria é o próprio usuário, ou melhor, seus dados. Com efeito, as vultosas verbas de publicidade auferidas pelo Google e outros gigantes da internet decorrem do fato de que seus usuários, além de consumidores, também são a mercadoria[467].

Para exemplificar o fenômeno, no ano de 2018 foi tornado público o maior escândalo de compartilhamento de dados de usuários do Facebook, que fez o valor de mercado da empresa recuar em 50 bilhões de dólares[468]. Em resumo, o escândalo se deu porque um aplicativo de teste de personalidade veiculado naquela rede social tinha acesso aos dados dos usuários que participavam daquele teste, supostamente com autorização do usuário. Ocorre que o aplicativo também acessava informações do perfil dos amigos dos 270 mil usuários que fizeram o teste, o que potencializou a coleta de dados para cinquenta milhões de usuários do Facebook. De posse das características e afinidades de milhões de usuários, a empresa GSR, proprietária do aplicativo, vendeu os dados dos milhões de usuários para a empresa Cambridge Analytica, a qual, de posse de dados tais como localização, curtidas, entre outros dados, realizou a análise psicológica destes usuários para fins de propaganda eleitoral[469].

Com base no perfil psicométrico dos usuários, a Cambridge Analytica potencializou suas campanhas políticas, havendo afirmações de que sua atuação tenha sido essencial à eleição presidencial de Donald Trump e para o êxito eleitoral do movimento conhecido como Brexit, que decidiu pela separação do Reino Unido da União Europeia[470]. O episódio revela uma grave situação de violação de dados pessoais dos usuários do Facebook que, se não conta

---

[465] AGÊNCIA O GLOBO. Google, Amazon e Apple Batem Recorde de Receitas e Lucros. **Pequenas Empresas & Grandes Negócios**, fev. 2018. Disponível em: <https://revistapegn.globo.com/Tecnologia/noticia/2018/02/google-amazon-e-apple-batem-recorde.html>. Acesso em: 10 mar. 2018.

[466] FITZPATRICK, Jason. If You're Not Paying for It; You're the Product. **LifeHacker**, nov. 2010. Disponível em: <https://lifehacker.com/5697167/if-youre-not-paying-for-it-youre-the-product>. Acesso em: 18 dez. 2017.

[467] SOLON, Olivia. Op. cit.

[468] G1. Em dois dias, Facebook perde quase US$ 50 bilhões em valor de mercado. **G1**, mar. 2018. Disponível em: <https://g1.globo.com/economia/noticia/em-dois-dias-facebook-perde-quase-us-50-bilhoes-em-valor-de-mercado.ghtml>. Acesso em: 20 mar. 2018

[469] O GLOBO COM AGÊNCIAS INTERNACIONAIS. Entenda o caso do escândalo de dados no Facebook e saiba como proteger sua privacidade. **O Globo**, mar. 2018. Disponível em: <https://oglobo.globo.com/economia/entenda-caso-do-escandalo-de-dados-no-facebook-saiba-como-proteger-sua-privacidade-22511997>. Acesso em: 22 mar. 2018.

[470]BRIGATTO, Gustavo. Após Trump e Brexit, Cambridge Analytica vai operar no Brasil. **Valor Econômico**, mar. 2017. Disponível em: <http://www.valor.com.br/empresas/4896618/apos-trump-e-brexit-cambridge-analytica-vai-operar-no-brasil>. Acesso em: 20 dez. 2017.

com a omissão deliberada do aplicativo, há no mínimo uma ausência de cautela quanto ao uso de dados pessoais por terceiros, o que pode implicar em duras sanções diante dos compromissos assumidos diante da Comissão Federal de Comércio do Estados Unidos[471].

A primeira violação que se pode notar é a ausência de consentimento ou consentimento viciado do usuário, vez que não se consentiu com o tratamento dos dados pessoais do usuário para fins de propaganda política e manipulação eleitoral[472]. Em segundo lugar, não houve consentimento informado para acesso aos dados dos amigos dos usuários, tampouco para a sua retirada do Facebook e fornecimento a terceiros para utilização em análises políticas. Por fim, a terceira e mais grave é a demonstração de absoluta falta de controle por parte do aplicativo Facebook da coleta e compartilhamento de dados dos usuários[473], permitindo, ainda que por omissão, que os dados coletados fossem livremente negociados, para as finalidades mais variadas, transformando o usuário em verdadeiro produto, objetificando suas preferências e mercantilizando sua dignidade.

Desta forma, o modelo privado de negócios na internet em alguma medida sempre envolve utilização de dados dos usuários. Tal modelo de negócios envolve o monitoramento dos usuários do serviço, prática que ficou conhecida como *stalker economy*[474], ou seja, é a economia baseada no rastreamento, monitoramento e utilização dos dados dos usuários.

O modelo de negócios baseado na *stalker economy* encontra-se em franca ascensão, o que significa dizer que a tendência das empresas do ramo, em coletar mais dados e dos mais variados tipos, tende a aumentar exponencialmente, exorbitando os seus lucros. Em virtude da resistência a técnicas tradicionais de rastreamento como o uso de *cookies* e de *spams*, a sofisticação da economia da internet passará por outros métodos que aparentam ser menos invasivos, mas nem por isso deixam de monitorar o usuário. Exemplo disso é o novo projeto do Google que procura um modelo alternativo[475] de *stalker economy* ao substituir os

---

[471] REDAÇÃO. Entenda as questões legais envolvendo o escândalo de dados do Facebook. **Folha de São Paulo**, mar. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/escandalo-de-dados-do-facebook-as-questoes-legais.shtml>. Acesso em: 22 mar. 2018.

[472] EDITORIAL. Facebook em novo caso de manipulação eleitoral. **O Globo**, mar. 2018. Disponível em: <https://oglobo.globo.com/opiniao/facebook-em-novo-caso-de-manipulacao-eleitoral-22513403>. Acesso em: 22 mar. 2018.

[473] REDAÇÃO. Coleta de dados de usuário era rotina, diz ex-funcionário do Facebook a jornal. **Folha de São Paulo**, mar. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/coleta-de-dados-de-usuario-era-rotina-diz-ex-funcionario-do-facebook-a-jornal.shtml>. Acesso em: 22 mar. 2018.

[474] SCHNEIER, Bruce. 'Stalker economy' here to stay. **CNN**, nov. 2013. Disponível em: <https://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html>. Acesso em: 22 mar. 2018.

[475] BARR, Alistair. Google may ditch 'cookies' as online ad tracker. **USA Today**, set. 2013. Disponível em: <https://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/#>. Acesso em: 22 mar. 2018.

tradicionais *tracking cookies* pela utilização de perfis pessoais, ou seja, nome de usuário e fotos, como meio de propaganda de determinado produto, sem que o titular do perfil consinta ou saiba da prática. Se um usuário avaliar algum produto ou serviço de forma positiva, seus contatos poderão ver anúncios daquele produto ou serviço com o nome e a foto do usuário. Da mesma forma, o Facebook tem cada vez mais ampliado o número de informações que de acordo com a configuração padrão do aplicativo é acessível a terceiros que não integram os contatos do usuário[476].

Fato é que a expansão da economia de rastreamento do usuário que alimenta a vigilância privada pode ter danos muito maiores que os já causados pela vigilância estatal, apresentadas por Edward Snowden[477]. Os escândalos dos atos praticados pela NSA podem ser potencializados se realizados por gigantes da internet por duas razões. Uma delas é que a vigilância estatal encontra limites no poder político de determinado Estado. Logo, a vigilância estatal apenas será facilitada no território sobre o qual determinado estado possui poder político ou com a colaboração de um parceiro estratégico que facilitará a expansão destes tentáculos.

Por outro lado, no caso de corporações privadas, a sua natureza global lhes permite ignorar limites geopolíticos, haja vista sua maciça presença em vários países, com usuários de diferentes nações que lhes permitem serem escrutinados diariamente. A possível resistência a esse avanço do monitoramento agressivo são os próprios concorrentes de mercado. Todavia, a inegável tendência de concentração de poder na mão dos barões dos dados, faz com este seja um mercado cada vez mais concentrado nas grandes companhias e cada vez mais resistentes a novos concorrentes. Portanto, mesmo em um contexto concorrencial, todas as empresas envolvidas se beneficiam de algum modo da *stalker economy*, de modo que é impossível imaginar que apresentem alguma resistência a qualquer postura mais invasiva.

A segunda provável resistência são os poderes políticos locais. Aqui é preciso lembrar a advertência de Bauman acerca da desintegração entre poder e política. Com a globalização a política se encontra cada vez mais circunscrita aos limites territoriais do estado, com

---

[476] Os termos de uso padrão do Facebook tem sido ao longo dos anos alterado para cada vez mais avançar sobre o tipo de informação que é pública por padrão. Vide relevante estudo que explicita o aumento do número de informações de perfil que são púbicas por configuração padrão, considerando-se o ciclo de amigos, contatos de amigos, todos os usuários ou mesmo pessoas externas ao aplicativo: THE EVOLUTION OF Privacy on Facebook. **Mattmckeon**, [s.d.]. Disponível em: <http://mattmckeon.com/facebook-privacy/>. Acesso em: 22 mar. 2018.

[477] TATE, Ryan. AMID NSA Outrage, Big Tech Companies Plan To Track You Even More Aggressively. **Wired**, nov. 2013. Disponível em: <https://www.wired.com/2013/10/private-tracking-arms-race/>. Acesso em: 22 mar. 2018.

dificuldades de solucionar problemas de natureza global; por outro lado, o poder econômico é cada vez mais globalizado, ignorando as fronteiras geopolíticas dos estados, até porque a maioria das sedes destas companhias estão localizadas nos Estados Unidos, de modo que essas empresas se recusam a cumprir normas de outros países.

Portanto, para empresas cujo modelo de negócios envolve a publicidade na internet, não se pode perder de vista o fato de que a *stalker economy* é vital à própria sobrevivência do modelo.

2.6***Big Data*, vigilância privadae a proporcionalidade como vedação à proteção insuficiente**

O constitucionalismo possui sua gênese na limitação do poder Estado em favor da liberdade individual. Foi a superação do estado absolutista que culminou com a submissão do Estado à lei e marcou o advento da modernidade. Portanto, o constitucionalismo moderno se assenta em três ideias fundantes, a saber, a contenção do poder dos governantes, por meio da separação de poderes; a garantia dos direitos individuais, concebidos como direitos negativos oponíveis ao Estado; e a necessidade de legitimação do governo através da do exercício da democracia representativa[478].

É fora de dúvida que a relação entre o usuário e o provedor de aplicação é de natureza privada. Em geral, para utilização dos serviços de determinado provedor, o usuário concorda com os termos de uso, em especial com as políticas de privacidade, em uma relação jurídico-contratual privada, celebrada entre dois particulares.

É de se ressaltar que a teoria da eficácia direta e imediata dos direitos fundamentais nas relações privadas foi primeiro defendida na Alemanha por Hans Carl Nipperdey, para quem, embora alguns direitos fundamentais previstos na Constituição alemã vinculassem apenas o Estado, há outros que por sua natureza poderiam ser invocados diretamente nas relações privadas, independentemente de intermediação legislativa, possuindo tais direitos oponibilidade *erga omnes*[479]. Segundo o autor, determinados perigos que ameaçam direitos fundamentais no mundo contemporâneo não possuem sua fonte apenas na atuação estatal, mas também nos poderes sociais e de terceiros em geral.

---

[478] SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. **Direito constitucional**: teoria, história e métodos de trabalho. Belo Horizonte: Forum, 2013, p. 70.

[479] SARMENTO, Daniel. A vinculação dos particulares aos direitos fundamentais: o debate teórico e a jurisprudência do STF. In: _____; SARLET, Ingo Wolfgang (Orgs.). **Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica. Rio de Janeiro: Lumen Juris, 2011, p. 142.

Deste modo, a existência do Estado Social – em razão dos deveres prestacionais que este encerra, para além do dever de abstenção - imporia o reconhecimento desta realidade que teria como consequência a extensão dos direitos fundamentais às relações particulares. Posteriormente, a teoria foi desenvolvida por Walter Leisner que defendeu a ideia de que a unidade da ordem jurídica não permitiria a concepção do direito privado como espaço impermeável à aplicação dos direitos fundamentais, como se fosse um gueto à margem da Constituição[480].

A tese, com a qual concordamos integralmente, foi inicialmente defendida na década de 50. Certamente que as instituições sociais e terceiros que representavam riscos aos direitos fundamentais foram substituídos por outros atores. Todavia, pouca dúvida resta de que as grandes corporações globais que dominam o mercado da internet possuem este risco potencial.

O Supremo Tribunal Federal caminha em sua jurisprudência para consolidar a teoria. Um dos exemplos mais citados no qual se faz uma análise teórica clara sobre a incidência dos direitos fundamentais nas relações privadas, admitindo sua aplicação direta, ou seja,independentemente de intermediação legislativa é o Recurso Extraordinário nº201819. O julgado tratava da exclusão de um sócio dos quadros da UBC – União Brasileira dos Músicos, sem que se tenha observado a ampla defesa e o contraditório. A princípio, como qualquer associação privada, observados os requisitos legais para o estabelecimento de normas associativas, a associação apenas possui por obrigação observar o próprio estatuto. Todavia, entendeu o Supremo neste julgado que a autonomia privada não pode ignorar os direitos fundamentais dos associados, vez que não confere aos particulares, no domínio de sua incidência e atuação, o poder de transgredir ou de ignorar as restrições postas e definidas pela própria Constituição, cuja eficácia e força normativa também se impõem, aos particulares, no âmbito de suas relações privadas[481]. Entendeu-se ainda que a referida associação, por possuir

---

[480] Ibidem.

[481] BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 201819*. Relatora Min. Ellen Gracie. p/ Acórdão Min. Gilmar Mendes. Segunda Turma. Julg. 11 out. 2005. ***DJ*** 27 out. 2006: "SOCIEDADE CIVIL SEM FINS LUCRATIVOS. UNIÃO BRASILEIRA DE COMPOSITORES. EXCLUSÃO DE SÓCIO SEM GARANTIA DA AMPLA DEFESA E DO CONTRADITÓRIO. EFICÁCIA DOS DIREITOS FUNDAMENTAIS NAS RELAÇÕES PRIVADAS. RECURSO DESPROVIDO. I. EFICÁCIA DOS DIREITOS FUNDAMENTAIS NAS RELAÇÕES PRIVADAS. As violações a direitos fundamentais não ocorrem somente no âmbito das relações entre o cidadão e o Estado, mas igualmente nas relações travadas entre pessoas físicas e jurídicas de direito privado. Assim, os direitos fundamentais assegurados pela Constituição vinculam diretamente não apenas os poderes públicos, estando direcionados também à proteção dos particulares em face dos poderes privados. II. OS PRINCÍPIOS CONSTITUCIONAIS COMO LIMITES À AUTONOMIA PRIVADA DAS ASSOCIAÇÕES. A ordem jurídico-constitucional brasileira não conferiu a qualquer associação civil a possibilidade de agir à revelia dos princípios inscritos nas leis e, em especial, dos postulados que têm por

a posição privilegiada para determinar a extensão do gozo e fruição dos direitos autorais de seus associados, já que a associação integrava a estrutura do ECAD, a sua atuação teria natureza pública, ainda que não estatal, pois a associação aos seus quadros era imprescindível ao exercício profissional dos associados. Por estas duas razões, entendeu a Suprema Corte que haveria no caso incidência direta de direitos fundamentais concernentes ao contraditório, à ampla defesa e ao devido processo legal. Sendo assim, embora a regra seja a mais ampla liberdade de associação, inclusive a de definir critérios de ingresso e exclusão, há direitos fundamentais básicos que devem ser observadas nas relações travadas entre os associados.

Antes mesmo da Constituição de 1988, há outros julgados relevantes a respeito do tema. O primeiro deles é o Recurso Extraordinário n. 85.439[482], de relatoria do Ministro Xavier de Albuquerque, julgado em 11/11/1977. Embora não se tenha invocado a eficácia horizontal dos direitos fundamentais, na prática, inadmitiu-se a utilização de gravação clandestina feita pelo marido de conversas telefônicas da mulher para provar o adultério em caso de divórcio. Em que pese ter havido a invocação de dispositivos de ordem

---

fundamento direto o próprio texto da Constituição da República, notadamente em tema de proteção às liberdades e garantias fundamentais. O espaço de autonomia privada garantido pela Constituição às associações não está imune à incidência dos princípios constitucionais que asseguram o respeito aos direitos fundamentais de seus associados. A autonomia privada, que encontra claras limitações de ordem jurídica, não pode ser exercida em detrimento ou com desrespeito aos direitos e garantias de terceiros, especialmente aqueles positivados em sede constitucional, pois a autonomia da vontade não confere aos particulares, no domínio de sua incidência e atuação, o poder de transgredir ou de ignorar as restrições postas e definidas pela própria Constituição, cuja eficácia e força normativa também se impõem, aos particulares, no âmbito de suas relações privadas, em tema de liberdades fundamentais. III. SOCIEDADE CIVIL SEM FINS LUCRATIVOS. ENTIDADE QUE INTEGRA ESPAÇO PÚBLICO, AINDA QUE NÃO-ESTATAL. ATIVIDADE DE CARÁTER PÚBLICO. EXCLUSÃO DE SÓCIO SEM GARANTIA DO DEVIDO PROCESSO LEGAL.APLICAÇÃO DIRETA DOS DIREITOS FUNDAMENTAIS À AMPLA DEFESA E AO CONTRADITÓRIO. As associações privadas que exercem função predominante em determinado âmbito econômico e/ou social, mantendo seus associados em relações de dependência econômica e/ou social, integram o que se pode denominar de espaço público, ainda que não-estatal. A União Brasileira de Compositores - UBC, sociedade civil sem fins lucrativos, integra a estrutura do ECAD e, portanto, assume posição privilegiada para determinar a extensão do gozo e fruição dos direitos autorais de seus associados. A exclusão de sócio do quadro social da UBC, sem qualquer garantia de ampla defesa, do contraditório, ou do devido processo constitucional, onera consideravelmente o recorrido, o qual fica impossibilitado de perceber os direitos autorais relativos à execução de suas obras. A vedação das garantias constitucionais do devido processo legal acaba por restringir a própria liberdade de exercício profissional do sócio. O caráter público da atividade exercida pela sociedade e a dependência do vínculo associativo para o exercício profissional de seus sócios legitimam, no caso concreto, a aplicação direta dos direitos fundamentais concernentes ao devido processo legal, ao contraditório e à ampla defesa (art. 5º, LIV e LV, CF/88). IV. RECURSO EXTRAORDINÁRIO DESPROVIDO".

[482]BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 85439*. Relator Min. Xavier de Albuquerque. Segunda Turma. Julg. 11 nov. 1997. ***DJ*** 02 dez. 1997: "PROVA CIVIL. GRAVAÇÃO MAGNETICA, FEITA CLANDESTINAMENTE PELO MARIDO, DE LIGAÇÕES TELEFONICAS DA MULHER. INADMISSIBILIDADE DE SUA UTILIZAÇÃO EM PROCESSO JUDICIAL, POR NÃO SER MEIO LEGAL NEM MORALMENTE LEGITIMO (ART. 332 CPC). RECURSO EXTRAORDINÁRIO CONHECIDO E PROVIDO".

infraconstitucional no acórdão (art. 332 do Código de Processo Civil de 1973[483]), o parecer da Procuradoria Geral da República invocou os artigos 153, parágrafos 9º e 10º da Constituição de 1967/69 que previam a garantia de inviolabilidade das comunicações telefônicas e do domicílio, vez que o cônjuge que realizou a gravação o fez penetrando na residência sem o seu consentimento.

Da mesma forma, no Recurso Extraordinário n. 100.094/PR[484], de relatoria do Ministro Rafael Mayer, julgado em 28 jun. 1984, abordou-se a questão da invalidade de prova realizada mediante gravação telefônica não consentida, afirmando-se expressamente que a sua admissão violaria o artigo 153, parágrafo 9º, da Constituição 1967, pois tanto os agentes públicos quanto particulares estariam vinculados aos direitos da personalidade[485].

Diante do exposto, é de se concluir que o Supremo Tribunal Federal, mesmo antes da ordem constitucional vigente, vem consolidando sua jurisprudência no sentido da eficácia dos direitos fundamentais nas relações privadas. Embora haja variações teóricas quanto ao tipo de eficácia horizontal dos direitos fundamentais - se direta ou indireta - há robustos argumentos para que se sustente a eficácia direta, diante das peculiaridades da sociedade brasileira, bem como da aspiração por igualdade que permeia a Constituição de 1988.

É certo que a aplicação direta e imediata de direitos fundamentais às relações privadas sempre terá em conta a necessária ponderação com a autonomia privada, da qual decorre a liberdade de celebrar negócios jurídicos e definir seu objeto. Por óbvio que aplicar direitos fundamentais às relações entre particulares não poderá servir como instrumento a aniquilar a autonomia do indivíduo, tampouco ignorar as normas de direito privado atinentes ao caso, até porque a Constituição garante o direito de propriedade[486] e possui como fundamento da

---

[483] Art. 332. "Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa".

[484] BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº100094*. Rel. Min. Rafael Mayer. Primeira Turma. Julg. 28 jun. 1984. ***DJ*** 24 ago. 1984:"DIREITO AO RECATO OU À INTIMIDADE. GARANTIA CONSTITUCIONAL. INTERCEPTAÇÃO DE COMUNICAÇÃO TELEFÔNICA. CAPTAÇÃO ILEGITIMA DE MEIO DE PROVA. ART-153, § 9º DA CONSTITUIÇÃO. ART-332 DO CÓDIGO DE PROCESSO CIVIL. INFRINGENTE DA GARANTIA CONSTITUCIONAL DO DIREITO DA PERSONALIDADE E MORALMENTE ILEGITIMO É O PROCESSO DE CAPTAÇÃO DE PROVA, MEDIANTE A INTERCEPTAÇÃO DE TELEFONEMA, À REVELIA DO COMUNICANTE, SENDO, PORTANTO, INADMISSIVEL VENHA A SER DIVULGADA EM AUDIÊNCIA DE PROCESSO JUDICIAL, DE QUE SEQUER É PARTE. LESIVO A DIREITO INDIVIDUAL, CABE O MANDADO DE SEGURANÇA PARA DETERMINAR O TRANCAMENTO DA PROVA E O DESENTRANHAMENTO, DOS AUTOS, DA GRAVAÇÃO RESPECTIVA. RECURSO EXTRAORDINÁRIO CONHECIDO E PROVIDO".

[485] Destaca-se do voto do relator o seguinte trecho: “sendo irrelevante indagar se o ilícito foi cometido por agente público ou particulares, porque, em ambos os casos, a prova terá sido obtida com infringência aos princípios constitucionais que garantem os direitos da personalidade”.

[486] Art. 5º. "(...) XXII - é garantido o direito de propriedade;".

República o valor social da livre iniciativa[487]. Ademais, a autonomia privada é elemento da dignidade humana, valor fundante da ordem constitucional democrática.

Portanto, não há dúvida da possibilidade da eficácia direta dos direitos fundamentais nas relações privada. Embora a tese não tenha encontrado adeptos no direito germânico, berço onde foi concebida, sua aplicação encontrou campo fértil no direito comparado, possuindo previsão expressa no texto constitucional de Portugal[488] e África do Sul[489].

Ora, no caso brasileiro, há especiais razões para se defender a eficácia direta e horizontal dos direitos fundamentais. A bem da verdade a Constituição não é compatível com a tese de total inaplicabilidade dos direitos fundamentais às relações privadas, adotada nos Estados Unidos. Isto porque a nossa Constituição consagra um modelo de Estado Social, que persegue a igualdade substantiva ao estabelecer como objetivo fundamental da república brasileira construir uma sociedade livre, justa e solidária (Art. 3º, I da CRFB). Tampouco há compatibilidade com a teoria que prevalece na Alemanha, que adota a eficácia horizontal indireta e mediata dos direitos fundamentais, dependendo para sua incidência da intermediação do legislador ordinário ou a sua aplicação pelo Judiciário, tão somente enquanto vetor interpretativo das cláusulas gerais de direito privado. Além de contar com extenso catálogo de direitos sociais, há inúmeras normas de direitos fundamentais destinadas a agentes privados, tais como os direitos trabalhistas (art. 7º). Em suma, o sistema de direitos fundamentais da Constituição brasileira possui uma ênfase muito maior na sociabilidade, de modo que as constituições alemã e estadunidense não são comparáveis à brasileira neste quesito[490].

Outra razão que justifica a aplicação das normas de direito fundamental às relações privadas é que a própria autonomia privada pressupõe certa paridade na relação. Ressalte-se que as políticas de privacidade das aplicações de internet mais populares em geral não trazem

---

[487] Art. 1º "A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) IV - os valores sociais do trabalho e da livre iniciativa;".

[488] Constituição da República Portuguesa, Artigo 18.º Força jurídica 1. "Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas".

[489]Constituição da República da África do Sul, 1996, "8 Application. (1) The Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state. (2) A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right".Em tradução livre: "8 Aplicação. (1) A Declaração de Direitos aplica-se a toda o direito, e vincula a legislatura, o executivo, a judiciário e todos os órgãos do estado. (2) Uma disposição da Declaração de Direitos vincula uma pessoa natural ou jurídica, no que for aplicável, tendo em conta a natureza do direito e a natureza de qualquer dever imposto pelo direito".

[490] Para verificar estes e outros contundentes argumentos para eficácia direta dos direitos fundamentais no Brasil, vide: SARMENTO, Daniel. Op. cit., p. 158-164.

a opção de modifica-las, ou seja, o acesso a determinada aplicação ou serviço é condicionada à concordância ou não há o acesso à aplicação, assemelhando-se a um verdadeiro contrato de adesão, cujas cláusulas são integralmente definidas pelo proprietário da aplicação.

Soma-se a esta assimetria da autonomia, o fato de a sociedade brasileira ser profundamente desigual e isso se reflete na internet, um ambiente bastante elitizado[491]. Portanto, o acesso à internet pelas pessoas de baixa escolaridade e/ou renda tende a se intensificar[492], na medida em que se populariza o acesso a telefones celulares com acesso à internet[493], aprofundando ainda mais a assimetria informacional.

O acesso à internet é mais um reflexo da desigualdade socioeconômica na sociedade brasileira, onde o acesso a bem e serviços se concentram nos grupos de melhor escolaridade e renda. Isso justificaria a aplicação horizontal de direitos fundamentais, especialmente quando há relação de assimetria. Nas palavras de Daniel Sarmento:

> Não bastasse, existe um dado fático relevante, que não pode ser menosprezado: a sociedade brasileira é muito mais injusta e assimétrica do que a da Alemanha, dos Estados Unidos ou que qualquer outro país do Primeiro Mundo. (...)
>
> Ademais, só existe efetivamente autonomia privada quando o agente desfrutar de mínimas condições materiais de liberdade. Isso não acontece em grande parte dos casos de aplicaça dos direitos humanos nas relações entre particulares, nas quais a manifesta desigualdade entre as partes obsta, de fato, o exercício da autonomia. Pensar a autonomia de fato, nu sentido pleno, é considerar também os constrangimentos que lhe são impostos por agentes não estatais, no contexto de uma sociedade profundamente assimétrica e excludente.[494]

---

[491] "A minoria dos internautas estudou até o ensino fundamental (20%), mesmo sendo maioria no país (45%); 29% dos internautas concluíram o ensinou superior (na população total, somam 17%)". Um em cada dez internautas pertencem às classes D/E e um em cada cinco internautas cursou apenas até o ensino fundamental. G1. Mulheres são maioria entre usuáios de internet no Brasil, diz pesquisa. **G1**, fev. 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/02/mulheres-sao-maioria-entre-usuarios-de-internet-no-brasil-diz-pesquisa.html>. Acesso em: 20 dez. 2017.

[492]No grupo dos sem instrução ou que estudaram até quatro anos, a percentagem de internautas subiu de 2,5% para 11% até a pesquisa de 2013. PNAD: número de internautas cresce 143,8% em seis anos. JORNAL DO BRASIL. PNAD: número de internautas cresce 143,8% em seis anos, **Jornal do Brasil**, mai. 2013. Disponível em: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2013/05/16/pnad-numero-de-internautas-cresce-1438-em-seis-anos/>. Acesso em: 10 jan. 2018.

[493] CAMPOS, Ana Cristina. IBGE: celular se consolida como o principal meio de acesso à internet no Brasil. **EBC Agência Brasil**, dez. 2016. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2016-12/ibge-celular-se-consolida-como-o-principal-meio-de-acesso-internet-no-brasil>. Acesso em: 18 dez. 2017: "A pesquisadora do IBGE diz que o fato de o acesso à internet móvel ser mais barato do que a internet fixa é uma das razões de o celular predominar no Norte do país. Outro motivo é a infraestrutura. 'A Região Norte tem uma dificuldade maior em passar cabo, o que poderia aumentar essa proporção de acesso à banda larga fixa', destaca Helena.".

[494] SARMENTO, Daniel. Op. cit., p. 160-161

Logo, não resta dúvidas de que há fundados argumentos a favor da eficácia horizontal direta dos direitos fundamentais. Todavia, embora o direito privado não mais seja um gueto infenso à incidência de normas de direito público, não se pode perder de vista que vige nesta seara do direito a autonomia da vontade, de modo que a eficácia das normas constitucionais deve observar as normas de direito privado em vigor, apenas as afastando em caso de inconstitucionalidade. Na ausência de direito infraconstitucional aplicável, deverá o aplicador da lei sempre ponderar a norma constitucional de incidência direta com o princípio da autonomia privada, utilizando como critério de ponderação o princípio da proporcionalidade[495].

Por outro lado, a par de a eficácia direta dos direitos fundamentais nas relações privadas ter por destinatário o particular, impondo-o que se abstenha da violação do direito fundamental de outrem, ainda que em relação de natureza privada, não pode o Estado se isentar do seu múnus de efetivação de direitos fundamentais nas relações privadas.

Com efeito, além da eficácia direta dos direitos fundamentais nas relações privadas, outra hipótese para proteção da privacidade nas relações entre particulares é a proporcionalidade como vedação à proteção insuficiente. A ideia é defendida por quem advoga a eficácia apenas indireta dos direitos fundamentais nas relações privadas, vinculando primeiramente o poder público – legislador e judiciário – e apenas remotamente o particular em virtude da criação de leis ou de interpretações de cláusulas abertas pelo Judiciário[496].

Conforme exposto acima, nos filiamos à teoria da eficácia horizontal direta dos direitos fundamentais. Todavia, a proporcionalidade como vedação à proteção insuficiente pode trazer valorosas contribuições para a proteção à privacidade nas relações privadas.

Tradicionalmente, o princípio da proporcionalidade foi apresentado pela doutrina como instrumento de controle das ações estatais, a fim de verificar se o ato estatal continha excessos que restringiam, de forma injustificável e, portanto, inconstitucional, os direitos fundamentais. Destarte, a proporcionalidade como vedação do excesso apresentou-se como

---

[495] Para Luís Roberto Barroso, a ponderação consiste em "técnica de decisão jurídica, aplicável aos casos difíceis, em relação aos quais a subsunção se mostrou insuficiente", ocorrendo em três etapas, a saber, "identificação das normas pertinentes, seleção dos fatos relevantes e atribuição geral de pesos, com a produção de uma conclusão". Em suma, a ponderação "socorre-se do princípio da razoabilidade-proporcionalidade para promover a máxima concordância prática entre os direitos em conflito". BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**. São Paulo: Saraiva, 2009, p. 333.

[496] A relação entre a proporcionalidade como vedação à proteção insuficiente ou a existência de deveres de proteção e sua relação com a eficácia indireta dos direitos fundamentais tem como maior defensor Claus-Wilhem Canaris. Vide o estudo CANARIS, Claus-Wilhem. A influência dos direitos fundamentais sobre o Direito Privado na Alemanha. In: SARLET, Ingo Wolfgang (Org). **Constituição, Direitos Fundamentais e Direito Privado**. Rio de Janeiro: Livraria do Advogado, 2003, p. 223-244 *apud* SARMENTO, Daniel. Op. cit.

valioso instrumento de ponderação das ações estatais, com vistas a evitar interferências desarrazoadas em direitos fundamentais, através da aplicação do critério da proporcionalidade, por meio de seus três subprincípios (adequação, necessidade e proporcionalidade em sentido estrito)[497].

Uma outra abordagem do princípio da proporcionalidade que pode contribuir com a eficácia horizontal dos direitos fundamentais é a proporcionalidade enquanto vedação à proteção insuficiente. Significa dizer que a proporcionalidade não serve tão somente para controlar as intervenções estatais, controlando seu excesso, mas também avaliar a legitimidade das omissões estatais, funcionando como um termômetro para definir em que medida deve se exigir do Estado atuar para proteger direitos fundamentais, e, neste caso, inclusive em relações privadas[498].

Com efeito, há um caráter dúplice nas funções desempenhadas pelos direitos fundamentais, que são designadas como defensiva e protetiva. Na função defensiva, o Estado é guiado pela "proibição de intervenção", ou seja, suas intervenções devem abster-se de violar direitos fundamentais e as restrições devem ser pautadas pela proporcionalidade. Na função protetiva, há o "imperativo de tutela" ou "imperativo de proteção"[499] . O caráter dúplice da proporcionalidade impõe que o estado não atue com excesso que viole direito fundamental (função negativa, vedação do excesso), mas que também não deixe de atuar positivamente para proteger o direito fundamental (função positiva, vedação da insuficiência).

Nesta perspectiva, a proporcionalidade como vedação à proteção insuficiente deriva da noção de que das normas de direitos fundamentais derivam inúmeros "deveres de proteção[500]" dos poderes públicos. Tais deveres podem assumir variados perfis, podendo-se exemplificar a obrigação do Estado em impor sanções penais e civis na situação em que há violação de direitos por terceiros e o dever de tutelar direitos sociais[501].

---

[497] PEREIRA, Jane Reis Gonçalves. Os imperativos da proporcionalidade e da Razoabilidade: Um panorama da discussão atual e da jurisprudência do STF. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Orgs.).**Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica. Rio de Janeiro: Lumen Juris, 2011, p. 167-206.

[498] Ibidem, p. 198.

[499] Os termos proibição de intervenção e imperativo de tutela relacionados, respectivamente às funções defensiva e protetiva de direitos fundamentais são citadas por Daniel Sarmento, apresentando a teoria de Claus-Wilhem Canaris. SARMENTO, Daniel. Op. cit., p. 145.

[500] GRIMM, Dieter. A função protetiva do Estado. In SARENTO, Daniel; SOUZA NETO, Cláudio Pereira de (Orgs.). **A Constitucionalização do Direito**. Fundamentos teóricos e aplicações específicas. Rio de Janeiro: Lumen Juirs, 2007 *apud* PEREIRA, Jane Reis Gonçalves. Op. cit., p. 198.

[501] PEREIRA, Jane Reis Gonçalves. Op. cit., p. 198.

Não cabe aqui se aprofundar sobre as origens e aplicações dos deveres de proteção, por não ser objeto do presente trabalho, bastando-se apontar um julgado exemplificativo do Supremo Tribunal Federal que admitiu a tese, tendo ela sido aplicada no Recurso Extraordinário no qual se discutia a extinção da punibilidade em crime de estupro contra menor, em virtude de o agressor haver constituído união estável com a vítima. Em voto vista do Ministro Gilmar Mendes, entendeu-se que a proporcionalidade como vedação à proteção insuficiente impediria ao Estado deixar de punir condutas com alto grau de reprovabilidade[502].

Com efeito, a compreensão da proporcionalidade como vedação à proteção insuficiente possui grande potencial para proteger o direito fundamental à privacidade dos internautas, haja vista que atualmente a vida necessariamente é eletronicamente intermediada para grande parte da população e as aplicações mais populares da web são geridas por grandes e poderosas corporações globais, cujos termos de uso apenas possibilitam as opções de ingresso e retirada e não a alteração da política de privacidade.

Neste sentido, do direito fundamental à privacidade, previsto no texto constitucional, não emergem apenas os deveres de abstenção de não violar a intimidade e vida privada ou de observar os parâmetros legais para interceptação telefônica, para ficar em alguns exemplos. Há um dever de agência estatal, vez que a inação será tanto ou mais violadora que a abstenção. Diante de grandes grupos econômicos com poder global de influência, há inescusável dever de proteção à privacidade dos usuários por parte do poder público, vez que este não é movido por interesses mercadológicos.

Uma das formas de observância desses deveres de proteção é a edição de legislações que protejam a privacidade dos usuários na internet. Ora, a pouco escolaridade média dos brasileiros, a assimetria informacional, além das desigualdades socioeconômicas históricas da sociedade brasileira impõem ao Estado uma atuação protetiva do direito fundamental à privacidade, no cumprimento dos deveres de proteção.

Nesse sentido é louvável que haja no Marco Civil da Internet normas que tratem da privacidade dos usuários, enquanto condição de pleno exercício de acesso à internet, bem como prevejam a nulidade de cláusulas contratuais que ofendam a inviolabilidade de comunicações[503] ou mesmo a previsão de sanções no artigo 12 da referida lei para condutas

---

[502] BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 418376*. Relator Ministro Marco Aurélio. Relator p/ Acórdão Min. Joaquim Barbosa. Tribunal Pleno. Julg. 09 fev. 2006. ***DJ*** 23 mar. 2007.

[503] Art. 8º "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que: I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou II - em contrato de adesão, não ofereçam como alternativa ao

que não observem osdireitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Todavia, isso não se mostra suficiente, os deveres de proteção impõem uma atuação mais efetiva na tutela dos direitos à privacidade nas redes. A previsão genérica do dever de observar a privacidade e da necessária obtenção de ordem judicial é importante, mas outros avanços são necessários. Desta forma, impõe-se a criação de uma lei específica para tratar de dados pessoais, as hipóteses de compartilhamento, a criação de um órgão regulador, entre outros. Nesta linha, mostra-se imprescindível o prosseguimento dos projetos de lei que tratam do marco normativo dos dados pessoais na internet ou fora dela.

Por outro lado, o dever de atuação proativa dos poderes públicos no cumprimento dos deveres de proteção, na tutela dos direitos fundamentais, não exime o particular da condição de destinatário do cumprimento de direitos fundamentais em suas relações de cunho privada. Portanto, a tese da aplicação direta de direitos fundamentais nas relações privadas não é incompatível com o cumprimento dos deveres de proteção do Estado.

A ideia de que apenas o Estado é potencial violador de direitos fundamentais é ultrapassada ou ao menos conta apenas uma parte da história. O Estado deve abster-se de violar direitos fundamentais, assim como deve protegê-los em face de sua violação por parte de agentes privados. A verdade é que nos dias atuais há atores privados com poder social superiores aos entes estatais, de capacidade de influência muito maior, o que impõem ao Esado deverem de proteção dos direitos fundamentais em face destes agentes.

Em síntese conclusiva, a eficácia horizontal dos direitos fundamentais impõe a sua aplicação direta nas relações privadas, bem como cabe ao Estado proteger direitos fundamentais em face de potenciais violações por parte destes agentes. São, portanto, concepções complementares, em sintonia com os tempos atuais, nos quais as corporações privadas representam perigo tão grande ou maior aos direitos fundamentais que aquele representado pelo Estado[504]. Por óbvio que tais concepções não podem perder de vista a necessária ponderação com a autonomia privada, elemento integrante da dignidade humana.

2.7*Big data* e dados pessoais: o atual estágio da proteção de dados pessoais na Europa, nos Estados Unidos e no Brasil

2.7.1 Aspectos gerais, conceito e classificação jurídica da proteção de dados pessoais

---

contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil".

[504] Esta é a posição de Daniel Sarmento. Vide SARMENTO, Daniel. Op. cit., p. 145.

Embora o tema deste trabalho seja o direito fundamental à privacidade diante das novas tecnologias de informação e comunicação, entendemos que a abordagem do fenômeno *big data* necessariamente passa pela compreensão do panorama da proteção à privacidade dos dados pessoais. É de se ressaltar que os dados pessoais não são o objeto central deste trabalho[505], cabendo neste tópico apenas a abordagem geral do tema, em virtude de sua íntima relação com o direito fundamental à privacidade.

A relação entre a proteção de dados pessoais e o *big data* é evidente, na medida em que o processamento volumoso e maciço de dados necessariamente envolve também o processamento de dados pessoais. Não significa dizer que todo dado processado pelo *big data* seja necessariamente dado pessoal. Apenas para ficar em um exemplo, sensores meteorológicos, de propulsores de energia eólica ou de uma refinaria de petróleo, a princípio,não estarão coletando dados pessoais.

Ocorre que, com o advento da internet das coisas (ou *internet of things* - IoT)[506], o número de sensores será multiplicado e dados que aparentemente não eram pessoais, ou melhor, identificáveis, após o processamento, passam a sê-lo. Logo, será cada vez mais fácil rastrear dados, fazendo o caminho inverso até sua origem para identificar o seu titular, revelando detalhes da vida do indivíduo que não seria identificável caso não fosse o *big data*[507]

A tutela de dados pessoais não é algo que mereça apenas preocupação recente. Na verdade, regimes autoritários ou não sempre se preocuparam com o controle de informações sobre seus cidadãos e estrangeiros. O que se mostra como fenômeno recente é a capacidade extraordinária de coleta e processamento de dados trazidas pela big data, em razão do volume, velocidade e variedade inigualáveis. Isso faz com que o *big data* não apenas aumente os riscos à privacidade, como também transformem o tipo de risco[508].

---

[505] Para obras de referência acerca do tratamento específico dos dados pessoais, vide: CERVASIO, Daniel Bucar. **Proteção de Dados da Pessoa Humana na Administração Pública**. 2008. Dissertação (Mestrado em Direito Civil) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2008.

[506] Vide explicação do termo no item 2.2.2.

[507] Viktor Mayer-Schonberer traz como exemplo os medidores das companhias de energia elétrica. Se antes estes dispositivos apenas media o consumo, os medidores inteligentes podem criar uma identidade elétrica para cada equipamento e definir, de acordo com o consumo, quais equipamentos são ligados ou desligados ao longo do dia. Desta forma, o mesmo dispositivo que permite identificar o número de chuveiros elétricos e lâmpadas pode expor a condição de saúde dos moradores ou mesmo o desempenho de atividades ilegais. MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. **Big Data**:… Op. cit., p. 152.

[508] Ibidem, p. 153.

Este fenômeno é potencializado pela vida digitalmente mediada[509], na qual cada vez mais a vida no ambiente cibernético substitui funções mais comezinhas da vida fora das redes. Mais preocupante ainda é o fato de que tais dados que eram coletados a partir tão somente de computadores, agora podem ser coletados de variados dispositivos inteligentes como TVs, smartphones, veículos, eletrodomésticos em geral, não havendo limites ao número de sensores para coleta e armazenamento de dados.

Conforme se viu no escândalo que revelou a vigilância estatal em massa nos Estados Unidos, a franca expansão da coleta e processamento de dados na era do *big data* não foi acompanhada pela necessária segurança destes dados diante da vigilância estatal e privada, de modo que quanto mais dados se coletam, menos haverá lugar para se esconder. Pode-se afirmar, portanto, que a intensidade dos impactos do *big data* sobre a privacidade se relacionam diretamente ao grau de proteção que é dado aos dados pessoais.

Inicialmente, cumpre perquirir a definição do que seja dado pessoal. Antes, porém, necessário se faz diferenciar dado e informação. Dado e informação dizem respeito ao mesmo campo semântico, mas não se confundem. O dado possui um caráter muito mais primitivo e fragmentado, representa a pré-informação. Por outro lado, a informação é o resultado do processamento do dado, ou seja, é o dado processado, com fins de constituir informação útil[510]. Em geral, o que é coletado diretamente do indivíduo pode ser definido como dado e o resultado do agrupamento, análise, correlação pode ser definido como informação. Todavia, convencionou-se designar o dado processado ou não de dado apenas, por ser um termo mais abrangente e de fácil compreensão.

Nessa perspectiva, desde a década de 1960, com o avanço das tecnologias de informação e comunicação, inicia-se um fluxo cada vez maior de informações dos indivíduos sendo coletadas e processadas pelos estes computadores. Disto, implementam-se iniciativas preocupadas com privacidade dos titulares destes dados.

A principal preocupação é quando dados deixam de se referir a fatos gerais e são subjetivizados, ou seja, dizem respeito a uma pessoa determinada ou determinável. Neste sentido, avulta a preocupação com a definição e proteção do que seja informação pessoal, ou seja, quando o objeto da informação é a própria pessoa. Embora o conceito de dado pessoal possa assumir variados enfoques no que tange ao seu conteúdo, a definição mais corrente de

---

[509] "Mas na Coreia do Sul, por exemplo, onde, no cotidiano, a maior parte da vida social já é eletronicamente mediada (ou melhor, onde a vida social já se transformou em vida eletrônica ou cibervida, e onde se leva a maior parte da "vida social" na companhia de um computador"BAUMAN, Zygmunt. Op. cit., p. 24.

[510] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 152.

dado pessoal é constante da Convenção Europeia nº 108 de 1981 define dado pessoal como qualquer informação relativa a uma pessoa singular identificada ou identificável[511].

O Projeto de Lei nº 5276 de 2016 adota o mesmo conceito amplo de dado pessoal, segundo o qual "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa" (art. 5º, I). Nos termos do projeto, dado pessoal é todo aquele que permita identificar uma pessoa determinada ou determinável. Significa dizer, portanto, que mesmo um dado anônimo pode ser considerado dado pessoal caso este processo de anonimização possa ser revertido. O próprio projeto de lei exemplifica dado pessoal como dados locacionais ou identificadores eletrônicos relacionados a uma pessoa. Portanto, os dados coletados pelos inúmeros sensores do *big data*, seja um aparelho de smartphone, seja um aplicativo de rotas de trânsito, deveriam observar a legislação de proteção de dados pessoais.

O conceito amplo é contestado, principalmente por empresas cujo modelo de negócios envolve o tratamento dados. Defende-se uma abordagem mais restrita que diga respeito apenas aos dados da pessoa natural que possam ser razoavelmente identificáveis, excluindo-se a previsão "quando estiverem relacionados a uma pessoa". Os defensores da tese não definem um critério do que seja a razoabilidade na possibilidade de identificação[512].

Para além dos dados pessoais, há outra categoria específica de dados cuja proteção justifica-se pela possibilidade de, a partir de seu conhecimento se utilizar práticas discriminatórias ou potencialmente mais lesivas aos direitos fundamentais que os dados pessoais em geral. Trata-se dos dados sensíveis. Não há consenso sobre a abrangência e conteúdo do que seja dado sensível que seja isento de críticas[513], partindo-se a sua conceituação da observação empírica e, assim como a privacidade, o conceito de dado sensível é contingencial, ou seja, variável temporal e espacialmente, de modo que a informação que é sensível em determinada sociedade e quadra histórica.

---

[511]Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, Art. 2º: "Para os fins da presente Convenção: a) «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados»);".

[512]Para este grupo, defende-se um conceito mais enxuto de definição de dados pessoais inspirado no conceito canadense que apenas protege os dados sobre uma pessoa natural. Segundo este argumento, a inclusão dos dados relacionados à pessoa incluiria toda e qualquer atividade humana, o que inviabilizaria o fluxo de dados necessário à vida cotidiana e, sem dúvida, ao seu modelo de negócios. Esse é o conceito apontado pela Google Brasil. ANTONIALLI, Dennys et al. O que são dados pessoais? **InternetLab**, jul. 2016. Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-o-que-sao-dados-pessoais/>. Acesso em: 10 jan. 2018.

[513] DONEDA, Danilo. Op. cit., p. 162.

Isso não isenta qualquer abordagem de proteção de dados pessoais da definição do que seja dado sensível, podendo-se definir como dado sensível informações relativas à origem social e étnica, à informação genética, aos dados biométricos, a informações de saúde, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular[514]. Todas essas informações, dentro do amplo leque de dados pessoais podem constituir justificativa para a limitação de oportunidades ou o tratamento discriminatório de indivíduos, de modo que sua publicização apenas poderá ocorrer com o consentimento e na exata extensão desejada pelo titular.

O fato de a Carta de Direitos Fundamentais da Europa tratar em tópicos apartados a privacidade doméstica e familiar e a privacidade de dados pessoais exibe a clara diferença entre o tratamento da concepção tradicional de privacidade e a privacidade na era eletrônica. Isso decorre também da relativa polêmica que existe acerca da natureza da proteção dos dados pessoais.

Para alguns a proteção de dados pessoais trata de direito distinto do direito à privacidade, argumento que se justificaria pelo seu tratamento em dispositivo distinto nos documentos internacionais. Defende-se ainda que, por possuir uma dinâmica própria decorrente do fluxoinformacional de dados, haveria uma necessidade de se desprender das amarras conceituais do direito à privacidade para contar com um tratamento jurídico diferenciado[515].

Em que pesem serem as premissas verdadeiras, ousamos discordar com a sua conclusão. É certo que pela compreensão da especificidade da proteção de dados, documentos internacionais e pátrios tenham optado por um tratamento específico, em virtude da necessidade de consentimento, de observância do princípio da finalidade, dos prazos para a manutenção dos dados e fluxo de dados armazenados, entre outros. Tudo isso não desafirma o fato de que todos os direitos decorrentes da proteção a dados não decorram do direito fundamental à privacidade, embora sob uma roupagem específica.

Já se abordouneste trabalho a posição de Mayer-Schonberer e Kenneh Cukier para quem a privacidade não apenas enfrenta um aumento dos seus desafios diante do *big data*, mas também uma modificação qualitativa destes desafios. Significa dizer que, se na vida de

---

[514] Esta lista exemplificativa aglutina a definição de dados sensíveis constantes dos Projetos de Lei nº 5276/2016 e 4060/2012, ambos em trâmite na Câmara dos Deputados. Por opção, exclui-se especificamente a informação quanto à atuação e filiação sindical, a uma por se entender que tal informação pode estar incluído nas convicções políticas, a duas porque tal atuação, embora possa ser enquadrada no conceito de dados pessoais, não parece ser necessariamente uma informação sensível, na medida que se trata de atuação de caráter relativamente público.

[515] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 153.

outrora importava à proteger comunicações telefônicas e sigilo de correspondência de serem interceptadas, como inicialmente importara a proteção da inviolabilidade do domicílio em face de busca sem mandados, atualmente, diante dos meios tecnológicos disponíveis, novos desafios são impostos à proteção da privacidade. Isso porque é possível saber detalhes íntimos da vida do indivíduo que sequer seus familiares mais íntimos saibam, sem necessariamente ingressar em seu espaço físico, bastando controlar o seu fluxo dos dados e comunicações, a sua localização, as preferências de compra, leitura e temas. Em outras palavras, o que se está resguardando é o mesmo direito fundamental à privacidade diante das possíveis violações que as novas tecnologias de informação e comunicação impõem. O fato de haver a necessidade de um tratamento jurídico próprio, com princípios e regramentos específicos não trasmuda a natureza do direito, apenas especializa a sua tutela em determinados casos. Exemplo prático que corrobora a tese é o fato de a Constituição brasileira, nos incisos X a XII do art. 5º, prever variadas manifestações do direito à privacidade e não variados direitos distintos.

Não se pode ignorar que a inflação de direitos fundamentais apenas dificulta a sua proteção e tratamento adequado, diluindo sua importância e relevância, diante do argumento falacioso de que há muitos direitos a proteger. Por esta razão, em que pese as transformações e variadas manifestações do direito a privacidade, este trabalho defende que a proteção aos dados pessoais é tão somente um dos desdobramentos da privacidade e não um novo direito[516]. Essa é inclusive a principal razão da dificuldade em se estabelecer um conceito único de direito à privacidade.

2.7.2 Diferenças entre o tratamento de dados pessoais nos Estados Unidos e na Europa: o histórico de *Safe Harbor* a *Privacy Shield*

No primeiro capítulo deste trabalho, realizou-se um debate acerca das culturas de privacidade estadunidense e europeia, comparando-se semelhanças e apontando-se diferenças. Faz-se essencial neste momento a diferenciação entre os dois modelos de tratamento de dados, a fim de se verificar se de fato há entre os modelos um denominador comum.

O cenário europeu, muito em razão dos horrores do nazismo e de outros regimes totalitários, possui uma histórica desconfiança do Estado em relação à proteção da privacidade dos indivíduos e de seus dados pessoais, o que gerou uma demanda maior por um controle

[516] Nesse sentido, GOMES, Rodrigo Dias de Pinho Gomes. Op. cit., p. 56.

rigoroso da privacidade de dados[517]. A partir da década de 1960, vários países do bloco passaram a editar legislações para proteger a privacidade em face do avanço tecnológico. Na chamada leis de primeira geração de proteção de dados[518], havia um tratamento essencialmente individualista, garantindo o acesso isolado e individual ao próprio cadastro nos bancos de dados de caráter público[519]. Pode-se citar como exemplo desta fase a Constituição Portuguesa de 1979[520] que estabelece regras para o controle de dados pessoais informatizados. A própria previsão do *habeas data* na Constituição brasileira de 1988 é reflexo desta concepção.

No bloco europeu, a previsão de proteção aos dados pessoais foi prevista na Convenção Europeia nº 108 de 1981, que trata da proteção das pessoas relativamente ao tratamento automatizado dos dados.Posteriormente, em 24 out. 1995, o Parlamento Europeu editou a Diretiva nº 95/46/CE[521], detalhada no tópico 1.3.1, a qual prevê que os sistemas de tratamento de dados devem respeitar as liberdades e os direitos fundamentais do homem. Prevê ainda o dever de os estados membros estabelecerem a previsão do direito à reparação pelo responsável de qualquer um que tenha sofrido dano em razão do tratamento ilícito de

---

[517] WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. **Congressional Research Service**, mai. 2016, p. 2. Disponível em: <https://fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 18 dez. 2018.

[518] As gerações das legislações de proteção de dados pessoais foram melhor desenvolvidas em BIONI, Bruno. **Autodeterminação informacional**: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2016, p. 128.

[519] CERVASIO, Daniel Bucar. Op. cit., p. 194.

[520] Constituição da República Portuguesa. Artigo 35.º "Utilização da informática. 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei".

[521]Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em:<http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>. Acesso em: 10 jan. 2018.

dados, bem como exige a necessidade de consentimento inequívoco para que haja tratamento de dados[522].

Em 2002, o Parlamento Europeu editou a Diretiva nº 2002/58/CE[523] que versa exclusivamente sobre dados pessoais e proteção da privacidade em comunicações eletrônicas. Na justificativa do projeto, a diretiva prevê em seu item 6 que a "internet está a derrubar as tradicionais estruturas do mercado(...). Os serviços de comunicações electrónicas publicamente disponíveis através da internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais". Entre as previsões da diretiva está a proteção ao sigilo das comunicações, ao tráfego dos dados, à localização do tráfego, proteção contra as chamadas não solicitadas, excepcionando tais proteções no caso de haver consentimento do usuário ou a anonimização dos dados. A diretiva obriga ainda o descarte dos dados após o tempo necessário à contestação da fatura[524].

No mesmo sentido, a Carta de Direitos Fundamentais da União Europeia, conforme visto no tópico 1.3.1, dedica um artigo inteiro tão somente à proteção de dados pessoais e estabelece o consentimento como meio principal para o tratamento leal e específico de dados.

Outro documento relevante é o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados que revogou a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). O referido regulamento encontra-se em vigor desde abril de 2016 e sua aplicabilidade se dará a partir de maio de 2018.

---

[522] Artigo 23º Responsabilidade. 1. "Os Estados-membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido. 2. O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável".

[523]Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT>. Acesso em: 18 dez. 2018.

[524] Artigo 9º. "Dados de localização para além dos dados de tráfego. 1. Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações electrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. Os utilizadores ou assinantes devem dispor da possibilidade de retirar em qualquer momento o seu consentimento para o tratamento dos dados de localização, para além dos dados de tráfego".

O novo regulamento consagra como direito fundamental a proteção de pessoas singulares no que tange ao tratamento de dados pessoais, com base na previsão da Carta de Direitos Fundamentais da União Europeia[525]. O novo regulamento prevê como meios legítimos ao tratamento de dados pessoais, além do consentimento, outros meios de igual hierarquia[526].

O Regulamento prevê ainda alternativas ao princípio da finalidade, quando não houver consentimento específico para a nova finalidade que se pretende utilizar o dado[527]. Ademais, há no mesmo regulamento tratamento diferenciado e mais protetivo no que tange aos dados pessoais sensíveis, exigindo-se para o seu tratamento o consentimento explícito[528].

---

[525] Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). "Considerando o seguinte: (1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt>. Acesso em: 18 fev. 2018.

[526]Artigo 6.º "Licitude do tratamento 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrônica"

[527] "Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta: a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento; c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º; d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização".

[528]Artigo 9.º "Tratamento de categorias especiais de dados pessoais 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. 2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos: a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas,

Verifica-se, portanto, haver um número significativo de normas europeias a respeito da proteção de dados pessoais, podendo-se dizer que ordenamento jurídico do bloco protege suficientemente os dados pessoais.

Com efeito, a abordagem europeia de proteção de dados costuma optar por normas gerais, aplicáveis a qualquer situação de tratamento de dados, tanto em atos normativos da comunidade europeia, quanto a legislação de cada país membro, inspirada nas normas comunitárias. Na visão estadunidense a abordagem europeia define-se por ser *"one-size-fits-all"*[529], vez que o tratamento de dados pessoais para as diversas áreas de interesse vem regulado em um documento consolidado,seja ele carta de direito fundamental, diretiva, regulamento e até constituições, muito em decorrência da tradição codicista romano-germânica que inspira os ordenamentos da maioria dos países do bloco.

Diferente do modelo europeu, a proteção de dados pessoais nos Estados Unidos não conta com previsão constitucional ou atos normativos gerais. É preciso lembrar que o direito à privacidade na cultura jurídica daquele país se fundamenta na interpretação jurisprudencial que é feita da Quarta Emenda. Conforme se viu no capítulo anterior, a cultura de privacidade norte-americana é muito mais preocupada com os riscos de violação da privacidade criados pelo Estado que pelos agentes privados. Por essa razão, a legislação de privacidade é focada em reparar danos ao consumidor e em equilibrar a privacidade com transações comerciais eficientes, enquanto no continente europeu a proteção de dados é entendida como direito fundamental que pode se sobrepor a outros interesses[530].

Desta forma, nos Estados Unidos, optou-se pela regulamentação setorial da proteção de dados, editando-se um estatuto para cada área, com uma proteção específica para cada setor, seja este o de análise de crédito[531], de sigilo bancário[532], de banco de dados

---

exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados;".

[529] WEISS, Martin A.; ARCHICK, Kristin. Op. cit., p. 2.

[530]SCHWARTZ, Paul M.; SOLOVE, Daniel J. Reconciling Personal Information in the United States and European Union. **California Law Review**, v. 102, n. 4, p. 877, 2014.

[531] Fair Credit Reporting Act de 1970, 15 USC § 1681 et seq. A norma protege as informações coletadas pelas agências de relatórios de consumidores, como agências de crédito, empresas de informações médicas e serviços de triagem de inquilinos. As informações de um relatório do consumidor não podem ser fornecidas a qualquer pessoa que não tenha finalidade especificada na Lei. Disponível em: <https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act>. Acesso: 10 jan. 2018.

[532] Bank Secrecy Act of 1970, Pub. L. nº 91-508.

governamentais[533], de comunicação eletrônica[534], de registros de saúde[535], de proteção à privacidade online de crianças[536], de privacidade dos registros escolares[537], entre outros.

Segundo os críticos das legislações gerais europeias sobre proteção de dados, o modelo estadunidense setorial seria mais eficiente e capaz de apresentar respostas mais rápidas dada a sua flexibilidade, haja vista que há diferentes normas sobre coleta e tratamento de dados para cada setor. Ainda de acordo com os entusiastas do modelo americano, isso permitiria promover e manter a inovação tecnológica promovida pelas grandes corporações da internet cuja sede se localiza nos Estados Unidos.

Por outro lado, críticos do modelo americano, afirmam que a legislação fragmentada constitui verdadeira colcha de retalhos, que deixaria de fora setores importantes como é o caso da coleta de dados de atividades na web. Isso demonstraria a necessidade de edição de uma legislação de proteção de dados mais geral e abrangente[538].

Seja qual for a posição adotada, não se pode negar que de fato a legislação europeia sobre proteção de dados é mais robusta e deixa um número menor de brechas, vez que regulamenta a matéria de modo uniforme para toda quaisquer atividades de coleta e tratamento de dados. A uniformidade do tratamento evita também situações díspares, nas quais os dados estão mais protegidos em determinado setor e em outro não. Dados são dados e independentemente se foram coletados off-line ou online merecem proteção jurídica, especialmente se se referirem a uma pessoa identificável.

Em suma, para a cultura jurídica norte-americana, a coleta e o processamento de dados pessoais é permitida, desde que não cause danos ou seja expressamente proibida pela legislação do Estados Unidos; de modo contrário, no cenário europeu, a presunção se inverte:

---

[533] Privacy Act of 1974, 5 U.S.C. § 522a. Trata-se de norma que estabelece um código de práticas justas de informação que rege a coleta, manutenção, uso e disseminação de informações sobre indivíduos mantidos em sistemas de registros pelas agências federais. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>. Acesso em: 18 mar. 2018.

[534] Electronic Communications Privacy Act ("ECPA") de 1986. A Lei de Privacidade de Comunicações Eletrônicas ("ECPA") foi aprovada em 1986 para expandir e revisar as disposições federais de escuta telefônica e de espionagem eletrônica. Disponível em: <https://epic.org/privacy/ecpa/>. Acesso em: 18 mar. 2018.

[535]Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. A lei exige que a autoridade Departamento de Saúde publique padrões para troca eletrônica, privacidade e segurança de informação de saúde. Coletivamente, estas são conhecidas como disposições de *Simplificação Administrativa*.

[536]Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501-6506 – a lei restringe o tipo de informação os sites podem coletar de crianças de idade inferior a 13 anos, á dando aos pais o controle sobre o que os sites de informações podem coletar de seus filhos. Disponível em: <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy>. Acesso em: 15 fev. 2018.

[537] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1221 note – 1232 g.

[538] WEISS, Martin A.; ARCHICK, Kristin. Op. cit., p. 4.

a coleta e processamento de dados é proibida, a não ser que haja previsão expressa em lei que a permita[539]

Não significa dizer que a proteção estadunidense de dados pessoais seja inferior ao grau de proteção de dados europeu. Conforme visto no capítulo anterior, as leis sobre privacidade tão somente refletem a cultura de determinado país. Portanto, o fato de haver uma proteção de dados mais ou menos rigorosa não a faz superior ou inferior, apenas reflete a consolidação de determinada cultura de privacidade naquele território.

Há intensa troca econômica entre os Estados Unidos e a União Europeia, de modo que, em 2013, os Estados Unidos direcionaram 56% do total de investimentos diretos externos (2,4 trilhão de dólares) e a União Europeia destinou cerca de 62% de seu investimento externo aos Estados Unidos, o que corresponde a 1,7 trilhão de dólares[540]. Reflexo disso é que o fluxo de dados entre Estados Unidos e Europa possui o maior percentual global, superando o dobro do fluxo de dados entre Estados Unidos e América Latina e 50% maior que o fluxo entre Estados Unidos e Ásia[541].

Esse intenso volume de negócios e dados desperta preocupações por parte do bloco europeu inclusive para a negociação de um acordo de livre comércio em curso. Isso porque o sucesso de um acordo de livre comércio envolve necessariamente a possibilidade de livre transferência de dados entre Estados Unidos e União Europeia e o padrão europeu de proteção de dados é mais rigoroso e exigente que o norte-americano. O receio do bloco europeu ocorre em virtude da concepção americana que não entende a proteção de dados como direito fundamental[542].

A primeira tentativa de equalizar um padrão comum de proteção de dados que atendesse aos padrões europeus e permitisse o livre fluxo de dados ocorreu com o Safe Harbor, criado em 2000 e validado pela Comissão Europeia em julho do mesmo ano, que entendeu que o nível de proteção de dados do acordo era adequado à Diretiva Europeia de

---

[539] Ibidem, p. 2.

[540] AKHTAR, Shayerah Ilias; JONES, Vivian C. Proposed Transatlantic Trade and Investment Partnership (T-TIP): In Brief. **Congressional Research Service**, jun. 2014. Disponível em: <https://fas.org/sgp/crs/row/R43158.pdf>. Acesso em: 10 mar. 2018.

[541] MELTZER, Joshua P. The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment. **Global Economy & Development**,working papern. N. 79, p. 1, out. 2014.

[542] WEISS, Martin A.; ARCHICK, Kristin. Op. cit., p. 4.

Proteção de Dados de 1995[543]. O acordo perseguia um nível adequado de proteção de dados, estabelecendo sete princípios básicos[544].

Em que pese o esforço do acordo, ele foi declarado inválido pela Corte de Justiça da União Europeia em outubro de 2015[545], a partir do julgamento do caso C-362/14, proposto por Maximilian Schrems, um ativista austríaco pela privacidade, que visava invalidar a decisão da Comissão Europeia que entendia haver em Safe Harbor um nível adequado de proteção de dados. O argumento do requerente era o fato de o Facebook transferir dados de europeus aos seus servidores situados nos Estados Unidos, especialmente após as revelações de vigilância de Edward Snowden, o que demonstrava um nível insuficiente de proteção[546].

Com efeito, críticos do acordo afirmaram que os esforços pelo cumprimento do acordo por parte dos Estados Unidos em seu território eram poucos, tanto que a Federal Trade Comission (FTC) adotou medidas no sentido de cumprir o acordo apenas em face de dez

---

[543]Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (JO 2000, L 215, p. 7).

[544]Pode-se citar, entre os princípios estabelecidos, o dever de notificar o titular dos dados sobre o propósito da coleta *(notice)*; o dever dar a opção de escolha ao titular do dado *(choice)*; o terceiro que receber os dados deve observar os mesmos princípios do Safe Harbor *(onward transfer)*; organizações que tratam dados pessoais devem tomar medidas de segurança razoáveis *(security)*; deve-se velar pela correção e completude do dado e pelo uso para a finalidade para a qual foi coletada *(data integrity)*; o indivíduo deve ter acesso aos seus dados e ter a possibilidade de corrigi-lo *(acess)*; a proteção efetiva da privacidade deve contar com mecanismos coercitivos eficazes *(enforcement)*.

[545] GIBBS,Samuel. What is 'safe harbour' and why did the EUCJ just declare it invalid? **The Guardian**, out. 2015. Disponível em: <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>. Acesso em: 15 fev. 2018.

[546] UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção), de 6 de outubro de 2015 (pedido de decisão prejudicial da High Court (Irlanda) – Maximilian Schrems / Data Protection Commissioner (Processo C-362/14): "«Reenvio prejudicial – Dados pessoais – Proteção das pessoas singulares relativamente ao tratamento desses dados – Carta dos Direitos Fundamentais da União Europeia – Artigos 7.°, 8.° e 47.° – Diretiva 95/46/CE – Artigos 25.° e 28.° – Transferência de dados pessoais para países terceiros – Decisão 2000/520/CE – Transferência de dados pessoais para os Estados Unidos – Nível de proteção inadequado – Validade – Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos – Poderes das autoridades nacionais de controlo». Recorrente: Maximilian Schrems. Recorrido: Data Protection Commissioner Dispositivo: O artigo 25.°, n.° 6, da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conforme alterada pelo Regulamento (CE) n.° 1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003, lido à luz dos artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), publicados pelo Ministério do Comércio dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.° desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado. A Decisão 2000/520 é inválida".

empresas, ao longo de treze anos de existência do acordo. Ademais, afirma-se que quando as negociações de *Safe Harbor* se iniciaram, ainda na década de 1990, a internet ainda estava em sua fase embrionária e que, havendo mudado radicalmente, não faria sentido uma reanálise do acordo após tanto tempo em virtude de seu anacronismo[547].

A anulação do acordo causou grande pressão por parte das corporações globais de tecnologia que utilizam dados como insumo. Para empresas cujas sedes e centro de dados se situam em território americano, como é o caso do Google, Apple, Microsoft, Facebook, mostrava-se essencial a criação de um acordo substitutivo que permitisse o tráfego de dados entre os continentes, a fim de que não fosse prejudicado seu modelo de negócios.

Em fevereiro de 2016, um grupo de trabalho constituído por autoridades estadunidenses e europeias anunciaram um modelo mais seguro de transferência de dados em relação ao *Safe Harbor* para substituí-lo de nome Privacy Shield. Em 12 de julho de 2016, a Comissão Europeia considerou que a proteção à privacidade proporcionada pelo novo acordo era adequada para permitir transferências de dados ao abrigo da legislação da UE[548]. Em 12 de janeiro de 2017, o governo suíço anunciou a aprovação do Swiss-US Privacy Shield Framework[549] como um mecanismo legal válido para atender aos requisitos suíços ao transferir dados pessoais da Suíça para os Estados Unidos.

Em suma, o acordo *Privacy Shield* cria uma estrutura que permite às empresas situadas nos Estados Unidos cumprir os requisitos de proteção de dados ao transferir dados pessoais da União Europeia e da Suíça aos Estados Unidos em apoio ao comércio transatlântico. O cumprimento do acordo é administrado pela *International Trade Administration (ITA)* no Departamento de Comércio dos EUA[550]. Em síntese, acordo traz disposições que tratam de princípios que já constavam no Safe Harbor, tais como a necessidade de notificação prévia; o

---

[547] WEISS, Martin A.; ARCHICK, Kristin. Op. cit., p. 2.

[548]Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho *[notificada com o número C(2016) 4176]*. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016D1250&from=EN>. Acesso em: 18 mar. 2018.

[549]"Bern, 11.01.2017: At its meeting on 11.01.2017, the Federal Council took note that a new framework has been established for transferring personal data from Switzerland to companies based in the USA. Switzerland will apply the same conditions as the European Union, which set up a comparable system with the USA last summer". Tradução livre: "Bern, 11.01.2017 - Na sua reunião de 11.01.2017, o Conselho Federal tomou nota de que foi estabelecido um novo quadro para a transferência de dados pessoais da Suíça para empresas com sede nos EUA. A Suíça aplicará as mesmas condições que a União Européia, que criou um sistema comparável com os EUA no verão passado". Disponível em:<https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-65210.html>. Acesso em: 18 mar. 2018.

[550]Privacy Shield Program Overview. Disponível em: <https://www.privacyshield.gov/Program-Overview>. Acesso em: 15 fev. 2018.

direito de escolha do titular dos dados; a responsabilidade por transferência a terceiros; a garantia de segurança dos dados; a garantia de integridade dos dados e sua limitação de propósitos, proteções de informações sensíveis, papéis das autoridades de privacidade de dados; dados sobre recursos humanos; dados sobre pesquisas de produtos farmacêuticos ou médicos, entre outros[551].

As principais diferenças entre o *Privacy Shield* e o *Safe Harbor* é que o primeiro possui compromissos mais efetivos por parte das autoridades de segurança nacional dos Estados Unidos, que dizem respeito às proteções dos dados dos cidadãos europeus. Há também um comprometimento com obrigações mais rigorosas por parte das empresas que desejem fazer uso do *Privacy Shield* para transferir dados. Da mesma forma, os mecanismos sancionatórios foram fortalecidos, bem como as hipóteses de acesso aos dados de europeus pelas autoridades dos Estados Unidos ficaram mais claras, com a imposição de obrigações mais transparentes, evitando-se episódios de vigilância em massa[552].

Do que se pode contatar, acordos como o *Privacy Shield* e *Safe Habor* aproximam cada vez mais o regramento jurídico da proteção de dados dos Estados Unidos e União Europeia. Por óbvio que por questões culturais, os estadunidenses tendem a ser mais permissivos com o que os agentes privados fazem com seus dados desde que isso garanta a eficiência das transações comerciais. Por outro lado, o tratamento jurídico de dados pessoais no bloco europeu parte do princípio de que tais proteções se sobrepõem aos interesses privados.

Todavia, grandes corporações possuem atuação cada vez mais globalizada e seus mercados não conhecem as fronteiras de blocos ou estados nacionais. Como a grande maioria possui origem e sede nos Estados Unidos, é natural que a integração com o bloco europeu ocorra com o necessário endurecimento de algumas normas gerais americanas de proteção de dados e com algum grau de abrandamento das tradicionais normas europeias a respeito, acomodando-se os ordenamentos jurídicos em nome da necessária integração econômica.

Cabe recorrer, portanto, recorrer ao retrospecto histórico feito no primeiro capítulo para questionar se de fato há diferenças essenciais entre a proteção de dados nos cenários

---

[551] Texto do Acordo disponível em: <https://www.privacyshield.gov/article?id=OVERVIEW>. Acesso em: 15 fev. 2018.

[552]O acordo visa, ainda, garantir uma proteção mais efetiva aos cidadãos europeus no que tange ao direito de reparação, inicialmente com prazo para que as empresas resolvam as reclamações dos titulares, caso reclamem diretamente à empresa, bem como poderá realizar reclamação diretamente às autoridades de proteção de dados, que poderá levar o caso à Federal Trade Comission. Há, ainda, mecanismos de resolução administrativa de conflitos por parte das autoridades. Cf. WEISS, Martin A.; ARCHICK, Kristin. Op. cit., p. 9.

estadunidenses e europeu. Por certo que há evidentes diferenças culturais, a impactar a prática da proteção de dados, mas nada que impeça uma aproximação entre os modelos.

A conclusão que se faz neste tópico é que, embora as culturas de privacidade europeia e estadunidense sejam marcadamente diferentes, havendo uma maior deferência ao mercado na primeira e ao Estado na segunda, caso de fato o *Privacy S*hield seja mantido, a tendência é que as corporações globais que atuam em ambos os continentes passem a observar regras mais uniformes no que tange à proteção de dados e à sua transferência intercontinental.

Com efeito, o acordo sobre proteção de dados que hoje conta com Estados Unidos, União Europeia e Suíça pode no futuro englobar outros países das américas do sul e central, bem como paulatinamente incluir países de outros continentes. Talvez essa seja o único caminho de resolver o paradoxo alertado por Bauman[553]: enquanto a política permanece local e com a soberania limitada pelas fronteiras territoriais, o poder encontra-se cada vez mais globalizado, criando dificuldades para que o poder político local resolva questões globais[554]. Logo, a forma de resolver problemas globais talvez seja globalizando a legislação sobre proteção de dados pessoais, em que pese se tenha que realizar concessões aqui e acolá.

2.7.3 Panorama atual da proteção de dados pessoais no Brasil

Atualmente no Brasil não há uma legislação que consolide e proteção a dados pessoais, tampouco que se direcione ao ambiente eletrônico, que parece ser o mais preocupante. Atualmente, há em trâmite três projetos de lei que tratam de dados pessoais, quais sejam o PL 5.276/2016, de autoria do Poder Executivo, o PL 330/2013 do Senado Federal e o PL 4.060/2012 da Câmara dos Deputados.

O primeiro e mais relevante projeto sobre dados pessoais é o PL 5.276/2016. A construção do texto desse projeto de lei foi o que sem dúvida melhor atendeu aos ditames da democracia participativa. Foram realizadas reuniões e consultas públicas organizadas pelo Ministério da Justiça[555] que envolveram empresas, organizações da sociedade civil e

---

[553] "As instituições de Estado arcam, hoje, com a pesada tarefa de inventar e fornecer soluções locais para problemas produzidos no plano global; em função de uma carência de poder, trata-se de um peso que o Estado não pode carregar, e uma tarefa que é incapaz de realizar com as forças que lhe restam e dentro do reduzido domínio das opções que lhe são viáveis". BAUMAN, Zygmunt. Op. cit., p. 77.

[554] BAUMAN, Zygmunt. Op. cit., p. 9.

[555] Para mais informações sobre o debate realizado no âmbito do Ministério da Justiça, vide: <http://pensando.mj.gov.br/dadospessoais2011/>. Acesso em: 10 mar. 2018.

representantes do poder público na discussão sobre o texto. Também no âmbito do Poder Legislativo, o texto foi alvo de consulta pública[556].

O diferencial desse projeto é a criação de uma autoridade administrativa competente pela implementação e fiscalização da lei[557], nos moldes das normas dos países europeus que criam autoridades para a proteção de dados pessoais. Cria também um Conselho de Proteção de Dados Pessoais e da Privacidade, que permite a participação da sociedade civil e possui entre suas funções a de fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade[558].

O PL 330/2013 que tramita no Senado Federal possui diferenças em relação ao projeto de autoria do Poder Executivo. Em que pese tratar a liberdade de expressão como um contraponto necessário à privacidade, em geral suas disposições parecem proteger menos a privacidade. Isso porque não há no projeto a criação de um órgão regulador da atividade, afirmando apenas caber à administração pública no âmbito de cada ente a aplicação das sanções previstas.

O PL 4.060/2012 é o que desperta maiores preocupações[559] em virtude de sua linguagem vaga que parece deixar pontos essenciais sem nenhuma regulamentação. Ademais, o projeto parece muito mais preocupado com o tratamento de dados do que com a sua proteção. O referido projeto não prevê um órgão responsável pelo tratamento de dados. No que tange à proteção de dados sensíveis, o projeto é lacônico e não se preocupa em protegê-los adequadamente, havendo apenas três menções aos dados pessoais sensíveis: uma delas trata de defini-los e, em outras duas, prevê genericamente um cuidado maior na segurança dos dados. A terceira menção, que deveria ser a mais importante, estabelece como requisito para

---

[556]CÂMARAREALIZASEMINÁRIOsobreDadosPessoais (PL 5276/16). **CNF**,jul. 2016. Disponível em: <http://www.cnf.org.br/noticia/-/blogs/camara-realiza-seminario-sobre-dados-pessoais-pl-5276-16-/maximized>/ Acesso em: 18 mar. 2018.

[557] Art. 53. "O órgão competente designado para zelar pela implementação e fiscalização da presente Lei terá as seguintes atribuições: I – zelar pela proteção dos dados pessoais, nos termos da legislação; II – elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;".

[558] Art. 54. "O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade contará com quinze representantes titulares e quinze suplentes designados pelo Ministro de Estado da Justiça, com mandato de dois anos, podendo ser renovado uma única vez por igual período, sendo: (...) VII – um representante da sociedade civil; VIII- um representante da academia; e IX - dois representantes do setor privado. (...)

Art. 55. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I - fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;".

[559] Para uma análise comparativa ampla dos três projetos de lei, vide BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional.**Artigo 19**, nov. 2016.

tratamento de dados sensíveis tão somente o consentimento do titular, por qualquer meio que permita sua manifestação de vontade[560].

Ao admitir genericamente qualquer forma de consentimento, o projeto deixa aberta a possibilidade da prática de termos de consentimentos truncados e longos nos quais se inclui nas entrelinhas a possibilidade de tratamento de dados pessoais, sem que o próprio titular saiba com o que está consentindo. Diferentemente dos outros dois projetos, este não prevê as hipóteses específicas nas quais se permite o tratamento de dados pessoais sensíveis. O risco desse projeto é que falta de regulamentação adequada deixa a critério exclusivo do agente público ou privado fazer o que bem entende com os dados pessoais sensíveis.

Conforme visto nos tópicos anteriores, a proporcionalidade enquanto vedação à proteção insuficiente impõe ao poder público deveres positivos, entre eles o dever de editar legislação que proteja de forma suficiente e adequada determinado direito fundamental. Portanto, o projeto de lei em análise, caso editado, padeceria de inconstitucionalidade em virtude da omissão do legislador no cumprimento dos deveres de proteção.

Verifica-se que cada projeto de lei possui uma definição específica do que se entende por dado pessoal. Para o PL 5276 de autoria do Poder Executivo, dado pessoal é "o dado relacionado à pessoa natural identificada ou identificável, inclusive dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa". O PL 330/2013, de autoria do Senado, define dado pessoal como "toda informação, de qualquer natureza e independentemente do respectivo suporte, passível de ser armazenada, processada ou transmitida, relativa a pessoas identificadas ou identificáveis". Por fim, o PL 4060/2012 prevê como dado pessoal "qualquer informação que permita a identificação exata e precisa de uma pessoa determinada".

Pode-se, portanto, concluir que o projeto de lei 4060/2012 adota um conceito restritivo de dado pessoal, admitindo como tal apenas aquele que permita a identificação exata e precisa de pessoa determinada.

O conceito é inadequado, pois, ao prever que o dado pessoal seja apenas aquilo que permita a identificação exata e precisa da pessoa, o dispositivo parece inverter o ônus da

---

[560] Art. 11. "O responsável pelo tratamento de dados, bem como eventuais subcontratados, deverão adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular. Parágrafo Único. As medidas a serem adotadas devem ser proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis.

Art. 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal".

prova, fazendo-o recair sobre o titular do dado. Não se deve ignorar que mera possibilidade de identificar o titular já o faz merecedor de proteção jurídica.

Não é demais dizer que embora o dado seja pessoal, não é necessário ter o seu titular perfeitamente identificável para que haja violações de direitos. Imagine que se pretenda identificar determinada parte da população que compareceu a protestos políticos contrários ao governo. Basta que se colete ilegalmente dados dos deslocamentos nos transportes públicos para se identificar qual a origem e o destino de parte dos manifestantes. Logo, ainda que não identificados de maneira exata e precisa, pode-se perseguir a população de determinado bairro por razões políticas. Tal fato não está longe da realidade, na medida em que, nos intitulados protestos de junho de 2013, a Agência Brasileira de Inteligência montou estrutura para monitorar nas redes sociais a movimentação de manifestantes cujo alvo preferencial de protestos era o governo[561].

Todavia, o fato de nenhuma lei que verse especificamente sobre proteção de dados pessoais estar em vigor não significa absolutamente que não haja nenhum tipo de tutela aos dados pessoais. Conforme visto neste trabalho, a proteção aos dados pessoais nos termos da lei é princípio da disciplina do uso da internet, previsto no art. 3º, II, do Marco Civil da Internet.

O mesmo diploma prevê entre os direitos do usuário da internet o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, VII); o direito de obter informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet (art. 7º, VIII).

Ademais, a referida lei exige que haja consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais - que deverá ocorrer de forma destacada das demais cláusulas contratuais (art. 7º, IX) - e que haja a exclusão definitiva dos dados pessoais

---

[561] RIZZO, Alana; MONTEIRO, Tânia. Abin monta rede para monitorar internet. **Estadão**, jun. 2013. Disponível em: http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500>. Acesso em: 18 mar. 2018: "Sem detectar as manifestações combinadas pelas redes sociais e que hoje terão como alvo o Palácio do Planalto, a Agência Brasileira de Inteligência (Abin) montou às pressas uma operação para monitorar a internet. O governo destacou oficiais de inteligência para acompanhar, por meio do Facebook, Twitter, Instagram e WhatsApp, a movimentação dos manifestantes. A agência avalia que as tradicionais pastas do governo que tratavam de articulação com a sociedade civil perderam a interlocução com as lideranças sociais".

que tiver fornecido a determinada aplicação de internet, a requerimento do usuário, ao término da relação entre as partes (art. 7º, X). Por fim, a lei em questão dedica um capítulo inteiro à proteção aos registros, aos dados pessoais e às comunicações privadas.

Embora o Marco Civil se aplique ao ambiente de internet, verifica-se na referida lei uma robusta proteção aos dados pessoais neste campo específico. Considerando que a vida contemporânea é cada vez mais mediada eletronicamente, pode-se dizer que relevante parte dos dados pessoais são tratados através de aplicações e sites que utilizam o ambiente de internet.

O Código de Defesa do Consumidor, Lei 8078/90 traz algumas proteções ao consumidor cujos dados integram bancoS de dados[562], tais como o direito de conhecer e retificar as informações. Todavia, a norma não impõe nenhuma responsabilidade quanto ao seu compartilhamento ou qualquer dever de observância da privacidade dos consumidores. A previsão é semelhante às garantias constitucionais do *habeas data*[563], não trazendo inovação relevante.

Pode-se citar ainda, a Lei de Acesso à Informação, louvável iniciativa que garante o direito à informação previsto no art. 5º, XXXIII, da Constituição da República e que possui algumas preocupações com a intimidade e a vida privada, bem como com a divulgação indevida de informações pessoais. O direito à informação, correlato à liberdade de expressão e

---

[562] Dos Bancos de Dados e Cadastros de Consumidores Art. 43. "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6o Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (Vigência)

Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor. § 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado. § 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código".

[563] Art. 5. "(...): LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;".

liberdade de imprensa, é conformado pelo direito à privacidade, funcionando como princípio contraposto a ser ponderado no caso concreto.

Por esta razão, as exceções na Lei de Acesso à Informação são justamente as informações pessoais a conformar o ponto ótimo entre o direito à informação e a privacidade. Nessa perspectiva, a referida lei restringiu o acesso às informações pessoais apenas aos agentes públicos legalmente autorizados, independentemente da classificação do sigilo da informação[564].

Outra hipótese de proteção aos dados pessoais ocorre na Lei nº 12.414/2011, conhecida como Lei do Cadastro Positivo, cujo objetivo é formar banco de dados de adimplemento de pessoas naturais ou jurídicas. A referida lei exige que o cadastrado seja informado acerca do armazenamento, a identidade do gestor do banco de dados e o objetivo do tratamento dos dados pessoais, além do destinatário dos dados em caso de compartilhamento; prevê ainda o direito de que os dados sejam aplicados de acordo com a finalidade para a qual foram coletados. Além do direito ao acesso e correção dos dados, embora não exija o consentimento para integrar o cadastro positivo, a lei permite que o titular dos dados possa obter o cancelamento do cadastro, mediante solicitação.

Em suma, pode-se concluir que, embora não haja uma lei específica tratando da proteção aos dados pessoais, o ordenamento jurídico brasileiro possui disposições importantes que, longe de serem ideais, trazem algum grau de proteção aos dados pessoais. Por certo que melhor seria se tais proteções constassem de um documento consolidado no qual se definisse com clareza o objeto de proteção, os requisitos para tratamentos de dados pessoais, os requisitos especiais para tratamento de dados sensíveis, as sanções cabíveis em caso de

---

[564] Das Informações Pessoais Art. 31. "O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal".

violação, bem como o órgão regulador responsável pela proteção de dados, a exemplo de alguns projetos atualmente em tramitação.

Não houvesse as legislações ordinárias tratando do tema, consoante abordado no tópico anterior, poder-se-ia recorrer à aplicação direta da norma constitucional que protege a privacidade ao caso concreto. Decerto que não seria fácil definir no caso concreto o grau de proteção aos dados pessoais conferido diretamente pela Constituição, quando nenhum dispositivo expressamente trata de dados pessoais[565].

Todavia, o dispositivo constante dos direitos e garantias fundamentais, atinente à privacidade[566] parece suficiente a se realizar uma ponderação com o princípio constitucional contraposto, a se estabelecer no caso concreto o princípio prevalente[567].

Por fim, deve-se advertir que a proteção aos dados pessoais, embora já tratada há algum tempo pela doutrina pátria e estrangeira não é tema de menor relevância ou que tenha perdido sua importância ao longo do debate. Isso porque, com a consolidação do *big data* como modelo de negócio privado ou mesmo como instrumento de vigilância, há um risco cada vez mais intenso de violações, seja por motivo de perseguição política, seja em virtude de estratégia de mercado.

Para ilustrar a concretude de tais riscos, basta observar que um representante da empresa *Cambridge Analytica*, responsável pelo maior escândalo de vazamento de dados de usuários do *Facebook* afirmou que atuará nas eleições brasileiras em outubro de 2018 e que utiliza métodos espúrios para alterar resultados eleitorais, manipulando as emoções dos usuários da rede[568].

Portanto, em que pesem proteções esparsas e a possibilidade de aplicação direita da Constituição inclusive às relações privadas, urge a edição de diploma normativo consolidado

---

[565] Ressalte-se que a Constituição prevê a inviolabilidade de dados. Todavia, o contexto da garantia constitucional nos parece muito mais restrita, haja vista que o dispositivo procura proteger a inviolabilidade das comunicações, ou seja, dos dados em movimento, em transmissão, partindo do remetente ao destinatário. Ocorre que nem toda a situação de proteção aos dados pessoais se refere à transmissão em si, mas à coleta, tratamento e compartilhamento de dados. Ademais, a inviolabilidade diz respeito ao conteúdo em si, em nada proibindo, a rigor que o dado seja tratado ou compartilhado. Logo, o dispositivo protege os dados de interceptação e não de seu uso ou compartilhamento com terceiros". A observação é de CARVALHO, Luiz Gustavo Grandinetti Castanho de. Direito à Privacidade. **Revista de EMERJ**, v. 1, n. 2, p. 55, 1998.

[566] Art. 5º: "(...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;".

[567] Sobre aplicação da ponderação, vide: BARCELLOS, Ana Paula de. **Ponderação, racionalidade e atividade jurisdicional**. Rio de Janeiro: Renovar, 2005.

[568] O GLOBO/AGÊNCIAS INTERNACIONAIS. 'Estamos indo para o Brasil', diz diretor da Cambridge Analytica. **O Globo**, mar. 2018. Disponível em: <https://oglobo.globo.com/mundo/estamos-indo-para-brasil-diz-diretor-da-cambridge-analytica-22510961>. Acesso em: 21 mar. 2018.

que proteja adequadamente os dados pessoais dos cidadãos, usuários ou não da internet. A referida medida trará maior segurança jurídica às empresas cujo modelo de negócios envolva a coleta e tratamento de dados pessoais, bem como dará instrumentos jurídicos ao titular dos dados para protegê-los, retificá-los e responsabilizar terceiros em face de seu uso indevido.

No capítulo a seguir serão abordadas formas de proteção e de resistência a possíveis violações à privacidade, discutindo-se ainda se o consentimento é o modelo mais adequado para proteger a privacidade.

Um dos escudos à possíveis violações à privacidade em tempos de *big data* é a criptografia, mecanismo que decodifica a mensagem e impossibilita que eventual interceptação tenha acesso ao seu conteúdo decifrado, vez que somente o destinatário possuirá a chave para abertura da mensagem enviada.

3CRIPTOGRAFIA E OS INSTRUMENTOS DE PROTEÇÃO À PRIVACIDADE

> Cryptography can be all these things, both good and bad, because encryption can serve two fundamentally different ends. In its “confidentiality” function it can be “used to keep communications secret.” In its “identification” function it can be “used to provide forgery-proof digital identities.” It enables freedom from regulation (as it enhances confidentiality), but it can also enable more efficient regulation (as it enhances identification).[569]
>
> *Lawrence Lessig*

Dentre as técnicas aplicáveis às novas tecnologias de informação e comunicação, nenhuma tem sido alvo de tamanha resistência ou objeto de defesa nos últimos anos como a criptografia. Embora a técnica não tenha nada de inovadora, pelo contrário, seja de aplicação milenar, o seu desenvolvimento no âmbito da ciência computação tem garantido a confidencialidade inviolável de comunicações e dados que trafegam na rede.

Enquanto esteve restrita à área militar e diplomática, a criptografia nunca foi tratada como um problema, mas como uma tecnologia que, detida por governos e grandes corporações, garantiam o fluxo seguro de transações bancárias e comunicações militares ou diplomáticas. Somente, a partir da popularização dos códigos-fontes de criptografia na web, associada ao uso de equipamentos e comunicações criptografadas em aparelhos portáteis,o uso da criptografia passa a ser um problema.

Com efeito, tamanha a relevância da criptografia que algumas legislações a consideram, junto a outros armamentos e munições, equipamento de defesa, cujo uso, comercialização e exportação deveriam ser controlados ou proibidos. Por outro lado, defensores do livre uso da criptografia, o que parece ser um consenso na área científica, a apresentam como instrumento essencial à liberdade de expressão e opinião, à garantia do trabalho jornalístico e à resistência a perseguições políticas[570] ou mesmo como instrumento

---

[569] Em tradução livre: "A criptografia pode ser tudo isso, tanto bom quanto ruim, porque a criptografiapode se prestar a duas finaliadades essencialmente distintas. Na sua função de 'confidencialidade', pode ser 'usado para manter as comunicações em segredo'. Em sua função de 'identificação' pode ser 'usada para fornecer identidades digitais à prova de falsificação'. Permite a liberdade da regulação (pois aumenta a confidencialidade), mas pode também permitir uma regulação mais eficiente (uma vez que aumenta a certeza da identificação)". LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006.

[570] REDAÇÃO. Criptografia e anonimato são centrais para liberdade de opinião e expressão na era digital, diz ONU. **Nações Unidas no Brasil**, jul. 2015. Disponível em: <https://nacoesunidas.org/criptografia-e-anonimato-sao-centrais-para-liberdade-de-opiniao-e-expressao-na-era-digital-diz-onu/>. Acesso em: 10 abr. 2018.

resistência à vigilância irrestrita e à militarização do ambiente de internet, enquanto garantia do livre fluxo de informações e discursos[571].

Tamanha controvérsia chegou a constituir plataforma de campanha da primeira ministra eleita do Reino Unido, Theresa May, segundo a qual a criptografia forte deveria ser banida, de modo a não se garantir espaços seguros a práticas de atividades criminosas[572]. A proposta não é exclusividade do Reino Unido, aparecendo com variações em outros países da Europa, como França e Alemanha, os quais intentam tornar ilegal a prática ou obrigar as companhias que a utilizam a descriptografar conteúdos, caso determinado pelos poderes públicos[573]. Por outro lado, em 2017, o Parlamento Europeu propôs a reforma da Diretiva de Privacidade de 2002, com fins de prever a proibição de que os estados membros adotassem medidas no sentido de enfraquecer sistemas de criptografia, com vistas a garantirem acesso ao conteúdo dos dados criptografados[574].

É fora de dúvida que o Reino Unido se classifica entre os países democráticos e com a proibição da criptografia se colocaria ao lado de países como Arábia Saudita, China, Rússia e Cazaquistão, os quais ou realizam um rígido controle sobre a criptografia ou a proíbem de modo absoluto. Tal fato, no entanto, não significa a condenação absoluta da primeira ministra britânica, mas evidencia a profunda controvérsia que desperta o uso da criptografia, especialmente a criptografia dita inquebrável ou criptografia forte e de acesso amplo.

Tanto é assim que o FBI, conhecida agência de investigação norte-americana, pressionou os congressistas a obrigarem que as empresas que comercializassem aparelhos portáteis criptografados disponibilizassem uma espécie de chave especial ou porta dos fundos às autoridades investigativas. De outro modo, no país símbolo da liberdade, há projetos de lei que visam proibir o uso da criptografia - tornando o seu uso ilegal - ou mesmo aqueles que

---

[571] LIRA, Isadora Teixeira de. Hacktivistas e Cypherpunks: A Resistência à Militarização e Vigilância do Ciberespaço na Sociedade de Controle. In: **40º Encontro Anual de Anpocs**, Caxambu, out. 2016. Disponível em: <http://www.anpocs.com/index.php/papers-40-encontro/st-10/st05-8/10169-hacktivistas-e-cypherpunks-a-resistencia-a-militarizacao-e-vigilancia-do-ciberespaco-na-sociedade-de-controle/file>. Acesso em: 18 mar. 2018.

[572] TAMBURRO, Paul. Theresa May's Plan to Stop Online Extremism Would Require an Impossible Encryption Ban. **Mandatory**, jun. 2017. Disponível em: <http://www.mandatory.com/living/1273027-theresa-mays-plan-stop-online-extremism-require-impossible-encryption-ban#P2phMksU3fH6lVJ0.99>. Acesso em: 18 mar. 2018.

[573] SUMARES, Gustavo. França e Alemanha querem leis para limitar criptografia. **Olhar Digital**, ago. 2016. Disponível em: <https://olhardigital.com.br/pro/noticia/franca-e-alemanha-querem-leis-para-limitar-criptografia/61501>. Acesso em: 18 mar. 2018.

[574] EUROPEAN PARLIAMENT. Reform of the e-Privacy Directive. **European Parliament**, set. 2017. Disponível em: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf>. Acesso em: 18 mar. 2018.

querem obrigar empresas de tecnologia a disponibilizarem uma porta dos fundos para fins de investigação.

Na maioria dos casos, o clamor pelo fim da criptografia se refere ao uso da criptografia ponta-a-ponta cuja engenharia de algoritmo é construída de modo que sequer o aplicativo ou servidor consiga acessar o conteúdo da mensagem, apenas acessível por emissor e destinatário, o que impede, a princípio, a sua interceptação ou espelhamento por agências de investigação.

O argumento para criação de uma chave mestra que permita a terceiros acessar o conteúdo criptografado, assim como no caso da vigilância em massa, é o combate ao terrorismo, tráfico de drogas, pedofilia ou qualquer outra atividade criminosa, especialmente as atividades que causem comoção à opinião pública.

No atual estágio civilizatório, nenhum indivíduo razoável seria contra o combate ao tráfico armado de drogas no Brasil, que oprime favelados e desafia o estado de direito. Tampouco seria contra o combate à pedofilia ou à exploração sexual de menores. Não parece ser o caso específico do Brasil, mas não há na sociedade brasileira qualquer tipo de conivência com práticas terroristas.

Ocorre que a questão da criptografia não se apresenta com a nitidez cristalina que permita distinguir vilões e virtuosos.As novas tecnologias informativas e comunicativas, ao tempo que viabilizam o exercício da cidadania, o aperfeiçoamento de práticas democráticas, o acesso ao emprego e à educação, também são a porta de entrada para a vigilância estatal, exposição pública de fatos privados, atividades criminosas com base em informações de perfil em rede social. Disto decorre a preocupação que a democratização do acesso a estas tecnologias não facilite ou potencialize violações arbitrárias dos direitos dos usuários da rede. Para tanto, a criptografia mostra-se coo valioso instrumento a equilibrar esse conflito.

Deve-se ressaltar que não se trata de abrir mão da privacidade em nome da segurança. Na verdade, é preciso situar o debate adequadamente, sob pena de maniqueísmos impedirem a marcha do progresso tecnológico ou mesmo a democratização dos meios de defesa em face do vigilantismo, seja ele estatal ou privado. Conforme visto no capítulo anterior, o fato de não ter nada a esconder não implica na necessária obrigação em tornar-se transparente, vez que isso viola frontalmente direitos fundamentais caros às sociedades democráticas. Conforme se verá neste capítulo, deve-se refletir se o embate entre criptografia e segurança é de fato um embate e quais os limites e possibilidades do uso da criptografia e do seu controle por parte do Estado.

3.1 **Do breve histórico da criptografia**

Embora recentemente tenha provocado intenso debate, o uso da criptografia é tão antigo quanto o da própria escrita ou ao menos tanto quanto a necessidade de se ocultar o conteúdo das comunicações por razões de estratégia ou militar. Cabe realizar um breve retrospecto histórico do uso da criptografia, citando-se alguns casos, a fim de compreender seu contexto e a quadra atual.

A criptografia clássica consiste no período que vai desde os povos antigos, passando pela Idade Média – que utilizavam a cifragem manual -até as máquinas de cifragem eletromecânicas, que foram utilizadas principalmente durante a Segunda Guerra Mundial[575]. A criptografia moderna ou contemporânea inicia-se no pós II Guerra e apenas foi possível com o advento dos computadores que possibilitaram novos saltos tecnológicos na encriptação, bem como a popularização do seu acesso, antes restrito a entidades estatais e grandes corporações[576].

Na Grécia antiga, por volta do século V a.c., há relatos do uso de mensagens cifradas por espartanoscuja técnica consistia em escrever mensagens secretas em um pergaminho translúcido enrolado em espiral, de tal modo que o texto era escrito no sentido longitudinal e cada letra era escrita separadamente a cada volta do pergaminho. Desenrolado o pergaminho, as letras dispersas deixavam de fazer sentido, de modo que cada letra fosse inscrita separadamente numa das voltas da tira de papiro. Para decifrar a mensagem, se fazia necessário um bastão da mesma espessura do que foi utilizado para escrever a mensagem original, permitindo-se, com a sobreposição das voltas do papiro, a compreensão de seu conteúdo[577].

Também na Roma Antiga, o imperador Júlio Cesar utilizava técnica de cifragem para suas mensagens, que consistia em substituir cada letra do texto pela terceira letra subsequente no alfabeto, de modo que apenas quem conhecesse a senha para decriptação poderia compreender o conteúdo da mensagem. A técnica ficou conhecida como cifra de César e foi

---

[575]CRYPTOID. Uma breve história sobre Criptografia. Disponível em: https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/. Acesso em 18 mar. 2018.

[576] OSBORNE, Charlie. As devastating as KRACK: New vulnerability undermines RSA encryption keys. **ZDNet**, out. 2017. Disponível em: <http://www.zdnet.com/article/as-devastating-as-krack-new-vulnerability-undermines-rsa-encryption-keys/>. Acesso em: 18 mar. 2018.

[577] CADAVID, Jhonny Antonio Pabón. La criptografia y la protección a la información digital. **Revista La propriedade inmaterial**, n. 14, p. 62, 2010.

largamente utilizada nas comunicações do imperador nas ações de expansão de seu império[578].

Durante a Idade Média, a criptografia também se desenvolveu, de modo que se pode dizer que todos os governos da Europa Ocidental usaram criptografia de uma forma ou de outra,em geral para manter contato com embaixadores. Nesse sentido, os primeiros grandes avanços na criptografia foram feitos em Veneza, que em 1452 criou uma organização que contava com três agentes de cifragem cuja função era descriptar textos, bem como criar cifras que para serem utilizadasusadas pelo governo[579].

Até a Primeira Guerra Mundial, todas as técnicas de criptografias eram desenvolvidas manualmente. Com o advento da Segunda Guerra, passou-se a utilizar modelos mecânicos de cifragem, cabendo o destaque da máquina Enigma, utilizada pelos alemães e reconhecida como o mais avançado engenho de codificação inventado até então. A utilização do sistema pelos alemães representou um avanço no estudo da criptografia, de modo que o sistema criado pela máquina apenas o que representou um grande salto nas técnicas de criptográfica, de modo que apenas anos depois de sua criação, matemáticos britânicos lograram êxito em decifrar o mecanismo de codificação[580].

A era digital multiplicou a possibilidade de codificação de textos, haja vista a capacidade de realização de cálculos complexos proporcionada pelo advento dos computadores. A criptografia contemporânea constitui basicamente a criação de chaves criptográficas de maneira automatizada, a partir de complexos cálculos matemáticos, cujo critério de cálculo é determinado pelo algoritmo, de modo que a complexidade de tais cálculos dificulta sobremaneira a decodificação das mensagens encriptadas.

Outro marco da criptografia digno de nota ocorreu em 1976. Até então, o acesso aos algoritmos criptográficos era monopolizado por governos e corporações. Naquele ano, o governo dos Estados Unidos tornou público o sistema DES *(Data Encryption Standart)*, sistema de criptografia criado pela IBM, cujo código foi disponibilizado ao público. A partir deste marco o código fonte da criptografia foi aberto a fins não militares e disponibilizada de encriptação ao público geral. O sistema DES constituía em uma chave pública simétrica de criptografia e representou uma mudança de paradigma no acesso à criptografia. Da

---

[578] Ibidem, p. 59.

[579]COHEN, Fred. A Short History of Cryptography. **All**, 1995. Disponível em: <http://all.net/edu/curr/ip/Chap2-1.html>. Acesso em 13 mar. 2018.

[580] MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia, São Paulo: Forense, 2010, p. 21.

publicização do sistema DES até os dias atuais, o acesso à criptografia sofreu avanços e retrocessos, o que será objeto de abordagem em tópico específico[581].

Na década de 90, o uso da criptografia direcionou-se a garantir a confidencialidade dos correios eletrônicos, da cifragem das páginas de acesso à internet e sistemas financeiros,das transações interbancárias, através do sistema criptográfico PGP*(Pretty Good Privacy)*. Phil Zimmerman, criador do PGP, é apontado como o responsável pela popularização e até mesmo a massificação da criptografia de alto padrão[582]. Em 1991, em resistência às severas restrições norte-americanas à exportação da criptografia forte, Zimmerman disponibilizou gratuitamente na internet o código fonte de seu sistema criptográfico.

A ousadia custou a Zimmerman uma investigação por exportação ilegal de equipamentos militares, iniciada em 1993, já que a criptografia e dispositivos que a utilizassem constavam entre os artigos militares de exportação controlada, constante da lista de armamentos e munições dos Estados Unidos, segundo as normas ITAR (*International Traffic Arms Regulation*). A disponibilização na internet foi considerada exportação da tecnologia e, para tanto, seria necessário construir o código fonte com chaves fracas - ou seja, chaves que não resistissem a ataque de força bruta[583]e permitisse a sua violação - ou mesmo a criação de uma *backdoor* - uma vulnerabilidade no sistema que permita a sua violação por quem a conheça. Três anos depois, diante do fato de o MIT(*Massachusetts Institute of Technology*)[584]disponibilizar na internet uma versão digital do livro do código PGP, bem como das pressões recebidas por instituições de direitos civis, como a EFF (*Electronic Frontier Foundation*)[585], a investigação foi arquivada[586].

---

[581]CADAVID, Jhonny Antonio Pabón. La criptografia y la protección a la información digital. **Revista La propriedade inmaterial**, n. 14, p. 65, 2010.

[582] MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia, São Paulo: Forense, 2010, p. 24.

[583] Em criptografia, um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, a chave criptográfica. Em outras palavras, trata-se da busca exaustiva da chave, ou seja, é um ataque criptoanalítico que pode, em teoria, ser usado contra quaisquer dados criptografados (exceto para dados criptografados de uma maneira segura na teoria da informação). Esse ataque pode ser usado quando não é possível tomar vantagem de outras fraquezas em um sistema de criptografia (se existir) que tornariam a tarefa mais fácil. Ele consiste de verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas. No pior dos casos, isto envolveria percorrer todo o espaço de busca.

[584]Em tradução livre,Instituto de Tecnologia de Massachusetts. É uma Universidade localizada em Cambridge, Massachusetts, Estados Unidos, reconhecida pelo desenvolvimento na área de tecnologia e ciências exatas.

[585]Em tradução livre, Fundação Fronteira Eletrônica. Trata-se de Organização sem fins lucrativos sediada em San Francisco, Califórnia, cujo objeto é a proteção da liberdade de expressão e outros direitos civis no contexto da era digital.

Diante das proibições de exportação do software criptográfico pronto, em novo movimento de resistência às restrições do intercâmbio tecnológico, Zimmerman publicou o *código-fonte* do programa na forma de livros, totalizando doze volumes, e obteve autorização judicial para exportá-los para outros países, invocando o direito à liberdade de expressão, haja vista ser a criptografia tão somente um sistema de segurança em forma de engenharia matemática[587]. De posse dos livros, um ativista europeu escaneou os arquivos e os disponibilizou na internet, para livre acesso a quem quisesse implementar o sistema P2P. De mesma forma, mesmo no caso da versão americana do P2P, logo após o seu lançamento nos Estados Unidos, verificou-se que o software estava disponível em outros países dias depois[588].

O episódio de resistência à proibição apenas demonstra o quão inócuo pode ser uma política restritiva à livre circulação tecnológica. De fato, a proibição não impede que criminosos tenham acesso à tecnologia criptográfica de ponta, mas limita o seu uso ao cidadão comum, que poderia ter a privacidade protegida e, em virtude das restrições, terá maior dificuldade em acessar a tecnologia. Limitar a circulação do código-fonte de sistemas criptográficos é o mesmo que limitar a liberdade de expressão da atividade intelectual e científica.

Deve-se ressaltar que, embora disponibilizado à IBM, na década de 1970, a exportação da criptografia de alta qualidade sempre foi objeto de controle pelos Estados Unidos, incluindo-se programas ou dispositivos que utilizem a criptografia entre os artigos militares de comercialização controlada[589]. Portanto, apenas por volta de 1997, a lista de munições e

---

[586] THE NEW YORK TIMES. ***Data-Secrecy Export Case Dropped by U.S.*** *Disponível em:* https://www.nytimes.com/1996/01/12/business/data-secrecy-export-case-dropped-by-us.html. Acesso 18 mar 2018

[587]MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia, São Paulo: Forense, 2010, p. 24.

[588] Ibidem, p. 25.

[589] A lista de equipamentos e tecnologias constantes da lista de munições controladas pelo governo norte-americano. Na Categoria XIII, "B", que trata dos "Materiais e Artigos Diversos" há cinco subcategorias de artigos militares que envolvem a criptografia, agrupados sob o título de sistemas e equipamentos de segurança da informação ou de garantia da informação, dispositivos criptográficos, software e componentes. São elas (1) Sistemas, equipamentos, conjuntos, módulos, circuitos integrados, componentes e software de criptografia militar ou de inteligência (incluindo a gestão de chaves) capazes de manter o sigilo ou a confidencialidade das informações ou sistemas de informação, incluindo equipamentos ou software para criptografia e descriptografia de rastreamento, telemetria e controle (TT & C); (2) Sistemas, equipamentos, conjuntos, módulos, circuitos integrados, componentes e software de criptografia, militares ou de inteligência (incluindo a gestão de chaves) (incluindo suas interfaces criptográficas) capazes de gerar códigos de propagação ou salto para sistemas ou equipamentos de espectro alargado; (3) Sistemas criptoanalíticos militares ou de inteligência, equipamentos, conjuntos, módulos, circuitos integrados, componentes e software; (4) Sistemas militares ou de inteligência, equipamentos, montagens, módulos, circuitos integrados, componentes ou software (incluindo todas as versões anteriores ou derivadas) autorizados a controlar o acesso ou transferir dados entre diferentes domínios de segurança, conforme listado no Unified Cross Domain Management Office. (UCDMO) lista de controle

armamentos do governo norte-americano amenizou as exigências quanto à circulação da criptografia, ao transferir o controle da exportação da criptografia do departamento de Estado ao departamento de Comércio, durante o governo Clinton, através da Ordem Executiva 13026[590], em virtude da cada vez maior utilização da criptografia para fins civis[591].

Portanto, a exportação da criptografia deixou de figurar entre os itens proibidos de exportação sob qualquer forma, constantes do ITAR, e passou a figurar entre os itens cujo comércio demandam autorização especial, nos termos do *Export Administration Act* de 1969[592]. As novas regras trouxeram ainda a flexibilidade à criptografia bancária, permitindo a exportação de criptografias com chaves de até 56 bits para entidades financeiras ou bancárias. As restrições estadunidenses à criptografia apenas não se aplicam no contexto do ensino acadêmico. Há ainda uma série de países democráticos do ocidente que figuram em uma lista de exceção, para os quais se flexibiliza ao máximo as restrições à exportação da criptografia, mantendo as restrições apenas aos países não aliados dos Estados Unidos, conforme será visto a seguir.

Portanto, inaugura-se, na década de 1990, as chamadas criptoguerras (do inglês *cryptowars*), caracterizada pelo movimento de resistência da sociedade civil face do controle e proibição da livre circulação dos códigos criptográficos por parte do governo[593].

Nesse contexto, outro caso que merece destaque é o caso *Bernstein v. US Department of Justice*. Bernstein era professor da Universidade da Califórnia em Berkeley e havia desenvolvido um sistema criptográfico "Snuffle". Com isso, o autor desejava publicar o algoritmo através de artigo acadêmico que descrevia e explicava a engenharia matemática do algoritmo, bem como disponibilizava o "código-fonte" necessário para a criação de um programa de computador. Bernstein buscava divulgar o resultado de sua pesquisa e discutir o

---

(UCL); ou (5) Equipamento auxiliar especialmente concebido para os artigos dos parágrafos (b) (1) - (b) (4) desta categoria.Vide *International Traffic In Arms Regulations* (ITAR), §121.1, The United States Munitions List, Category XIII— Materials and Miscellaneous Articles. Disponível em: <https://www.ecfr.gov>. Acesso em 13 mar. 2018.

590 CLINTON, William J. Executive Order 13026—Administration of Export Controls on Encryption Products. **The American Presidency Project**, nov. 1996. Disponível em: <http://www.presidency.ucsb.edu/ws/index.php?pid=52252>. Acesso em: 10 abr. 2018.

591 CADAVID, Jhonny Antonio Pabón. Op. cit., p. 79.

592 Para consulta à norma de 1969 e a um compilado atualizado de atos sobre controle de exportação dos Estados Unidos, vide *Legal Authority Export Administration Regulations* do Departamento de Comércio dos Estados Unidos. Disponível em: <https://www.bis.doc.gov>. Acesso em 10 mar. 2018

593 Cf. UNITED STATES. Electronic Code of Federal Regulations. **Government Publishing Office**, abr. 2018. Disponível em: <https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=36613dec83f28e22c86fd9a4c9c7f632&mc=true&n=pt15.2.740&r=PART&ty=HTML>. Acesso em: 12 abr. 2018. Veja, em especial, o Title 15: Commerce and Foreign Trade PART 740—LICENSE EXCEPTIONS, §740.17 Encryption commodities, software, and technology (ENC).

sistema Snuffle em palestras e conferências, entre outras atividades acadêmicas. Ocorre que, segundo o ITAR, softwares criptográficos deveriam se submetem aos mesmos controles dos armamentos e munições, demandando um registro e licença para comercialização e divulgação[594].

Para obter seu intento, Bernstein ingressou em juízo, afirmando que o sistema criptográfico nada mais era que exercício de sua liberdade de expressão, não devendo sofrer nenhuma restrição. Embora o governo alegasse que o código-fonte consistisse meramente em informações técnicas, e, portanto, controláveis,a Corte do Distrito de Northern, na Califórnia, autorizou a divulgação do código-fonte, sob o fundamento de que o sistema criptográfico que o autor havia desenvolvido deveria ser considerado uma forma de expressão e, portanto, protegida pela Primeira Emenda à Constituição dos Estados Unidos. Posteriormente, a Corte de Apelações no Nono Circuito jugou a apelação do governo e manteve a sentença, sob o argumento que com a criptografia se protegia tanto a liberdade de expressão dos criadores do código como os direitos constitucionais dos cidadãos beneficiários em potencial da criptografia, além da sua privacidade e intimidade[595].

Outro caso que merece destaque foi a tentativa do governo dos Estados Unidos em implementar um tipo de criptografia com o fornecimento de chaves criptográficas às agências de segurança. Conhecido como Chip Clipper, o mecanismo consistia em um sistema de depósito de chaves de criptografia, que se dividiamem dois dispositivos e ficavam em confiança de terceiros. No entanto, as chaves apenas funcionariam com a junção das duas partes, o que ocorreriam apenas mediante ordem judicial aos dois depositários. Segundo o governo estadunidense, esse modelo equilibraria a privacidade com a necessidade de segurança e de investigação judicial. O sistema Clipper implementado pelo governo em fevereiro de 1994 e ficou conhecido como *Escrow Encryption Standart* (Padrão de Criptografia de Custódia, em livre tradução). Todavia, em que pese inicialmente se haver pensado em se impor uma obrigatoriedade de adotar o modelo Clipper, logo após o seu lançamento, descobriu-se uma vulnerabilidade que permitia a terceiros trocar as suas chaves, de modo que a implementação do modelo fracassou não tendo havido adesão da indústria[596].

---

[594] CADAVID, Jhonny Antonio Pabón. Op. cit., p. 83-84.

[595] UNITED STATES OF AMERICA. United States Court of Appeals, Ninth Circuit. Bernstein v. United States Department of Justice. No. 97-16686. Disponível em: <http://caselaw.findlaw.com/us-9th-circuit/1317290.html>. Acesso em: 18 mar. 2018.

[596] CADAVID, Jhonny Antonio Pabón. Op. cit., p. 86.

O último e mais recente caso que merece menção ocorreu na Califórnia e parece haver reinaugurado as criptoguerras no século XXI. Trata-se do massacre em San Bernardino, que deixou 14 mortos em 2016 e ocorreu em uma instituição que auxiliava pessoas com deficiência, o que despertou clamores das autoridades norte-americanas pela implementação de uma super-chave ou chave mestra para dispositivos criptografados.

A polícia apreendeu o telefone de um dos criminosos envolvidos, um aparelho modelo iPhone modelo 5C, da fabricante Apple. O dispositivo possui proteção por chave criptografada e o seu conteúdo é apagado após repetidas tentativas de acesso.Desta forma, interessava ao FBIacessar o conteúdo do aparelho, para saber com quem o terrorista se comunicava, de modo que Departamento de Justiça ingressou em juízo para obrigar a Apple a desenvolver vulnerabilidade que permitisse acessar o conteúdo protegido por chave criptografada[597]. A empresa se recusou[598],sob a alegação de que a ferramenta tornaria vulneráveis todos os outros aparelhos da fabricante, embora o FBI afirmasse que apenas lhe interessava quebrar o código de aparelho determinado. No entanto, às vésperas da audiência, resolveu o FBI desistir da ação, afirmando que teria conseguido acessar os dados do aparelho, mesmo sem a ajuda da Apple[599].

A agência se recusa a informar por quais meios violou o aparelho, mas especula-se que o FBI tenha conseguido quebrar o código do aparelho, através da contratação de empresa israelense, especialista em recuperação de dados forenses. A empresa teria utilizado a técnica

---

[597] A rigor, a decisão judicial teria obrigado a Apple a projetar e assinar digitalmente *software* sob medida que ajudasse a desbloquear o iPhone 5C em questão. Em um movimento sem precedentes, a ordem exigia que a Apple criasse uma nova versão de seu sistema operacional com características de segurança intencionalmente enfraquecidas das quais o governo poderia se aproveitar para entrar no telefone. Em outras palavras, trata-se da criação de uma versão do sistema operacional com *backdoor*.CARDOZO, Nate. Lei e criptografia em 2016. **Actantes**, jan. 2017.Disponível em: <https://actantes.org.br/leis-e-criptografia-em-2016/>. Acesso em: 13 abr. 2018. É preciso esclarecer que, pelo que o aparelho da referida fabricante não possui a chave de acesso ao aparelho criptografada. Contudo, arquivos armazenados no aparelho são protegidos por critpografia, de modo que os níveis de criptografia apenas são desativados mediante a digitação da senha de acesso e, ainda assim, há a proteção adicional de apagamento do conteúdo caso haja muitas tentativas com a senha incorreta. Outrossim, como para atualizar o sistema operacional e remover a proteção da senha deveria haver uma atualização do sistema operacional, essa atualização vulnerável apenas poderia ocorrer com o envio da assinatura criptografada da Apple. Do contrário, o aparelho não aceitaria a atualização por não reconhecer a chave criptográfica. Portanto, vê-se que há no caso variadas aplicações da criptografia. Vide: APPLE. É assim que nós protegemos sua privacidade. Disponível em: https://www.apple.com/br/privacy/approach-to-privacy/. Acesso em 10/04/2018. Vide ainda ACTANTES. 7 motivos pelos quais a Apple não deve criar uma backdoor para o governo norte-americano. Disponível em: https://actantes.org.br/7-motivos-pelos-quais-a-apple-nao-deve-criar-uma-backdoor-para-o-governo-norte-americano/. Acesso em 10/04/2018.

[598] REDAÇÃO. Apple se nega a hackear iPhone de atirador de San Bernardino. **Época**, fev. 2016. Disponível em: <https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/apple-se-nega-hackear-iphone-de-atirador-de-san-bernardino.html>. Acesso em: 18 mar. 2018.

[599] KOPFSTEIN, Janus. É assim que o FBI destravará o iPhone de San Bernardino sem a ajuda da Apple. **Motherboard**, mar. 2016. Disponível em: <https://motherboard.vice.com/pt_br/article/kb34kz/e-assim-que-o-fbi-destravar-o-iphone-de-san-bernardino-sem-a-ajuda-da-apple>. Acesso em: 18 mar. 2018.

de espelhamento da memória NAND[600] do telefone em outro aparelho que não possuísse o dispositivo de segurança, de modo que as sucessivas tentativas não tenham implicado no bloqueio e apagamento da memória. Logo, a prática exitosa contradiz a afirmação anterior do FBI de que havia esgotado os meios para acessar o dispositivo, necessitando de colaboração da fabricante[601].. Há ainda a especulação que tenha havido a descoberta de alguma vulnerabilidade no sistema da Apple do qual a fabricante ainda não tenha ciência, capaz de transgredir o bloqueio criptográfico.

Contudo, o FBI faz questão de manter em sigilo o nome da empresa que realizou a quebra do dispositivo, bem como a técnica utilizada, provavelmente pois isso o permitirá repetir o feito em casos futuros, já que, em que pese haver encerrado o caso de San Bernardino, há no país inúmeras outras ações promovidas pelo FBI em face da Apple com vistas a obriga-la a criar uma chave mestra, em nome de investigar os mais variados crimes[602].

Em conclusão, tanto no caso das criptoguerras do final da década de 1980 e início dos anos noventa, como no caso de San Bernardino há alguns elementos comuns. Ambas as situações envolvem alguma medida necessária de segurança, seja repressiva, seja o regular andamento de investigação em curso. No caso de San Bernardino, evidencia-se o risco no qual se impõe a milhões de usuários que possuem o aparelho, sob o argumento falacioso de que não há nenhuma outra alternativa.

Do mesmo modo, parece não fazer sentido impedir a exportação da criptografia ou restringir sua circulação, na medida que isto apenas limita o acesso da população em geral a uma tecnologia essencial à proteção da privacidade do indivíduo. Por outro lado, grupos

---

[600] "(NAND mirroring). NAND é a memória usada no iPhone e o "espelhamento" dela é nada menos do que a cópia e restauração de dados por meio de uso de um equipamento especial de leitura e gravação.A primeira possibilidade é que o FBI "clonou" o chip de memória inteiro presente no iPhone de Farook e, a cada 10 tentativas incorretas, restaurou a cópia feita anteriormente, permitindo mais 10 tentativas. A segunda é que o FBI identificou os pontos modificados na memória NAND com cada tentativa e restaurou apenas as partes alteradas, retornando a NAND ao estado da primeira tentativa. Esse método é mais elegante e seria uma evolução do método do IP BOX usado no iOS 8" G1. **Como o FBI pode ter desbloqueado o iPhone sem a ajuda da Apple?**. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-o-fbi-pode-ter-desbloqueado-o-iphone-sem-ajuda-da-apple.html>. Acesso em 10 mar. 2018.

[601] CHAMY, Constanza Hola. Como o FBI conseguiu desbloquear o iPhone de suspeito de ataque à revelia da Apple. **BBC Brasil**, mar. 2016. Disponível em: <http://www.bbc.com/portuguese/noticias/2016/03/160330_fbi_apple_lab>. Acesso em: 18 mar. 2018.

[602] Há caso que o Departamento de Justiça em Nova Iorque requereu o acesso a um aparelho da Apple utilizado por um traficante de drogas. Cf. BARATA, Clara. O FBI entrou num iPhone, mas a guerra com a Apple não acabou. **Publico**, mar. 2016. Disponível em: <https://www.publico.pt/2016/03/29/tecnologia/noticia/fbi-desbloqueia-iphone-de-atacante-de-san-bernardino-e-poe-fim-a-conflito-com-a-apple-1727420>. Acesso em: 18 mar. 2018.

criminosos sempre conseguirão meios de acessar à tecnologia recente, a despeito da proibição da sua comercialização.

Em resumo, se pode dizer que, no final do século XXI, a aplicação da criptografia se deu predominantemente na encriptação de disco para mídia removível. Na última década, a principal aplicação da criptografia tem ocorrido em dispositivos móveis, tanto para criptografar o conteúdo do dispositivo, quanto para encriptar o conteúdo de mensagens trocadas entre dispositivos. Com a popularização da criptografia para estes dispositivos móveis, o uso da tecnologia enfrenta resistência e tentativas de banimento por parte de órgãos de investigação e governos dos mais variados espectros políticos.

Do breve retrospecto histórico que se fez, pode-se concluir que, embora esteja em constante evolução, a criptografia, seja ela artesanal ou informatizada, não se mostra como assunto inédito, sofrendo vez ou outra resistência de autoridades no que tange a sua utilização.

3.2 **Contexto, conceito, evolução**

A criptografia consiste no conjunto de técnicas de segurança da tecnologia da informação que realiza a cifragem do conteúdo da comunicação (encriptação), o que garante que somente as pontas da comunicação tenham acesso ao seu conteúdo. Em outras palavras, consiste no conjunto de técnicas empregadas para transmitir uma informação de um emissor a um receptor por meio de códigos secretos que impossibilitem sua compreensão por terceiros[603].

A se considerar a etimologia do termo, a criptografia provém do grego *kryptós* e *gráphein*, que significam respectivamente "escondido" e "escrita", ou seja, pode ser definida como a habilidade de ocultar o conteúdo da mensagem. A criptografia não envolve necessariamente ocultar a existência da mensagem em si, mas impedir que terceiros que tenham acesso à mensagem não consigam compreender seu conteúdo, vez que a cifragem garante um nível de segredo ao real conteúdo da mensagem[604].

---

[603] VIANA, Tulio Lima. **Transparência pública, opacidade privada**: o Direito como instrumento de limitação do poder na sociedade de controle. 2006. Dissertação (Mestrado em Direito) - Universidade Federal do Paraná, Curitiba, 2006, p. 151.

[604] *"El objeto de la criptografia no es ocultar la existencia de um mensaje, sino más bien ocultar su significado, um processo que se conoce como codificación"*. Livre tradução: "O objetivo da criptografia não é ocultar a existência de uma mensagem, mas sim ocultar seu significado, um processo conhecido como codificação". SGARRO, Andrea. **Codigos Secretos**. Madrid: Ediciones Parámide, 1990, p.20.

Essa é inclusive a diferença entre criptografia e a esteganofragia. Enquanto na primeira o conteúdo da mensagem é cifrado, impossibilitando o seu conhecimento, é possível que se saiba que há uma comunicação entre emissor e destinatário sem que se possa, contudo, compreender seu conteúdo vez que se encontra cifrado, seja fisicamente em uma sequência de letras que não faz sentido, seja digitalmente, quando o conjunto de códigos binários ficam embaralhados de tal modo que não se compreende o sentido de determinada mensagem[605].

A criptografia consiste no estudo de técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário. A criptografia é parte da criptologia, do grego *kriptos (oculto)* e *logos (ciência)* que consiste na ciência, no campo das ciências exatas, cujo objeto de estudo inclui tanto as técnicas de cifragem da mensagem – a criptografia – quanto as técnicas para decifrar mensagens criptografadas – a criptoanálise[606].

Por se tratar de garantia de segurança da informação, a criptografia visa garantir alguns atributos necessários a toda informação, quais sejam, a confidencialidade, a integridade, a autenticação e o não repúdio. A confidencialidade é o principal objetivo da criptografia. É o atributo da informação que mantém o seu conteúdo não acessível a todos, mas tão somente aos que estão autorizados a acessá-la.

A integridade visa impedir a alteração não autorizada dos dados. Para assegurar a integridade, faz-se necessário um sistema capaz de detectar manipulação de dados por partes não autorizadas. A manipulação de dados pode incluir condutas tais como inserir, apagar ou substituir a informação original.

A autenticação diz respeito à identificação, tanto da informação propriamente quanto das partes interlocutoras. A autenticação da informação ocorre por meio da identificação de sua origem, data de origem, conteúdo dos dados, momento do envio, entre outros. Neste ponto, a contribuição da criptografia é relevante, haja vista que a chave criptográfica de cada interlocutor garantirá a autenticidade das partes e das informações.

Por fim, o atributo do não repúdio ou irretratabilidade (não repúdio) consiste na impossibilidade de negar a autoria em relação a uma transação anteriormente feita, ou seja,

---

[605] Em resumo apertado, enquanto pela criptografia a mensagem é escrita em alguma forma de código, a esteganografia é a arte de esconder a mensagem. Combinada com a criptografia, pode incrementar em muito a segurança da comunicação, pois é possível primeiramente cifrar a mensagem e, depois, escondê-la em um arquivo inocente antes de ser remetida. Recebido o arquivo, o destinatário primeiro iria extrair dele a mensagem cifrada, para depois decifrá-la e lê-la. Com esta combinação, um intruso que interceptasse o arquivo - contendo uma simples imagem da natureza, por exemplo - sequer poderia desconfiar que uma mensagem cifrada está sendo enviada por seu intermédio. MARCACINI, Augusto Tavares Rosa. Op. cit., p. 59.

[606] MARCACINI, Augusto Tavares Rosa. Op. cit., p. 19.

nenhuma entidade pode negar qualquer operação que tenha feito em relação à informação, seja ela uma alteração ou uma simples consulta. Para tanto a criptografia assimétrica é essencial, na medida em que, autenticado o autor de determinada transação por meio verificação de compatibilidade das chaves, a autoria não poderá ser negada[607].

A criptografia, após longo processo de amadurecimento da tecnologia, pode ser classificada em simétrica e assimétrica. Antes de definir cada classificação, é preciso ressaltar que a criptografia em geral é definida por um critério ou fórmula de cifragem – que na era da tecnologia da informação pode ser chamada de algoritmo – bem como de uma chave ou senha. Apenas para se exemplificar, no caso da cifra de César, o critério ou a fórmula era a substituição de letras da mensagem por outras letras sequenciais do alfabeto. Já a chave era a segunda letra sequencial. De posse das informações do critério e chave seria possível decifrar qualquer mensagem cifrada com base na cifra de César[608].

A criptografia simétrica ou criptografia convencional pode ser definida como o modelo de cifragem que se utiliza de apenas uma chave tanto para cifrar quanto para decifrar o conteúdo[609]. Por esta razão, o modelo de criptografia simétrica exige que haja algum contato entre emissor e receptor para que um dos interlocutores tome conhecimento da chave utilizada, vez que ambos precisam combinar de forma segura a chave do método utilizado, sob pena de se inviabilizar a comunicação.

A cifra de César é um exemplo de criptografia simétrica, ou seja, é necessário que emissor e receptor tenham conhecimento da chave criptográfica e esta mesma chave será utilizada para cifrar e decifrar qualquer conteúdo. Decerto que o modelo simétrico sofre limitações quanto ao seu uso, embora tenha sido largamente utilizado até recentemente ser criado o modelo assimétrico.

A primeira delas é o fato de que o modelo apenas é aplicável caso haja um modo seguro de troca da chave e isso compromete de certo modo a confidencialidade da informação, vez que, qualquer um que tenha acesso à chave poderá cifrar ou decifrar a mensagem. Uma outra limitação é que o modelo não garante a demonstração da autenticidade perante terceiros, uma vez que apenas o destinatário da mensagem teria alguma certeza que a

---

[607] Sobre os atributos da informação e sua garantia pela criptografia, vide MENEZES, Alfred J.; OORSCHOT, Paul C. van.; VANSTONE, Scott A. (Eds.). **Handbook of applied cryptography**. New York: CRC Press Book, p.4.

[608] Ibidem, p. 27.

[609]OLIVEIRA, Ronielton Rezende. **Criptografia simétrica e assimétrica: os principais algoritmos de cifragem.** Disponível em: <https://pt.scribd.com/document/138463629/Principais-Algoritmos-de-Cifragem>. Acesso em: 20 abr. 2018.

mensagem é de autoria do emissor que possui a mesma chave, não podendo demonstrar isso inequivocamente. Do mesmo modo, ficaria comprometida a autenticidade perante o destinatário, vez que qualquer pessoa que por algum meio possua a chave pode cifrar uma mensagem no lugar do interlocutor, o que comprometeria também a integridade da informação.

Outra limitação que pode ser citada é a dificuldade de gerenciar as chaves da criptografia simétrica. Isso porque para a troca de dados com vários destinatários, deverá ser combinado previamente com cada um deles uma chave, a não ser que sejam todos pertencentes a um mesmo grupo que possam ter acesso a todas as informações encriptadas.

Ainda assim, haverá um sério comprometimento da confidencialidade e da autenticidade, já que, expandidos os usuários,haverá risco de vazamento da chave única, bem como da violação e alteração da mensagem por terceiros.Desta forma, o uso da criptografia simétrica é muito mais recomendado à cifragem de arquivos que não serão transmitidos – como é o caso da cifragem de mídias removíveis, como pen drives e HDs -vez que isto reduz a possibilidade de vazamento da chave.

As citadas limitações impulsionaram o desenvolvimento da criptografia assimétrica ou de chave pública. Por definição, a criptografia assimétrica se utiliza de duas chaves, uma para cifrar o conteúdo e outra para decifrá-lo.Deste modo, a criptografia assimétrica utiliza um par de chaves diferentes entre si, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra chave do mesmo par e cada chave desempenhe apenas uma das funções, sendo uma chave para cifrar e outra para decifrar o conteúdo[610].

As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. A chave pública pode ser conhecida pelo público em geral, enquanto que a chave privada somente deve ser de conhecimento de seu titular. Em outras palavras, a criptografia assimétrica é chamada de criptografia de chave pública porque o conteúdo é cifrado por uma chave criptográfica pública, disponível a todos, e decifrado por uma chave privada, de posse do destinatário. Portanto, cada usuário possui uma chave pública e outra privada.

---

[610] BRASIL. Supremo Tribunal Federal. Transcrição da audiência pública. ADI 5527 e ADPF 403. Marco Civil da Internet e bloqueio judicial do Whatsapp, p. 305, manifestação de Pablo de Camargo Cerdeira (Centro de Tecnologia e Sociedade da Escola de Direito da FGV-Rio). Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

Com efeito, determinado par de chaves pública e privada se relaciona mediante complexo cálculo matemático, de modo que uma chave funcione como contrassenha única da outra, ou seja, a chave privada em poder do destinatário apenas funcionará se for a única existente compatível com a chave pública de encriptação. É como se houvesse dois cadeados distintos a serem abertos para funções distintas, de cifrar ou decifrar, impedindo que quem possua apenas acesso à chave pública possa acessar o conteúdo criptografado, mediante a realização do caminho inverso.

Por outro lado, como na criptográfica simétrica a chave única, é possível se realizar o caminho inverso para realizar a decriptação, basta que se tenha conhecimento do algoritmo e da chave única que foi usada para cifragem. No caso da criptografia assimétrica, o uso da chave pública não permite decifrar o conteúdo, sequer pelo próprio emissor da mensagem, que apens possui a chave pública, usada para cifragem. Caso se utilize a chave pública sobre a mensagem cifrada o que ocorrerá é que a mensagem será cifrada mais uma vez, já que sua função é apenas de cifragem, assim como a chave privada apenas possui a função oposta[611].

Deve-se ressaltar ainda que as chaves não são transmitidas com o conteúdo cifrado, mas ficam armazenadas no dispositivo do usuário, o que garante maior segurança na confidencialidade da comunicação.

Portanto, conclui-se que o uso da criptografia assimétrica supera em muito as limitações da criptografia simétrica. Entre elas, além da maior confidencialidade, é possível garantir a autenticidade e integridade da comunicação. Tais atributos são garantidos porque, ao emitir determinada mensagem, o emissor a assina com sua chave privada e o receptor pode utilizar a chave pública do emissor para conferir se é compatível com a assinatura da chave privada. Se a chave privada pertence de fato ao par da chave pública do emissor, o sistema confirma sua assinatura. A integridade da comunicação é garantida, na medida em que é possível verificar a autenticidade do emissor, mediante a verificação de compatibilidade entre as chaves, o que impede que a mensagem seja adulterada antes de chegar ao destinatário. Esse é basicamente o funcionamento da criptografia assimétrica utilizado nos certificados digitais.

Ademais, na criptografia assimétrica não se faz necessária a comunicação prévia entre as partes para se acordar a chave da comunicação como ocorre no modelo simétrico. Isto porque cada interlocutor possui a respectiva chave privada que permite a decifragem de mensagens que foram cifradas com a correspondente chave pública. Desta forma, a criptografia assimétrica mostra-se ideal para as situações nas quais os interlocutores não

[611] MARCACINI, Augusto Tavares Rosa. Op. cit., p. 32.

tiveram ou não puderam travar nenhum contato prévio. Sua aplicabilidade mostra-se útil justamente em virtude da menor segurança que apresenta o modelo simétrico, tanto em relação à integridade, autenticidade ou confidencialidade. Tanto é assim que a criptografia assimétricase firmou como o modelo mais avançado de cifragem e é largamente utilizado na transmissão de dados, tendo se popularizado através dos aplicativos de troca de mensagens para dispositivos móveis como Telegram e WhatsApp.

Uma segunda classificação da criptografia a divide em criptografia forte ou fraca. A classificação leva em consideração o tamanho da chave criptográfica.

A linguagem de máquina é binária e utiliza a contagem em bits, ou seja, cada número, caracter ou informação é traduzida em uma sequência de algarismos "zero" ou "um" . O tamanho da senha ou chave é indicado em número de *bits*, ou seja, as chaves são números e a quantidade de *bits* indica quantos algarismos têm essas senhas em linguagem binária. Logo, uma chave com 8 bits poderia estabelecer uma senha entre 0 e 255 na representação decimal, vez que as possibilidades numéricas são calculadas a partir do código binário (0 ou 2) representada até a oitava potência (2^8). Por outro lado, uma chave com 128 bits, representaria uma senha que poderia ir do número 0 até 39 casas decimais (2^{128})[612].

Em 1999, após o lançamento de um desafio público, o esforço conjunto entre a *Electronic Frontier Foundation (EFF)* e a *Distributed.Net* conseguiu, em menos de 23 horas quebrar, ou no linguajar técnico craquear, a chave de 56 bits do algoritmo *Data Encryption Standard* (DES), que passou a ser entendido desde então como um modelo de criptografia fraca em virtude do tamanho de sua chave.

Desta forma, há algum consenso na comunidade científica de que a criptografia considerada fraca atualmente seria aquela de chave de até 58 bits para chaves simétricas; de até 512 bits para RSA, que é um tipo de criptografia de chave pública, e de até 112 bits para criptografias de curvas elípticas[613]. Esse é também o critério utilizado pelo governo dos Estados Unidos para definir que produtos que utilizam a criptografia podem ser exportados sem qualquer restrição, conforme se verá a seguir.

Por óbvio que o conceito de criptografia forte e fraca será sempre relativo e mutável na medida da evolução tecnológica, já que o critério para definir uma criptografia como forte

---

612 MARCACINI, Augusto Tavares Rosa. Op. cit., p. 48.

613 "Se hizo entonces una división en productos criptográficos fuertes y débiles; se en- tiende por débiles aquellos de clave simétrica de hasta 56 bits, productos rsa de hasta 512 bits y productos desarrollados por teoría de curvas elípticas de hasta 112 bits". CADAVID, Jhonny Antonio Pabón. Op. cit., p. 59.

é o grau de dificuldade para o seu craqueamento. Portanto, o que hoje é virtualmente inquebrável, em um futuro próximo poderá não o ser.

3.3 **Aplicabilidade e benefícios da criptografia**

Conforme visto no tópico antecedente, a criptografia integra a história da humanidade desde ao menos a Idade Antiga, a partir do momento em que surgiu a necessidade, por razões militares ou estratégicas, de ocultar o conteúdo de mensagens transmitidas.

Na era digital, a criptografia revela-se como uma das principais garantias de confidencialidade das novas tecnologias comunicativas e de informação, estando presente na maioria dos fluxos de dados trocados na rede.

A criptografia tem aplicabilidade das mais variadas na vida cotidiana. As transações financeiras em geral são criptografadas; o acesso do usuário ao internet banking ocorre através do protocolo de página segura https; as transações com cartão de crédito contam com um chip que possui chave criptografada; o sinal de TV a cabo criptografado apenas é decifrado após o uso da chave, constante do cartão de acesso do assinante; os aplicativos de conversa instantânea via web possuem criptografia fim-a-fim, o que garante que apenas as pontas da comunicação possam acessar seu conteúdo; os sistemas de assinatura digital também usam a criptografia para fornecer chave privada, que garante autenticidade da assinatura em documentos digitais, através da verificação de sua compatibilidade com a chave pública. Da mesma forma, arquivos sigilosos de natureza civil ou militar somente são transmitidos por meio de chave criptografada, em razão da elevada relevância e necessária confidencialidade de tais informações.

O exemplo mais consolidado de criptografia assimétrica ocorre na navegação por páginas que utilizam a criptografia para transmitir dados, nas quais os dados transmitidos possuem natureza de confidencialidade. A aplicação das páginas criptografadas pode ocorrer nos dados transmitidos através de um webmail, ou seja, o acesso de e-mail através do site[614]

[614] "Desde 2008 o Gmail já apresentava uma opção de sempre usar HTTPS — em outras palavras, criptografar tudo que trafega entre seu computador e os servidores do **Google** ao usar o Gmail. Desde essa quarta-feira (13) porém, isso deixa de ser apenas uma opção a ser ativada e passa a ser padrão para todos os usuários do **e-mail** do Google" . MACCARINI, Juarez Lencioni. O Gmail agora é todo criptografado. **Tecnoblog**, 2010. Disponível em: <https://tecnoblog.net/14260/o-gmail-agora-e-todo-criptografado/>. Acesso em: 10 abr. 2018.

ou nos sistemas de pagamentos eletrônicos, nos quais são colocados dados de cartão de crédito que precisam ser transmitidos através da rede com segurança[615].

É muito comum que o uso da criptografia assimétrica dos dadostransmitidos através do navegadorocorra por meio do protocolo “https:”, em vez do uso do protocolo “http”, mais comumente utilizado. Nos sites de instituições financeiras, por exemplo, a navegação é feita através do protocolo “https”. A letra “s”adicionada ao protocolo comum (*http*) é em referência à segurança da informação (*security*). Portanto, o protocolo httpsé utilizado para estabelecer uma conexão segura com o servidor através da criptografia. A segurança na transmissão á garantida pois o servidor da web do site que se está acessando envia ao navegador do usuário sua chave pública para que o servidor seja identificado através do certificado, bem como seja criptografado o conteúdo a ser enviado de modo seguro e apenas o servidor possa ter acesso ao seu conteúdo, mediante uso de sua chave privada[616]. Portanto, quando se trata de site que utiliza o citado protocolo, além do endereço do site se iniciar pelo termo https, aparece o símbolo de um cadeado para advertir de que aquela é uma transmissão que se realiza da maneira segura.

No tópico seguinte, serão tratados os casos mais relevantes de aplicações da criptografia.

3.3.1Criptografia e assinatura digital

Relevante aplicação da criptografia assimétrica ocorre na utilização de certificação digital de assinaturas. Com efeito, a assinatura digitalé resultado de complexas operações matemáticas para a criação de chaves, a partir dos algoritmos de criptografia. Anteriormente, havia se explicado que a criptografia assimétrica consiste no uso de chaves distintas, sendo a chave pública utilizada para criptografar o conteúdo e a chave privada para decifrá-lo.

No caso da assinatura digital, a utilização da criptografia assimétrica ocorre do modo inverso. Ao assinar digitalmente determinado documento ou mesmo ao autenticar-se em um site com o certificado digital, o titular da assinatura faz uso de um dispositivo - token ou cartão, por exemplo - que contém sua chave privada. Esta chave privada é enviada juntamente

---

[615] Conforme consta no site do PayPal quanto à criptografia de dados, "[p]roteger suas informações financeiras e pessoais é uma das prioridades mais importantes. Por este motivo, criptografamos automaticamente todas as informações confidenciais enviadas entre seu computador e nossos servidores”. Disponíel em: <https://www.paypal.com/pt/webapps/mpp/security/buy-dataencryption>. Acesso em: 10 mar. 2018.

[616] MARCACINI, Augusto Tavares Rosa. Op. cit., p. 37.

com o documento assinado e é verificada a sua compatibilidade através da chave pública daquele mesmo titular e, somente sendo compatível, a assinatura será autenticada. De modo simplificado, apenas o titular da assinatura pode assinar documentos digitais, tais como arquivos de texto, e-mails, fotos, vídeos, entre outros. Por outro lado, qualquer destinatário pode certificar-seda autenticidade de determinada assinatura, verificando se a assinatura do documento gerada pela chave privada é compatível com a chave pública do titular daquela assinatura.

A rigor, a chave privada não criptografa todo o conteúdo do documento assinado. O que ocorre é que a chave privada, ao gerar assinatura sobre determinado arquivo cria um resumo daquele arquivo assinado, uma vez que criptografar todo o arquivo demandaria uma assinatura excessivamente grande, proporcional à mensagem. Para tanto, utiliza-se uma *hash function*[617] ou função digestora que, aplicada sobre a mensagem assinada, gera um resumo singular do documento assinado, identificado por um número único de controle.

Com efeito, gerado o resumo da mensagem com a assinatura, qualquer alteração realizada no documento – seja ele um simples espaço entre duas palavras - gerará alteração de seu número de controle. Esse número de controle é único e não permiteadulterações não advertidas do documento assinado. Significa dizer que a assinatura digital fica vinculada ao documento eletrônico e, caso seja feita qualquer alteração no documento, a assinatura se torna inválida, vez que a *hash* será modificada. Portanto, a certificação digital permite não apenas verificar a autoria do documento, como também estabelece uma imutabilidade de seu conteúdo, o que garante a sua integridade e autenticidade[618].

Significa dizer que o próprio arquivo assinado compõe a assinatura, sendo o resumo da mensagem uma variável levada em consideração para a criação da assinatura de determinado documento. Portanto, tendo em conta essas variáveis, a assinatura eletrônica de uma mesma pessoa será sempre diferente, pois sempre carregará em si a vinculação de determinada assinatura a determinado arquivo assinado. O que é objeto da criptografia, portanto, é o

---

[617] "O hash é o conceito mais simples entre os que vamos abordar. Trata-se de uma função matemática aplicada sobre um conjunto de dados que gera outro número, este conhecido como hash. De forma bem simplista, pode ser equivalente a um dígito verificador. (...) A assinatura digital é um hash mais elaborado. Também consiste de uma função matemática aplicada sobre os dados de entrada – um arquivo, uma mensagem de texto, etc. Porém neste caso além de garantir que o conteúdo não foi alterado, também queremos garantir a autenticidade de quem o gerou. CARNEIRO, Luis Sergio F. Criptografia, Hash, Assinatura Digital: Qual a Diferença? **Matera**, fev. 2015. Disponível em: <http://matera.com/br/2015/02/27/criptografia-hash-assinatura-digital-qual-diferenca/>. Acesso em: 13 mar. 2018.

[618] CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA. Certificação Digital. **Instituto Nacional de Tecnologia da Informação**, jun. 2017. Disponível em: <http://www.iti.gov.br/perguntas-frequentes/41-perguntas-frequentes/112-sobre-certificacao-digital>. Acesso em 18 mar. 2018.

resumo da mensagem *(messages digest)* juntamente com a chave privada do usuário, gerando a assinatura digital.

Por essa razão, não será possível transpor a assinatura eletrônica de um individuo realizada em um documento para outro. A uma porque a *hash* utilizada para identificar determinado documento é um código único - e não é possível se realizar a operação de retorno para alterar o código criado pela chave privada, adulterando o documento assinado[619] - e a duas porque qualquer modificação do documento assinado invalida a assinatura que é única para determinado arquivo. A verificação da autenticidade da assinatura é possível pela verificação da compatibilidade matemática entre a chave privada que gerou a assinatura e a chave pública disponível a todos para a realização desta conferência.

Em suma, ao se submeter o documento assinado à chave pública será verificada a compatibilidade do código da assinatura gerada pela chave privada, o que assegurará a autenticidade da assinatura, bem como será calculada o resultado da *hash* sobre o arquivo transmitido, a fim de verificar sua conferência com a *hash* criptografada juntamente com a assinatura, a fim de assegurar que o arquivo transmitido é exatamente o arquivo cujo resumo foi criptografado.

O benefício do uso da criptografia nas assinaturas digitais é permitir que dois interlocutores que jamais tiveram contato prévio tenham assegurada a autenticidade de seus interlocutores, bem como a garantia de integridade do documento assinado.

3.3.2 Criptografia, as criptomoedas e a *Blockchain*

Decerto que a aplicação da criptografia que tem despertado mais interesse são as criptomoedas. As criptomoedas são moedas virtuais cuja segurança e autenticidade são garantidas por complexas operações de criptografia. Essas moedas podem ser recebidas e enviadas pela internet em transações financeiras das mais variadas, seja para adquirir um produto ou serviço, incluindo-se até mesmo a compra de um imóvel. Assim como a moeda tradicional as criptomoedas possuem um número de série. No caso, trata-se de um código criptografado que impede adulterações.

A grande vantagem apontada pelas criptomoedas é que se trata de um modelo que não se submete a nenhum sistema financeiro, tampouco necessita da intermediação de bancos ou

[619] Como a *hash function* é uma função matemática sem retorno (*one-way function*), não é possível realizar uma operação inversa para, a partir do "resumo da mensagem", chegar-se à mensagem que o produziu. MARCACINI, Augusto Tavares Rosa. Op. cit., p. 42.

estados para a sua operacionalização. Ademais, o uso da moeda é feito mediante sua aquisição para carteiras virtuais. Todavia, a identidade dos titulares destas carteiras é protegida por anonimato em operações que utilizam criptografia forte.

As moedas virtuais são geradas a partir de complexos cálculos matemáticos que demandam computadores potentes e um gasto elevado de energia elétrica, atividade conhecida como mineração de criptomoedas. Para tanto, os computadores possuem um software específico que geram novas moedas resolvendo fórmulas complexas.

A primeira e principal criptomoeda criada chama-se Bitcoin foi desenvolvida por alguém que utiliza o pseudônimo de Satoshi Nakamoto - que pode ser uma pessoa ou um grupo de programadores, vez que a identidade do criador do método é desconhecida[620].

Em 2008, o criador da Bitcoin divulgou um documento no qual detalhou como funcionaria sua moeda totalmente descentralizada baseada no sistema P2P (*peer-to-peer*). A rede P2P consiste em uma sistemática na qual todos os nós da rede funcionam ao mesmo tempo como cliente e como servidor, não havendo, portanto, uma autoridade central. O sistema P2P é muito utilizado para downloads de conteúdos pelos conhecidos *torrents*. O diferencial no sistema P2P é que cada terminal possui o mesmo nível de privilégio e toda e qualquer operação é transmitida a todos os nós da rede que o processam simultaneamente.

Para garantir a autenticidade das transações, as moedas virtuais em geral, entre elas o Bitcoin, o fazem por meio da *blockchain* – do literal – rede de blocos. A tecnologia *blockchain* faz uso da lógica do P2P, na medida em que cada transação realizada com Bitcoin, por exemplo, é disponibilizada e processada por cada nó da rede que verificará sua autenticidade para confirmar a transação. Chama-se processamento em blocos porque ocorre através do agrupamento de transações que integram um bloco criptografado, o qual, após verificadaa autenticidade das transações pela rede de computadores, é validada e constará no registro, sendo praticamente impossível sua adulteração. O processamento das transações é feito pelos chamados mineradores de dados que tanto descobrem novas moedas quanto autenticam transações e são recompensados com criptomoedas[621].

A *Blockchain* consiste em um sistema de autenticação distribuído por toda a rede. A rigor trata-se de um grande banco de dados separados em pedaços (blocos) cuja confiabilidade

---

[620] RICO.COM.VC O Que é Bitcoin e Como Funciona: Guia Atualizado. **Rico**, set. 2017. Disponível em: <https://blog.rico.com.vc/bitcoin-o-que-e>. Acesso em: 13 mar. 2018.

[621] GOMES, Helton Simões; LAPORTA, Taís. Entenda o que é blockchain, a tecnologia por trás do bitcoin. **G1**, fev. 2018. Disponível em: <https://g1.globo.com/economia/noticia/entenda-o-que-e-blockchain-a-tecnologia-por-tras-do-bitcoin.ghtml>. Acesso em: 13 mar. 2018.

é obtida por consenso entre os computadores da rede. Portanto, a certificação das operações financeiras da *Blockchain* não é centralizada na figura de um Estado ou de seu banco central, tampouco descentralizada como ocorre com instituições financeiras. Trata-se de um sistema de certificação por meio de consenso, cujo banco de dados está distribuído por todos os computadores da rede[622].*Por* se tratar de um banco de dados distribuído e protegido por criptografia, a autenticação por meio da tecnologia *blockchain* fica praticamente insuscetível a ataques e fraudes, vez que a operação constará de vários computadores da rede e apenas será validada se os cálculos matemáticos que representam a transação forem confirmadospor consenso, ou seja, pela maioria dos computadores que processam a operação.

Desta forma, aBlockchain constitui um protocolo de confiança que apenas registra a transação em um "livro-caixa" após a confirmação de sua autenticidade. Todavia, o banco de dados para verificação dessas transações não se concentra em um único terminal ou servidor, mas em todos os computadores da rede, o que dificulta ataques concentrados ou mesmo adulteração. ABlockchainé, portanto, uma espécie de cartório digital de transações, validadas em blocos e amplamente divulgadas e registradas em toda a rede.

Embora esteja acessível a toda a rede, as transações são identificadas por assinatura digital e fortemente criptografadas, o que garante preservaçãoda identidade das partes na operação, em que pese se verifique a autenticidade da transação em si. Logo, aBlockchain também contribui para a preservação da privacidade dos contratantes, mas não significa que se trate de uma operação que não possa ser rastreada, haja vista que as operações são replicadas em todos os nós descentralizados da rede.

Com efeito, as vantagens da utilização das criptomoedas e da*Blockchain* se confundem, podendo-se citar a agilidade na autenticação das transações em relação aos métodos tradicionais, a descentralização dos meios de pagamento, a menor possibilidade de fraudes e ataques, haja vista o processamento em rede, os menores custos gerados, a garantia de privacidade das operações, a transparência da autenticidade das operações e a possibilidade de um mercado global auto-regulado que não se submete às intempéries e decisões econômicas dos governos locais.

Todavia, Blockchain e criptomoedasnão são sinônimos, na medida em que a primeira consiste no sistema de autenticação e registro de transações que garante a livre circulação das criptomoedas, bem como certifica a quantidade de moeda que cada negociante possui.

---

[622]ITS RIO. **Como usar a Blockchain para promover o interesse público?** Disponível em: https://feed.itsrio.org/como-usar-a-blockchain-para-promover-o-interesse-publico

É certo que a razão de criação da Blockhain inicialmente esteve vinculada à certificação das transações realizadas com criptomoedas. Todavia, seu potencial de aplicação é muito maior.Tamanho caráter disruptivo da tecnologia que governos cogitam incorporar o modelo da Blockchaina seus sistemas oficiais de registros, garantindo maior segurança que o modelo tradicional[623]. Há quem afirma que o Blockchain possuium potencial revolucionário cujo impacto será muito maior nos países em desenvolvimento, especialmente para fins de registro de operações imobiliárias e para combater a volatilidade do câmbio[624]. No Brasil, a aplicação da Blockchain possui um campo fértil para potencializar a democracia, através da melhor viabilização de projetos leis de iniciativa popular,mediante a autenticação eletrônica da identidade dos eleitores com menores custos; para desburocratizar os registros públicos e sistemas notariais; e para tornar mais transparentes as doações eleitorais e processos licitatórios; bem como gerar certificados confiáveis para madeiras, auxiliando no combate ao desmatamento[625]. No que tange às criptomoedas, o mercado tem despertado interesse pelo modelo, a ponto de se iniciar a negociação das criptomoedas em bolsa de valores como um ativo[626]. Há ainda quem preveja que o Bitcoin pode se tornar uma moeda global legítima[627], a exemplo do dólar.

Verifica-se, portanto, que a criptografia permeia tanto a lógica do *Blockchain*, protegendo as transações de ataques maliciosos, quanto as moedas virtuais, fornecendo identidade virtual criptografada, a partir de complexos cálculos matemáticos que executam algoritmos de verificação[628].Portanto, considerando que o grande diferencial das criptomoedas e da tecnologia *blockchain*é a confiança e a segurança das operações, tais tecnologias apresentam a contribuição do uso da criptografia para além das transações bancárias

---

[623] CRIPTOMOEDAS FÁCIL. **Japão estuda o uso de Blockchain para registros imobiliários**

https://www.criptomoedasfacil.com/japao-estuda-o-uso-de-blockchain-para-registros-imobiliarios/

[624]WILLIAMS-GRUT, Oscar. Forget the West — blockchain will have the biggest impact in emerging markets. Disponível em http://www.businessinsider.com/exotix-impact-of-blockchain-in-developing-markets-2018. Acesso em 10/04/2018

[625] ITS RIO. **Como usar a Blockchain para promover o interesse público?** Disponível em: https://feed.itsrio.org/como-usar-a-blockchain-para-promover-o-interesse-publico

[626] ROBEIRO, Rafael de Souza. Bitcoin dispara após bolsa de Chicago confirmar lançamento de contratos futuros da moeda. **InfoMoney**, dez. 2017. Disponível em: <http://www.infomoney.com.br/mercados/bitcoin/noticia/7119990/bitcoin-dispara-apos-bolsa-chicago-confirmar-lancamento-contratos-futuros-moeda>. Acesso em: 13 mar. 2018.

[627] BUSINESS INSIDER. Bitcoin can become a legit global currency — in theory, Goldman says. Disponível em: http://www.businessinsider.com/bitcoin-as-money-faces-problems-goldman-sachs-says-2018. Acesso em 10/04/2018.

[628]CIO.COM. Blockchain: o que é e como funciona. **ComputerWorld**, jun. 2016. Disponível em: <http://computerworld.com.br/blockchain-o-que-e-e-como-funciona>. Acesso em: 13 mar. 2018.

tradicionais, demonstrando que, quanto mais forte a proteção criptográfica, mais seguras serão as transações financeiras e a confiabilidade social.

3.3.3 Criptografia fim-a-fim nos aplicativos de mensagem

Outra inovadora –e não menos polêmica - aplicação da criptografia se dá nos aplicativos de mensagem instantânea, utilizado em dispositivos móveis ou mesmo na versão web, estando entre os mais conhecidos o WhatsApp, o Telegram e o Signal. De acordo com os termos de uso de ambos os dispositivos[629] as mensagens trocadas no aplicativo são criptografadas, com o diferencial que as mensagens trocadas no Telegram não são criptografadas por padrão, havendo a funcionalidade apenas no chamado "chat secreto"[630]. Outrossim, o Signal constitui-se em aplicativo de mensagens criptografadas de código aberto, com algumas funcionalidades diferenciais, tais como a de trocar as chaves de sessão, mesmo quando a mensagem enviada não é respondida; a possibilidade de impedir captura de tela; a possibilidade de senhas para certas conversas; e uma criptografia de extremo a extremo, segundo alguns especialistas, o que dificultaria ainda mais a sua violação em relação aos outros modelos[631].

Um ponto comum entre os aplicativos citados é que todos eles utilizam a criptografia ponta-a-ponta que, de forma resumida, consiste na integração entre criptografia simétrica e assimétrica, com vistas a garantir que apenas as pontas de uma comunicação, ou seja, emissor e destinatário tenham acesso a determinada mensagem, impossibilitando a sua interceptação por terceiros.

Entre os aplicativos citados, embora todos em geral tenham funcionamento semelhante, se utilizará o WhatsApp para explicitar o funcionamento da criptografia ponta a ponta ou fim a fim, do inglês, *end-to-end*. Ressalte-se que o aplicativo WhatsApp utiliza, na

---

[629] No site do WhatsApp constam algumas informações legais sobre o aplicativo. Confira: "Suas mensagens são suas e nós não podemos lê-las. Implementamos privacidade, criptografia de ponta-a-ponta e outras ferramentas de segurança no WhatsApp. Nós não mantemos suas mensagens após o envio das mesmas. Quando elas estão criptografadas de ponta a ponta, nós e terceiros, não podemos lê-las de maneira alguma." Disponível em: <https://www.whatsapp.com/legal/?l=pt_br#key-updates>. Acesso em: 14 mar. 2018.

[630] Confira uma das perguntas frequentes do site e sua respectiva resposta: "P: E se eu for mais paranóico que um usuário comum? Pensamos em você. Os chats secretos especiais do Telegram utilizam criptografia ponta-a-ponta, não deixam rastros em nossos servidores, possuem mensagens auto-destrutivas e não permitem encaminhamento para outros usuários. A única coisa que os chats secretos não possuem é armazenamento na nuvem — eles só podem ser acessados em seus dispositivos de origem. Disponível em: <https://telegram.org/faq/br#p-quo-seguro-o-telegram>. Acesso em: 20 mar. 2018.

[631] BBC. Como funciona o App 'ultrasseguro' de mensagens usado por Snowden. **BBC Brasil**, nov. 2016. Disponível em: <http://www.bbc.com/portuguese/geral-37821449>. Acesso em: 18 mar. 2018.

criptografia de seus serviços, o protocolo Signal[632], que consiste em código-fonte aberto, permitindo a qualquer um a utilização do referido protocolo para criar um aplicativo de troca de mensagens com a mesma segurança.

Portanto, a criptografia ponta a ponta implementada pelo protocolo Signal combina utilizações de criptografia simétrica e assimétrica conforme se explicitará. Cabe lembrar que, na criptografia assimétrica há a utilização de duas chaves, uma pública e outra privada, com funções distintas. Enquanto a chave pública serve apenas para cifrar o conteúdo, a chave privada apenas servirá para decifrá-lo. Esta é uma vantagem em relação à criptografia simétrica, na qual a chave para codificar e decodificar é única, o que cria riscos à confidencialidade da troca de mensagens.

Ao instalar oWhatsApp em um dispositivo móvel, o aplicativo cria um par de chaves pública e privada, compatíveis entre si - vinculada ao número de celular que instalou o aplicativo. A compatibilidade das chaves é criada por meio de complexos cálculos matemáticos. Desta forma, todos os usuários podem ter acesso à chave pública criptografar e enviar mensagens a determinado usuário, o que é feito de modo automático pelo aplicativo. Todavia, o conteúdo da mensagem apenas será acessado pelo destinatário da mensagem que possui a chave privada armazenada tão somente em seu aparelho e não é transmitida durante o processo comunicativo.

Iniciada uma conversa entre dois usuários, o aplicativo cria uma chave de sessão *(session key)*, que consiste em uma chave simétrica, gerada aleatoriamente, que se modifica frequentemente ao longo da conversa. A chave de sessão criptografa a mensagem a ser transmitida. Após isso, é aplicada a criptografia assimétrica, ou seja, a chave de sessão é criptografada com a chave pública do destinatário. Isso significa que apenas o destinatário poderá, por meio da sua chave privada, ter acesso à chave de criptografia simétrica que cifrou o conteúdo da mensagem.

O citado procedimento é realizado para cada mensagem individualmente, dificultando o acesso ao seu conteúdo. Em suma, a garantia de sigilo da comunicação, através da criptografia ponta a ponta, ocorre com a aplicação de técnicas de criptografia simétrica -

---

[632]STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do Whatsapp, p. 240. Manifestação de Dennys Marcelo Antonialli (Associação Internetlab de Pesquisa em Direito e Tecnologia). Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

chave única, para a chave de sessão – e assimétrica – chave pública e privada com funções distintas[633].

Disto decorre a noção de túnel criptográfico, ou seja, as mensagens são trocadas através de um túnel cuja inviolabilidade é garantida por dupla criptografia, apenas descriptografada pela chave privada de posse do destinatário. O centro do aplicativo apenas é responsável por permitir a troca de chaves entre os usuários e a mensagem criptografada, não possuindo acesso ao conteúdo da mensagem, transmitida pelo túnel criptográfico[634]. Outrossim, caso o par de chaves pública e privada seja substituído, com vistas a viabilizar a visualização da mensagem por terceira pessoa, é permitido ao usuário conferir se a chave utilizada para criptografar a mensagem é compatível com a sua chave do dispositivo, possibilitando que se percebam eventuais fraudes.

O uso da criptografia ponta a ponta em dispositivos móveis, que até o presente momento tem apresentado segurança superior aos outros modelos, e, em que pese garantir a privacidade dos interlocutores, tem gerado reações contrárias ao seu uso, seja no sentido de descrença de que a tecnologia seja mesmo inviolável[635], seja no sentido de exigir que se criem hipóteses de vulnerabilidade que garantam acesso ao conteúdo das mensagens, ainda que restrito a autoridades.

3.4 **Criptografia e bloqueio judiciais de aplicativos: há fundamento no Marco Civil da Internet? Um debate ainda em curso na ADPF 403 e ADI 5572.**

No Brasil, a utilização de aplicativos de troca de mensagem que utilizam criptografia ponta a ponta tem sofrido dura repressão judicial, seja através da imposição de multas coercitivas,prisão dos representantes da empresa no país ou mesmo suspendendo o funcionamento da aplicação, em razão da alegada impossibilidade de interceptação do conteúdo das mensagens. Em que pese a inviolabilidade do conteúdo transmitido constituir característica essencial deste modelo de criptografia, não é raro que tal alegação seja

---

633 MARCACINI, Augusto Tavares Rosa. Op. cit., p. 59.

634 Informações prestadas por Brian Acton, co-fundador do aplicativo de mensagens WhatsApp em audiência pública realizada no Supremo Tribunal Federal. STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do Whatsapp, p. 39.Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

635 ÉPOCA NEGÓCIOS. WhatsApp tem vulnerabilidade que permite interceptar mensagens, diz jornal. **Época Negócios**, jan. 2017. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2017/01/whatsapp-tem-vulnerabilidade-que-permite-interceptar-mensagens-diz-jornal.html>. Acesso em: 13 abr. 2018.

interpretada pelo Poder Judiciário como desobediência injustificada à decisão judicial, o que tem ocasionadoas consequências citadas.

Pode-se citar como exemplo duas decisões judiciais. A primeira delas foi tomada pela 2ª Vara Criminal da Comarca de Duque de Caxias, no Rio de Janeiro, em 19 de julho de 2016[636], que determinou suspensão do funcionamento do aplicativo WhatsApp, bem como a imposição de multa até o efetivo cumprimento da decisão de interceptação do fluxo de dados do aplicativo.

Outra decisão no mesmo sentido, foi tomada pelo juízo da Vara Criminal de Lagarto, município de Sergipe, de 2 de maio de 2016, que determinou que as operadoras de telefonia fixa e móvel bloqueassem o aplicativo WhatsApp por 72 horas[637]. O mesmo juízo havia determinado a prisão do vice-presidente do Facebook na América Latina, no mês anterior do mesmo ano. Embora ambas as decisões tenham sido cassadas[638], a prática reacende o debate sobre a constitucionalidade da suspensão dos serviços de aplicações da internet por descumprimento de decisão judicial, podendo-se noticiar medidas semelhantes nos estados do Piauí[639] e São Paulo[640], entre outros entes da federação.

A decisão do juízo da Comarca de Lagarto/SE motivou a propositura da Ação de Descumprimento de Preceito Fundamental nº 403, perante o Supremo Tribunal Federal, pelo Partido Popular Socialista, cujo objeto era liminarmente a suspensão da decisão de bloqueio do aplicativo pelo juízo de Sergipe e, no mérito, reconhecer a existência de violação ao preceito fundamental da liberdade de comunicação, nos termos do art. 5º, inciso IX, com a

---

636 TJ-RJ. Poder Judiciário do Estado do Rio De Janeiro.2ª Vara Criminal Da Comarca De Duque De Caxias. Veja decisão da lavra da juíza de direito Daniela Barbosa Assumpção de Souza na íntegra: http://www.omci.org.br/m/jurisprudencias/arquivos/2016/rj_062001642016_19072016.pdf. Acesso em 10/03/2018.

637 ROVER, Tadeu. Juiz determina bloqueio do WhatsApp a partir das 14h desta segunda. **Consultor Jurídico**, mai. 2016. Disponível em: <https://www.conjur.com.br/2016-mai-02/juiz-determina-bloqueio-whatsapp-partir-14h-segunda>. Acesso em: 17 mar. 2018.

638CONJUR. Decisão que suspendia WhatsApp em todo o Brasil é derrubada no TJ-PI. **Consultor Jurídico**, fev. 2015. Disponível em: <https://www.conjur.com.br/2015-fev-26/decisao-suspendia-whatsapp-brasil-derrubada-tj-pi>. Acesso em: 19 mar. 2018.

639 Em fevereiro de 2015, o juízo da Central de Inquéritos de Teresina/PI, no bojo da ação n. 0013872-87.2014.8.18.0140 determinou a interrupção dos serviços do referido aplicativo. Posteriormente, tal decisão foi suspensa liminarmente pelo Eg. Tribunal de Justiça do Piauí no Mandado de Segurança n. 2015.0001.001592-4. Ibidem.

640 Em dezembro de 2015, o juízo da 1ª Vara Criminal da Comarca de São Bernardo do Campo/SP, no bojo do procedimento de Interceptação Telefônica nº. 0017520-08.2015.8.26.0564, determinou a suspensão temporária das atividades do WhatsApp pelo prazo de 48 (quarenta e oito) horas em todo o território nacional. Contudo, tal decisão foi cassada por decisão liminar proferida pelo Eg. Tribunal de Justiça do Estado de São Paulo nos autos do Mandado de Segurança nº. 2271462-77.2015.8.26.0000. Vide Ibidem.

finalidade de não mais haver suspensão do aplicativo de mensagens WhatsApp por qualquer decisão judicial.

Os bloqueios por todo o país também motivaram a propositura da Ação Direta de Inconstitucionalidade, proposta pelo Partido da República, que requer, liminarmente, a suspensão dos dispositivos do Marco Civil da Internet e no mérito a declaração da inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14[641] - ou subsidiariamente a sua declaração de nulidade parcial sem redução de texto ou mesmo a interpretação conforme do dispositivo[642] - bem como a interpretação conforme do art. 10, §2º[643], a fim de que seja limitado o seu alcance aos casos de persecução criminal.

O questionamento de dispositivos do Marco Civil da Internet na ação de controle abstrato supracitada, deve-se ao fato de a maioria das recentes decisões judiciais que determinaram o bloqueio do aplicativo no Brasil tenham invocado como fundamento as sanções previstas no art. 12 da referida lei, entre elas a previsão de suspensão ou mesmo a proibição do exercício das atividades.

Todavia, a interpretação sistemática do dispositivo citado apenas possibilita a suspensão quando cometidas algumas condutas ali previstas, que atentem contra a privacidade, a proteção de dados pessoais e o sigilo das comunicações e registros, ou seja, as condutas descritas nos artigos 10 e 11 da mesma lei. O que o juízo que determinou a suspensão solicitava era justamente a quebra dos sigilos resguardados pelo Marco Civil. Certo é que em um Estado Democrático de Direito todos os indivíduos devem cumprir decisões judiciais e colaborar com investigações criminais, ocorre que a decisão judicial em questão, ao contrário de se fundamentar no Marco Civil, contraria seus ditames, ao estabelecer a

---

[641] Art. 12, *caput* e incisos da Lei n° 12.965/14.

[642] O pedido de nulidade parcial sem redução de texto das sanções de suspensão e de proibição da atividade visa afastar a sua aplicação aos aplicativos de troca de mensagens virtual; ou, por último, que se dê interpretação conforme a tais dispositivos, condicionando-se, em consequência, a aplicação das sanções de suspensão temporária e de proibição do exercício das atividades somente após as sanções previstas no art. 12, I e II, mostrarem-se frustradas. Segundo Gilmar Ferreira Mendes, a nulidade parcial sem redução de texto se aplica aos "casos de inconstitucionalidade da aplicação da lei a determinado grupo de pessoas ou de situações". Portanto, se "se pretende ressaltar que determinada aplicação do texto normativo é inconstitucional, dispõe o Tribunal da *declaração de inconstitucionalidade sem redução de texto*, que, além de mostrar-se tecnicamente adequada para essas situações tem a virtude de ser dotada de maior clareza e segurança jurídica, expressas na parte dispositiva da decisão". No nosso entender, a diferença é que no caso da interpretação conforme, entre as múltiplas interpretações de um texto normativo, exclui-se aquele que se entende incompatível com a Constituição da República. MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2008, pp. 1248 e 1253.

[643]Lei n° 12.965/14, art. 10 (...),"§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º."

suspensão quando a hipótese de suspensão do aplicativo é estrita para os casos de violação à privacidade.

Ademais, ainda que se entendesse cabível a suspensão para todo e qualquer caso de descumprimento de decisão judicial, se mostraria a decisão desproporcional, haja vista que o Marco Civil da Internet foi editado para proteger o usuário e não para inviabilizar o uso das funcionalidades da rede. Tanto é assim que a sanção mais gravosa no âmbito do marco civil é a suspensão das atividades. Ressalte-se que uma decisão desta natureza, ao tempo em que sanciona uma companhia, prejudica milhões de usuários do serviço de troca de mensagens, os quais não possuem nenhuma relação com a conduta ilícita. Ora, o alcance de um aplicativo como o WhatsApp, que comparativamente é o mais popular no país, é da ordem de 120 milhões de aparelhos[644], o que demonstra um amplo alcance da população, de modo que o uso do aplicativo se mostra essencial.

Com efeito, as decisões judiciais determinando a suspensão do aplicativo foram em virtude do não fornecimento de conteúdo das conversas por parte do aplicativo. Todavia, os gestores dos aplicativos de mensagens instantâneas afirmam não poder acessar o conteúdo das mensagens por estarem protegidas por chaves de criptografia, às quais sequer o próprio aplicativo pode acessar.

Ora, o Marco Civil da Internet não impõe como obrigação o registro e arquivamento do conteúdo das mensagens, impondo-se apenas a guarda temporária dos registros de acesso e ainda assim pelo prazo máximo de seis meses[645], salvo se houver solicitação de autoridade administrativa ou Ministério Público para extensão do período de guarda. Logo, se não há obrigação legal em se manter arquivado o conteúdo da conversa, ainda que criptografado, como se exigir judicialmente, sob pena de suspensão das atividades este conteúdo?

---

644 REDAÇÃO. WhatsApp chega a 120 milhões de usuários no Brasil. **Estadão**, mai. 2017. Disponível em: <http://link.estadao.com.br/noticias/empresas,whatsapp-chega-a-120-milhoes-de-usuarios-no-brasil,70001817647>. Acesso em: 19 mar. 2018.

645 Art. 15 "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. § 1o Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. § 2o A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13. § 3o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 4o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência".

Ademais, as condutas mencionadas nos artigos 10 e 11 que ensejariam a suspensão do aplicativo não possui em seu rol o descumprimento de decisão judicial, e, portanto, isso não poderiam ser invocados como fundamento de medida tão gravosa como a suspensão do funcionamento da aplicação. Os dispositivos tratam apenas da necessidade de observação da legislação brasileira na guarda dos registros de conexão, de acesso à aplicação e de conteúdo das comunicações[646]. Todavia, os dispositivos têm por preocupação vedar que seja violada a privacidade dos usuários, ou seja, quando trata de guarda de conteúdo de comunicação impõe justamente o dever de observar a privacidade, tanto é assim que se exige ordem judicial para a disponibilização destas informações. No entanto, sequer há obrigação legal de guarda do conteúdo em si das comunicações, de modo que esta obrigação não pode ser inferida de nenhum dispositivo, já que o marco civil visa proteger o usuário e sua privacidade e não os interesses estatais. Tanto é assim que a seção na qual se inserem os artigos citados trata da "Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", o que deixa evidente a teleologia do dispositivo.

Deste modo, respondendo de forma objetiva, as sanções previstas no marco civil da internet não são aplicáveis às hipóteses de não fornecimento de conteúdo protegido por criptografia ponta a ponta. Outrossim, não se mostra incompatível com o marco civil da internet o modelo de comunicação que envolva este tipo de criptografia, já que o marco normativo tem por objetivo justamente proteger os direitos e garantias fundamentais do usuário na rede, entre eles a privacidade.

O conflito entre a democratização da criptografia ponta a ponta e o interesse das investigações criminais é um debate sem resposta sobre o qual este trabalho visa se debruçar. Decerto que não há como se estabelecer aprioristicamente a prevalência de qualquer dos

---

[646] Art. 10. "A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros".

interesses constitucionais em conflito. Não há dúvidas que a segurança pública, o combate ao racismo, a proteção à integridade sexual e moral de crianças e adolescentes – em outras palavras, o combate à pedofilia - e a investigação de outros crimes tais como os financeiros, assassinatos e sequestros é interesse de toda a sociedade e tem fundamento constitucional.

Por outro lado, diante da inegável capacidade de vigilância estatal e privada, que o atual quadro tecnológico permite, praticada de modo direcionado ou geral, também se mostra de elevada relevância a garantia da privacidade dos indivíduos face a monitoramentos invasivos que tenham por consequência calar discursos e limitar a liberdade de autoconformação.

Nessa perspectiva, no âmbito da ADPF 403 e da ADI 5572 foi realizada Audiência Pública da qual participaram órgãos de persecução penal e investigação criminal, bem como setores ligados ao estudo da tecnologia e entidades de defesa de direitos na esfera digital. Embora tenha havido uma contundente defesa por parte dos órgãos de investigação da necessidade de fornecimento de mensagens criptografadas em nome do necessário combate ao crime, setores de tecnologia e de defesa de direitos na internet foram assertivos de que qualquer vulnerabilidade em sistemas de segurança enfraquecem a segurança de todo o sistema.

Embora o tema das ações direta versem mais sobre bloqueio de aplicativos que utilizam a criptografia, a discussão parece ainda prematura e de necessário amadurecimento. Ademais, qualquer decisão que seja tomada pelo Supremo Tribunal Federal deverá levar em conta o pressuposto da essencialidade da criptografia para a garantia da privacidade e de outros direitos correlatos e de que a vigilância é uma ameaça concreta à liberdade de expressão e ao livre desenvolvimento da personalidade, bem como pode ser um instrumento de perseguição política, religiosa e com fins econômicos.

O objeto central deste capítulo é discutir a constitucionalidade do modelo de negócios que envolva a comunicação garantida por um sistema criptográfico fim a fim que seja inviolável pelo próprio criador do aplicativo e suas implicações diante dos anseios por segurança face às ameaças do presente século.

3.5 **Privacidade e liberdade de expressão: do caráter instrumental da criptografia e do anonimato**

No primeiro capítulo, restou demonstrado o quanto a privacidade é essencial a outras liberdades, tais como a autonomia pessoal, a liberdade de expressão, a liberdade de

participação política, entre outras. Da mesma forma, na era digital, a criptografia e o anonimato mostram-se essenciais à garantia da privacidade e, indiretamente, à liberdade de opinião e de expressão.

A criptografia, responsável por garantir a confidencialidade de comunicações, de arquivos armazenados em dispositivos, de mensagens trocadas por e-mail ou mesmo de chamadas de voz realizadas pela internet, constitui poderoso instrumento de resistência à vigilância estatal e privada, seja direcionada ou não.

Com a popularização da criptografia, disponibilizando-se ao livre acesso os códigos-fonte de criptografia de chave pública ou mesmo com o advento de aplicações que utilizam a criptografia assimétrica para criptografar as comunicações, a criptografia passa a ser uma funcionalidade à disposição de todos, permitindo-se que opiniões e informações permaneçam a salvo da vigilância massiva.

Enquanto a criptografia garante a confidencialidade da informação, seja ela armazenada em dispositivos ou trocada em atividade de comunicação, o anonimato garantirá a livre expressão do indivíduo, independente de constrangimentos ou sem a obrigação de identificação. Neste sentido, o relator especial sobre promoção e proteção da liberdade de expressão da ONU emitiu relatório no sentido de que a criptografia e o anonimato são essenciais à liberdade de expressão[647]. Para o relator, criptografia e anonimato, juntos ou separados, são responsáveis por criar uma zona de privacidade para proteger opiniões e crenças.

Isso porque a vigilância tem a capacidade de influenciar mais sensivelmente os grupos mais vulneráveis e os que possuem opiniões minoritárias. Logo, a criptografia permite que cada um possa ter e formar a própria opinião sobre um tema, sem constrangimento de terceiros. A criptografia e o anonimato são particularmente importantes em ambientes de hostilidade política, social, religiosa e jurídica. Logo, a conjugação da garantia da criptografia e do anonimato propiciam empoderamento de indivíduos para romper barreiras impostas por governos opressores e acessar informações e ideias antes proibidas, caso tenham a segurança de que não estejam sendo monitorados[648].

O relatório repudia ainda qualquer tentativa de enfraquecimento por parte dos estados da criptografia. Adverte que com a criação de vulnerabilidades ou a concessão de acessos

---

[647] KAYE, David. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/29/32). **Human Rights Council**, maio de 2015. Disponível em: <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>. Acesso em: 10 abr. 2018.

[648] KAYE, David. Op. cit., p. 5.

especiais às autoridades investigativas, a vulnerabilidade criada também estará exposta a pessoas não tão bem intencionadas e que possuam expertise para explorar pontos fracos dos sistemas de segurança da informação. Portanto, a criptografia que é enfraquecida enfraquece também a confidencialidade das comunicações como um todo, não havendo nenhuma garantia que a chave mestra ou porta dos fundos disponibilizada aos governos será utilizada apenas por este, vez que o sistema, uma vez vulnerável, é vulnerável para todos[649].

Ademais, ainda que se apresente o argumento de que a criptografia pode permitir a confidencialidade de atividades ilícitas tais como tráfico de drogas, terrorismo, crime organizado, pornografia infantil, entre outros, deve-se lembrar que a atividade criminosa também é realizada na vida offline e o seu cometimento online é apenas um reflexo disso. Portanto, limitar ou enfraquecer a criptografia seria o mesmo que impedir o uso de estradas porque criminosos a usariam para realizar atividades ilícitas. O equívoco estaria em inviabilizar o meio em sim que nada possui de ilícito, em vez de distinguir o meio utilizado da atividade criminosa em si. Não custa lembrar que as mesmas ferramentas criptográficas utilizadas por criminosos para atividades ilícitas também são utilizadas por estados, empresas e autoridades de segurança para garantir a confidencialidade da comunicação na condução das investigações, do trânsito de informações econômicas estratégicas, das comunicações diplomáticas, entre outros. Do mesmo modo, fará uso da tecnologia membros de grupos vulneráveis ou minoritários como único meio hábil a garantir sua privacidade diante de seus perseguidores que em geral possuem poder econômico, aparatos de vigilância e comandam a máquina estatal.

O relatório condena também tentativas de impor o enfraquecimento da criptografia ou mesmo a imposição de fornecimento de chaves mestras ou porta dos fundos (*backdoor*) por meio de lei. Para relator da ONU, qualquer restrição legal à criptografia e ao anonimato, deve observar o teste de três etapas, quais sejam: (i) qualquer limitação à liberdade de expressão deve ser prevista em lei, que siga o devido processo legislativo; (ii) deve ser imposto com fins legítimos; e (iii) deve passar pelo crivo do que chama de necessidade e proporcionalidade[650].

Quanto à necessidade de previsão legal implica dizer que a lei deve ser precisa, pública e transparente e não deve recorrer à conceitos jurídicos indeterminados ou fundamentar-se na discricionariedade da autoridade para impor limitações à criptografia e anonimato. A legislação deve ser submetida à livre deliberação democrática e seguir o regular

[649] Ibidem, p. 4.

[650] Ibidem, p. 11.

processo legislativo, bem como a restrição deve ser determinada por autoridade judicial ou outra autoridade independente.

No que tange ao segundo teste, a restrição apenas pode estar baseada em legítimos interesses, tais como direito ou reputação de terceiros, segurança nacional, ordem pública ou saúde pública. Ademais, mesmo que os legítimos interesses sejam invocados, não podem servir de pretexto para alcançar propósitos ilegítimos ocultos, vez que tal prática configuraria desvio de finalidade. Aqui cabe uma crítica, principalmente no Brasil que atravessou longo regime de exceção, durante a ditadura militar e cuja tradição democrática carece de maior consolidação. Conceitos como segurança nacional[651], ordem pública ou paz social sempre foram invocados na tradição autoritária brasileira com vistas a ocultar perseguições e arbitrariedades, de modo que as restrições a tecnologias tão caras à privacidade e à liberdade de expressão, caso ocorram, devem ser fundamentadas em interesses presentes no caso concreto, sendo vedado o recurso a conceitos jurídicos indeterminados cujo conteúdo fica ao sabor do intérprete, que, na maioria das vezes, será a autoridade da ocasião.

O terceiro teste consiste na necessidade e proporcionalidade. A necessidade impõe que a medida restritiva seja realmente necessária, não bastando que a medida seja tão somente útil, desejável, mas deve ser realmente imprescindível[652]. Ademais, a proporcionalidade é verificada através do tradicional teste de proporcionalidade criado pela doutrina alemã já tratado neste trabalho. A medida restritiva deve ser adequada ao objetivo que se quer alcançar; deve ser a menos onerosa possível ao direito que se restringe; bem como deve ser proporcional, no sentido de os benefícios advindos devem justificar as restrições impostas.

O relatório repele ainda qualquer prática estatal no sentido de banir, controlar ou mesmo enfraquecer a criptografia, como ocorre nos casos de exigir uma “porta dos fundos” para acesso estatal;de tornar ilegal a criptografia para uso individual;de impor que as chaves

---

[651] Basta lembrar que a Lei de Segurança Nacional, presente no ordenamento jurídico brasileiro desde 1935, foi o principal fundamento dos governos militares para a prática de atos violadores de garantias individuais e antidemocráticos, a partir da formulação da chamada “doutrina da segurança nacional”, elaborada pela Escola Superior de Guerra e incorporada ao Decreto-Lei nº 314, de 13 de Março de 1967. A versão mais recente da Lei de Segurança Nacional em vigor é a Lei nº 7170 de 1983. Vide: FGVCPDOC. **Anos de Incerteza (1930 - 1937).**Lei de Segurança Nacional**.** Disponível em: <http://cpdoc.fgv.br/producao/dossies/AEraVargas1/anos30-37/RadicalizacaoPolitica/LeiSegurancaNacional>. Acesso em: 10 mar. 2018.

[652] Esse é o sentido de necessidade adotado pela Corte Europeia de Direitos Humanos “The Court has noted that, whilst the adjective "necessary", within the meaning of Article 10 (2) (art. 10-2), is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" and that it implies the existence of a "pressing social need" (p. 22, para. 48).”EUROPEAN COURT OF HUMAN RIGHTS. *Case of The Sunday Times v. The United Kingdom (application no. 6538/74)*. Em tradução livre: “O Tribunal observou que, enquanto o adjetivo "necessário", na acepção do artigo 10(2) (art.10-2), não é sinônimo de "indispensável", nem a flexibilidade de expressões como "admissível", "ordinário", "útil", "razoável" ou "desejável" e que implica a existência de uma "necessidade social premente" (p. 22, para. 48)".

de qualquer mecanismo criptografado sejam entregues ao estado *(key scrows)*; de ordens estatais de suspensão da criptografia ou criminalização geral da tecnologia. Cita especialmente o caso da China, que exige adesão ao algoritmo de criptografia aprovado pelo governo; da autoridade de comunicação paquistanesa ou do governo cubano, que exigem aprovação prévia do algoritmo para uso da criptografia, ou o caso da Índia, que restringe a utilização de criptografia em massa, exigindo que qualquer uso de criptografia forte, com chaves maiores que 40 bits, impõe a obrigação de entregar ao governo uma cópia de chave criptográfica[653].

No que diz respeito ao anonimato, seu benefício reside justamente na possibilidade de livremente exercer sua autonomia sem ser identificado. O anonimato pode permitir ao indivíduo explorar e compartilhar ideias e opiniões mais do que faria se tivesse que assumir sua real identidade. Até mesmo para formar a própria opinião ou desenvolver a própria personalidade é necessário que isso se dê sem qualquer intrusão de terceiros.

Portanto, apenas sob o véu do anonimato, fontes jornalísticas se sentem encorajadas a denunciar poderosas autoridades, cidadãos a se expressar de forma contrária a maioria, ainda que esta conformação cause incômodo. No caso do Brasil, no qual há 5570 Municípios, nos quais pode haver conluio de autoridades locais para reprimir dissidentes, inspira preocupação o fato de ser o sétimo país do mundo em número de jornalistas mortos[654]. Não é por outra razão que uma das primeiras medidas de governos autoritários quando foram alvos de protestos, no que ficou conhecido como Primavera Árabe, foi adquirir aparatos de vigilância para monitorar e controlar as atividades na internet, bem como bloquear os aplicativos que viabilizavam os protestos[655].

No âmbito da União Europeia não é diferente. A proposta do Parlamento Europeu para reformar a Diretiva de Privacidade na Internet[656], através do Conselho Europeu, consistiu em propor, em junho de 2017, o fortalecimento das políticas de privacidade, admitindo-se ressalvas para a proteção da privacidade tão somente nas situações em que a criptografia ponta a ponta desafie a tarefa de combate ao terrorismo, sem descuidar da necessidade de

---

653 KAYE, David. Op. cit., p. 5.

654 LOTT, Diana. Brasil é sétimo país do mundo em número de jornalistas assassinados. **Folha**, São Paulo, out. 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2017/10/1930121-brasil-e-o-setimo-pais-do-mundo-em-numero-de-jornalistas-assassinados.shtml>. Acesso em: 18 mar. 2018.

655 REDAÇÃO. Maior manifestação antigoverno da era Mubarak deixa 3 mortos no Egito. **Estadão**, jan. 2011. Disponível em: <http://internacional.estadao.com.br/noticias/geral,maior-manifestacao-antigoverno-da-era-mubarak-deixa-3-mortos-no-egito-imp-,671222>. Acesso em: 18 mar. 2018.

656 EUROPEAN PARLIAMENT. Op. cit., p. 5-8.

resguardar os benefícios da tecnologia à privacidade[657]. O Comitê Europeu Econômico e Social entendeu também que a internet das coisas é muito mais invasiva à privacidade, de modo que se faz necessária, não a redução do grau de proteção do regulamento geral de proteção de dados, em nome do interesse da indústria da tecnologia, mas o seu fortalecimento, cujas prioridades devem incluir, além educação do usuário, o anonimato e a criptografia.

Por outro lado, é certo que o exercício da liberdade de expressão, assim como todas as outras atividades do indivíduo, necessariamente sofre a migração para o ambiente cibernético, de modo que suas comunicações, opiniões públicas, fontes de informação, assuntos de preferência ficam vinculados ao seu perfil na rede, como se fossem impressões digitais de sua personalidade. Qualquer atividade no ambiente online deixa rastros e já se demonstrou no segundo capítulo que pouca coisa deixa de passar pelo filtro da vigilância estatal, havendo pouquíssimas possibilidades de se ocultar à vigilância massiva. Ora, nos arquivos revelados por Snowden, há informação acerca da possibilidade de se acessar dados protegidos por criptografia. Embora nunca se poderá contar com uma versão oficial da NSA a respeito do tema, vez que a o governo estadunidense considera as revelações do ativista criminosas, causa perplexidade tamanho avanço da vigilância. Portanto, não sendo a criptografia por si só suficiente, faz-se necessário o reforço da privacidade através do anonimato.

Por esta razão, o relator da ONU condenou veementemente tentativas de reduzir o anonimato, através da limitação de instrumentos que o garantam, tais como o uso da VPN[658], da tecnologia Tor[659] ou de *proxies*[660], além de exigir identificação do indivíduo para acesso à

---

[657] EUROPEAN COUNCIL. European Council meeting (22 and 23 June 2017) – Conclusions. **European Council**, jun. 2017. Disponível em: <http://data.consilium.europa.eu/doc/document/ST-8-2017-INIT/en/pdf>. Acesso em: 13 mar. 2018.

[658] A tecnologia VPN (Virtual Private Network), consiste no estabelecimento de uma rede virtual privada para ligar diretamente dois ou mais computadores, que é construída usando a infraestrutura da internet, mas garante a confidencialidade da comunicação, uma vez que utiliza a criptografia para a troca de dados. Logo, trata-se de um túnel virtual criado sobre a estrutura da internet, garantindo o acesso apenas a terminais autorizados. RUGGIERI, Ruggero. VPN e Criptografia. **Crypto ID**, dez. 2015. Disponíel em: <https://cryptoid.com.br/banco-de-noticias/vpn-e-criptografia/>. Acesso em: 18 mar. 2018. Para Glaydson de Farias Lima, a "ferramenta (VPN) se utiliza de um túnel criptografado de conexão entre a rede e os equipamentos remotos, não possibilitando que os dados que transitem nesta rede expandida sejam interceptados". LIMA, Glaydson de Farias. **Manual de Direito Digital**: Fundamentos Legislação e Jurisprudência. Curitiba: Apris, 2016, p. 57.

[659] O Tor (*The Onion Router*), é um programa que protege a identidade do usuário enquanto ele navega, dificultando a sua identificação. A analogia com a cebola é feita em virtude das camadas de transmissão criadas, ocultando-se o seu miolo, uma vez que a cada atividade dado transmitido na rede, o programa faz o dado circular por inúmeros terminais até chegar ao seu destinatário com o objetivo de confundir e dificultar a identificação do usuário e seu monitoramento indevido. HARADA, Eduardo. Tor: entenda como esta rede garante o seu anonimato na internet. **TecMundo**, mai. 2016. Disponível em: <https://www.tecmundo.com.br/seguranca/104364-tor-entenda-rede-garante-anonimato-internet.htm>. Acesso em: 10 abr. 2018.

internet por meio de dados pessoais ou registro de chip de telefone. Tais tecnologias contribuem sobremaneira para a garantia do anonimato de indivíduos, especialmente grupos minoritários ou dissidentes do poder.

O uso do anonimato para a liberdade de expressão é prática consagrada nas culturas ocidentais e protegida juridicamente. Sua utilização ocorre sobretudo quando o sujeito que assume um pseudônimo ou não revela sua real identidade se permite expressar com mais liberdade e clareza suas ideias, especialmente quando a assunção da sua real identidade lhe provocará danos tão maiores que calarão seu discurso, seja por receio de perseguição, seja por timidez. Basta lembrar que William Shakespeare[661], dramaturgo do século XVI mundialmente reconhecido, e Elena Ferrante[662], autora contemporânea das obras mais vendidas, são pseudônimos sobre cujas reais identidades não se possui certeza. Do mesmo modo, durante o regime militar, Chico Buarque assinava algumas de suas canções por pseudônimos, com vistas a driblar a censura, vez que suas canções eram censuradas tão somente em virtude de sua autoria[663].

Na cultura estadunidense, o anonimato é consagrado como integrante da própria liberdade de expressão, havendo inclusive uma identidade entre a história do federalismo naquele país e o uso do pseudônimo nos *Federalist Papers*. Logo, entende-se que o anonimato completo ou mesmo a livre expressão por meio de pseudônimos que permitam ou não identificar a sua real identidade, estaria albergada pela Primeira Emenda, que garante a liberdade de expressão, vez que o anonimato viabilizaria a livre expressão de opiniões e ideias sem constrangimentos, perseguições e represálias. O anonimato permite, portanto, o exercício

---

[660] *Proxie* pode ser definido como um intermediário utilizado na navegação, com vistas a proteger o número do IP e tornar oculta a navegação do real usuário. Isso garantiria um certo grau de anonimato ao usuário ao mascarar seu número de IP, permitindo-se que se proteja a identidade do computador do usuário. Em geral, proxies funcionam como firewall e filtro de conteúdo. É um mecanismo de segurança para proteger a identificação da máquina por qualquer servidor. OLIVEIRA, Arize. O que é proxy? Descubra o significado desse termo.**TechMundo**, mai. 2011. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2011/05/o-que-e-proxy-descubra-o-significado-desse-termo.html>. Acesso em: 10 abr. 2018. Para uma discussão sobre o uso de proxies e atividades ilícitas, vide também LIMA, Glaydson de Farias. Op. cit., p. 56.

[661] ALONSO, Pedro. A Identidade de Shakespeare, uma dúvida polêmica que ressurge no Reino Unido**. G1**, set. 2017. Disponível em: <http://g1.globo.com/Noticias/PopArte/0,,AA1630128-7084,00-A+IDENTIDADE+DE+SHAKESPEARE+UMA+DUVIDA+POLEMICA+QUE+RESSURGE+NO+REINO+UNIDO.html>. Acesso em: 10 mar. 2018.

[662] REDAÇÃO. Elena Ferrante: suposta revelação da identidade da autora causa polêmica. **G1**, out. 2016. Disponível em: <http://g1.globo.com/pop-arte/noticia/2016/10/elena-ferrante-suposta-revelacao-da-identidade-da-autora-causa-polemica.html>. Acesso em: 10 abr. 2018.

[663] "Julinho da Adelaide nasceu quando Chico Buarque passou a ser muito conhecido entre os censores do regime militar, na década de 70. Suas músicas eram proibidas somente porque levavam sua assinatura. A saída para burlar censura foi a criação de um heterônimo." JULINHO DE ADELAIDE, 24 anos depois. **Sanatório Geral**, [s.d.]. Disponível em: <http://www.chicobuarque.com.br/sanatorio/julinho.htm>. Acesso em: 10 abr. 2018.

da autonomia individual sem o receio de sofrer preconceitos, bem como a livre circulação de ideias, sem que haja qualquer resistência a sua recepção em razão da identidade do autor[664].

Da mesma forma, na cultura europeia, conforme visto no capítulo anterior, é amplamente consagrado o princípio da autonomia informativa, segundo o qual compete ao indivíduo determinar que dados sobre si podem ser revelados e tratados. Com efeito, é condizente com a cultura europeia de privacidade a proteção da liberdade de expressão por meio de anonimato, havendo inclusive recomendação de seu fortalecimento no ambiente digital, diante da maior possibilidade de monitoramento. Tanto é assim que o órgão consultivo da Comissão Europeia recomenda o fortalecimento do anonimato não somente por sua função garantidora da liberdade de expressão e a privacidade, mas também porque, na era digital,o comportamento individual pode ser pesquisado e monitorado em um grau que nunca foi possível antes[665].

No direito brasileiro, a previsão de um dos aspectos do direito fundamental à liberdade de expressão vem associada ao anonimato, nos seguintes termos: *"é livre a manifestação do pensamento, sendo vedado o anonimato"* (art. 5º, IV). A leitura isolada do dispositivo pode levar à equivocada conclusão de que a manifestação do pensamento apenas pode ocorrer quando o indivíduo revela sua real identidade.

Todavia, a Constituição não pode ser lida em tiras. Deve-se observar que a manifestação do pensamento é apenas uma das formas de exercício da liberdade de expressão, havendo outras disposições no mesmo catálogo. Exemplo disso é a previsão da liberdade de expressão intelectual, artística, científica e de comunicação, independentemente de censura ou

---

664 "Identification can inhibit one's ability to be anonymous or pseudonymous. Anonymous speech has a long history as an important mode of expression. Between 1789 and 1809, numerous U. S. Presidents and congressmen published anonymous political writings. Benjamin Franklin used more than forty pen names. James Madison, Alexander Hamilton, and John Jay published The Federalist Papers using the pseudonym "Publius", and the Anti Federalists also used pseudonyms. (…) Anonymity and pseudonymity protect people from bias based on their identities and enable people to vote, speak, and associate more freely by protecting them from the danger of reprisal. Anonymity can enhance the persuasiveness of one's ideas because identification can shade the reception of ideas with reader's biases and prejudices. This is why, in many universities and schools, exams are graded anonymously. Anonymity provides people with the ability to criticise the companies for which they work and to blow the whistle on illegal activities. Anonymity also protects people who read or listen to certain unpopular ideas". SOLOVE, Daniel J. **Understanding Privacy**. London & Cambridge: Harvard University Press, 2009, p. 125.

665 "In other situations guaranteed anonymity serves to underpin not only privacy but also freedom of expression, such as in the cases of political dissidents subject to a totalitarian political regime wishing to express their opposition to the political system in which they live and draw attention to human rights abuses. But the need for anonymity goes much wider than these specific cases. For identifiable transactional data by its very existence will create a means through which individual behaviour can be surveyed and monitored to a degree that has never been possible before". EUROPEAN COMMISSION. Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Recommendation 3/97: Anonymity on the Internet. **European Commission**, dez. 1997, p. 5. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf>. Acesso em: 10 abr. 2018.

licença (art. 5º, IX)[666]. Embora a previsão de vedação ao anonimato esteja associada no texto à liberdade de manifestação do pensamento, certo é que esta vedação se aplica à liberdade de expressão em geral[667]. Todavia, a compreensão da vedação ao anonimato deve ser feita de maneira temperada com a teleologia da norma, conforme se explicitará.

Deve-se observar ainda que, em seguida à previsão da liberdade de pensamento e da liberdade de expressão da atividade intelectual, artística, científica e de comunicação, há respectivamente a previsão do direito de resposta, com reparação moral e material ou à imagem[668], bem como a previsão de indenização por dano moral e material, em virtude de violação à honra, imagem, à vida privada e à intimidade[669].

A localização topográfica do catálogo de direitos fundamentais permite concluir que há variadas formas do exercício da liberdade de expressão, entre elas a liberdade de pensamento. Em alguma das vezes que tratou de liberdade de expressão, o legislador constituinte deixou claro que seu exercício não se submeteria a qualquer tipo de censura prévia, deixando para o inciso seguinte a responsabilização em virtude do abuso do referido direito, como é o caso do direito de resposta, em geral correlato ao exercício da liberdade de informação.

Todavia, no que diz respeito à liberdade de manifestação do pensamento, há a vedação ao anonimato sem qualquer ressalva. Ocorre que, assim como nenhum direito fundamental é absoluto, antes deve ser harmonizado com outros direitos fundamentais previstos na Carta, se pode dizer que a liberdade de manifestação de pensamento também não o é, vez que encontra limites na honra e na imagem de terceiros. Esta é a razão para que seja vedado o anonimato: uma vez havendo abuso no exercício da liberdade de expressão, a vedação ao anonimato evita que se impeça a identificação do ofensor, obstando sua responsabilidade. Neste sentido é o entendimento esposado em julgados do Supremo Tribunal Federal[670]. Todavia, tal vedação não pode ser tomada como absoluta, conforme se demonstrará.

---

[666]Art. 5º. "(...). IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;".

[667]Este é o entendimento do professor Ingo Sarlet. SARLET, Ingo; MARINONI, Luiz Guilherme; MITIDIERO, Daniel *et al*. Curso de Direito Constitucional. 5. ed. rev. e atual. São Paulo: Saraiva, 2016. *p. 498.*

[668]Art. 5º. "(...). V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;".

[669]Art. 5º. "(...). X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;".

[670]"O veto constitucional ao anonimato, como se sabe, busca impedir a consumação de abusos no exercício da liberdade de manifestação do pensamento, pois, ao exigir-se a identificação de quem se vale dessa extraordinária prerrogativa político-jurídica, essencial à própria configuração do Estado democrático de direito, visa-se, em última análise, a possibilitar que eventuais excessos, derivados da prática do direito à livre expressão, sejam

É possível que em algumas situações haja o completo anonimato, pois a ponderação no caso concreto fará prevalecer o interesse da moralidade administrativa, quando, por exemplo, se tratar de denúncia anônima de desvio de recurso por autoridade pública. Da mesma forma, pode ser que prevaleça o interesse da criança ou adolescente em uma denúncia de pedofilia ou mesmo a necessidade de combate à impunidade, nos crimes de homicídio e tráfico. Não é por outra razão que há formas de se denunciar anonimamente atividades criminosas, vez que apenas o anonimato encoraja o indivíduo a se engajar em situações que envolva perigo de represálias, com riscos à integridade física[671].

Ademais, ainda que se entenda que o objetivo do legislador tenha sido vedar qualquer manifestação anônima por presumir a prática de condutas criminosas, deve-se realizar a releitura do dispositivo à luz de outros interesses constitucionais legítimos. Ora, se nenhum direito fundamental é absoluto, nenhuma restrição a direito fundamental também o será. Deste modo, uma interpretação teleológica da norma impõe a conclusão de que apenas seria vedado o anonimato nas situações as quais sejam praticados atos ilícitos em prejuízo de terceiro. Portanto, no nosso entender, a regra é que haja o anonimato relativo, havendo o seu levantamento apenas nas situações nas quais se identifique atividade ilícita ou que cause dano a terceiros, haja vista que o anonimato não pode ser véu a impunidade.

Todavia, em razão da sensibilidade do direito em jogo e do efeito silenciador ou resfriador do debate decorrente da identificação do autor, principalmente na internet, defende-se que o levantamento deste anonimato apenas ocorra por ordem fundamentada de autoridade judicial, como interpretação decorrente do art. 22 do Marco Civil da Internet[672].

---

tornados passíveis de responsabilização, 'a posteriori', tanto na esfera civil, quanto no âmbito penal.". BRASIL. Supremo Tribunal Federal. *Mandado de Segurança nº 24369 MC/DF*. Rel. Min. Celso de Mello. Julg. 10 out. 2002. **DJ** 16 out. 2002.

671 O modelo de denúncia anônima foi reputado constitucional em julgados do Supremo Tribunal Federal. "Nada impede, contudo, que o Poder Público, provocado por delação anônima ("disque-denúncia", p. ex.), adote medidas informais destinadas a apurar, previamente, em averiguação sumária, "com prudência e discrição", a possível ocorrência de eventual situação de ilicitude penal, desde que o faça com o objetivo de conferir a verossimilhança dos fatos nela denunciados, em ordem a promover, então, em caso positivo, a formal instauração da "persecutio criminis", mantendo-se, assim, completa". BRASIL. Supremo Tribunal Federal.*Habeas Corpusnº 106664 MC/SP*. Segunda Turma. Rel. Min. Celso de Mello. Julg. 19 mai. 2011. **DJ** 23 mai. 2011.

672"**Seção IVDa Requisição Judicial de Registros**

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

Deve-se ainda distinguir o anonimato absoluto daquele apenas relativo, que proporciona alguma segurança ao usuário, sem que impossibilite totalmente sua identificação pelos órgãos investigativos. Neste sentido, há vozes na doutrina que advogam a possibilidade de um anonimato relativo, sem que isso inviabilize o funcionamento de determinada plataforma que tenha por base algum grau de anonimato[673]. Sabe-se que toda atividade na internet ocorre através da utilização do IP *(internet protocol)* que permite a identificação da máquina da qual partiu, através do registro de acesso a determinada aplicação[*674*]. Em regra,usuários comuns se aproveitam do pseudônimo e do anonimato, mas em geral não fazem uso de complexos mecanismos que reforçam seu anonimato como o uso de *proxies* e Tor, o que facilita sua identificação em caso de cometimento de ilícitos.

Todavia, pode ocorrer que haja o anonimato absoluto, ou seja, que a atividade do usuário seja de tal modo protegida e mascarada a ponto de não permitir a sua completa identificação, seja porque utiliza IP privado[675] em uma conexão corporativa ou de *lan house*, seja porque utiliza mecanismos aqui citados que facilitem seu anonimato. A utilização destes mecanismos por si só não é ilícita, até porque nem sempre se impossibilita por completo a identificação do usuário.

Outrossim, ainda que haja a impossibilidade absoluta de identificação do usuário, esse é um preço que se paga por se viver em um regime democrático que preza pela promoção das

---

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro".

673 Carlos Affonso Pereira de Souza, ao tratar do aplicativo Secret, no qual se poderia fazer críticas supostamente anônimas a terceiros não vê ilegalidade de *per se* na plataforma, vez que se trata de anonimato apenas relativo: "Ao permitir a identificação do autor de mensagens postadas em sua plataforma, mantendo apenas o pretenso anonimato entre os seus usuários, pode ser mesmo questionado se o aplicativo Secret criou um ambiente que pode ser reputado anônimo. Parece mais apropriado caracterizar o anonimato disponibilizado pelo aplicativo como relativo, ou na melhor das hipóteses, como uma mera expectativa de anonimato, que pode ser quebrada na exata circunstância em que o autor da mensagem viola os termos de uso da ferramenta ou causa um dano". SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no Marco Civil da Internet. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III**. Tomo II: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015, p. 377-408 *apud* sentença nos autos n.º 0600957-73.2016.8.01.0070. 3º Juizado Especial Cível da Comarca de Rio Branco – Acre.

674 Prevê o Marco Civil da Internet os conceitos de IP e de registro de acesso. Art. 5º "Para os efeitos desta Lei, considera-se: (...) II - terminal: o computador ou qualquer dispositivo que se conecte à internet; III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais; VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

675 Para Glaydson de Farias Lima, o uso de vários IPs privados dentro de um IP público dificulta bastante a identificação dos autores na internet. Todavia, defende que a própria engenharia da internet foi construída para ser um ambiente livre, de modo que a existência de cadastro para toda e qualquer atividade pode inviabilizar a democratização do acesso. LIMA, Glaydson de Farias. Op. cit., p. 53-55.

liberdades em face da vigilância massiva e da perseguição política, especialmente porque qualquer restrição a liberdade preferencial, como é o caso da liberdade de expressão, deve passar por um filtro mais rigoroso, denominado na doutrina norte-americana como *strict scrutiny*[676]. Pretender controlar toda atividade protegida por redes de anonimato na *web* é utopia parecida com a pretensão de permitir o livre tráfego nas estradas porque criminosos também a usam para o tráfico de drogas ou vedar o uso da internet porque terroristas a utilizam para suas práticas criminosas.

Com efeito, o que se deve coibir é a utilizaçãodo anonimato para práticas ilícitas em uma situação concreta. Não se pode dizer, por outro lado, que o anonimato absoluto seja uma prática totalmente alheia a nossa cultura já que atualmente há sistemas de disque denúncia que garantem anonimato, o sistema eleitoral consagra o voto secreto e as ouvidorias e corregedorias de órgãos públicos de todo o país iniciam procedimento de verificação prévio de irregularidade, com base em denúncia anônima. Todas essas figuras consagram o caráter instrumental do anonimato em nossa cultura.

Certamente que os danos decorrentes de uma obrigação de identificação total[677] e plena para uso da rede, seja por meio de dados pessoais, seja por uso do nome real, por utilização de chip ou de qualquer outro modo são muito maiores que eventuais obstáculos ao trabalho investigativo, que não são de todo intransponíveis. Não se ignoram os efeitos danosos de crimes cometidos na chamada *Dark Web*[678], que consistem redes não indexadas nas quais se permite o anonimato e nas quais pode haver a prática de crimes, aproveitando-se

---

[676] Para Ana Paula de Barcellos, "[o] strict scrutiny na jurisprudência norte-americana determina que, em casos envolvendo as chamadas classificações suspeitas (classificações com base em raça, por exemplo) ou restrições a direitos fundamentais (como as liberdades previstas no Bill of Rights), a Corte aplique como teste os seguintes parâmetros: que a medida cuja constitucionalidade está sendo revisada esteja associada à proteção de um relevante interesse estatal (compelling government interest), que ela seja a menos restritiva possível (least restrictive measure) e que tenha sido desenhada de forma estrita para proteger o interesse estatal em questão (narrowly tailored)." BARCELLOS, Ana Paula de, Intimidade e pessoas notórias. Op. cit., p. 32.

[677] O grupo ativista Geek Feminism Wiki, destaca os grupos mais prejudicados por uma política de nome real, ou seja, que proíba o anonimato e o pseudonimato. Embora o objetivo destas políticas possa ser coibir assédio e danos a terceiros, a vedação do anonimato atinge especialmente grupos vulneráveis como ativistas, mulheres, LGBTs, crianças, confessores de determinada crença religiosa que, em função da revelação de sua real identidade no exercício da liberdade de expressão podem ser vítimas de assédio, práticas discriminatórias no ambiente de trabalho, agressão física, entre outros. REDAÇÃO. Who is harmed by a "Real Names" policy?. **Geek Feminism Wiki**, [s.d.]. Disponível em: <http://geekfeminism.wikia.com/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F>. Acesso em: 10 mar. 2018.

[678] "A *dark web* é uma parte não indexada e restrita da *deep web*. Para acessar, é necessário um software e autenticação. Esta parte da web é realmente mais escondida e possui um enorme mercado ilegal: drogas, pornografia infantil, venda de órgãos humanos e tortura. Lá você pode contratar hackers e assassinos". MORETTO, Julia. Qual é a diferença entre a deep web e dark web? **Jornal Ciência**, nov. 2016. Disponível em: <http://www.jornalciencia.com/qual-e-a-diferenca-entre-a-deep-web-e-dark-web/>. Acesso em: 10 mar. 2018.

de sua relativa ocultação. Todavia, a *Dark Web* constitui uma pequena parte[679] da *Deep Web*, ambiente não indexado da internet, que é utilizado por ativistas para não serem monitorados e denunciarem abusos estatais com relativa liberdade[680].

Deve-se observar que há variados graus de anonimato nas redes, uma vez que a adoção de um pseudônimo ou mesmo a criação de um perfil falso na rede enseja apenas um anonimato superficial, não havendo uma obrigação apriorística por quem quer que seja de se identificar na rede. Significa dizer que, com base em alguns dados do indivíduo, tais como atividades na internet, localização do IP utilizado, rede de fluxo de dados, ou seja, através dos metadados, é possível rastrear o indivíduo e identificá-lo com relativa precisão. Portanto, situações há em que o anonimato é tão somente aparente, permitindo-se que, com uma expertise razoável, a informação seja desanonimizada, conforme visto no capítulo anterior. Logo, a não identificação por si só ou o uso de pseudônimos não é razão para tornar ilegal o exercício da liberdade de expressão, garantida pelo anonimato[681].

Em suma, o que se propõe neste tópico é uma releitura da vedação constitucional ao anonimato no exercício da liberdade de expressão, mais consentânea com os tempos atuais,

---

679 "É aí que entra a Dark Web, uma fatia pequena da Deep Web que é intencionalmente mantida escondida e não pode ser acessada por nenhum browser comum justamente por conter materiais que envolvem crimes e outras coisas muito mais pesadas". FARINACCIO, Rafael. Dark Web revelada: afinal, o que mais existe no canto obscuro da internet? **TecMundo**, set. 2016. Disponível em: <https://www.tecmundo.com.br/internet/109781-dark-web-revelada-existe-canto-obscuro-internet.htm>. Acesso em: 10 mar. 2018.

680 Para Francisco Brito Cruz, diretor do Internet Lab, "TOR é uma ferramenta de segurança importantíssima para uma série de pessoas que correm risco de vida em países e regimes autoritários que monitoram a internet. Ela foi criada com o objetivo muito nobre de proteger o anonimato desses dissidentes [...] sendo a deep web uma ferramenta de segurança tão poderosa, ela foi apropriada por pessoas com motivos menos nobres que aquelas que a criaram." MOREIRA, Matheus. O que é a deep web e por que ela está encolhendo. **Nexo Jornal**, mar. 2017. Disponível em:<https://www.nexojornal.com.br/expresso/2017/03/17/O-que-%C3%A9-a-deep-web-e-por-que-ela-est%C3%A1-encolhendo>. Acesso em: 13 mar. 2018.

681 Cabe aqui apresentar trecho de sentença do Juizado Especial Cível da Comarca de Rio Branco no Acre, que contém relevante valor doutrinário, no qual a D. magistrada, Giordane de Souza Dourado, conclui que "o mero fato de não haver autor identificado a primeira vista não implica na suspensão de perfil em rede social, especialmente quando o anonimato é apenas aparente, propondo-se uma releitura do que seja vedação ao anonimato na Constituição, especialmente no ciberespaço: No caso concreto que motivou esta demanda, o exame superficial das postagens do perfil "Empate Digital" induz no leitor a aparência de anonimato, já que não estão visíveis os autores (pessoas naturais) das manifestações. Ocorre que a liberdade de expressão e a noção de anonimato nos domínios da rede mundial de computadores exigem do intérprete olhar acurado e orientado pelas peculiaridades do ciberespaço, sítio regido, como visto, por normas próprias e adequadas ao fenômeno que se pretende regular. Dessa forma, é necessário repensar o que será ou não anonimato quando se examinam publicações feitas na internet. (...) Embora de certa forma trabalhoso esse percurso, observa-se que a utilização de um tipo de "nome fantasia" no perfil do Facebook não impede a identificação da autoria das postagens difamatórias, elidindo-se então a ideia de anonimato. (...) Não diviso, dessa forma, a existência de real anonimato que justifique a exclusão do perfil "Empate Digital" da rede social Facebook, cabendo ao demandante insurgir-se especificamente, na via judicial, contra as publicações que reputar ofensivas ao seu estado de dignidade". A sentença foi proferida nos autos n.º 0600957-73.2016.8.01.0070 do 3º Juizado Especial Cível da Comarca de Rio Branco/Acre.

nos quais a regra é a liberdade. Na reflexão sobre as limitações ao anonimato, deve-se ter em consideração a efetiva tutela da liberdade de expressão, da privacidade, e da autonomia privada, valores decorrentes da dignidade humana, com vistas a entender constitucional a proteção ao anonimato absoluto para atividades lícitas e que não causem danos a terceiros. Quanto às atividades ilícitas, no nosso entender, incide plenamente a vedação constitucional e, portanto, apenas poderá haver o anonimato relativo. Todavia, a fim de se evitar arbitrariedades, a verificação de eventual ilicitude de conduta, para fins de identificação de seu autor, deve ser apreciada no caso concreto por autoridade judicial competente, que determinará o levantamento do anonimato[682].

3.6 **A criptografia forte e as possibilidades de sua violação ou enfraquecimento: as possíveis alternativas à investigação policial**

Retornando ao objeto central deste capítulo, cumpre verificar mais detalhadamente se as hipóteses em geral apontadas como alternativas à violação ou enfraquecimento da criptografia são viáveis e eficazes nos objetivos lícitos que se propõem, a saber, a contribuição para investigações criminais, sem que isso comprometa a privacidade de outros usuários.

Sabe-se que o vilão das agências de investigação em todo o mundo são os sistemas de criptografia assimétrica ou criptografia forte cujo conteúdo é praticamente impossível se violar,caso não se possua a chave privada. Conforme salientado, um tipo de criptografia forte muito utilizada atualmente é a criptografia fim a fim ou ponta a ponta, técnica de segurança que garante a confidencialidade entre as pontas da comunicação, protegendo seu conteúdo de ataques de adversários.

Tamanha é a controvérsia sobre a legalidade da utilização da criptografia ponta a ponta que, nos Estados Unidos, houve projeto de lei para obrigar as empresas de tecnologia a descriptografarem dados ou mesmo oferecer assistência técnica necessária para tanto[683], bem

---

[682] Também neste sentido, CAPANEMA, Walter Aranha. O direito ao anonimato... Op. cit., p. 8-9. uma nova interpretação do art. 5º, IV, CF. **A Voz do Cidadão**, [s.d.], p. 8-9. Disponível em: <http://www.avozdocidadao.com.br/images_02/artigo_walter_capanema_o_direito_ao_anonimato.pdf>. Acesso em: 13 mar. 2018. Para uma discussão sobre a flexibilização da regra de vedação ao anonimato, vide MELO, Mariana Cunha e. Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil. **ITS Rio**, mar. 2017, p. 4-7. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf>. Acesso em: 13 mar. 2018.

[683] O projeto de lei foi proposto em 2016 pelos Senadores Richard Burr e Dianne Feinstein, mas diante das fortes objeções de instituições de direitos civis, a ausência de apoio ao projeto no Congresso e o compromisso do

como para proibir qualquer tentativa de enfraquecimento da criptografia. Do mesmo modo, na União Europeia, em que pese haver recomendação do Parlamento no sentido de proteger a criptografia forte, países ainda se dividem em controvérsias ou incertezas sobre a legalidade da criptografia ponta a ponta, sem a criação de um *backdoor*, tendo sido aprovado no Reino Unido em 2016 a *Investigatory Powers Act* (Lei de Poderes Investigativos) que permite, em tese, que o governo britânico emita uma ordem secreta ao operador de telecomunicações que remova a proteção eletrônica aplicada a qualquer comunicação ou dado, o que poderia ser interpretado como a obrigação de criar ou fornecer uma chave mestra ou disponibilizar um acesso governamental ao conteúdo criptografada através de uma porta dos fundos[684].

No Brasil, como não poderia ser diferente, instituições policiais e de persecução penal defendem a obrigação de fornecimento do conteúdo criptografado por empresas de tecnologia, sob pena de bloqueio de seus serviços, após a imposição de vultosas multas pecuniárias, enquanto setores de tecnologia afirmam ser impossível impor acesso especial às autoridades sem que isso comprometa a segurança do sistema de forma global[685].

A solução da questão ao que parece não está na escolha trágica entre segurança e privacidade, como se a opção pelo segundo significasse abdicar o compromisso do Estado no combate à prática criminosa. O falso dilema pouco contribui para a resolução da questão. Cumpre verificar se as hipóteses propostas pelas autoridades investigativas para contornar a criptografia são eficazes e observam os requisitos constitucionais.

A primeira e mais extremada proposta neste campo é o banimento da criptografia forte, que pode ocorrer de várias maneiras, seja com o estabelecimento de uma criptografia com chaves violáveis por padrão - ou seja, criptografia fraca- ou mesmo a criminalização do uso, construção ou comercialização da criptografia forte.

Não obstante, banir a utilização da criptografia,proibindo-a por lei, apenas afetará o uso da tecnologia de segurança por parte do cidadão comum, deixando-o exposto com sua privacidade desprotegida diante da vigilância estatal ou privada, realizada esta com fins

---

governo Obama em não aprová-lo, fez com que os autores desistissem do projeto. O projeto está disponível em: <https://www.eff.org/document/burr-feinstein-encryption-bill-discussion-draft>. Acesso em: 13 abr. 2018.

[684] Entre outras medidas que se permite ao governo britânico está a emissão de ordem secreta aos operadores do serviço também para para a realização de qualquer processo, incluindo a prestação de serviços de instalações que o governo britânico considerar necessário em nome da segurança nacional. CARDOZO, Nate. Op. cit.

[685] Vide STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 13-40. Manifestações do Departamento de Polícia Federal e do Ministério Público Federal. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

legítimos ou não. Isto fará com que a criptografia seja exclusividade de organizações criminosas, vez que essas jamais deixarão de utilizar um aparato tecnológico porque é crime. Do mesmo modo, organizações estatais não terão dificuldade em ter acesso à criptografia, assim como ocorria com órgãos militares antes da popularização da tecnologia.

Logo, a proibição pura e simples, além de faticamente inviável, é juridicamente questionável. Isso porque a criptografia nada mais é que a tradução em forma de tecnologia de segurança da informação de complexa engenharia matemática, que resulta em software que garante a confidencialidade da comunicação contra ataques de terceiros. Criminalizar a criação e o uso da criptografia é criminalizar a liberdade de expressão da atividade científica, a pesquisa acadêmica e o uso da matemática[686]. Não custa lembrar que na primeira fase das guerras criptográficas dos anos noventa, a proibição da importação do sistema criptográfico P2P causou o efeito contrário, a saber, a sua imediata popularização por computadores situados fora dos Estados Unidos.

A segunda alternativa apresentada constituiria no depósito das chaves dos sistemas criptográficas em repositórios*(key escrow),* confiadas a um terceiro na condição de depositário. A proposta consiste em duplicar as chaves criptográficas para que autoridades estatais delasfaçam uso quando necessário. O estabelecimento da *key escrow* a rigor não se afasta muito de uma *backdoo,* na medida em que também estabelece uma vulnerabilidade no sistema que pode ser utilizada por terceiros[687]. Tal medida poderia ser implementada de duas formas. Uma delas imporia a entrega das chaves ou da chave mestra a uma autoridade independente que apenas a forneceria no caso concreto, após a verificação dos requisitos legais. Outra possibilidade seria a duplicação da chave, havendo a chamada*ADK - Additional Decryption Key*, ou chave adicional. Deste modo, a mensagem seria cifrada com uma segunda chave pública, que seria a adicional, cuja chave privada correspondente estaria em poder da autoridade[688].

O primeiro óbice que um repositório de chaves encontra é que se estaria impondo obrigatoriamente um tipo de criptografia que permita realizar a cópia das chaves e relegando à ilegalidade todas as outras variações de código-fonte. Na prática, se estaria tornando ilícita

---

[686]Manifestação de Diego De Freitas Aranha (Instituto de Computação da Universidade Estadual de Campinas - UNICAMP). STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 135.Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

[687] Ibidem, 226.

[688] MARCACINI, Augusto Tavares Rosa. Op. cit., p. 116.

parte dos modelos criptográficos, com todas as implicações que disso decorre, não precisando muito esforço para concluir que, naturalmente, pessoas receosas do monitoramento, para a realização de atividade criminosa ou não, migrariam para o modelo tornado ilícito, no qual não haveria cópia de chaves, e o objetivo de combate ao crime não seria alcançado.

O segundo óbice é que o modelo de depósito das chaves depende essencialmente da confiança na integridade da terceira parte depositária das chaves e, no pior das vezes, essa autoridade seria estatal, suscetível às pressões das mais variadas. Ora, além de passar a ter um exacerbado poder sobre toda e qualquer comunicação criptografada, sempre há o risco da própria autoridade corromper-se e utilizar as chaves para fins ilegítimos. Ademais, qualquer possibilidade de utilização das chaves por pessoas diversas dos interlocutores sempre representará uma vulnerabilidade, vez que tais chaves serão objeto de cobiça de criminosos, constituindo ativo valioso, sem contar que a base de dados onde estão depositadas as chaves poderá sofrer ataques de hackers. O exemplo da utilização do modelo vem da Turquia, país de tradição autoritária, o que demonstra o risco da sua utilização em estados democráticos[689].

O terceiro e mais defendido meio pelas forças de segurança é a criação de *backdoor*, que consiste na criação intencional de uma vulnerabilidade, ou seja, ocorre a implantação proposital de uma falha de segurança no protocolo criptográfico. Essa vulnerabilidade seria fornecida às autoridades governamentais. Há variadas formas de se introduzir um *backdoor*, que pode ocorrer através da sucetibilidade a um programa de vírus, capaz de acessar as chaves geradas; pela introdução de uma falha na programação; ou a possibilidade de se programar uma intervenção em que se consegue captar a mensagem antes da encriptação ou logo após a decriptação[690].

A utilização do *backdoor* encontra alguns obstáculos. É consenso na comunidade científica que a criação de vulnerabilidades intencionais como porta dos fundos, deixa vulnerável a tecnologia para todos, ou seja, há a aplicação da lógica do tudo ou nada, ou seja, qualquer tipo de excesso excepcional torna a tecnologia vulnerável para todos a ataques de terceiros, uma vez que pessoas mal intencionadas também explorarão a mesma vulnerabilidade criada para servir pessoas bem intencionadas[691].

---

[689] KAYE, David. Op. cit., p. 15.

[690]Manifestação de Diego De Freitas Aranha (Instituto de Computação da Universidade Estadual de Campinas - UNICAMP). STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 135.Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

[691] KAYE, David. Op. cit., p. 15.

Nesta linha, a criptografia é baseada em complexos cálculos e todo sistema de segurança é desenhado para garantir sua integridade. Se há alguma vulnerabilidade, esta vulnerabilidade ocorrerá para todos os usuários, deixando todo o conjunto inseguro e disto estarão inseguras as atividades lícitas ou ilícitas. Portanto, os custos técnicos da criação de uma vulnerabilidade serão elevadíssimos, vez que se abrirá uma porta de entrada para ataques de invasores e causará danos à inovação tecnológica, que sempre estará obrigada a criar sistemas vulneráveis, o que comprometerá inclusive a livre concorrência e o crescimento econômico.

Não há como negar ainda que a autoridade moral dos países que impõem a utilização de porta fundos fica comprometida, pois a mesma vulnerabilidade que permite a porta dos fundos também viabiliza o vigilantismo estatal. Ora, embora o Estado possa estar bem intencionado no combate ao crime, pode ter em suas mãos uma arma em potencial para praticar crimes mais graves, decorrentes da intrusão na vida privada de seus cidadãos, tais como perseguições, assédios, violação de direitos de opositores políticos, entre outros.

Veja-se que a lógica da vigilância contemporânea não é definir um suspeito e investigá-lo, mas realizar a investigação massiva de todos, para a partir daífiltrar os suspeitos. Repise-se, a vigilância permite encontrar uma agulha no palheiro após escrutiná-lo por completo.

Portanto, é de se questionar que autoridade moral terá o Estado para possuir acesso à portas dos fundos de criptografia, com a qual é capaz de realizar vigilância, impondo arbitrariamente ao cidadão a obrigação de utilizar um sistema de segurança vulnerável[692]. Aliás, tecnicamente, a vulnerabilidade será global, haja vista que os aplicativos criptografados atualmente utilizados são popularizados por toda a rede. Logo, sendo global a fragilidade, também o será a chance de sofrer ataques.

Por fim, por se tratar de sistema de segurança da informação, ao se criar uma vulnerabilidade a ser acessada apenas por pessoas autorizadas, a criptografia deverá redesenhar seu complexo código fonte para esconder essa porta dos fundos de ataques maliciosos. Logo, o protocolo criptográfico que é projetado para ser um sistema de segurança contém falha de segurança que a ninguém aproveita. Uma vez que os criminosos percebam esta falha, migrarão para outra aplicação na qual não haja esta vulnerabilidade ou criarão seu

[692] ABELSON, Harold et al. Keys under Doormats: mandating insecurity by requiring government acess to all data and comumunications. **Schneier**, jul. 2015. Disponível em: <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf>. Acesso em: 10 abr. 2018.

próprio canal de comunicação criptografado, sem a vulnerabilidade, já que o código-fonte do protocolo Signal é público. No fim das contas será o cidadão que restará desprotegido.

Há outras hipóteses menos citadas que envolvem tornar vulnerável ou enfraquecido o sistema de criptografia ou contorná-lo. Um deles seria realizar o ataque *man-in-the-middle*, que consiste em trocar a chave pública do usuário sem que este perceba e, estando de posse do par de chaves pública e privada, descriptografar a mensagem antes que chegue ao seu destinatário.

Ocorre que para usuários experimentados, que utilizam o aplicativo justamente por conta da criptografia assimétrica, terão o cuidado de conferir se houve troca de sua chave pública ou de seu interlocutor, uma vez que esta informação é acessível. A desvantagem da utilização do *man-in-the-midlle* é que a sua realização será percebida e a atividade criminosa migrará para outro ambiente que lhe pareça mais seguro. Basta lembrar que aplicativos mais populares, como o WhatsApp que utilizam o sistema de criptografia ponta a ponta contam com a funcionalidade de verificação de segurança, através da comparação da chave que o usuário possui no dispositivo e a chave utilizada para encriptação. Tendo havido a troca de chaves, a verificação de segurança não terá sucesso. a verificação de segurança consiste no modelo de negócios do aplicativo cujo produto visa garantir aos usuários a segurança necessária à confidencialidade das comunicações, de modo que, se, por algum motivo, houver a suspensão da criptografia ou a troca de chaves desavisada, usuários mais atentos perceberão.

Decerto que quem estiver imbuído em atividades criminosas terá o cuidado de regularmente conferir as chaves e desconfiará se a funcionalidade de verificação de segurança não estiver mais disponível. Outrossim, para se ter uma vaga ideia do que significa suspender a criptografia em relação a um único usuário, isso significará realizar a troca de todos os pares de chaves do usuário e de seus contatos. Portanto, haverá tantas trocas de chaves quanto o investigado possuir de contatos. Soma-se a isto o fato de que as trocas deixarão todos os contatos do usuário investigado com a chave trocada, o que eleva as chances de a manobra ser descoberta por qualquer um deles, que imediatamente encerrará a comunicação através daquele meio, antes mesmo que qualquer evidência útil à investigação seja coletada.

Ademais, parece contrariar a proporcionalidade impor ao particular responsável pelo aplicativo a extinção da verificação de segurança, vez que a segurança da informação é a espinha dorsal de seu modelo de negócios, de modo que tal imposição violaria o princípio constitucional da livre iniciativa (art. 170 da CRFB).

Ora, nada garante que a vulnerabilidade criada, seja ela porta dos fundos ou repositório de chaves, apenas será explorada para os fins incialmente previstos, tampouco que o serão apenas por pessoas bem intencionadas, vez que serão objeto de desejo de governos autoritários que não medirão esforços para acessá-la. Sem dúvida, a história está cheia de exemplos a respeito. O primeiro deles e mais recente foram os ataques conhecidos como *wannacry*, que exploravam uma vulnerabilidade constante dosistema operacional Microsoft Windows[693]. Ora, a falha de segurança explorada no *wannacry* foi desenvolvida pela NSA,imbuída dos mais nobres fins de proteger a segurança nacional daquele país, mas a agência de investigação não foi capaz de manter em sigilo tão poderosa ferramenta que caiu em mãos não tão bem intencionadas assim, o que afetou dezenas de milhões de computadores. O ponto fulcral é demonstrar que vulnerabilidades ou pontos fracos o são para atividades lícitas ou ilícitas e assim serão explorados por quem quer que seja e nem a agência de investugação mais poderosa do planeta poderá impedir o uso desvirtuado da vulnerabilidade.

Ademais, por se tratar o *wannacry* de um cripto ***ransomware***, um tipo de software malicioso que sequestra e encripta os arquivos dos computadores e pede um resgate financeiro em *bitcoins*, o que demonstra que altas técnicas de criptografia sempre estarão ao alcance de criminosos.

Da mesma forma, entre 1996 e 2006, na Itália, um sistema de interceptação legal foi utilizado indevidamente para espionar as comunicações de seis mil pessoas, incluindo líderes políticos, líderes do mundo dos negócios, magistrados e jornalistas. Entre 2004 e 2005, um sistema semelhante foi utilizado de maneira indevida para espionar membros do alto escalão do governo grego, sem se saber quem foi o autor da espionagem, o que demonstra que mesmo que a ferramenta seja legal, não necessariamente permanecerá nas mãos dos agentes estatais[694].

Portanto, diante da reedição das criptoguerras contemporâneas, o enfraquecimento da criptografia ponta a ponta conta com forte repúdio de instituições de proteção dos direitos humanos e do setor de tecnologia. O decálogo do Comitê Gestor da Internet no Brasil prevê que a segurança na rede deve observar medidas técnicas compatíveis com padrões

---

[693]HIGA, Paulo. Ransomware WannaCry já infectou 200 mil computadores em 150 países. **Tecnoblog**, [s.d.]. Disponíel em: <https://tecnoblog.net/214656/wannacry-ataque-disseminacao-150-paises/>. Acesso em: 13 abr. 2018.

[694] STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 89. Manifestaçao de Anderson Nascimento (Universidade de Washington - Tacoma). Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

internacionais[695]. Ademais, a comunidade científica, que é unânime na defesa da manutenção de uma criptografia forte[696], entregou carta ao então presidente dos Estados Unidos, assinada por 150 organizações da sociedade civil, empresas de tecnologia e especialistas em segurança na rede[697], defendendo o fortalecimento das políticas que promovam a criptografia forte.

Em suma, deve-se ressaltar que promover a vulnerabilidade de uma tecnologia de segurança parece não ser a melhor medida, especialmente quando não há nenhuma garantia de de que o uso da vulnerabilidade será feito de boa fé e de forma exclusiva pelas autoridades competentes. Ademais, organizações criminosas estarão atentas a qualquer movimento de fragilidade de um meio, migrando para meio mais seguro caso se sintam ameaçadas.

Em geral, as tentativas de controle do acesso à criptografia forte ocorrem em países de reduzida tradição democrática, mas não constitui uma exclusividade. Não é por outra razão que alguns países como o Paquistão estabelecem qual o padrão criptográfico permitido, criminalizando a fabricação de equipamentos de telecomunicação que contrariem este padrão[698]. Na Arábia Saudita, a criptografia é totalmente proibida. Em outros países, há um controle rígida da criptografia, através da necessidade de autorização específica, quais sejam, China, Rússia, Cazaquistão, Egito, Marrocos, Ucrânia, dentre outros.

Portanto, a legítima preocupação dos estados afetados pelos horrores do terrorismo não os dispensa da preocupação com os direitos fundamentais de seus cidadãos, sob pena de, sob o argumento do combate aos crimes de um inimigo latente, se praticarem violações ainda maiores aos direitos individuais dos cidadãos. Logo, urge a rejeição de toda e qualquer proposta que vise tornar a criptografia vulnerável, estabelecendo-se um padrão de criptografia fraca, vez que, ao tempo em que viola liberdades individuais dos cidadãos, não cumpre a promessa de garantir maior segurança.

---

695 "8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas." É o que consta da Resolução CGI.br/RS/2009/003/P, disponivel em:<https://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 13 abr. 2018.

696REDAÇÃO."Signal" é consenso na comunidade científica, diz professor da Universidade de Washington. **Crypto ID**, jun. 2017. Disponível em: <https://cryptoid.com.br/banco-de-noticias/signal-e-consenso-na-comunidade-cientifica-diz-professor-da-universidade-de-washington/>. Acesso em: 13 abr. 2018.

697 A carta está disponível em: <https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf>. Acesso em: 10 abr. 2018.

698 KAYE, David. Op. cit., p. 14.

3.7 **A investigação criminal possui alternativas à criação de vulnerabilidades na criptografia? Aplicaçoes do subprincípio da necessidade enquanto etapa da proporcionalidade**

O discurso oficial das agências de investigação é de que a criptografia forte inviabilizaria por completo o trabalho dos órgãos de investigação e persecução penal. As autoridades em geral estão focadas na utilização criminosa dos recursos tecnológicos como se esta utilização não fosse minoritária.

Conforme se viu em tópicos anteriores, o relatório da ONU para liberdade de expressão impõe que qualquer restrição à criptografia seja feita por meio de lei que observe o princípio da necessidade, ou seja, a medida deve ser imprescindível ao objeto legítimo que se deseja alcançar. Ademais, a restrição deve observar os três elementos da proporcionalidade sobre os quais não cabem maiores considerações neste ponto, cabendo-se apenas destacar que o subprincípio da menor onerosidade impõe, em caso de restrição a direito fundamental, que o meio escolhido seja o menos restritivo possível ao direito fundamental em questão. Em que pese a restrição imediatamente recair sobre a criptografia, não há dúvida de seu efeito mediato sobre o próprio direito fundamental à privacidade. Desta feita, incumbe perquirir que alternativas são possíveis à investigação criminal que não a fragilização da criptografia em si, com todos os efeitos danosos disso decorrentes.

Após o ocorrido no caso de San Bernardino perde força o argumento da imprescindibilidade de uma vulnerabilidade que permita superar a criptografia dos dispositivos. Isso ocorre porque a tecnologia está em constante evolução e assim também estão as ações e técnicas de hackeamento, de modo que o que parece impossível no atual momento pode ser alcançado em um futuro breve, o que obriga companhias de tecnologia a superarem seus limites na criação de sistemas cada vez mais fortes, à medida em que se aperfeiçoam as técnicas investigativas. Foi exatamente o que aconteceu após as revelações de vigilância estatal pela NSA feitas por Snowden. Sabendo que a a criptografia de seus dispositivos já poderia ser quebrada pela referida agência, Google[699] e Apple[700] fortaleceram

---

[699]SOGHOIAN, Chris. Keeping the Government Out of Your Smartphone. **ACLU**, set. 2012. Disponível em: <https://www.aclu.org/blog/national-security/keeping-government-out-your-smartphone?redirect=blog/technology-and-liberty-national-security-free-speech/keeping-government-out-your-smartphone>. Acesso em: 18 abr. 2018.

[700] GREEN, Matthew. Why can't Apple decrypt your iPhone? **Cryptography Engineering**, out. 2014. Disponível em: <https://blog.cryptographyengineering.com/2014/10/04/why-cant-apple-decrypt-your-iphone/>. Acesso em: 18 abr. 2018.

os seus sistemas criptográficos com vistas a não mais terem seus dispositivos violados e garantir a manutenção de suas parcelas de mercado.

Impende ressaltar que é sempre menos danoso que as próprias autoridades encontrem meios de acessar arquivos criptografados a obrigar as fabricantes de aparelhos e criadores de aplicativos a criarem vulnerabilidades no sistema, que servirão para afetar a todos. Ora, impor este ônus aos fabricantes implica em impor que viole seu próprio modelo de negócios, baseado na garantia da segurança de seus dispositivos, obrigando-o a criar vulnerabilidade geral que compromete a eficiência de sua atividade econômica. Não deve ser comum em regimes democráticos que, em uma democracia, empresas sejam impelidas a fazer as vezes de agência de vigilância estatal.

Cumpre verificar se, para as situações em que autoridades de investigação efetivamente não consigam acesso ao conteúdo criptografado da comunicação, é possível se pensar em alternativas que não comprometam a integridade de todos os dados que utilizam determinado protocolo criptográfico.

A primeira alternativa à obtenção dos dados em si seria a obtenção dos metadados. Conforme se viu no capítulo anterior, os metadados podem revelar muito mais que o conteúdo da comunicação, vez que revelará dados de localização dos interlocutores, volumes de dados trocados, dia e horário da comunicação, a lista de contatos frequentes. Todas essas informações permitirá a formação de um dossiê digital que certamente revelará muito mais que a própria comunicação. Tamanha é a importância dos metadados que a União Europeia reconheceu a necessidade de protegê-los enquanto direito à privacidade na era digital. Todavia, no caso do Brasil, o Marco Civil da Internet[701] permite a coleta e o fornecimento de metadados, constituindo uma alternativa viável e menos invasiva que o acesso ao conteúdo da comunicação em si.

Embora a comunicação esteja cifrada, outra alternativa viável é se acessar algum backup do aparelho que tenha sido feito pelo usuário. Não é incomum que seja realizado um backup dos dados do celular que ficam armazenado nas nuvens (*cloud computing*). Ressalte-se que a criptografia ponta a ponta protege o conteúdo dos dados trocados de uma ponta ou outra, mas uma vez realizada cópia de segurança dos dados do celular para uma nuvem, esta

[701] Art. 15. "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.(...)§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo".

não necessariamente estará protegida pela criptografia, o que facilita o trabalho da investigação[702].

A terceira alternativa que se apresenta é a apreensão do próprio dispositivo em poder do criminoso, caso o desbloqueio do aparelho não esteja protegido por criptografia. Ora, aqui as possibilidades de se obter o conteúdo da comunicação aumentam, sem que se comprometam os outros usuários. Isso porque pode-se apreender o aparelho de qualquer das pontas de comunicação, aumentando a probabilidade de êxito. Não custa repisar, no entanto, que mesmo nos aparelhos de acesso criptografado, o caso de San Bernardino já provou que um espelhamento da memória permitiria acessar o conteúdo do dispositivo.

3.8 **Do suposto conflito entre criptografia e segurança pública: há solução?**

Conforme tratado no capítulo anterior, qualquer objeção à utilização indiscriminada de dados que vise proteger a privacidade dos usuários e limitar atividades invasivas, costuma desaguar no debate manipulado de que haveria uma escolha binária: caso se queira mais privacidade na limitação da atividade de vigilância, haverá menos segurança.

Isso não é diferente no caso da criptografia. Os apelos de setores técnicos e de instituições de defesas de direito civil que se opõem ao enfraquecimento não pouco frequentemente esbarram em oposição das agências de investigação que afirmam que, sem um acesso privilegiado à informação criptografada, haverá menos segurança para os cidadãos. Este discurso é reverberado por líderes populistas que, em vez de encontrar soluções de combate ao crime que exponham menos o cidadão, propõem medidas legislativas que obrigam empresas de tecnologia a fraudarem os próprios sistemas de segurança que integram seu próprio valor de mercado.

Alega-se desta forma que crimes como pedofilia, pornografia infantil, sequestro, tráfico internacional de armas e drogas, ciberbullying, assédio, atentados terroristas ou execuções em massa somente seriam elucidados caso não houvesse a proteção da criptografia nos dispositivos dos criminosos. Tal visão ignora que a atividade criminosa migrará para o ambiente mais seguro, de modo que, identificada qualquer vulnerabilidade em um protocolo criptográfico, a atividade criminosa passará a optar por outros meios mais seguros. Não custa

[702] No caso dos dispositivos da Apple, há a informação que os backups de arquivos armazenados no iCloud são criptografados tanto no trânsito quanto no armazenamento, embora no armazenamento, apenas alguns arquivos contem com a criptografia. As informações estão disponíveis na página de suporte da Apple: <https://support.apple.com/pt-br/HT202303>. Acesso em: 14 abr. 2018.

lembrar que, com as decisões do judiciário brasileiro de bloqueio do aplicativo WhatsApp, imediatamente a base de clientes de outros aplicativos que também utilizam criptografia como o Telegram foi inflada, causando uma artificial migração da parcela de mercado[703]. Decerto que boas ou más pessoas migraram de aplicativo, com a intenção apenas de ver mantida a sua privacidade ou mesmo de praticar atos ilícitos.

Qualquer tentativa de limitar a qualidade da criptografia ou condenar sua utilização, porque eventualmente seu uso poderá ser distorcido, é o mesmo que inviabilizar o acesso de todos aos portos e rodovias porque se utilizam estes modais para a prática de crimes, o que causará necessariamente uma mudança de rota para outras estradas ou portos.

Conforme tratado, é consenso na comunidade cientifica que a introdução de qualquer vulnerabilidade no protocolo de criptografia, implica em uma menor segurança geral, já que esta fraqueza poderá ser explorada por terceiros, como foi no passado e recentemente. Ora, o enfraquecimento da criptografia não trará mais segurança de fato, apenas haverá uma falsa sensação de segurança, de modo que estados, grandes corporações e organizações criminosas terão expertise para garantir sistemas criptográficos fortes e o cidadão comum terá sua privacidade exposta.

Há que se relacionar o direito fundamental à privacidade diretamente com a garantia de segurança e não o contrário. Garantir a privacidade implica em garantir mais segurança à integridade psíquica e física do cidadão. Da mesma forma, caso se fragilizem os meios de se garantir a privacidade, fragilizada será também a segurança da comunicação de todos.

Portanto, assim como no *big data* o real dilema é a oposição entre privacidade/criptografia e vigilância, essa última viabilizada pela falta de segurança nas comunicações. Desta forma, ao contrário de trazer mais segurança, a criação de vulnerabilidades intencionais aumentará o grau de incerteza sobre as íntegras relações do estado no uso do acesso privilegiado ao conteúdo criptografado, bem como quanto ao momento que este acesso privilegiado cairá na mão de criminosos ou estados totalitários.

Repise-se que a criptografia, seja qual for a sua finalidade, é baseada em protocolos padronizados de segurança. Significa dizer que, uma vez exposta a vulnerabilidade da criptografia de aplicativo de mensagem instantânea, é possível que esta vulnerabilidade seja também explorada em outras comunicações criptografadas.

---

[703]AGRELA, Lucas. Telegram ganha 1,5 mi de usuários com bloqueio de WhatsApp. **Exame**, dez. 2015. Disponível em: <https://exame.abril.com.br/tecnologia/telegram-ganha-1-5-mi-de-usuarios-com-bloqueio-de-whatsapp/>. Acesso em: 17 abr. 2018.

A relação entre privacidade e segurança é direta, de modo que o sigilo das informações médicas, o sigilo das informações bancárias, o sigilo entre advogado e cliente, o sigilo entre o jornalista e a sua fonte, o sigilo das denúncias realizadas por ativistas de direitos humanos, a oposição de grupos minoritários, especialmente em regimes totalitários, mas não tão somente, todos esses casos demandam privacidade, que se relaciona intimamente com a segurança social. Do contrário, não havendo privacidade, haverá menos segurança ao se transmitir dados médicos entre hospitais ou entre hospital e pacientes; a fonte da atividade jornalística se colocará em risco de vida; o ativista de direitos humanos sofrerá intimidação em suas atividades caso seja monitorado; as oposições minoritárias deixarão de fiscalizar o poder e terão seu discurso calado[704].

Logo, o que há é um *trade off* com os padrões ouro de segurança da informação, representado pela criptografia forte, sem que haja em troca qualquer benefício aparente. O benefício temporário obtido pelos órgãos de investigação será às custas da privacidade de todos os outros usuários não inseridos na atividade criminosa, de maneira que a sanção de algum modo passará do investigado a alcançar aqueles que praticam atividades lícitas.

Com o uso de *backdoors* ou chave mestra, a vulnerabilidade se espraia por todo o sistema. Sendo consenso de que há perda de segurança, resta saber que grau de segurança se está disposto a perder ou mesmo se juridicamente há grau negociável de perda de privacidade.

Neste sentido, o relatório da Comissão Especial das Nações Unidas, para além de defender que os estados membros se abstenham de enfraquecer mecanismos de criptografia e anonimato – também defende que, com vistas a preservar a liberdade de expressão e de opinião dos usuários, o marco normativo de persecução penal que vise acessar o conteúdo da comunicação deverá preferir o uso da desencriptação direcionada (*target decryption orders*)à exigência de uma chave de revelação (*key disclosure*)[705].

A diferença é que a chamada *key disclosure* funcionaria como uma espécie de chave de abertura que poderia ser utilizada para todo o sistema criptográfico, enquanto a ordem direcionada de decifragem se direcionaria apenas ao suspeito. Neste trabalho, não se sabe precisar se é tecnicamente viável a adoção de uma ou outra medida, em razão do fato de as

---

[704] Essa foi a colocação de Diego Aranha, especialista em criptografia, em sua exposição na audiência pública que tratava do bloqueio de aplicativos e Marco Civil da Internet, ressaltou tais pontos. STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 132.Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

[705] KAYE, David. Op. cit., p. 15.

empresas de tecnologia afirmaram que a criptografia ponta a ponta é segura a ponto de impedir que o próprio aplicativo tenha acesso ao conteúdo da mensagem, de modo que cada mensagem enviada seria cifrada com uma chave diferente[706]. A parte as possíveis variáveis tecnológicas, interessa verificar a juridicidade destas medidas.

Desta forma, caso o sistema criptográfico permita o fornecimento de chaves, a violação observará mais a proporcionalidade, na medida em que a ordem de decifragem for direcionada ao indivíduo específico *(target decryption orders)* e não com a utilização de um mecanismo que em tese possa alcançar a todos os indivíduos (*key disclosure)*, vez que isso revelará muito mais do que uma comunicação específica e poderá alcançar o conjunto de comunicações criptografadas com aquela chave.

Deve-se noticiar que alguns países da Europa adotam a obrigatoriedade de que as empresas de comunicação apresentem uma "chave de revelação", podendo-se citar o Reino Unido, França e Espanha[707]. Não se sabe se há viabilidade técnica para a medida e se de fato se lançou mão destes instrumentos, pois, a exemplo do caso do Reino Unido aqui já tratado, tais ordens de desencriptação costumam ser secretas.

Portanto, caso possível e, emregra, a ordem de desencriptação deve ser antes de mais nada limitada ao escopo de indivíduos definidos, determinado por autoridade judicial independente e apenas implementado quando imprescindível à investigação, quando não há outros meios disponíveis[708].

Em conclusão a este tópico, ao tratarmos da inviolabilidade de criptografia assimétrica nas comunicações privadas e da contraposição do interesse das autoridades investigativas, não

---

[706] "Mais um ponto importante aqui - e já foi citado anteriormente - é que o WhatsApp gera uma chave única de encriptação para cada mensagem, ou seja, a cada mensagem que é enviada, uma chave diferente é utilizada. Isso é um ponto importante. Isso se chama, no meio, de *forward secrecy*, que é a segurança para frente, segurança futura. Por quê? Porque, se você, por algum modo, por algum meio, tiver acesso a uma chave, ela só servirá para decriptar aquela única mensagem; você não pode usá-la para voltar atrás e decriptar as mensagens anteriores. Então, é uma chave por mensagem. E, mais importante, essas chaves de encriptação e decriptação não deixam os aparelhos dos usuários, elas não saem dos terminais, não passam pelos servidores do WhatsApp. Isso é um ponto importante. Existem chaves nos servidores do WhatsApp? Existem, mas não são as chaves de encriptação e decriptação; são as chaves públicas". STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 178. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInternetеBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

[707] No Reino Unido, foi estabelecida a obrigação de fornecimento da chave criptográfica (UNITED KINGDOM. Regulation of Investigatory Powers Act, 2000. Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf>. Acesso em: 10 abr. 2018). Na França também se estabeleceu o de fornecimento da chave criptográfica, desde que autorizada por um juiz (França, Lei No. 2001-1062); Na Espanha, da mesma forma se estabeleceu a obrigação de chave criptográfica (Epanha, Lei de Telecomunicações n. 25/2007).

[708] KAYE, David. Op. cit., p. 16.

se pode afirmar que há um conflito entre privacidade e segurança. A abordagem maniqueísta cria uma falsa oposição a ideias que são próximas: tanto a investigação criminal quanto a criptografia promovem a segurança do indivíduo, ainda que em campos distintos, é bem verdade. A colocação da discussão no lugar devido evita discussões apaixonadas e polarizadas que tem caracterizado o Brasil nos últimos tempos, como se quem militasse pela privacidade tivesse algum fato criminoso a esconder e quem defendesse o fim da criptografia forte estivesse sempre imbuído das melhores intenções. Em resposta à pergunta que inicia este tópico, talvez não seja possível resolver definitivamente o conflito existente entre o uso da criptografia e as investigações policiais. É certo que a criptografia remete ao direito à privacidade (art. 5º, X) e à liberdade de comunicação, admitindo-se a sua restrição apenas em virtude de conflitos com outros bens constitucionais ou direitos fundamentais relevantes cuja legitimidade de restrição apenas poderá ser aferida no caso concreto[709]. Todavia, tentar-se-á no tópico seguinte estabelecer alguns parâmetros.

3.9 **Criptografia e combate ao crime: a harmonização possível entre interesses conflitantes**

Do que foi apresentado até aqui, pode-se perceber que o principal óbice à implementação da criptografia de amplo acesso e inviolável é o interesse das agências de investigação, para as quais a alegada impossibilidade de acessar o conteúdo criptografado seria ilegal, vez que acobertaria práticas criminosas das mais variadas.

Deve-se ressaltar que o objetivo deste tópico não é verificar se a Constituição brasileira, nos termos do art. 5º, inciso XII, permite a interceptação de dados. Embora o tema encerre algumas controvérsias, a questão foi brevemente discutida no item 1.3.2, no capítulo anterior, no qual nos posicionamos pela possibilidade de quebra de sigilo de dados, desde que haja ordem judicial, tanto para os dados armazenados, quanto para os dados em transmissão, entendimento este consentâneo com as disposições adotadas pelo Marco Civil da Internet. Ademais, em que pese a matéria estar submetida à Suprema Corte, através da ADI 4112/DF, não há sinais concretos de que a Corte deverá conceder medida cautelar, suspendendo o dispositivo previsto no art. 1º, parágrafo 1º da Lei 9296/96.

Se a possibilidade de haver uma chave privilegiada ou porta dos fundos fizesse parte do protocolo criptográfico, consoante o modelo de negócios concebido, a despeito de toda

[709] Essa é a opinião de Ingo Sarlet. SARLET, Ingo; MARINONI, Luiz Guilherme; MITIDIERO, Daniel *et al*. Curso de Direito Constitucional. 5. ed. rev. e atual. São Paulo: Saraiva, 2016, p. 447.

recomendação contrária dos setores de tecnologia, não resta dúvidas que havia o dever por parte do gestor do aplicativo de cumprir as decisões judiciais que determinassem o fornecimento do conteúdo das comunicações, vez que entendemos constitucional a legislação que regula a quebra do sigilo de dados.

Todavia, ainda que se parta do pressuposto da possibilidade de determinação judicial da quebra do sigilo de dados, neste tópico cumpre analisar questão diversa, a saber, a constitucionalidade da determinação judicial ou legal da quebra de sigilo de dados, na hipótese em que estes dados estão protegidos por criptografia forte, pressupondo-se que sua violação seja tecnicamente inviável por terceiros, bem como pelo responsável pela aplicação, a não ser que se criem vulnerabilidades que coloquem em risco todos os outros usuários.

Dos fatos até agora apurados, não há informação precisa se há a possibilidade de se atacar e obter sucesso na quebra da cifragem de apenas uma conversa ou um usuário. Não se sabe ainda com precisão como o FBI norte americano violou a criptografia do criminoso no caso de San Bernardino, havendo-se apenas especulações. Atendo-se ao caso específico da utilização da criptografia nos aplicativos de troca de mensagem via web, a fim de delimitar a hipótese concreta, cumpre investigar duas hipóteses: (i) é constitucionalmente legítima a criação de protocolos criptográficos fortes, cujo conteúdo seja inviolável pelo próprio criador e por terceiros, sem que se institua um acesso privilegiado para autoridades investigativas?; (ii) poderia o poder público obrigar o proprietário do aplicativo que crie uma vulnerabilidade para permitir o acesso de autoridades ao conteúdo criptografado?

Portanto, verifica-se haver duas ideias em oposição: de um lado, a criptografia, que garante a confidencialidade das comunicações, e, por conseguinte, a privacidade e outras liberdades existenciais como a liberdade de expressão, as autonomias privada e pública, entre outros; de outro, está o interesse público de que as investigações de condutas criminosas cheguem a termo, com a responsabilização dos envolvidos, a fim de se garantir a estabilização social. Por certo que ninguém se opõe que haja investigação criminal. Todavia, no mundo real, a fronteira entre as boas intenções de agentes estatais e o desvio de poder é bastante tênue, devendo-se levar em consideração ainda que, em matéria de tecnologia de segurança da informação, a vulnerabilidade, uma vez criada, pode ser explorada por todos que a descubram.

Ambas as ideias remetem a valores constitucionalmente protegidos. A primeira delas remete ao direito fundamental à privacidade, cuja sede geral se localiza no artigo 5º, inciso X, da Constituição da República, havendo outras passagens que protegem manifestações da privacidade. Em sentido oposto está o direito à segurança, cuja previsão está contida em

variados dispositivos constitucionais, destacando-se o *caput* do art. 5º que garante a sua inviolabilidade[710], ao enunciar os direitos e garantias individuais; o *caput*do art. 6º que prevê entre os direitos sociais o direito à segurança[711], sendo de maior adequação ao caso a previsão do *caput* do artigo 144 da Constituição que prevê a segurança pública como dever do Estado, direito e obrigação de todos[712]. Por vezes, pode ser que a segurança pública seja concretizada na situação fática através de ação de policiamento investigativo ou mesmo ostensivo, que evite a ocorrência de situação danosa, como é o caso do impedimento de um atentado terrorista. Por outro, pode ser que a ação de segurança pública através da ação de polícia judiciária, na investigação de infrações penais, com vistas a elucidar crimes e evitar a instabilidade social trazida pela impunidade e pelos altos níveis de criminalidade.

As normas supramencionadas não estabelecem uma regra explícita acerca da conduta a ser adotada diante do uso da criptografia e sua inviolabilidade por autoridades investigativas. O que há são dois princípios constitucionais, igualmente aplicáveis ao caso. Nesta situação, os elementos tradicionais de interpretação (gramatical, histórica, semântica e teleológica), aplicados através da técnica da subsunção não são suficientes, vez que há a incidência de normas constitucionais da mesma hierarquia, indicando soluções distintas, caracterizando o que se chama de *hard case* ou caso difícil[713]. Para tanto, é aplicável a técnica da ponderação ou sopesamento, destinada a resolver conflitos entre normas válidas e incidentes sobre um caso e promover, o tanto quanto for possível, a otimização de ambas as normas incidentes em conflito. O uso dessa técnica envolve a identificação dos interesses contrapostos em determinado caso concreto e a eventual restrição de um deles com vistas a otimizar ambos na máxima medida possível. Casos há nos quais não será possível prestigiar ambos os interesses e necessariamente haverá a priorização de um dos interesses em conflito[714].

---

[710]Art. 5º "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:".

[711]Art. 6º "São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição".

[712]Art. 144. "A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:".

[713] Sobre as técnicas tradicionais de interpretação jurídica e resolução de colisões entre normas constitucionais, vide BARROSO, Luís Roberto. **Curso**... Op. cit., p. 334-335.

[714] SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. Op. cit., p. 511.

Com efeito, não se pode dizer aprioristicamente sempre o que prevalecerá na ponderação, vez que a ponderação levará sempre em conta as circunstâncias do caso, o cenário fático e as alternativas eventualmente existentes. Portanto, apenas diante da situação concreta poderá se dizer, sob a ótica da proporcionalidade, qual será o princípio prevalente, não havendo que se falar em prevalência abstrata no interesse da segurança pública ou do direito à privacidade.

Não nos ateremos neste trabalho aos objetos específicos tratados na Ação Direta de Constitucionalidade nº5527 e na Ação de Descumprimento de Preceito Fundamental n ADPF 403, as quais, por vias distintas, visam evitar ordens judiciais de bloqueio de aplicativos de mensagens instantâneas via web que utilizam a criptografia forte como técnica de segurança. Também não será objeto deste tópico a pretensão de resolver com caráter de definitividade o conflito entre criptografia forte e o interesse público existente nas investigações criminais. O que se fará neste tópico será analisar algumas hipóteses concretas, vez que a ponderação é técnica cujo resultado apenas pode ser defendido contingencialmente.

A primeira hipótese formulada acima consiste em questionar se é constitucionalmente legítima a criação de protocolos criptográficos fortes, cujo conteúdo seja inviolável pelo próprio criador e por terceiros, sem que se institua um acesso privilegiado para autoridades investigativas. Para resolver a hipótese colocada, pode-se objetar que este não seja um caso de ponderação, criando-se desnecessariamente uma inflação ponderativa[715], a partir da ampliação artificial do âmbito de proteção de determinada norma, a ponto de vulgarizar a ponderação para casos típicos de subsunção.Particularmente, entendemos que esta é a melhor forma de solucionar a questão, conforme se explicitará.

Neste sentido, poder-se-ia afirmar que sobre o caso apenas incidiria o princípio da livre iniciativa, insculpido no art. 170, *caput*, da Constituição da República e, portanto, poder-se-ia concluir que a conduta estaria afeta ao âmbito de proteção da livre iniciativa permite a criação de qualquer modelo de negócio que não cause dano a terceiros e, em uma economia de mercado, as ideias não são submetidas ao Estado, mas ao escrutínio dos consumidores que decidiram a conveniência ou não do uso da ferramenta.

Todavia, especialmente em sendo a Constituição de 1988 de inegável caráter social como é a brasileira, que possui entre seus objetivos a redução das desigualdades sociais (art. 3º, III), não parece coerente afirmar o indivíduo como ser atomizado, livre para qualquer iniciativa que lhe aprouver, sem compreender que, no contexto constitucional brasileiro, o

[715] A expressão é de Daniel Sarmento e Cláudio Pereira de Souza Neto. Ibidem, p. 517.

indivíduo não pode ignorar os vínculos que possui com a comunidade e deixar de observar deveres sociais impostos a todos.

Logo, em uma outra abordagem pode-se defender que a livre criação de softwares de segurança, mediante estabelecimento de chaves criptográficas fortes, constitui decorrência da autonomia do indivíduo, em razão da capacidade de realizar escolhas morais autônomas, enquanto elemento da dignidade da pessoa humana. Nesta linha existencial, e para recorrer a um direito fundamental menos abstrato que a dignidade humana, pode-se dizer que a criação de dispositivos e aplicações criptográficas, constitui manifestação da liberdade de expressão da atividade intelectual (art. 5º, IX da Constituição), já que a construção de protocolos criptográficos nada mais são do que criação de chaves, através de complexos cálculos matemáticos, convertidos em linguagem de programação. Com efeito, é a complexidade do código fonte e sua pouca suscetibilidade a ataques e outras vulnerabilidades que garantem a inviolabilidade da transmissão do dado criptografado.

Partindo do pressuposto que incidiria no caso apenas a liberdade de expressão, não havendo que se falar em segurança pública em abstrato, há que se ressalter que, em regra, a liberdade de expressão se exerce sem condicionantes prévios, responsabilizando-se a posteriori seu autor em caso de dano. Isso não significa dizer que a liberdade de expressão não sofra conformações com outros direitos fundamentais de similar relevância.

Com efeito, da diferenciação entre princípios e regras, é possível apontar variadas formas de eficácia dos princípios constitucionais. A eficácia direta permite a aplicação do princípio à situação concreta, sem intermediação legislativa, regendo a realidade semelhantemente a uma regra e extraindo-se do princípio um comando para a situação concreta. No que tange à eficácia interpretativa, trata-se da propriedade de condicionar o sentido e o alcance de outras normas jurídicas em geral. Dentro da eficácia interpretativa, cabe destacar o papel integrativo desempenhado pelos princípios, que permite que a dignidade humana seja fonte de direitos não expressamente enumerados ou como critério de preenchimento de lacunas normativas[716].

Neste caso, pode-se aplicar diretamente a liberdade de expressão ao caso para entender que não há óbices à criação e utilização de um software que utiliza criptografia forte, sem que necessariamente haja regra legal permitindo ou regulamentando a prática.Aplicar-se-ia ao caso ainda o princípio da dignidade da pessoa humana, que constitui fundamento moral e

[716]BARROSO, Luís Roberto. **A dignidade da pessoa humana... Op. cit., p. 300**

jurídico dos direitos fundamentais[717]. Enquanto fundamento e vetor interpretativo dos direitos fundamentais, a dignidade da pessoa humana possui um conteúdo mínimo, composto por três elementos essenciais, quais sejam, o valor intrínseco da pessoa humana, a autonomia da vontade e o valor comunitário[718]. Importa tratar aqui do valor intrínseco da pessoa humana, cujo conteúdo contempla um postulado de ordem antiutilitarista e antiautoritário. A perspectiva antiutilitarista parte da máxima kantiana do homem enquanto fim em si mesmo, obstando qualquer tentativa de instrumentalização da pessoa humana para o atingimento de metas coletivas ou mesmo projetos sociais de terceiros[719]. O elemento autonomia compreende a pessoa humana enquanto ser autônomo, capaz de realizar escolhas morais, escolhas tais que não podem ser submetidas a considerações coletivizantes ou escolhas morais de terceiros.

Neste sentido, o valor intrínseco da pessoa humana obstaria qualquer medida utilitarista que visasse limitar o uso da criptografia - que, repise-se, garante a privacidade e a liberdade de expressão, apenas para citar alguns exemplos – em nome de pretensões sociais. Portanto, uma alusão genérica às necessidades da sociedade ou mesmo às razões de Estado para limitar a criptografia, revela um viés utilitarista ou mesmo autoritário, vedado pela dignidade da pessoa humana.

Por outro lado, caso se admita haver conflito de normas, em razão da incidência de normas igualmente constitucionais, em sentido contrário à utilização da criptografia sem acesso privilegiado estaria o direito à segurança pública, o que se colocaria em oposição à livre criação de softwares de transmissão criptografada. Ocorre que aqui se estaria opondo o direito à segurança pública apenas em tese, sem que se possa precisar que efeitos a ausência da criação do acesso privilegiado teria sobre a redução da segurança pública. Significa dizer que, sem a situação de risco concreto à segurança dos demais cidadãos, que enseje fundamento à quebra do código criptográfico, há relevante dificuldade em fundamentar uma restrição geral à criptografia usufruída por todos.

Ora, não se pode alegar um risco geral à segurança como se a comunicação por aplicativos criptografados fosse o único meio de prova disponível, sem se fundamentar em concreto quais seus impactos no andamento de investigações. Por outro lado, sem se afirmar qual o risco concreto a criptografia impõe à segurança pública, mas apenas abstrato,

---

[717] Ibidem.

[718] Neste ponto, adota-se a classificação da Luís Roberto Barroso. Todavia, em nota de rodapé no tópico 1.3 deste trabalho, poder-se-á conferir as definições dos elementos da dignidade humana, bem como as abordagens doutrinárias alternativas do relevante princípio.

[719] BARROSO, Luís Roberto. Op. cit., p. 306.

fundamenta-se uma restrição geral e abstrata à privacidade de todos os usuários, com a exigência de vulnerabilidades que comprometem a segurança do próprio meio.

Pode-se cogitar de alguns impactos da criptografia concretos à segurança pública, afirmando-se que os crimes de natureza cibernética ou que utilizam a internet teriam o seu combate seriamente comprometido, sendo possível exemplificar com a articulação de células terroristas, a circulação da pornografia infantil, o aliciamento sexual de crianças e adolescentes, os crimes de ódio, praticados sob relativo anonimato, entre outros.

Todavia, não é verdade que a criptografia, especialmente a utilizada por aplicativos de mensagens inviabilizem as investigações. A investigação policial se processa como um quebra-cabeças, na qual se reúnem variados indícios para se apurar a autoria e materialidade da ação delituosa. Dificilmente a atividade criminosa ocorrerá exclusivamente através de um meio. Pode até ser que se utlize o referido aplicativo como meio principal para crimes digitais, mas nunca de modo exclusivo, vez que a atitude criminosa deixará outros rastros digitais e físicos. Logo, uma imagem ou vídeo trocada pelo aplicativo estará no aparelho físico de todos os membros do grupo criminoso; eventualmente, as imagens de pedofilia serão baixadas para os celulares, computadores e tablets dos membros da organicação, bastando que se realize a busca e apreensão de apenas um dos dispositivos.

Ademais, pela localização das antenas de transmissão será possível determinar a localização dos aparelhos telefônicos dos membros da organização, verificando-se em que locais, ocasiões e com que frequência se encontraram, possibilitando operações policiais nos locais onde possa haver indícios da atividade criminosa. Os metadados podem informar o fluxo de dados trocados entre os criminosos, os contatos preferenciais, o tipo de arquivo trocado, as pesquisas de interesse na internet, entre outros. Sem contar que as forças policiais sempre poderão, com a expertise que possuem, infiltrar seus agentes nos grupos de mensagens das organizações criminosas, como já ocorreu com êxito. Diante de todas as possibilidades apresentadas, há difícildade em afimar que a comunicação por meio de aplicativos é o único ou um dos poucos indícios que resta à investigação judicial ou que mesmo o conteúdo das comunicações não possa ser obtido por outros meios, especialmente que não comprometa a privacidade de outros indivíduos. Logo, revela-se essencial que neste conflito se demontre eventual dano concreto à segurança pública que justifique tamanha restrição a direito fundamental. Do contrário, o subprincípio da necessidade não estará atendido.

Cabe ainda realizar análise da questão sobre a ótica da proporcionalidade em sentido estrito. Vê-se que a proibição da criação do aplicativo constitui restrição elevada à autonomia

privada e, por conseguinte, à liberdade de expressão, sem que se demonstre que benefícios concretos, superiores aos riscos aos direitos fundamentais correlatos à privacidade, a restrição propicia.

Portanto, em resposta à primeira formulação, tanto no caso de se entender que a resolução da questão se dará pela subsunção, com a aplicação direta da liberdade de expressão, quanto no caso de entender haver ponderação com outros valores constitucionais contrapostos, pode-se afirmar ser constitucionalmente legítima a criação de protocolos criptográficos fortes, cujo conteúdo seja inviolável pelo próprio criador e por terceiros, sem que se institua um acesso privilegiado para autoridades investigativas, vez que ninguém deve ter obstada ou limitada a sua liberdade de expressão, através da atividade intelectual, em nome de metas coletivas, de viés utilitário ou autoritário.

Cumpre investigar a resposta à segunda hipótese estabelecida, qual seja, se poderia o poder público obrigar o criador de aplicativo ou dispositivo criptografado a criar uma vulnerabilidade para permitir o acesso de autoridades ao conteúdo protegido para fins de investigação criminal.

Nesta hipótese, inequivocamente há em rota de colisão normas constitucionais igualmente aplicáveis, de modo que a técnica interpretativa adequada será a ponderação. Na situação proposta de há, em primeiro lugar e de modo mais vidente, o direito à privacidade que a criptografia visa resguardar, além da liberdade de expressão dos criadores da aplicação ou dispositivo.

Do outro lado, a decisão de determinar a criação de uma porta dos fundos nas aplicações que utilizam criptografia apenas pode ser remetida ao interesse público em apurar o cometimento de infrações penais ou mesmo na investigação que visa evitar ou interromper o cometimento de infração penal. Portanto, tais interesses constitucionalmente legítimos podem ser remetidos à segurança pública, cuja principal sede reside no art. 144, *caput*, da Constituição da República.

Como se sabe, a ponderação entre normas colidentes igualmente aplicáveis é realizada em três etapas: (i) a identificação de normas relevantes para a solução do caso, identificando eventuais conflitos entre elas; (ii) identificar os fatos e circunstâncias do caso concreto e sua interação com a norma; (iii) a realização da ponderação propriamente dita, a partir do critério da proporcionalidade, com a verificação das normas e fatos em conjunto, para definir qual

norma será aplicada com maior ou menor intensidade, à luz das circunstâncias jurídicas e fáticas[720].

Portanto, no caso que se propôs resolver, na primeira etapa, cumpre identificar os grupos de fundamentos normativos como já foi feito: de um lado, figuram a liberdade de expressão, a privacidade e a autonomia pessoal; de outro, o interesse público consistente nas ações de segurança pública que pode estar imbuído no mister de proteger a vida, a integridade física, a integridade sexual, a proteção à criança e adolescência, entre outras condutas criminosas.

Pois bem, as circunstâncias gerais do caso concreto são conhecidas. Setores ligados à tecnologia alegam que qualquer vulnerabilidade propositalmente introduzida, tais como porta dos fundos ou chave mestra, comprometerá a segurança do sistema como um todo e poderá ser explorada por qualquer um que descobrir tais falhas, isso sem contar o risco deste acesso especial chegar a mãos criminosas ou a estados totalitários. Por outro lado, setores ligados à investigação afirmam que a criptografia favorece à criminalidade na medida que cria espaços de impunidade, não alcançados pelas autoridades policiais.

Cumpre na terceira etapa realizar a ponderação propriamente dita, para a qual será utilizado como critério o princípio da proporcionalidade, a partir de seus três subprincípios (adequação, necessidade e proporcionalidade em sentido estrito), o que não significa dizer que ponderação e proporcionalidade se confundam. Em que pese serem conceitos próximos, ponderação e proporcionalidade não se confundem, vez que a ponderação pode utilizar critérios outros para além da proporcionalidade, não se resumindo a este, bem como pode a proporcionalidade ser aplicada a outros conflitos que não o de normas constitucionais[721]. No entanto, permanece a proporcionalidade sendo o principal critério de resolução de conflito normativo através da técnica da ponderação.

O primeiro subprincípio da proporcionalidade é a adequação ou idoneidade, segundo o qual toda a restrição a determinado direito fundamental deve servir a um fim constitucionalmente legítimo. Portando, há que se verificar duas hipóteses: se o fim que justifica a restrição é constitucionalmente legítimo e se consiste em um instrumento adequado ao atingimento deste fim[722]. No caso proposto, o interesse público presente na realização de

---

[720] Sobre as técnicas tradicionais de interpretação jurídica e resolução de colisões entre normas constitucionais, vide BARROSO, Luís Roberto. **Curso**... Op. cit., p. 334-335.

[721] Veja MATHEWS, Jud; SWEET, Alec Stone. All Things in Proportion? American Rights Doctrine and the Problem of Balancing. **Emory Law Journal**, v. 60, n. 4, p. 799-875, mar. 2010.

[722] PEREIRA, Jane Reis Gonçalves. Os imperativos da proporcionalidade e da Razoabilidade... Op. cit., p. 174.

ações de segurança pública possui legitimidade constitucional, haja vista sua localização específica no art. 5º, *caput*, e 144, *caput*, da Constituição, apenas para citar alguns exemplos. Ainda que assim não o fosse, permaneceria a sendo um fim constitucionalmente legítimo, haja vista sua missão em proteger a vida, à integridade física e o patrimônio diante de danos iminentes ou causados. Do mesmo modo, nos parece que o levantamento da criptografia forte através do fornecimento de uma chave mestra se mostra idôneo a realizar o interesse público presente nas ações de segurança pública, seja para evitar o cometimento de um crime, seja para apurar a autoria e materialidade de infrações penais já cometidas.

O segundo subprincípio a ser verificado é o da necessidade, também conhecido como subprincípio da menor onerosidade, da indispensabilidade, do meio menos restritivo, da intervenção mais restringida possível ou do direito à menor desvantagem possível, entre outras nomenclaturas[723]. O referido subprincípio consiste na imposição de que a restrição a direito fundamental adotada observe o meio menos lesivo ao direito restringido, envolvendo a análise comparativa entre os variados meios igualmente idôneos para atingir determinado fim, optando-se necessariamente pelo menos oneroso. Portanto, há duas fases no atendimento ao princípio da necessidade, a saber, a verificação dos meios de igual idoneidade ao atingimento do fim e a escolha do meio menos oneroso ao direito fundamental restringido.

No caso em análise, a utilização de meio privilegiado de acesso ao conteúdo criptografado, embora adequada ao atingimento do fim segurança pública, não parece o único meio idôneo ao seu atingimento. No contexto da investigação policial, atendo-se ao exemplo da chave criptográfica de aplicativos de mensagens ou de conteúdo armazenados em dispositivos, é possível apontar outros meios que permitam fornecer informações importantes à atividade de investigação.

Para os aplicativos de mensagem, o primeiro meio alternativo é o uso de um agente infiltrado. Isso porque estes aplicativos permitem a criação de grupos com interesses semelhantes, de modo que um agente infiltrado, que simule partilhar os interesses de determinado grupo, poderia obter acesso ao conteúdo das mensagens trocadas, sem colocar em cheque toda a segurança do sistema, com o estabelecimento de uma vulnerabilidade. A prática foi adotada no Brasil durante a Copa do Mundo em 2014 e obteve êxito na identificação e prisão de célula terrorista do Estado Islâmico no país, que havia iniciado atos preparatórios para o cometimento de atentados[724]. Pode-se alegar que a alternativa do agente

[723] Ibidem, p. 183.

[724] A operação Hashtag da Polícia Federal foi realizada com a inserção de agente infiltrado em grupo de bate-papo que possui o conteúdo das mensagens criptografado. A operação foi a continuidade de um potencial

infiltrado é menos protetiva à segurança pública que a obtenção pura a simples do conteúdo da mensagem. A bem da verdade não o é. Isto porque a obtenção do conteúdo da mensagem ocorreria com a troca das chaves do aplicativo – através do ataque *man in the middle* - o que deixaria a manobra exposta a todos os membros do grupo, que, uma vez percebendo o monitoramento, poderiam deixar de trocar informações essenciais à investigação por aquele meio. Ademais, não se deve ignorar o fato que o uso do agente infiltrado é muito menos danoso que um acesso privilegiado que possa expor todos os usuários do aplicativo.

Mesmo no caso de dispositivos de conteúdo criptografado seria possível o acesso ao conteúdo criptografado sem que se tivesse acesso privilegiado. Conforme visto, após a recusa da Apple em criar uma versão de seu sistema operacional com vulnerabilidade para desbloqueio do acesso ao aparelho, o FBI obteve êxito no espelhamento da memória aparelho para conseguir quebrar a senha de acesso e assim desbloquear a criptografia. Decerto que a alternativa imposta pelo juízo no caso seria muito mais onerosa ao direito fundamental à privacidade, vez que a criação de uma versão do sistema operacional com a assinatura criptografada do assinante que contivesse vulnerabilidade capaz de permitir burlar a senha de acesso poderia ser usado naquele e em todos os outros aparelhos do fabricante, colocando em risco todos os usuários da marca que é conhecida no mercado pelos avançados mecanismos de segurança. Ademais, tal medida não seria apenas onerosa à privacidade, mas também à livre iniciativa, vez que a colaboração da empresa na criação de uma vulnerabilidade em seus dispositivos depreciaria seu valor de mercado, na medida em que os consumidores interpretariam a atitude como uma quebra de confiança e um risco de segurança em seus aparelhos. Logo, a medida imposta de se estabelecer vulnerabilidade no sistema operacional do dispositivo, não atenderia ao subprincípio da necessidade, haja vista os ônus que todos os usuários do aplicativo teriam que suportar.

Da mesma forma, há quem afirme que, no caso do WhatsApp, seria possível a violação das mensagens desde que se efetuasse a troca das chaves das mensagens que estão em espera antes de chegar ao dispositivo do destinatário que não está conectado à internet no momento da mensagem[725]. Esta vulnerabilidade é negada pelo aplicativo[726]. Sendo verdadeira

---

terrorista que era monitorado pela Agência Brasileira de Inteligência – Abin, por suspeita de vínculos com a organização terrorista Estado Islâmico. MASCARENHAS, Gabriel. Polícia Federal recorreu a infiltrado para obter dados de grupo suspeito. **Folha de São Paulo**, Brasíia, jul. 2016. Disponível em: <http://www1.folha.uol.com.br/esporte/olimpiada-no-rio/2016/07/1794611-policia-federal-recorreu-a-infiltrado-para-obter-dados-de-grupo-suspeito.shtml>. Acesso em: 17 abr. 2018.

[725] G1. **WhatsApp tem falha que permite ler conversa mesmo com criptografia, diz jornal.** Disponível em: https://g1.globo.com/tecnologia/noticia/whatsapp-tem-falha-que-permite-ler-conversa-mesmo-com-criptografia-diz-jornal.ghtml. Aceso em 10/04/2018

ou não a possibilidade, entende-se que impor ao proprietário do aplicativo explorar a vunerabilidade em seu próprio aplicativo violaria a livre iniciativa e a autonomia privada. Por óbvio que as autoridades investigativas, no legítimo exercício de suas funções, sempre poderão explorar vulnerabilidades descobertas e os responsáveis pelo aplicativo sempre poderão melhorar a segurança de suas aplicações, fechando essas e outras brechas. Não há nada de ilegal em nenhuma das condutas.

Outro meio alternativo menos oneroso é a utilização dos metadados para se obter informações úteis à investigação. Metadados são informações complementares a adicionais sobre os próprios dados que não estão protegidas pela criptografia. Conforme visto quando se tratamou de vigilância, os metadados assumem especial importância em relação à privacidade[727], na medida em que revelam muito mais sobre o indivíduo que os próprios dados, vez que é possível verificar seus dados de localização, contatos frequentes, fluxo de informações trocadas, dia e horário que as informações são trocadas.

Apenas para exemplificar, o aplicativo de mensagens WhatsApp informa em sua política de privacidade quais dados são coletados automaticamente, a saber, os dados fornecidos pelos usuários, por terceiros, os dados coletados por serviços terceirizados do aplicativo ou mesmo os dados coletados de empresas parceiras. Basicamente, tudo que não se refere ao conteúdo da mensagem pode ser coletado pelo aplicativo, variando de dados de contatos a informações do perfil, dados pessoais que constem em sites parceiros, localização, hábitos de navegação, entre outros[728]. Há ainda a possibilidade de se identificar determinado

---

[726] THE GUARDIAN. **The Guardian slammed WhatsApp for a "security backdoor"— it's actually just standards encryption**. Disponível em: https://qz.com/885212/whatsapp-says-its-security-backdoor-is-what-makes-encryption-easy-to-use/. Aceso em 10/04/2018

[727] Sobre a coleta de metadados e as redes sociais, cf. GRESCHBACH, Benjamin; KREITZ, Gunnar; BUCHEGGER, Sonja. The devil is in the metadata — New privacy challenges in Decentralised Online Social Networks. In:**Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on Pervasive Computing and Communications Workshops**, 2012, p. 333-339. Disponível em: <https://ieeexplore.ieee.org/document/6197506/>. Acesso em: 16 abr. 2018.

[728] Segundo consta da política de privacidade do aplicativo WhatsApp, entre os ditos dados fornecidos pelo usuário – e aqui não há a opção de deixar de fornecer pois há autorização nos termos de uso - está o número do telefone; os contatos atualizados frequentemente da agenda do usuário, seja este contato usuário do aplicativo ou não; os grupos e listas de transmissão de que o usuário participa; o nome e a foto do perfil; e a mensagem de status. Entre os dados coletados automaticamente uso e dados de registro (registros de diagnóstico, como o usuário interage com outros, como os serviços são utilizados); dados sobre transações (recibo de pagamento e processamento de pagamento pelos serviços em sites de terceiros, caso o aplicativo passe a ser pago); dados sobre dispositivos e conexões (características do dispositivo no qual é utilizado o aplicativo, dados do sistema operacional, dados sobre o navegador, endereço de IP, dados sobre a rede móvel, incluindo o número do telefone, e identificadores do dispositivo, informações de localização caso a localização seja compartilhada com terceiros, bem como localizações próximas ao usuário); cookies que coletam preferências do usuário e hábitos de navegação para personalizar os serviços. Entre os dados coletados de terceiros estão o contato do usuário constante da agenda ou de conversas com terceiros; os dados fornecidos pelos prestadores de serviço terceirizados sobre o usuário. Entre os dados coletados de serviços de terceiros estão forem usados com serviços

arquivo, mesmo sem que se tenha acesso ao seu conteúdo, utilizando-se a investigação do fluxo de conteúdo entre os usuários, especialmente se se tratar de arquivo viral[729], possibilitando-se estabelecer o caminho de determinados arquivos, ainda que não se viole o seu conteúdo. Na visão de técnicos, o viral poderia ser identificado porque, conforme visto aqui, cada arquivo ao ser criptografado ganha um resumo criptográfico único chamado de *hash*. Portanto, para especialistas, tal ferramenta poderia identificar, por exemplo, se pessoas estão compartilhando imagens de pornografia infantil, o que seria importante para cooperar com as autoridades investigativas, sem que se comprometa a privacidade de todos os usuários[730].

Para especialistas da área de tecnologia, os metadados dos aplicativos de mensagem que utilizam criptografia são capazes de resolver a maioria dos casos, sem que possa acessar as mensagens. Os metadados são, portanto, um importante instrumento à disposição das forças de investigação que revelam informações muito mais detalhadas sobre o usuário[731] e seria muito menos oneroso à privacidade de todos os usuários, haja vista o risco que representa uma quebra da criptografia. Conforme visto, o ordenamento jurídico brasileiro não impede o fornecimento dos metadados, bastando haver ordem judicial específica, vez que há

---

de terceiros estão os dados fornecidos pelo serviço ao utilizar o botão compartilhar no WhatsApp com os contatos, grupos e listas de transmissãodo aplicativo em um serviço de notícias, por exemplo de nossos ou ao optar por acessar os serviços por meio de promoção feita realizada por operadora de celular ou pela fornecedora do dispositivo. As informações estão disponíveis no site do aplicativo: <https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect/>. Acesso em: 10 abr. 2018.

729 "Viral é um termo que surgiu junto com o crescimento do número de usuários de blogs e redes sociais na internet. A palavra é utilizada para designar os conteúdos que acabam sendo divulgados por muitas pessoas e ganham repercussão (muitas vezes inesperada) na web". Saiba o que significa "viral na internet". EBC. http://www.ebc.com.br/tecnologia/2012/11/o-que-e-viral

730 Esta é a opinião do perito da Polícia Federal, Ivo de Carvalho Peixinho que representou a instituição na audiência pública realizada no Supremo Tribunal Federal. Todavia, a informação é controversa pois, segundo o criador do aplicativo Whatsapp, a identificação e armazenamento de arquivos virais ocorre pela identidade digital atribuída ao arquivo. Todavia, segundo o criador do aplicativo, o aplicativo não possui acesso ao conteúdo do arquivo, vez que este também estaria criptografado. Aqui neste trabalho, fazemos questão de mencionar esta hipótese, pois poderá ser um caminho futuro que as autoridades poderão seguir com o aperfeiçoamento das técnicas de investigação. Imagine-se, por exemplo, que as autoridades realizem a encriptação com a chave pública do usuário de determinado arquivo de conteúdo ilegal e a identificação seja a mesma do vídeo viral compartilhado. Neste caso, se poderá ter alguma certeza de onde partiu o conteúdo sem que se acesse o conteúdo. Todavia, trata-se de mera especulação deste autor, vez que os gestores do aplicativo não são claros quanto às técnicas desenvolvidas. Vide STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, pp. 49 e 96.Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

731 Manifestação de Demi Getchko (Conselheiro do Comitê Gestor da Internet no Brasil - Cgi.Br), Diretor/Presidente do Núcleo de Informação e Coordenação do Ponto Br.STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 81. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

previsão legal para que as aplicações efetuem a guarda dos registros de acesso a aplicações, bem como dos registros de conexão[732].

Há ainda outras medidas menos invasivas que não envolvem necessariamente a violação do conteúdo criptografado.Uma delas consiste na apreensão do dispositivo utilizado na comunicação e neste caso há a possibilidade de apreender tanto o dispositivo de ambos os interlocutores. Conforme visto, há ainda a possibilidade de se verificar se foi realizado um *backup* de segurança do dispositivo em servidores de armazenamento nas nuvens, conhecido como *cloud computing*. Desta forma,*backup* incluiria todo o conteúdo do dispositivo, inclusive mensagens trocadas. Em geral, os serviços de *cloud computing*não possuem criptografia para proteger os arquivos e, portanto, se poderia obter o conteúdo da mensagem sem se comprometer a segurança de todo o sistema de criptografia[733].

Há ainda a alternativa de se realizar o ataque conhecido como *man-in-the-middle*, que consiste na troca das chaves criptográficas pública e privada do usuário para que assim se possa replicar o conteúdo criptografado e decifrá-lo de posse das chaves falsamente criadas, encriptando novamente para entrega ao real destinatário. O problema dessa alternativa é sua viabilidade fática. Uma vez estabelecido o alvo suspeito, caso não saiba quem é o parceiro do usuário na empreitada criminosa, deverão ser trocadas todas as duplas de chaves de seus contatos. Ademais, os aplicativos de troca de mensagem, por padrão, permitem aos usuários conferirem as chaves de seus interlocutores, a fim de verificar se as chaves do interlocutor foram trocadas. Portanto, a medida mostra-se pouco eficaz no longo prazo, pois, uma vez divulgada a informação que o aplicativo realiza troca de chaves, usuários migrarão para outros aplicativos semelhantes ou criarão seu próprio aplicativo de mensagens criptografadas, visto que o código é aberto.

A medida ainda é onerosa pois compromete a privacidade de outros usuários. Decerto que as autoridades investigativas não saberão quem são, entre todos os interlocutores do usuário suspeito, criminosos ou não, até porque atualmente se utiliza o aplicativo para as atividades mais corriqueiras. Portanto, a troca das chaves deixará expostos um conjunto de interlocutores eventuais que nada têm a ver com a empreitada criminosa.

---

[732] Vide art. 15, caput, e parágrafo primeiro da Lei nº 12.965 de 2014, já citado neste trabalho.

[733] Essa é a opinião de Marcos Antônio Simplício Júnior, professor do Departamento De Engenharia e Computação e Sistemas Digitais da Escola Politécnica da Universidade de São Paulo – USP. Vide STF. Transcrição da audiência pública. ADI 5527 e ADPF 403.Marco Civil da Internet e bloqueio judicial do WhatsApp, p. 154.Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 20/02/2018.

Outrossim, a medida será onerosa ao modelo de negócios do aplicativo, uma vez que, conforme visto aqui, criado qualquer óbice a um aplicativo, usuários migram para o concorrente. Além disso, cedo ou tarde os usuários saberiam da colaboração do aplicativo com autoridades, o que despertaria desconfianças sobre sua real confiabilidade. Não se trata de defender que não se colabore com as autoridades, mas fato é que, se determinado modelo de negócios tem por produto central a confidencialidade das informações, a possibilidade de troca de chaves não informada compromete a confiabilidade daquele produto, influenciando em seu valor de mercado. Portanto, obrigar o aplicativo a realizar a troca das chaves sem notificar o usuário compromete a livre iniciativa, uma vez que obriga o aplicativo a romper de forma substancial o seu modelo de negócios quando há outros meios menos onerosos para tanto.

Outra alternativa que resta é a criação de uma vulnerabilidade na criptografia presente no dispositivo ou no aplicativo, fornecendo um acesso especial às autoridades, geralmente através de uma porta dos fundos *(backdoor)* ou mesmo com a criação de uma chave mestra. A onerosidade desta medida foi tratada de forma esparsa neste trabalho. Qualquer vulnerabilidade introduzida em ferramenta cujo objeto é a segurança da informação, haverá um comprometimento geral do sistema. Ademais, a medida apresenta um ônus excessivo, vez que criada uma vulnerabilidade, estarão em risco todos os usuários, na medida em que qualquer hacker, bem intencionado ou não, pode explorar a mesma vulnerabilidade criada pela porta dos fundos para acessar o conteúdo das mensagem. Outrossim, a imposição de criação de uma porta dos fundos viola a livre iniciativa, na medida em que, ao criar determinada vulnerabilidade, o gestor do aplicativo terá um ônus adicional em ocultar tal vulnerabilidade, que não estava prevista no projeto original do protocolo criptográfico e terá a segurança de seu aplicativo sempre comprometida. Além de todos esses ônus, no caso da chave mestra, a onerosidade ainda se dará para todos os usuários, na medida em que esta chave poderá ser “hackeada” e cair em mãos de criminosos ou de governos autoritários.

Deste modo, demonstradas variadas hipóteses de meios menos onerosos, entende-se que a medida de imposição de que o responsável pelo aplicativo forneça um acesso privilegiado às autoridades é excessivamente mais onerosa que outros meios igualmente ou mesmo mais idôneos a atingir finalidade constitucionalmente legítima.

Todavia, pode ser que haja alguma controvérsia quanto à menor onerosidade dos meios alternativos apresentados ou mesmo que se questione a idoneidade dos meios alternativos à obtenção do conteúdo das mensagens ou mesmo da obtenção dos metadados,

para atingir o fim de elucidar as investigações. Portanto, compete avançar na próxima etapa da proporcionalidade, a fim de verificar como se comporta a restrição em relação a este filtro, bem como para que se promova o debate

Na terceira etapa da proporcionalidade, cumpre verificar o atendimento ao subprincípio da proporcionalidade em sentido estrito, que consiste na própria estrutura lógica do raciocínio ponderativo, uma vez que apenas se terá cumprido a proporcionalidade nesta etapa se o grau de restrição ao direito fundamental se justifica pela importância da realização do princípio antagônico[734].

Em outras palavras, esta etapa constitui na prática de atribuir peso a determinado princípio e, de acordo com o seu grau de importância, aferir o grau de restrição que lhe é feito. Da mesma forma, deve-se verificar a relevância do princípio antagônico e se o benefício obtido com sua realização supera o grau de restrição ao princípio contraposto. Trata-se de uma verificação de custo-benefício, ou seja, se os custos com a restrição de determinado princípio são superados pela realização de outro.Todavia, esta verificação não se baseia em cálculo matemático exato, vez que os princípios não são a priori categorizados e hierarquizados entre si. Trata-se de atribuir peso a cada princípio, tendo em conta a sua importância para o sistema e o seu grau de relevância ao caso concreto.

Desta forma, inicialmente, deve haver a investigação do peso abstrato de determinado princípio para o sistema, o que significa dizer que se deve verificar o grau de importância dado pelo ordenamento jurídico a determinado princípio. Isso faz com haja uma prevalência, ao menos *prima facie* – que pode ser superada - de princípios que tutelam valores existenciais em relação aqueles que tutelam valores patrimoniais[735]. Deve-se verificar na aferição do peso abstrato, o grau de fundamentalidade do direito que aquele princípio promove, ou seja, maior peso abstrato terá relação direta com o grau maior de promoção da dignidade da pessoa humana, também com os valores basilares do constitucionalismo, quais sejam, o princípio da autonomia, o princípio democrático e o princípio da igualdade[736]. Por óbvio que a atribuição de peso abstrato a determinado princípio incumbe em aferir a carga axiológia que este encerra e inevitavelmente esta tarefa, para além da importância atribuída pelo direito constitucional positivo, envolve algum grau de valoração moral e política, que estão longe de serem incontroversas. Por exemplo, no conflito clássico entre a privacidade e a liberdade de

[734] PEREIRA, Jane Reis Gonçalves. Op. cit., p. 189.

[735] SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. Op cit., p. 519.

[736] PEREIRA, Jane Reis Gonçalves. Op. cit., p. 191

expressão, o peso abstrato de ambos os princípios ficará próximo, na medida em que são valores existenciais que apenas o caso concreto poderá traçar um caminho ponderativo.

No que tange ao peso concreto, este diz respeito ao aspecto quantitativo, ou seja, consiste na análise concreta do grau de restrição ao bem jurídico atendido pela medida, bem como o nível de realização do princípio constitucional antagônico. Neste momento, peso abstrato e concreto se relacionam, vez que uma restrição leve em um bem jurídico relevante pode se justificar pela realização em grau elevado de um bem jurídico de menor relevância; por outro lado, a restrição alta a um bem jurídico de pouca relevância pode não se justificar mesmo diante da realização leve de um bem jurídico de relevância alta[737].

Em que pese a análise da proporcionalidade em sentido estrito em geral ser resolvida pela análise do peso abstrato e concreto dos princípios em conflito, assume especial importância a premissa empírica[738] na qual se apoiou a medida restritiva. É o caso da proibição do consumo e comercialização de determinada substância porque se parta da premissa empírica de que a substância é altamente cancerígena, como é o caso da utilização do amianto crisotila (asbesto) na construção civil[739]. Neste caso concreto, pode ser que se justifique uma forte restrição da autonomia privada, diante da alta promoção do direito à saúde pública que possui forte peso abstrato. Todavia, caso posteriormente se constate que os danos causados à saúde não são tão intensos ou mesmo se constate que não há dano algum à saúde, a relação de forças entre os princípios contrapostos se altera, em razão do enfraquecimento da premissa empírica, podendo-se chegar a conclusão diametralmente oposta. Portanto, quanto maior o grau de certeza que se deposita sobre a premissa empírica, maior peso concreto terá o princípio que essa premissa empírica fortalece. Por outro lado, se a premissa empírica que promove determinado direito é fraca, menor será a importância concreta do bem jurídico por ela promovido.

De posse das premissas teóricas brevemente apontadas, cumpre analisar a ponderação entre o direito fundamental à privacidade e o interesse público nas ações de segurança pública. Por certo que foram selecionados os princípios antagônicos mais evidentes, com

---

[737] SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. Op. cit., p. 519.

[738] O exemplo dado por Alexy que inspirou este exemplo é a criminalização do consumo de *cannabis sativa*, criticando a decisão do Tribunal Constitucional alemão que reputou compatível com a constituição daquele país norma que criminalizava o consumo da substância. Todavia, o Tribunal considerou a premissa empírica de que motivou o legislador como sustentável, embora seja discutível se a criminalização do consumo de drogas tem o efeito se promover a saúde ou é contraproducente diante das alternativas. ALEXY, Robert. On Balancing and Subsumption: a Structural Comparison. **Ratio Juris**, v. 16, n. 4, p. 433-449, nov. 2003.

[739]BRASIL. Supremo Tribunal Federal.*Ação Direta de Inconstitucionalidadenº 4066/DF*. Tribunal Pleno. Relatora Minisra Rosa Weber. Julg. 24 ago. 2017. **DJe** 07 mar. 2018.

vistas a viabilizar uma melhor clareza do argumento. Todavia, nada impede que haja a ponderação após a definição de grupos de interesses antagônicos em rota de colisão, agrupando-se os inúmeros fundamentos normativos que apontam a solução em um sentido e outros fundamentos antagônicos que apontam no sentido contrário[740]. Desta forma, pode-se localizar, no grupo do direito fundamental à privacidade, o direito à liberdade de expressão, de manifestação do pensamento, direito à informação e à autonomia privada. Assim como pende a favor da segurança pública o direito à incolumidade física e psicológica, o direito de propriedade, entre outros. Ante o exposto, por se tratar de bens jurídicos que garantem outros bem jurídicos, foi necessário expor que outros bens jurídicos são garantidos, a despeito de a privacidade e a segurança pública serem os princípios em clara rota de colisão.

No que tange ao valor abstrato, a privacidade inegavelmente possui alto grau de fundamentalidade, haja vista sua relação intrínseca com a dignidade humana, a autonomia privada e a liberdade de expressão. Embora a segurança conste do *caput* do art. 5º, não é sem nenhuma controvérsia a afirmação de que a segurança pública constitua direito materialmente fundamental[741]. Em que pese a localização topográfica no *caput* do artigo, que define os direitos e garantias fundamentais[742], bem como direitos individuais e coletivos, há direitos que não possuem carga axiológica o bastante para serem definidos como materialmente constitucionais[743]. Não cabe aqui neste trabalho discutir a natureza jusfundamental e a carga axiológica do direito à segurança. Fato é que se trata muito mais de um direito garantidor de outros direitos fundamentais, ora existenciais, como o direito à vida e incolumidade física, ora patrimoniais, como é o direito de propriedade.

Deve-se observar que um outro critério alternativo de ponderação é aquele que confere prevalência *prima facie* dos direitos e liberdades existenciais, dos ligados à garantias e pressupostos da democracia e das condições essenciais de vida sobre aqueles de conteúdo

---

[740] BARROSO, Luís Roberto. **Curso**... Op. cit., p. 334-335.

[741] BOZZA, Fábio da Silva. Segurança não é direito fundamental. **Canal de Ciências Criminais**, fev. 2016. Disponível em: <https://canalcienciascriminais.com.br/seguranca-nao-e-direito-fundamental/>. Acesso em: 13 abr. 2018.

[742] Para o Ingo Sarlet, o direito à segurança constitui direito fundamental correlato à integridade física e psíquica. O autor entende que os direitos previstos no Título II da Constituição (TÍTULO II
Dos Direitos e Garantias Fundamentais) possuem presunção de fundamentalidade. Todavia, devem ser submetidos ao critério material dos direitos fundamentais, que é orientado pela verificação de se fundarem diretamente no princípio maior da dignidade da pessoa humana. SARLET, Ingo; MARINONI, Luiz Guilherme; MITIDIERO, Daniel *et al*. Curso de Direito Constitucional. 5. ed. rev. e atual. São Paulo: Saraiva, 2016, pp. 330-334, 423.

[743] Sobre o catálogo de direitos fundamentais protegidos pela cláusula pétrea prevista no art. 60, parágrafo 4º da Constituição e os variados posicionamentos a respeito, vide BRANDÃO, Rodrigo. **Direitos fundamentais, cláusulas pétreas e democracia**. Rio de Janeiro: Renovar, 2008, p. 195-210. Vide

meramente econômico e patrimonial[744]. Para além da dúvida acerca da natureza jusfundamental do direito à segurança, fato é que este exprime um valor existencial um tanto menos evidente que a própria privacidade, cuja natureza existencial e de pressuposto à democracia é incontestável, vez que não há regime democrático sem que se garanta ao indivíduo um espaço impenetrável para formar as próprias convicções políticas e realizar escolhas morais autonomamente.

Afora a possível discussão, o que se quer pontuar é que o peso abstrato do direito à privacidade face o direito à segurança é superior, uma vez que a privacidade melhor realiza a dignidade humana e os valores do constitucionalismo, entre eles a autonomia privada, diante de sua inegável superior carga axiológica.

No que tange ao peso em concreto, a análise pode ser relativamente prejudicada. Por ser a segurança princípio que protege outros direitos fundamentais, há que se saber que direito estaria a proteger, a fim de relativizar a privacidade.

Na hipótese que se propõe analisar, a matéria está relativamente abstrata, analisando-se a colisão entre privacidade e segurança pública. Do que foi visto até agora, a imposição da criação de uma vulnerabilidade nos aplicativos criptografados pelo poder público é uma restrição elevada à privacidade para um benefício incerto à segurança pública.

A restrição à privacidade é de grau alto pelo risco de dano à privacidade de todos os usuários e não apenas do investigado, vez que a vulnerabilidade alcança o código fonte do aplicativo. Ademais, uma porta dos fundos coloca nas mãos do Estado um poder extremado não só para investigações criminais, mas para a prática de vigilância estatal, confundindo atribuições legítimas com violações inconstitucionais, vez que, na atual quadra histórica, quem detém a informação também concentra poder. Soma-se a isto o fato de todos os direitos garantidos pela privacidade estarem comprometidos de elevada jusfundamentalidade, a exemplo da liberdade de expressão.

Não se deve ignorar ainda que a proteção à livre criação de protocolos criptográficos protege a livre expressão da atividade intelectual e científica, a liberdade do cidadão para o exercício da autonomia pessoal. A imposição estatal de que os criadores da aplicação tornem vulneráveis os próprios sistemas não apenas restringem, mas aniquilam por completo a livre manifestação da atividade intelectual e vulneram o indivíduo de forma relevante, ao impor limites à sua capacidade criativa. Deve-se alertar que a criação de um protocolo criptográfico não constitui armamento bélico ou químico e a criação de um sistema invulnerável decorre da

[744] SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. Op. cit., p. 519.

própria competição e evolução do mercado da tecnologia. Se o uso da tecnologia é feito de modo desvirtuado, isso não é e não pode ser responsabilidade de seu criador. Ora, o sétimo princípio do decálogo do Comitê Gestor da Internet é peremptório ao afirmar que o combate a ilícitos na rede deve atingir o responsável final e não os meios de acesso e transporte[745].

Ademais, a medida restringe a liberdade de iniciativa, na medida em que interfere drasticamente no modelo de negócios do responsável pelo aplicativo ao impor a criação de fragilidades. É o mesmo que impor ao criador de um sistema seguro e inviolável de uma aeronave que fosse obrigado a deixar uma porta dos fundos para que as autoridades, quando quisessem, pudessem ativar os comandos do avião remotamente em caso de atentado terrorista. Pelas mesmas razões, não se justifica tamanha restrição à liberdade de iniciativa do indivíduo.

É fora de dúvida que a criptografia é a nova fronteira da privacidade, constituindo-se em seu instrumento de garantia e de democratização do acesso à internet com segurança e confidencialidade, privilégio que até tempo atrás era exclusivo de grandes corporações e órgãos estatais.

No que tange às eventuais vantagens obtidas com a restrição do direito, poder-se-ia alegar que haveria êxito nas investigações criminais. Todavia, este êxito é abstrato e já se tratou aqui que pode ser um êxito meramente temporário e relativo. Não há nada de concreto que afirme que o acesso a conteúdos criptografados aumentará a elucidação das investigações. É preciso repisar que a criptografia possui aplicação da ampla e variada que vai desde a comunicação interbancária e militar, até a troca de mensagens entre particulares. Impor que cidadãos comuns faça uso de criptografia vulnerável enquanto empresas e órgãos estatais farão uso de criptografia forte não implica em combater o crime, mas apenas tornar vulnerável o cidadão comum, vez que os criminosos e *experts* sempre terão acesso à melhor tecnologia, dispondo o Marco Civil da Internet no mesmo sentido, além de consagrar a regra da liberdade de modelos de negócios na internet[746].

Em conclusão, dimensionando o peso concreto da ponderação entre privacidade e segurança, na situação fática proposta, a conclusão a que se chega é que não pode o poder

745COMITÊ GESTOR DA INTERNET. Decálogo. “7.Inimputabilidade da rede. O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos”.

[746] Art. 3º "A disciplina do uso da internet no Brasil tem os seguintes princípios:(...)II - proteção da privacidade;(...)VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;(...)VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei".

público impor ao particular que se crie uma vulnerabilidade especial em sistema criptografado que garanta acesso especial ao conteúdo transmitido sem que isso se afigure inconstitucional por manifesta desproporcionalidade.

Aqui cabe uma distinção, ao se tratar de ordem do poder público, propositadamente não se tratou expressamente se esta ordem derivava de lei ou diretamente de sentença judicial. Deve-se ressaltar que, embora a ponderação seja técnica de decisão judicial para a resolução de conflito de normas constitucionais, nada impede ao legislador que este realize a ponderação entre bens jurídicos constitucionais, sendo essa a tarefa por excelência do Poder Legislativo: dentro do seu poder de conformação, harmonizar de forma geral e abstrata os princípios constitucionais colidentes, especialmente em uma sociedade pluralista.

Portanto, caso a fonte normativa da obrigação de criar vulnerabilidades no aplicativo criptografado seja a lei, a nosso ver, esta lei é manifestamente inconstitucional, vez que não observa o subprincípio da necessidade ou menor onerosidade, haja vista haver inúmeras alternativas igualmente idôneas e menos onerosas para o atingimento do fim, não se justificando tamanha restrição ao direito à privacidade. Ainda que assim não o fosse, ao se verificar a observância da proporcionalidade em sentido estrito, haveria um excessivo grau de restrição à privacidade, à liberdade de expressão do indivíduo, diante de um duvidoso benefício à segurança pública, de modo que a medida legislativa se afiguraria desproporcional.

No entanto, imagine-se que, em um caso concreto, determinado órgão de segurança pública tenha por objetivo a localização de vítima sequestrocuja vida esteja em risco iminente. Após ampla investigação, as autoridades não lograram alcançar qualquer pista do paradeiro da vítima, tendo utilizado todos os instrumentos à sua disposição.

Neste caso, não estará em jogo apenas a segurança, mas se evitará a violação da vida, bem jurídico de maior carga axiológica e dotado de elevada jusfundamentalidade. Nesta situação, há um claro impasse, partindo-se do pressuposto que seja impossível ao aplicativo acessar o conteúdo criptografado sem ser percebido pelo usuário. Portanto, diante da periclitação da vida e da integridade física do indivíduo, poderia o magistrado, de forma excepcionalíssima, ordenar aos responsáveis pelo aplicativo que efetuem a troca das chaves[747]

[747] A vulnerabilidade da troca das chaves teria sido descoberta por Tobias Boelter, um pesquisador especializado em codificação da Universidade de Berkeley, na Califórnia, nos Estados Unidos. O pesquisador descobriu que a troca de chaves é uma medida aplicada após o usuário ficar off-line, seja por ter reinstalado o aplicativo ou mesmo por haver trocado de aparelho. Ao retornar ao aplicativo, o usuário receberá nova chave criptográfica. As mensagens que aguardavam por seu retorno serão enviadas automaticamente ao usuário que trocou a chave. REDAÇÃO. WhatsApp tem vulnerabilidade que permite interceptar mensagens, diz jornal. **Época Negócios**,

do suspeito do crime, considerando que haja um. Para efetuar a troca das chaves dos interlocutores, deverá ser observada uma ordem de precedência, ou seja, deve-se adotar a cautela de apenas realizar a troca das chaves dos interlocutores que também sejam suspeitos de serem copartícipes no crime.

Em que pese tratar-se de eventual restrição à privacidade de outros usuários, a troca de chaves é medida menos onerosa na medida que atinge o menor número de usuários possíveis. Ademais, não haverá nenhuma imposição de criação de vulnerabilidade que fragilize o próprio aplicativo, violando em menor grau a livre iniciativa. Pelo contrário, o que ocorre com a troca das chaves é a exploração de uma vulnerabilidade que em tese já existiria no aplicativo, para quem a admite – e aqui trata-se do aplicativo WahtsApp -conforme abordado neste trabalho. Logo, ao ordenar aos responsáveis que se explore uma vulnerabilidade do próprio aplicativo, caso as forças de segurança por si não possuam a expertise para fazê-lo, a violação à livre iniciativa é mais branda, na medida que não se determinou a criação de vulnerabilidade, mas a exploração de uma fragilidade anteriormente existe.

Com efeito, sustentou-se que apenas poderia o juiz, no caso concreto, ordenar que o aplicativo efetuasse a troca de chaves do usuário, caso esteja em jogo direito fundamental de maior carga axiológica que a privacidade e outros direitos fundamentis correlatos. Todavia, a lei não poderia prever a obrigatoriedade de criação da vulnerabilidade. Isso violaria o princípio democrático, vez que em um regime democrático, cidadãos livres e conscientes escolhem representantes para que legitimamente criem leis que criam direitos e obrigações, em razão do mandato popular conferido.Ocorre que neste caso a previsão da violação do aplicativo pela lei, além de alertar pessoas mal intencionadas ao fato da vulnerabilidade, daria a impressão de se criar uma regra geral e abstrata, o que deixaria uma porta aberta para o enfraquecimento da criptografia. Portanto, a melhor medida é que se permita ao juiz a aplicação direta dos princípios constitucionais pertinentes, ponderando os bens jurídicos antagônicos na situação concreta.

Este tópico poderia ter sido encerrado antes da última sugestão. Ocorre que o mundo real não é pintado com preto e branco e as soluções nem sempre podem ser claras e definidas. Portanto, pode ser que o intérprete se depare com uma situação na qual tenha que relativizar o uso da criptografia forte, como meio imprescindível ao atingimento do fim público.

---

jan. 2017. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2017/01/whatsapp-tem-vulnerabilidade-que-permite-interceptar-mensagens-diz-jornal.html>. Acesso em: 13 abr. 2018.

No entanto, o risco para o qual se alerta é de que o remédio que aqui foi se foi proposto, enquanto medida de extrema excepcionalidade, se torne a regra, como as outras exceções no Brasil, fragilizando de modo geral o uso da criptografia. Nesse caso, o antídoto se tornará veneno, o que contrariará orientações de diferentes organismos internacionais, os quais defendem o uso livre, democrático e sem qualquer acesso especial ao poder público da criptografia, enquanto garantia da privacidade e de outros direitos do indivíduo, seja em face de regimes autoritários, seja diante da vigilância indevida sobre os indivíduos.

Cabe salientar que nenhuma tecnologia por mais avançada que seja pode ser considerada insuperável. Portanto, quando se afirma que determinado sistema de criptografia é inviolável, apenas se está referindo a determinada quadra histórica, até que se supere aquela invocação.

O que as forças de segurança devem fazer é investir no aperfeiçoamento de seus agentes e do uso da tecnologia, bem como na utilização de novas práticas investigativas. Diante da revelação de escândalos de vigilância em massa, bem como da existência de um mercado privado de vigilância altamente lucrativo, indivíduos e empresas passaram a se preocupar em utilizar dispositivos e aplicativos mais seguros e que garantam a confidencialidade através da criptografia forte. Portanto, tendo havido evolução das aplicações da criptografia, haverá também a necessária atualização das forças de segurança. Não é sem razão que o FBI é uma das agências que mais contrata hackers no mundo, justamente para contornar sistemas de segurança.

Logo, caso seja para o alcance de um fim constitucionalmente legítimo, devem as forças de segurança investir no desenvolvimento de técnicas de hackeamento, adaptando-se aos novos tempos, assim como ocorreu em San Bernardino. Devem ainda as autoridades investigativas explorar formas alternativas de investigação, constituindo o uso dos metadados a nova mina de ouro informacional à disposição das autoridades.

Estas são as soluções aos conflitos apresentados que entendemos adequadas diante da relevância do direito fundamental à privacidade, garantida por novas tecnologias acessíveis a todos, e seu eventual conflito com a segurança pública.

3.10 **O direito fundamental à privacidade, *big data* e criptografia: algumas proposições**

Pode-se ainda questionar, no emaranhado de novas possibilidades que as novas tecnologias apresentam, por qual razão se tenha selecionado o *big data* e a criptografia. Sua

escolha não é aleatória. Embora se trate de fenômenos tecnológicos distintos, a adequada abordagem do processamento massivo de dados e do uso da cifragem podem ser úteis à melhor proteção do direito fundamental à privacidade, no contexto da vida digitalmente intermediada.

Portanto, big data e criptografia funcionam como lados da mesma moeda. Se por um lado o *big data* traz preocupações no que tange à privacidade, não se pode ignorar os avanços e benefícios trazidos pelo uso da tecnologia, que cada vez será mais essencial para facilitar a vida e tornar as relações mais eficientes, desde que sejam estabelecidos parâmetros sérios para a sua realização. O *big data* é uma locomotiva marcada pelo elevado volume de dados processados como em nenhum momento precedente.

Do outro lado da moeda, há a criptografia que seria uma espécie de freio à locomotiva do *big data*, ao processamento irrefreado de dados, que não observe a privacidade. Portanto, a criptografia determina até que ponto ético pode ir o *big data* desde que observe a privacidade dos cidadãos. Enquanto o *big data* consiste na prática de vasculhar e processar grande quantidade de dados, a criptografia seria o escudo contra vigilância, estatal ou privada.

Com efeito, o *big data*,se não inaugura, decerto que consolida uma nova era, a era na qual a coleta de dados não encontra limites quanto ao volume, velocidade e variedade. Esse processamento massivo apenas é possível graças ao barateamento dos custos de armazenamento e processamento de dados, bem como a coleta massiva através de um crescimento exponencial do número de sensores, que será ainda mais intensificado pela consolidação da internet das coisas. Todo esse volume de dados recebido é processado por algoritmos, códigos de programação automatizados, responsáveis por análises diagnósticas, mas também prognósticas e, porque não preditivas, que processam o passado, resolve conflitos presentes e se arrisca a prever o futuro de candidatos a vagas de empregos a acusados de crimes.

Todavia, o termo automatizado é utilizado para ressaltar que a automatização é apenas do processo. No entanto, o algoritmo é programado por seres humanos com seus vieses, paixões e visões limitadas. Ademais, o algoritmo pode, a título de análise preditiva, reproduzir as viciadas estruturas sociais, reforçando discriminações religiosas, de gênero, raciais e socioeconômicas, aprofundando as desigualdades existentes. Uma visão otimista pode apostar em algoritmos transparentes que levem em conta a limitação de amostragem dos dados que processa e que esteja comprometido com o combate às desigualdades que se perpetram na sociedade.

O processamento massivo dos dados desperta especial preocupação com o uso dos dados pessoais por instituições privadas e públicas, de modo a violar a privacidade dos potenciais consumidores – mediante a prática de economia de rastreamento ou capitalismo de vigilância[748]; bem como em razão da prática do vigilantismo estatal, principalmente após os escândalos revelados por um ex agente da NSA americana.

A abordagem inicial europeia diante de grandes bancos de dados que coletavam amontoados de dados pessoais foi exigir o consentimento informado, a partir da aplicação do princípio *notice and consent*. Não que o consentimento seja dispensável, ocorre que o consentimento associado ao princípio da finalidade específica, que apenas permite o uso do dado na finalidade para a qual foi coletada, pode parecer inadequado aos dias atuais, na medida que traz uma excessiva restrição ao modelo de negócios baseado em dados e não traz em contrapartida uma proteção eficiente à privacidade, na medida em que o consentimento pouco influencia na integração do banco de dados e no processamento aglutinado de informações das mais variadas fontes.

Nessa perspectiva, o uso secundário de dados se tornou o grande nicho de mercado de aplicação de dados, potencializando um mercado em franca ascensão. Portanto, não se pode consentir genericamente com o uso do dado em uma finalidade que não se sabe qual será no momento da coleta. Por outro lado, o consentimento não garante ao titular do dado o rastreamento e controle de todas as utilizações secundárias dos dados ou a exigência de consentimento a cada utilização revela-se contraproducente, na medida que nega a realidade dos fatos.

Não se ignora a importância do controle do uso de dados pessoais do indivíduo, enquanto exercício da privacidade, enquanto autonomia informacional[749], especialmente diante de sucessivos escândalos de uso indevido de dados, inclusive para exitosa manipulação eleitoral[750]. Ocorre que a abordagem da privacidade focada no indivíduo atomizado enfraquece o indivíduo diante de grandes corporações privadas ou estatais e não lhe traz o controle necessário. Em que pesem os direitos fundamentais terem por primazia o foco no indivíduo e no exercício da autonomia, a abordagem individualizada é pouco eficiente e

---

[748] ZUBOFF, S. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology**, v. 30, p. 75-89, 2015.

[749] RODOTÁ, Stefano. Op. cit., p. 24.

[750] Vide o escândalo da Cambridge Analytica aqui já citado que utilizou indevidamente dados do Facebook para favorecer o então candidato Donald Trump, posteriormente presidente eleito dos Estados Unidos da América. Dificilmente um regime de proteção à privacidade baseado no consentimento evitaria a ocorrência desta situação.

talvez a privacidade, embora um direito de gozo individual, deva ter a sua proteção e controle de maneira difusa, através da criação de organismos estatais ou não, preferencialmente de forma descentralizada, responsáveis pela garantia da privacidade de toda a sociedade[751]. A mesma internet que permite a coleta, o rastreamento, o monitoramento e o processamento massivo de variados dados possui instrumental suficiente para permitir a governança destes dados[752].

Na era do *big data* uma ideia que assume especial protagonismo é a privacidade diferencial[753]. Diante da constatação de que não há forças que detenham o advento do processamento massivo de dados, tampouco seu aproveitamento secundário e, diante das apontadas limitações do consentimento, a privacidade diferencial *(differential privacy)* assume especial papel, diante da necessidade dos mercados em cada vez mais tratar mais dados para definir suas estratégias.

Deste modo, a privacidade diferencial consiste em prática de desanonimização de dados, segundo a qual apresentam-se os dados de forma embaralhada e nebulosa, além de apresentar os números estatísticos apenas de forma aproximada. A privacidade diferencial, diferente da desidentificação tradicional, apenas apresenta dados aproximados, impedindo a identificação dos indivíduos envolvidos. O embaralhamento dos dados é feito através da colocação de "ruídos" matemáticos nas informações, para impedir a identificação de sua origem, mas permitem que haja dados suficientes para estatísticas. Desta forma, o algoritmo seria alimentado não com um fluxo de dados puro, mas um conjunto de dados "sujos" pelo ruído estatístico que, contudo, não comprometeria o resultado[754].

Se a referida prática de fato garantirá uma anonimização eficaz dos dados, ainda não se sabe, mas fato é que a a privacidade diferencial pode constituir uma alternativa à anonimização tradicional que, conforme visto neste trabalho se mostrou falha. Há que se

---

[751]RODOTÁ, Stefano. Op. cit., 37.

[752]VITORINO, Fabricio.Facebook reforça luta contra o fake news e diz que mudança no algoritmo é só o começo.**G1**, mar. 2018. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/facebook-reforca-luta-contra-o-fake-news-e-diz-que-mudanca-no-algoritmo-e-so-o-comeco.ghtml>. Acesso em 31/03/2018.

[753] Segundo o vice-presidente sênior de engenharia de software da Apple, Craig Federighi "[a] privacidade diferencial é um tópico de pesquisa na área de estatísticas e análise de dados que usa hashing, subamostragem e injeção de ruído para permitir esse tipo de aprendizado em crowdsourcing, mantendo as informações de cada usuário completamente privado" (tradução livre). LOMAS, Natasha.What Apple's differential privacy means for your data and the future of machine learning.**TechCrunch**, jun. 2016. Disponível em: <https://techcrunch.com/2016/06/14/differential-privacy/>. Vide ainda importante artigo da fabricante Apple que melhor explicita como é praticada a privacidade prefencial. APPLE. Differential Privacy Overview. Dispnível em: https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf Acesso em: 13 abr. 2018.

[754]BYRNE, Michael. O Que É Privacidade Diferencial?**MotherBoard**, jan. 2015. Disponível em: <https://motherboard.vice.com/pt_br/article/nz3avw/o-que-e-privacidade-diferencial>. Acesso em: 13 abr. 2018.

advertir que a privacidade diferencial apenas se mostra eficaz na proteção da privacidade em grandes bancos de dados, pois quanto menos indivíduos participem do banco, mais difícil será o embaralhamentoe o tratamento coletivizado[755]. A experiência já é feita pela Apple nas versões mais atualizadas de seu sistema operacional, IOS 10. A fabricante garante que o algoritmo apenas colhe parte dos dados e insere ruídos responsáveis por possibilitar que se saiba cada vez mais sobre o grupo e menos sobre o indivíduo, transmitindo o conteúdo em massa por meio de técnica de criptografia[756]. Em resumo, a Apple afirma que a coleta através do conceito de privacidade diferencial utilizará como técnicas as tabelas de dispersão de dados (*hashing*), sub-amostragem (*subsampling*) e adição de ruídos (*noise injection*) para permitir a aprendizagem coletiva (*crowdsourced learning*) de modo que ainda mantenha os dados de cada um dos usuários totalmente privados[757].

No que diz respeito ao consentimento, enquanto paradigma para coleta compartilhamento de dados, consagrado em variados tratados continentais e internacionais, embora se respeite o seu protagonismo, não se deve perder de vista a gradativa perda de eficácia do modelo, diante do uso secundário dos dados para finalidades outras que não a originária. Portanto, o que se propõe é que haja a migração de um regime de privacidade por consentimento para um regime de responsabilidade dos gestoresde bancos de dados (*from privacy to accountability*)[758]. Na dinâmica atual, impõe-se ao indivíduo o controle do complexo volume de dados a seu respeito, exigindo-o que emita um consentimento que não protege a privacidade, tampouco contribui para o aperfeiçoamento da economia. Conforme tratado nos tópicos 2.7.2 e 2.7.3 do capítulo antecedente, a relativização do consentimento como único e principal critério de tratamento de dados já vem ocorrendo tanto em documentos internacionais, a exemplo da Carta de Direitos Fundamentais da União Europeia; do Regulamento nº 2016/679 do Parlamento Europeu e do Conselho da União Europeia; quanto no Brasil, cuja Lei de Acesso à Informação prevê critérios outros que não o

---

[755] UNITED NATIONS. Report of the Special Rapporteur of the Human Rights Council on the right to privacy. A/72/43103, out 2017, p. 19. Disponível em: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>. Acesso em: 13 abr. 2018.

[756]GREENBERG, Andy. Apple's 'Differential Privacy' is About Collecting Your Data—But Not*Your*data. **Wired**, jun. 2016. Disponível em: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>. Acesso em: 31 mar. 2018.

[757] Veja interessante trabalho acadêmico detalhando como funciona a prática da privacidade diferencial DWORK, Cynthia; ROTH, Aaron. The Algorithmic Foundations of Differential Privacy. **Foundations and Trends in Theoretical Computer Science**,v. 9, n. 3–4, p. 211-407, 2014. Disponível em: <https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf>. Acesso em 31 mar. 2018.

[758] MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. Op. cit., p. 173.

consentimento para divulgação e acesso de dados pessoais[759], bem como o Projeto de Lei nº 5276/2016 prevê outros critérios além do consentimento para tratamento de dados pessoais.

A proposta desloca o eixo de responsabilidade do indivíduo e o coloca diretamente sobre os diferentes tipos de usuários de dados, mediante um regime que propicie salvaguardas adequadas à proteção dos dados, mas ao mesmo tempo não proiba terminantemente o uso secundário, impondo a exclusão definitiva dos dados. Para tanto, seria necessário um regime jurídico sancionatório que garantisse a responsabilização dos usuários de dados, com órgão fiscalizatório eficiente. Nas palavras de Mayer-Schonberer e Cukier, a responsabilização dos usuários de dados apenas funciona quando possui dentes[760].

Desta forma, o regime de responsabilização dos tratadores de dados traz a eles vantagens competitivas, entre elas alguma margem liberdade para o uso secundário dos dados, sem a necessidade de perseguir um novo consentimento a cada uso, desde que observe as cautelas legais. Portanto, será dever do profissional de dados adotar cautelas em seu tratamento, realizando a adequada avaliação dos riscos, decorrentes do tratamento daquele dado, sob pena de responsabilização. A proposta é adequada na medida em que o profissional de dados - mais que as autoridades e indivíduos - saberá exatamente qual a finalidade adequada dos dados e que cautela deverá adotar para tanto, responsabilizando-se caso o uso se mostre inadequado. Trata-se, portanto, de regime de autorregulação, com rigoroso controle sancionatório[761].

Por óbvio que o uso secundário dos dados não pode ser indeterminado, sob pena de o indivíduo viver o resto da vida assombrado pelos dados do passado. Há que se fazer uma análise de razoabilidade. Para tanto, compete à sociedade refletir e democraticamente deliberar sobre qual prazo de reuso entende razoável para cada dado e que medidas de segurança diferenciadas devem ser adotadas pelas empresas que processam dados para o tratamento, compartilhamento e reuso de dados. Por fim, em que pese se defenda o desuso do consentimento específico para cada finalidade, este não se mostra dispensável na coleta dos dados, devendo haver consentimento informado do objetivo da coleta, do objeto social de quem coleta e da possibilidade de reuso dos dados e compartilhamento com empresas parceiras. Outra hipótese é que o consentimento para compartilhamento seja dado por áreas de

[759]Art. 31, parágrafo 3º, incisos I a V da Lei nº 12.527/2011.

[760]Ibidem, p. 173.

[761] Ibidem, p. 174.

atuação do tratador de dados[762]. A divulgação da lista de parceiros no momento do consentimento e sua atualização periódica pode trazer um razoável panorama ao indivíduo das possíveis utilizações secundárias que se farão dos dados futuramente. Deve-se ainda garantir o completo acesso e retificação dos dados onde quer que estejam, havendo a completa transparência do caminho dos dados até a chegada àquele banco de dados. Para tanto, as empresas que coletam, tratam e compartilham dados deverão manter atualizadas informações sobre o fluxo de dados, informando o local e momento de sua coleta e sua chegada até determinado base de dados, informando ainda os outros bancos de dados onde possivelmente constam a mesma informação, vez que este controle é plenamente possível na era do *big data.*

A transparência no tratamento dos dados garantirá ao usuário o exercício da cidadania informativa, bem como que haja uma política transparente de governança dos dados, garantindo-se a confidencialidade em face de terceiros, sob pena de responsabilização. Se partirmos do pressuposto que o uso secundário de dados é inevitável, defende-se que sua prática deve ser a mais transparente possível, competindo às empresas que tratam dados garantir a máxima confidencialidade dos dados tratados. Por esta razão a privacidade diferencial desponta como um dos instrumentos do futuro da privacidade.

Da mesma forma, a análise preditiva realizada pelo *big data* inspira preocupações na medida em que a previsão de tendências de comportamento pode limitar oportunidades de trabalho, de acesso à educação, bem como definir sanções criminais e benefícios de progressão de regime. Caso desconsiderada a autonomia do indivíduo, a prática pode ser danosa, vez que não levará em consideração a liberdade da pessoa em realizar escolhas morais, a despeito das tendências, o que aprofundará o viés discriminatório das instituições.

Em relação à vigilância estatal e privada, a criptografia se apresenta como instrumento de resistência[763] a intromissões indevidas na esfera privada do indivíduo, de modo que

---

[762]Em sentido semelhante, está o Regulamento 2016/679 da União Europeia sobre proteção de dados pessoais cujo considerando admite que para fins de pesquisa científica o consentimento seja dados por área de investigação, conforme consta dos considerandos do regulamento: " 32 (...) Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido. (33) Muitas vezes não é possível identificar na totalidade a finalidade do tratamento de dados pessoais para efeitos de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida".

[763] Deve-se citar o movimento Cipherpunk, movimento que utiliza a criptografia como movimento de resistência à vigilância estatal. "Os*cypherpunks*defendem a utilização da criptografia e métodos similares como meios para provocar mudanças sociais e políticas. O movimento teve início em 1990, atingiu o auge de suas atividades

constitui dever dos estados absterem-se de proibir ou mesmo dificultar o uso da criptografia forte, tampouco impor a criação de acesso privilegiado, ainda que sob o argumento de proteção à segurança e combate ao crime. Na reedição contemporânea das cripto guerras, o enfraquecimento da criptografia interessa apenas ao avanço da vigilância estatal sobre os indivíduos, de modo que a responsabilidade por atos criminosos não pode punir um número indiscriminado de terceiros estranhos à ação delituosa, sob pena de se violar o direito fundamental à privacidade, à autonomia privada, à liberdade de expressão e informação, aniquilando liberdades básicas do indivíduo. Adotar postura contrária significaria o enfraquecimento da privacidade apenas dos indivíduos comuns, enquanto Estado, corporações e criminosos garantiriam a privacidade de suas comunicações por outros meios.

Portanto, o que se propõe é que, constatado que o *big data* é um processo irreversível que tende a se intensificar, deve ser criado um regime rigoroso de responsabilização das empresas usuárias de dados, especialmente os dados pessoais sensíveis, impondo-se o dever de garantir o sigilo das informações do indivíduo, anonimizando-as o máximo possível. Por outro lado, defende-se que deve haver o fortalecimento permanente das práticas de segurança da informação, democratizando-se o acesso ao uso da criptografia, como instrumento de proteção do direito fundamental à privacidade, essencial ao exercício de outros direitos fundamentais correlatos, além de se garantir práticas que garantam o anonimato do indivíduo, apenas se admitindo tentativas de identificação do usuário caso tenha havido a prática de ato ilícito, mediante ordem fundamentada de autoridade judicial.

Apenas haverá um balanceamento entre a necessidade cada vez maior de coleta e tratamento de dados e a necessidade de se preservar a privacidade do indivíduo, caso se exija a maior transparência dos poderes públicos e organizações privadas no tratamento de dados, ao tempo em que se garanta a proteção à esfera privada do indivíduo.

À medida que a vigilância pública e privada expande seus tentáculos, a tendência é que o indivíduo seja cada vez mais meticulosamente escrutinado, através do monitoramento ininterrupto. Por outro lado, o avanço da vigilância é obscuro quanto às medidas de vigilância adotada, os princípios éticos seguindos pela máquina da vigilância e o uso que é feito com os dados do indivíduo. O cenário inevitável da vigilância descontrolada é a transparência cada vez maior do indivíduo, como se tratasse de um homem de vidro e uma obscuridade cada vez

---

durante as "criptoguerras" e, sobretudo, após a censura da Internet em 2011 na Primavera Árabe. O termo *cypherpunk*, uma derivação (criptográfica) de *cipher* (escrita cifrada) e *punk*, foi incluído no Oxford English Dictionary em 2006." ASSANGE, Julian et al. Cipherpunks: **Liberdade e futuro da internet**. Tradução de: Cristina Yamagami. São Paulo: Boitempo, 2013, p. 2.

maior das sorrateiras ações de vigilância[764]. Diante desse quadro, se propõe que o rumo do tratamento da privacidade, sobretudo na internet, seja o contrário. A internet, concebida como território livre deve, por esta razão, garantir a liberdade de uso, de informação, de expressão e de opinião, utilizando-se, se necessário, a criptografia e outras técnicas que resguardem o indivíduo da vigilância. O binômio a ser perseguido não deve ser outro que o da transparência das ações do poder público e corporações e opacidade dos aspectos atinentes a intimidade e à vida privada, garantindo-se ao indivíduo o pleno desenvolvimento livre de interferências arbitrárias.

[764] BAUMAN, Zygmunt. Op. cit., p. 13.

CONCLUSÃO

Embora o direito norte-americano seja essencialmente jurisprudencial, curiosamente, no caso do direito à privacidade, a sua construção foi inicialmente doutrinária, contando com o reconhecimento jurisprudencial décadas depois. A obra inaugural, citada até os dias atuais, é datada de 1890, de autoria de Samuel Warren e Louis Brandeis, "The right to privacy", que concebe a privacidade como o direito a ser deixado só e sua particularidade é justamente reconhecer a privacidade como um direito autônomo e unitário, embora ainda inspirado em institutos típicos do direito de propriedade, de proteção à propriedade intelectual, a quebra de contrato, a violação de confiança, entre outros.

Na década de 1960, William Prosser aperfeiçoou e sistematizou as ideias lançadas no artigo inaugural e, utilizando-o como ponto de partida, critica a abordagem da privacidade como concepção única do "direito a ser deixado só", para tratar a privacidade a partir de quatro formas de violação, a saber, (i) invasão na esfera de privada da pessoa *(intrusion)*; (ii) divulgação pública de fatos privados embaraçosos *(public disclousure of privact facts)*; (iii) exposição pública desonrosa ou distorcida (*false light in the public eye*; e (iv) apropriação do nome ou de dados do indivíduo (*appropriation*).

A concepção da privacidade *(right of privacy)* na doutrina norte-americana enquanto direito pessoal e intransmissível, pleiteável apenas pelo seu titular trazia dificuldades a sua adaptação aos interesses patrimoniais do indivíduo na exploração econômica da própria imagem. Para tanto, a solução jurisprudencial foi a criação do *right of publicity*, concebido enquanto direito autônomo, de caráter patrimonial e transferível e que não envolve a discussão do atingimento da honra e dos sentimentos do titular, tratando tão somente do aproveitamento econômico da imagem pública.

Com efeito, a concepção de privacidade sofre influência do contexto histórico, social e sobretudo cultural, sendo a privacidade um conceito cambiável no tempo e no espaço, reflexo de determinada cultura. Há diferenças marcantes entre a cultura americana e europeia de privacidade.

A cultura americana de privacidade centra-se no valor liberdade, tanto a liberdade do indivíduo, da imprensa, e da atividade econômica. Ademais, a cultura de privacidade americana é fundada na sacralidade do lar, ou seja, na concepção um espaço físico inviolável, que é condizente com a espectativa razoável de privacidade. Nesta linha, a grande ameaça à privacidade dos indivíduos é o Estado, não havendo grande resistência ao papel da imprensa

em noticiar fatos ou à atuação do livre mercado. Não é sem razão que os americanos não se incomodam que empresas de crédito tenham um perfil detalhado de seus dados de consumo e a liberdade de imprensa costume se sobrepor a alegações de violação à privacidade.

Por outro lado, a cultura europeia de privacidade se funda no valor dignidade do indivíduo. Significa dizer que o importante é preservar o indivíduo da situação de humilhação, que comprometa a sua imagem pública. Esta dignidade pode estar ameaçada tanto pelos excessos do livre mercado, quanto pela atuação invasiva da imprensa. Todavia, o Estado não integra a lista de inimigos preferenciais da privacidade.

Apenas para ficar em alguns casos, a desconfiança em relação ao mercado na cultura europeia faz com que haja um rígido controle no que tange ao acesso e utilização de relatório de crédito sobre cidadãos, em alguns casos, centralizando sob poder do Estado este banco de dados. Na cultura americana não há este tipo de resistência, na medida que a iniciativa privada é vista como um parceiro, no intuito de permitir transações econômicas mais eficientes. Da mesma forma, enquanto a cultura norte-americana tranquilamente permitiria a retratação de casos de nudez em público, pois o indivíduo teria se afastado da expectativa de privacidade que ocorre em relação ao ambiente privado; na cultura europeia a nudez, mesmo que praticada no espaço público, para ser retratada e noticiada deveria contar com autorização prévia do fotografado, vez que este tem controle sobre a própria imagem pública, em respeito à sua dignidade.

O regime jurídico da privacidade também é distinto, na medida em que o direito norte-americano optou por regular a privacidade setorialmente, editando uma legislação para cada área de interesse – o que garantiria eficiência no setor regulado-, o direito europeu em geral edita estatutos generalistas, que sejam aplicáveis a todas as áreas, o que garantiria uniformidade.

As diferenças não fazem de uma ou outra cultura mais ou menos protetiva à privacidade, embora possa restar claro que a legislação europeia é muito mais rigorosa com a atuação do setor privado em relação à privacidade. Desta forma, a privacidade em determinada região apenas reflete a história e a cultura de determinado povo.

Há muito a privacidade deixou de ser entendida como o direito a ser deixado só. Na sociedade da informação hiperconectada, da evolução das tecnologias de informação e comunicação, não é razoável pleitear-se a reclusão como direito. Todavia, pelas manifestações sempre multifacetadas da privacidade, mostra-se um desafio a concepção de um conceito contemporâneo à privacidade, que determine suas características comuns. Fato é

que há uma relação direta entre o direito fundamental à privacidade e a dignidade da pessoa humana, especialmente em relação aos elementos autonomia privada e valor intrínseco, ou seja, apenas exerce a própria autonomia quem possui o espaço de conformação e reflexão preservado e o indivíduo tem valor em si mesmo, não se prestando a práticas utilitaristas, sendo a realização do indivíduo a função central do Estado.

Propomos neste trabalho, com os naturais riscos de incompletude e falhas, mas por entender essencial a adoção de determinada concepção, que se construa o conceito de privacidade a partir da ideia de expectativa razoável de privacidade, expectativa essa que deve ser formada não pelo sujeito atomizado, mas pelo sujeito enraizado que se constrói intersubjetivamente, respeitando-se determinada cultura, que legitimará tais expectativas, sem vinculá-la a limites físicos (lar, residência ou escritório). Propõe-se que a dignidade humana, através de seus elementos, auxilie na construção do que seja expectativa de privacidade, admitindo que esta expectativa seja um conceito socialmente construído, geograficamente e historicamente localizado. Ademais, a conformação do que seja expectativa razoável de privacidade deve observar o princípio da proporcionalidade, admitindo-se sua restrição apenas se passar pelo crivo de seus três subprincípios.

Declarações transnacionais como a Carta de Direitos Fundamentais da União Europeia em geral fazem clara distinção entre os elementos clássicos da privacidade - como a vida privada, familiar, o domicílio e as comunicações – e, em dispositivo distinto, a proteção aos dados pessoais. Embora em dispositivos distintos e sem ignorar a profunda controvérsia, entendemos que não se pode afirmar tratar-se de direito autônomo, mas de decorrência do direito fundamental à privacidade.

O *big data* pode ser definido como fenômeno tecnológico caracterizado pelo grande volume de dados, processado em alta velocidade e com grande variedade de dados. Alguns fatores propiciaram o fenômeno, tais como o barateamento dos custos de armazenamento de dados, o aumento considerável do número de sensores e o advento da internet das coisas, que permite que a comunicação direta entre máquinas colete os mais variados dados do indivíduo.

O *big data* permite que a análise de dados seja mais precisa, a partir do processamento de grande volume de dados, havendo quem se arrisque a afirmar que os dados são o novo petróleo na era da informação. Os benefícios do *big data* podem ser percebidos na melhora da agricultura de precisão, no aperfeiçoamento da medicina personalizada, na realização de ações humanitárias, ou mesmo na criação de condições igualitárias de oportunidade de acesso ao emprego, educação e ao crédito, especialmente a populações de baixa renda. O *big data* pode

ainda contribuir com a melhora dos índices de segurança pública. O processamento de dados da mancha criminal pode antecipar as probabilidades de locais e horários de cometimento de crime, permitindo às forças policiais que se posicionem e antecipem ao fato criminoso e que haja uma melhor alocação dos recursos escassos.

Todavia, não se pode ignorar que o *big data* pode trazer inegáveis riscos à privacidade, ao permitir processar de modo integrado, variados dados que antes não se relacionavam, que permitam revelar informações sensíveis sobre o indivíduo, tais como orientação política, religiosa, sexual, entre outros, que permitam a identificação, o monitoramento e a perseguição.

Do mesmo modo que apresenta um elevado potencial para a promoção da igualdade, no conjunto de dados coletados, o *big data* pode refletir estruturas sociais viciadas e perpetuar práticas discriminatórias, que limitam o acesso de grupos minoritários ao emprego, renda e educação. Também inspira preocupação o uso cada vez maior da chamada análise preditiva que utiliza os dados existentes para definir a probabilidade de comportamentos futuros e definir oportunidades ou limitar direitos.

Neste sentido, pode a análise preditiva definir um candidato adequado à vaga de emprego, de acordo com o risco que ele possui de permanecer no trabalho. Ocorre que a análise preditiva não prevê o futuro, mas apenas expressa uma probabilidade estatística com base em comportamentos anteriores. Tais estatísticas podem refletir desigualdades de gênero, racial e social, de modo que o algoritmo que orienta o processamento do dado deve estar preparado para perceber o enviesamento de determinado dado, a fim de evitar que sejam reproduzidos resultados discriminatórios.

No policiamento preditivo, deve-se ter em conta, por exemplo, que o elevado índice de ocorrência policial em determinada região pode estar relacionado com uma maior incidência de crimes, mas também pode ter relação com um rigor manifestamente excessivo das forças policiais ao atuar em determinados bairros, perpetuando um rigor cada vez maior sobre grupos estigmatizados.

O uso da análise preditiva no sistema de justiça - em que pese vise tornar mais objetiva a definição de sanções - mediante previsão de risco do apenado reincidir criminalmente, pode ocasionar discriminações na medida em que, em geral, os acusados negros apresentaram uma probabilidade de reincidência geral e de reincidência em crimes violentos mais alto que em relação aos acusados brancos, nos locais que o sistema foi implantado. Todavia essa proporção não se confirmava na prática.

O que se deve ter em conta na análise preditiva é que seu uso pode limitar oportunidades, como pode também agravar a situação do acusado ou da liberdade condicional do apenado. Ocorre que a análise preditiva é mero calculo de probabilidade, que pode reproduzir preconceitos, se não levar em consideração que sempre será possível ao indivíduo exercer seu livre arbítrio, no sentido de realizar escolhas morais.

Portanto, para que não se cometam abusos, o algoritmo da análise de dados deve levar em conta as desigualdades sociais envolvidas - tentando corrigi-las, sempre que possível – e os preconceitos do qual se partiu ao estruturar o algoritmo, de modo que seja o mais igualitário possível. Outrossim, a base de dados deve refletir a realidade da melhor forma possível, a fim de que o resultado do processamento dos dados não seja parcial ou incorreto.

O processamento de dados não raro envolve o tratamento de dados pessoais, que conta com uma proteção diferenciada. No Brasil, há três projetos de lei que visam regulamentar o tema. A despeito de não haver uma lei específica, a legislação brasileira possui inúmeros dispositivos esparsos que podem servir de fundamento para a proteção de dados pessoais, podendo-se citar como exemplos as disposições constantes do Marco Civil da Internet e da Lei de Acesso à informação.

Para o livre fluxo de dados e negócios entre o bloco europeu e os Estados Unidos tem havido um esforço, no sentido de estabelecer padrões comuns de tratamento de dados. A aplicação do acordo de proteção de dados conhecido como *Safe Harbor* foi suspensa em virtude de sua anulação, por entender a Corte de Justiça da Comissão Europeia que o ajuste não protegia suficientemente os dados dos cidadãos europeus. O novo acordo, *Privacy Shield*, apresentava compromissos mais efetivos por parte das autoridades estadunidenses, com uma maior transparência das obrigações, um sistema sancionatório mais rigoroso e exigências mais rígidas para as empresas globais que participarem do acordo. Portanto, em que pesem as diferenças culturais no qua tange à privacidade, existentes entre os Estados Unidos e o bloco europeu, a tendência é que os acordos de proteção de dados sirvam cada vez mais para aproximar as normas sobre proteção de dados praticadas em ambos, especialmente pelo interesse de corporações globais em contar com a liberdade do fluxo de dados entre os continentes.

Outra preocupação que o *big data* inspira é a possibilidade de um ambiente propício à vigilância estatal ou privada. Ora, o processamento de um elevado volume de dados pode favorecer que estes dados sejam coletados por órgãos de inteligência estatais para monitorar e perseguir indivíduos. Os documentos revelados por Edward Snowden deixam claro que há um

enorme aparato de vigilância a serviço de interesses econômicos e políticos, com a prática de espionagem não só de criminosos, mas de adversários políticos e econômicos. Apenas com o *big data* foi possível, por exemplo, a façanha de se processar três bilhões de ligações telefônicas e emails em apenas um mês. O *biga data* também facilita a vigilância privada, na medida em que os dados coletados de consumidores podem propiciar a prática da *stalker economy*, que é o monitoramento da atividade do consumidor nas redes, com vistas a convencê-lo a adquirir determinado produto ou serviço.

Em relação à vigilância estatal, salta aos olhos o programa de crédito social chinês, que não poupará esforços para monitorar as atitudes dos cidadãos daquele país na vida *on line* e fora dela, para definir, a partir de opiniões, atitudes e vínculos de amizade, um sistema de classificação do indivíduo que terá repercussão sobre o seu acesso a bens e serviços. Trata-se de criticável mecanismo baseado em perfeccionismo moral que aniquila por completo a dignidade e autonomia dos indivíduos, ignorando a capacidade de Auto conformação e de realização de escolhas morais razoáveis.

No que diz respeito à vigilância privada, os dados se apresentam como a mercadoria cada vez mais valiosa, sendo objeto de vultosas negociações. Ocorre que a liberdade econômica não pode se sobrepor à dignidade da pessoa humana. Portanto, a aplicação de horizontal de direitos fundamentais orienta que não só o Estado atue de forma a não violar e promover os direitos fundamentais, mas que também os particulares em suas relações, se abstenham de violar direitos fundamentais. A eficácia horizontal dos direitos fundamentais impõe aos poderes públicos, além da atuação negativa, uma atuação positiva, no sentido de impedir que particulares violem direitos fundamentais, especialmente as grandes corporações globais da área de tecnologia. Outrossim, a aplicação da proporcionalidade como vedação à proteção insuficiente impõe a atuação positiva dos poderes públicos no sentido de construir no ordenamento jurídico um sistema adequado e suficiente de proteção do direito fundamental à privacidade e uma das formas que isso pode ser implementado no Brasil é através da implementação de uma legislação sobre dados pessoais. Ora, os grandes escândalos de vazamento de dados pessoais, de manipulação eleitoral e de pouco rigor na proteção dos dados de seus usuários por parte de redes sociais bem demonstram a elevada necessidade de atuação positiva dos poderes públicos. Por fim, a eficácia horizontal dos direitos fundamentais não pode ignorar a livre iniciativa e a proteção constitucional à propriedade privada, de modo que sempre deve ser ponderado o direito fundamental à privacidade com a liberdade de contratar dos indivíduos.

Enfim, em que pesem os inegáveis efeitos positivos do *big data* para a sociedade atual, não se pode ignorar seus riscos. Para que a atividade econômica garanta maior eficiência e as políticas públicas sejam mais eficazes são essenciais as contribuições trazidas pela análise e processamento de dados. Todavia, deve-se ter em conta que a relação estatística entre determinadas variáveis não implica necessariamente em um vínculo de causa e efeito. O *big data,* ao fim e ao cabo, trata de pessoas, que possuem liberdade de escolha e podem ter tolhido o livre desenvolvimento de sua personalidade caso as oportunidades lhe sejam limitadas em virtude da probabilidade antes mesmo do cometimento de um ato.

Em uma sociedade democrática, as práticas de *big data* devem ser as mais transparentes possíveis, permitindo-se que os algoritmos projetados para análise de dados sejam submetidos ao escrutínio público e que tanto a base de dados quanto os dados do indivíduo analisados sejam tornados públicos, a fim de que se identifiquem e coibam práticas discriminatórias. O potencial de promoção da igualdade de acesso a oportunidades é altíssimo, a depender do uso que será feito da tecnologia. Por outro lado, o Estado Democrático de Direito, embora permita ao Estado o uso da tecnologia no combate ao crime e na promoção do bem-estar da população, impõe aos poderes públicos uma atuação transparente e legítima, que não estabeleça tratamento desigual ou que os efeitos destas políticas tenham impactos desiguais sobre grupos vulneráveis. Deste modo, um dos grandes instrumentos de resistência à vigilância estatal é a criptografia.

A criptografia, que consiste em técnica de ocultar o conteúdo da mensagem, tem sua origem desde a Idade Antiga, tendo sido aplicada por motivos estratégicos e militares, com vistas a transmitir mensagens, sem que o seu conteúdo pudesse ser conhecido por adversários, destacando-se neste período o modelo conhecido como cifra de César, utilizada por Júlio César para comunicar-se com seus exércitos. A técnica também foi muito utilizada durante a II Guerra Mundial com o uso de máquinas eletromecânicas, o que garantiu relativa vantagem à Alemanha no conflito.

Na era digital, a criptografia passou a consistir em chaves criadas por complexos cálculos matemáticos, traduzidos em linguagem de máquina, de modo que, quanto maior o número de bits da chave, mais forte será a criptografia. A técnica da criptografia simétrica ocorre mediante uso de apenas uma chave para cifrar e decifrar o conteúdo das mensagens. No caso da criptografia assimétrica, há a utilização de um par de chaves pública e privada, tendo cada uma delas funções distintas, servindo uma apenas para cifrar a mensagem, outra

para apenas para decifrar. A criptografia assimétrica é a que melhor garante os atributos da informação, quais sejam, a confidencialidade, a integridade e a autenticidade e o não repúdio.

A partir do início da popularização do uso da criptografia, quando deixou de ser uma exclusividade de forças militares ou de grandes corporações, passa a haver resistência à livre circulação da técnica, tendo havido na década de noventa as *cripto wars*, ou cripto guerras, movimento de resistência estatal à democratização do uso da criptografia. A primeira fase das cripto guerras se encerraram no governo Bill Clinton, quando a criptografia, que constava da relação de munições do ITAR, passa a ser de competência do Departamento de Comércio e não do Departamento de Estado, admitindo-se seu uso para fins civis.

Recentemente, houve uma reedição das cripto guerras, especialmente diante de atentados terroristas que envolveu a utilização de dispositivos cujo conteúdo era protegido por criptografia, como no caso de San Bernardino, nos Estados Unidos. Tal fato tem despertado reações enérgicas de líderes de países ocidentais, no sentido de se defender a proibição do uso da criptografia ou a criação de vulnerabilidade que permita o acesso privilegiado das autoridades investigativas ao conteúdo criptografado.

Os benefícios decorrentes da aplicação da criptografia são os mais variados, destacando-se a comunicação interbancária e a realização de transações financeiras, através de páginas seguras do protocolo *https*; a criação de assinaturas digitais com o uso da criptografia assimétrica; a criação de moedas digitais e a sua certificação pelo sistema *blockchain*; bem como a utilização de aplicativos de mensagem, com criptografia ponta a ponta, que garante que apenas emissor e destinatário acessem a mensagem, mediante combinação de técnicas de criptografia simétrica e assimétrica, podendo-se citar como exemplos os aplicativos Telegram, WhatsApp e Signal.

No Brasil, após inúmeras ordens judiciais oriundas das mais diversas comarcas do país, ordenando a suspensão do aplicativo WhatsApp, a questão foi submetida ao Supremo Tribunal Federal, através da ADPF 403 e da ADI 5572, tendo a primeira contado com decisão liminar suspender decisão do juízo, restabelecendo o funcionamento do aplicativo. A discussão objeto das referidas ações de controle concentrado tem por cerne a possibilidade de bloqueio dos aplicativos de mensagem com criptografia ponta a ponta e a aplicabilidade do Marco Civil da Internet, diante do não fornecimento das mensagens trocadas pelo aplicativo. Trata-se de discussão ainda prematura, mas fato é que, tratando-se de uso da criptografia ponta a ponta não há como se definir a priori qual interesse deve prevalecer, se o interesse das investigações policiais ou a privacidade dos cidadãos.

Não há dúvida que a criptografia encerra em si um caráter instrumental, garantidor da liberdade de expressão e de opinião. A criptografia e o anonimato mantêm a salvo o sigilo da fonte do jornalista investigativo, protege grupos minoritários contra perseguição e monitoramento, impede perseguições de ordem religiosa, política e étnica, garante o anonimato de denúncias por ativistas de direitos humanos, entre outros. Por esta razão, defendemos que a cláusula geral de vedação ao anonimato prevista na Constituição brasileira deve ser interpretada harmonizando-se com a teleologia da norma e a natureza da internet, para concluir que o anonimato vedado pela Carta Magna é apenas o anonimato absoluto utilizado para práticas ilícitas. No caso da utilização do anonimato relativo, ou seja, aquele no qual é possível identificar o autor dos atos, não há nenhuma vedação constitucional. Neste sentido, há forte repúdio da Comissão de Direitos Humanos da ONU a qualquer tentativa de sua limitação do anonimato e da criptografia

Sempre houve muita resistência ao uso da criptografia forte e atualmente as forças policiais pressionam os criadores dos aplicativos a proverem meios de acesso aos conteúdos criptografados, mediante a criação intencional de vulnerabilidades, seja através do fornecimento de chaves mestras ou da criação de uma porta dos fundos. A medida é rechaçada pelos setores de tecnologia, uma vez que qualquer vulnerabilidade cria uma brecha de segurança que poderá ser explorada por qualquer um, o que causa insegurança para todos os usuários. Exemplo disso foi a recente série de ataque de hackers a computadores conhecido como wannacry, no qual se explorou fragilidades antes conhecidas apenas pelas forças de segurança.

Por outro lado, a investigação criminal possui alternativas idôneas que não o acesso privilegiado por meio de vulnerabilidades criadas nas aplicações. As alternativas exigem criatividade e aperfeiçoamento das forças de segurança, que podem utilizar agentes infiltrados nos grupos de mensagens, o espelhamento dos dispositivos móveis utilizados, a interceptação dos backups não criptografados, a busca e apreensão de um dos aparelhos utilizados, bem como a exploração dos metadados, que podem revelar conexões para além da comunicação em si, permitindo a criação de um dossiê digital que muito contribuirá para a investigação. Portanto, pela aplicação do subprincípio da necessidade, apenas na ausência de meios idôneos de igual eficácia e menos onerosos que se justificaria o enfraquecimento da criptografia ou a imposição de criação de uma vulnerabilidade intencional, o que não é o caso.

Com efeito, não se pode dizer que haja um conflito entre criptografia e segurança. Isto porque, ao se controlar a criptografia ou se impor vulnerabilidades intencionais a

consequência será também menos segurança para a garantia de confidencialidade de questões existenciais atinentes à intimidade, para as comunicações em geral, para o sigilo bancário, médico, fiscal, empresarial, entre outros.

Por fim, caso seja imprescindível o levantamento da criptografia e isto seja viável tecnicamente, a melhor conduta a ser adotada é de que este levantamento seja direcionado a um indivíduo em específico, o que será bem menos danoso do que possibilitar o uso de uma chave geral que permita um permanente estado de vigilância.

Não é possível afirmar em abstrato a prevalência apriorística da inviolabilidade da criptografia ou das ações de segurança pública. São formuladas duas hipóteses concretas a respeito: (i) é constitucionalmente legítima a criação de protocolos criptográficos fortes, cujo conteúdo seja inviolável pelo próprio criador e por terceiros, sem que se institua um acesso privilegiado para autoridades investigativas?; (ii) poderia o poder público obrigar o proprietário do aplicativo que crie uma vulnerabilidade para permitir o acesso de autoridades ao conteúdo criptografado?

Quanto à primeira hipótese, a resposta é positiva, vez que a criação de protocolos criptográficos está protegida pela liberdade de expressão e pela liberdade de inciativa, que amparam a livre criação de produtos e serviços, desde que não sejam ilícitos. A aplicação do valor intrínseco, elemento da dignidade da pessoa humana, impede a instrumentalização do indivíduo para o alcance de metas coletivas, não sendo lícito exigir que se crie um sistema de proteção vulnerável.

Da mesma forma, na segunda hipótese, entendemos que a resposta a ser dada deve utilizar a técnica da ponderação. Estando em conflito o direito à privacidade e o direito à segurança pública, entendemos que a medida não passa no filtro da proporcionalidade, uma vez que, embora adequada ao fim a ser atingido, não parece ser a medida menos onerosa, pois há inúmeras outras alternativas menos restritivas à privacidade que a imposição de criação de vulnerabilidade, conforme demonstrado. Outrossim, deve-se ressaltar que a medida não observa a proporcionalidade em sentido estrito. Isto porque os direitos fundamentais protegidos pela criptografia, a saber, a privacidade e a liberdade de expressão possuem elevada carga axiológica em relação à segurança pública, vez que melhor realizam o princípio da dignidade humana (peso abstrato). Na verificação do peso concreto, há uma elevada restrição à privacidade, vez que a criação da vulnerabilidade deixará todos expostos, em nome de benefício em abstrato à investigação criminal. Logo, lei que obrigasse a criação de

vulnerabilidade em criptografia, seria inconstitucional, diante da violação da privacidade, da autonomia privada e da liberdade de expressão.

Por fim, diante das fracassadas tentativas de anonimização de dados pessoais, desponta como protetiva à privacidade na era do *big data* o uso da privacidade diferencial, que enfatiza o processamento de dados do grupo e não do indivíduo. A prática amenizaria os efeitos danosos do big data à privacidade: se por um lado não impede a atividade econômica e o planejamento políticas públicas; por outro, dificulta a identificação do titular do dado, através do embaralhamento e inserção de ruídos nos dados.

No que tange à exigência do consentimento, enquanto único meio para coleta e tratamento de dados, entende-se que, diante do inegável uso secundário dos dados, o modelo de consentimento seja alterado para admitir que o consentimento seja mais amplo, incluindo outras hipóteses de uso dos dados, desde que coerente com as finalidades da cessão. Propõe-se que modelo da privacidade por consentimento migre para a privacidade por a responsabilidade dos gestores de bancos de dados, mediante a estrutura de um rígido modelo sancionatório que não obste o uso secundário de dados, mas estabeleça parâmetros para sua realização e sanção em caso de descumprimento. Portanto, a responsabilidade pela preservação da privacidade seria compartilhada entre o titular dos dados e os tratadores de dados, de modo que sempre será mais fácil fiscalizar as atividades de empresas do que violações individuais, desde que haja um regime jurídico transparente e eficiente. A medida é consentânea com o caráter difuso que cada vez mais assume o direito à privacidade na sociedade da vigilância, diante de novas técnicas de comunicação e informação. O fim a ser perseguido é que haja a máxima transparência pública no tratamento de dados e ações de vigilância e a preservação da privacidade dos indivíduos. O binômio transparência pública e opacidade privada nunca foi tão relevante.

REFERÊNCIAS

A BRIEF HISTORY of the Right of Publicity. **Right of Publicity**, [s.d.]. Disponível em: <http://rightofpublicity.com/brief-history-of-rop>. Acesso em: 22 jul. 2017.

ABELSON, Harold et al. Keys under Doormats: mandating insecurity by requiring government acess to all data and comumunications. **Schneier**, jul. 2015. Disponível em: <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf>. Acesso em: 10 abr. 2018.

ABOUT THE 911 Program. **911**, [s.d.]. Disponível em: <https://www.911.gov/about_national_911program.html>. Acesso em: 11 jan. 2018.

AGÊNCIA O GLOBO. Google, Amazon e Apple Batem Recorde de Receitas e Lucros. **Pequenas Empresas & Grandes Negócios**, fev. 2018. Disponível em: <https://revistapegn.globo.com/Tecnologia/noticia/2018/02/google-amazon-e-apple-batem-recorde.html>. Acesso em: 10 mar. 2018.

AGRELA, Lucas. Telegram ganha 1,5 mi de usuários com bloqueio de WhatsApp. **Exame**, dez. 2015. Disponível em: <https://exame.abril.com.br/tecnologia/telegram-ganha-1-5-mi-de-usuarios-com-bloqueio-de-whatsapp/>. Acesso em: 17 abr. 2018.

AKHTAR, Shayerah Ilias; JONES, Vivian C. Proposed Transatlantic Trade and Investment Partnership (T-TIP): In Brief. **Congressional Research Service**, jun. 2014. Disponível em: <https://fas.org/sgp/crs/row/R43158.pdf>. Acesso em: 10 mar. 2018.

ALDRICH, John. Correlations Genuine and Spurious in Pearson and Yule. **Statistical Science**, v. 10, n. 4, p. 364-376, 1995.

ALEXY, Robert. On Balancing and Subsumption: a Structural Comparison. **Ratio Juris**, v. 16, n. 4, p. 433-449, nov. 2003.

ALONSO, Pedro. A Identidade de Shakespeare, uma dúvida polêmica que ressurge no Reino Unido**. G1**, set. 2017. Disponível em: <http://g1.globo.com/Noticias/PopArte/0,,AA1630128-7084,00-A+IDENTIDADE+DE+SHAKESPEARE+UMA+DUVIDA+POLEMICA+QUE+RESSURGE+NO+REINO+UNIDO.html>. Acesso em: 10 mar. 2018.

AMERICAN LAW INSTITUTE. Restatement (Third) of Unfair Competition. **Masaryk University**, 2009. Disponível em: <https://is.muni.cz/th/169953/pravf_m/Extract_III.pdf>. Acesso em: 22 jul. 2017.

AMERLAND, David. 3 Ways Big Data Changed Google's Hiring Process. **Forbes**, jan. 2014. Disponível em: <https://www.forbes.com/sites/netapp/2014_jan._21/big-data-google-hiring-process/#2de787061452>. Acesso em: 08 jan. 2018.

ANDREWS, Edmund. A new statistical test shows racial profiling in police traffic stops.**Stanford**, jun. 2016. Disponível em: <https://engineering.stanford.edu/magazine/article/new-statistical-test-shows-racial-profiling-police-traffic-stops>. Aceso em: 08 jan. 2018.

ANDWIN, Julia et al. Machine Bias. **ProPublica**, mai. 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 10 jan. 2018.

ANTONIALLI, Dennys et al. O que são dados pessoais? **InternetLab**, jul. 2016. Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-o-que-sao-dados-pessoais/>. Acesso em: 10 jan. 2018.

ARCHIVES PARLEMENTAIRES, 2e série, tome XXIV, p. 71-73, 27 avril 1819. Disponível em: <https://droitcultures.revues.org/3073#ftn17>. Acesso em: 22 jul. 2017.

AS DIFERENÇAS ENTRE análise prescritiva, preditiva, descritiva e diagnóstica. **Blog Vert**, [s.d.]. Disponível em: <http://www.vert.com.br/blog-vert/as-diferencas-entre-analise-prescritiva-preditiva-descritiva-e-diagnostica/>. Acesso em: 20 dez. 2017.

ASSANGE, Julian et al. Cipherpunks: **Liberdade e futuro da internet**. Tradução de: Cristina Yamagami. São Paulo: Boitempo, 2013.

AYUSO, Silvia. Os hispânicos, vítimas silenciosas da violência policial nos EUA. **El País**, jul. 2016. Disponível em: <https://brasil.elpais.com/brasil/2016/07/17/internacional/1468715146_128605.html>. Acesso em: 08 jan. 2018.

BANDEIRA, Gustavo. **A Interceptação do Fluxo de Comunicações por Sistemas de Informática e sua Constitucionalidade**. 2002. Trabalho apresentado como exigência final da disciplina Processo e Garantias Fundamentais. Mestrado em Direito, Rio de Janeiro, 2002.

BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional. **Artigo 19**, nov. 2016.

BARATA, Clara. O FBI entrou num iPhone, mas a guerra com a Apple não acabou. **Publico**, mar. 2016. Disponível em: <https://www.publico.pt/2016/03/29/tecnologia/noticia/fbi-desbloqueia-iphone-de-atacante-de-san-bernardino-e-poe-fim-a-conflito-com-a-apple-1727420>. Acesso em: 18 mar. 2018.

BARBARO, Michael; ZELLER JR., Tom. A face is exposed for AOL searcher no. 4417749. **The New York Times**, ago. 2006.Disponível em: <http://www.nytimes.com/2006/08/09/technology/09aol.html>. Acesso em: 08 jan. 2018.

BARCELLOS, Ana Paula de. Intimidade e pessoas notórias. Liberdades de expressão e informação e biografias. Conflito entre direitos fundamentais. Ponderação, caso concreto e acesso à justiça. Tutelas específica e indenizatória. **Migalhas**, 2014. Disponível em: <http://www.migalhas.com.br/arquivos/2014/5/art20140522-01.pdf>. Acesso em: 20 dez. 2017.

_____. **Ponderação, racionalidade e atividade jurisdicional**. Rio de Janeiro: Renovar, 2005.

BARR, Alistair. Google may ditch 'cookies' as online ad tracker. **USA Today**, set. 2013. Disponível em: <https://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/#>. Acesso em: 22 mar. 2018.

BARROSO, Luís Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo - natureza jurídica, conteúdos mínimos e critérios de aplicação. In: _____. **O novo direito constitucional brasileiro**: contribuições para a construção teórica e prática da jurisdição constitucional no Brasil. Belo Horizonte: Fórum, 2013, p. 307-313.

_____. **Curso de Direito Constitucional Contemporâneo**. São Paulo: Saraiva, 2009.

BATISTA, Henrique Gomes. CIA controla celulares, PCs e até smart TVs, indica WikiLeaks. **O Globo**, mar. 2017. Disponível em: <https://oglobo.globo.com/mundo/cia-controla-celulares-pcs-ate-smart-tvs-indica-wikileaks-21025130>. Acesso em: 20 dez. 2017.

BAUMAN, Zygmunt. **Vigilância Líquida**. Diálogos com David Lyon. Zahar Editora, 2014.

BAZELON, Emily. Sentencing by the Numbers.**The New York Times**, jan. 2005. Disponível em: <http://www.nytimes.com/2005 jan. 02/magazine/sentencing-by-the-numbers.html>. Acesso em: 18 jan. 2018.

BENTHAM, Jeremy et. al. **O panóptico**. Tradução de: Guacira Lopes Louro, M. d. Magno, Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica Editora, 2008.

BERK, R.A. et al. Forecasting Murder within a Population of Probationers and Parolees: A High Stakes Application of Statistical Learning. **Journal of the Royal Statistics Society**, series A, n. 172, Part 1, p. 191–211, 2008.

BERSIN, Josh. Google For Jobs: Potential To Disrupt The $200 Billion Recruiting Industry. **Forbes**, mai. 2017. Disponível em: <https://www.forbes.com/sites/joshbersin/2017/05/26/google-for-jobs-potential-to-disrupt-the-200-billion-recruiting-industry/#544c89f74d1f> .Acesso em: 08 jan. 2018.

BIG DATA: A TOOL FOR Fighting Discrimination and Empowering Groups. In: **Future Of Privacy Forum and Anti-Defamation League**, [s.l.], [s.d..Disponível em: <https://fpf.org/wp-content/uploads/Big-Data-A-Tool-for-Fighting-Discrimination-and-Empowering-Groups-Report1.pdf>. Acesso em: 10 jan. 2018.

BIONI, Bruno. **Autodeterminação informacional**: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2016.

BLOUSTEIN, Edward J. Privacy as an aspect of human dignity: an answer to dean Prosser. **New York University Law Review**, v. 39, p. 962, 1964 apud ZANINI op cit, p. 22.

BOGART, Nicole. Research in big data analytics working to save lives of premature babies. **Global News**, jul. 2013. Disponível em: <https://globalnews.ca/news/696445/research-in-big-data-analytics-working-to-save-lives-of-premature-babies/>. Acesso em: 20 dez. 2017.

BOOTH, Alison. Minority Report in Chicago as police aim to stop crime before it happens. **Naked Security**, mai. 2017.Disponível em: <https://nakedsecurity.sophos.com/2017/05/10/minority-report-in-chicago-as-police-aim-to-stop-crime-before-it-happens/>. Acesso em: 18 jan. 2018.

BOYD, Danah; CRAWFORD, Kate.Critical questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. **Information, Communication & Society**, v. 15, n. 5, p. 663, jun. 2012.

BOZZA, Fábio da Silva. Segurança não é direito fundamental. **Canal de Ciências Criminais**, fev. 2016. Disponível em: <https://canalcienciascriminais.com.br/seguranca-nao-e-direito-fundamental/>. Acesso em: 13 abr. 2018.

BRANDÃO, Rodrigo. **Direitos fundamentais, cláusulas pétreas e democracia**. Rio de Janeiro: Renovar, 2008, p. 195-210.

BREVOORT, Kenneth P.; GRIMM, Philipp; KAMBARA, Michelle. Data Point: Credit Invisibles. **CFPB Office of Research**, mai. 2015. Disponível em: <http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf>. Acesso em: 20 dez. 2017.

BRIGATTO, Gustavo. Após Trump e Brexit, Cambridge Analytica vai operar no Brasil. **Valor Econômico**, mar. 2017. Disponível em: <http://www.valor.com.br/empresas/4896618/apos-trump-e-brexit-cambridge-analytica-vai-operar-no-brasil>. Acesso em: 20 dez. 2017.

BROOKMAN, Justin. Browser History Sniffing in the News. **Center for Democracy & Technology**, dez. 2010. Disponível em: <https://cdt.org/blog/browser-history-sniffing-in-the-news/>. Acesso em: 20 dez. 2017.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **Revista FAMECOS**, Porto Alegre, v. 15, n. 36, p. 10-16, ago. 2008.

BYRNE, Michael. O Que É Privacidade Diferencial? **MotherBoard**, jan. 2015. Disponível em: <https://motherboard.vice.com/pt_br/article/nz3avw/o-que-e-privacidade-diferencial>. Acesso em: 13 abr. 2018.

CADAVID, Jhonny Antonio Pabón. La criptografia y la protección a la información digital. **Revista La propriedade inmaterial**, n. 14, p. 62, 2010.

CALMON, Fernando. Ford lança sistema que chama o Samu em caso de acidente com o novo Ka. **Carros**, jul. 2014. Disponível em: <https://carros.uol.com.br/colunas/alta-roda/2014/07/29/ford-lanca-sistema-que-chama-o-samu-em-caso-de-acidente-com-o-novo-ka.htm>. Acesso em: 20 dez. 2017.

CÂMARAREALIZASEMINÁRIOsobreDadosPessoais (PL 5276/16). **CNF**,jul. 2016. Disponível em: <http://www.cnf.org.br/noticia/-/blogs/camara-realiza-seminario-sobre-dados-pessoais-pl-5276-16-/maximized>/ Acesso em: 18 mar. 2018.

CAMPOS, Ana Cristina. IBGE: celular se consolida como o principal meio de acesso à internet no Brasil. **EBC Agência Brasil**, dez. 2016. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2016-12/ibge-celular-se-consolida-como-o-principal-meio-de-acesso-internet-no-brasil>. Acesso em: 18 dez. 2017>.

CAMPOS, Luiz Fernando de Barros. METADADOS DIGITAIS: revisão bibliográfica da evolução e tendências por meio de categorias funcionais. **Enc. Bibli: R. Eletr. Bibliotecon. Ci. Inf.**, Florianópolis, n. 23, p. 16-46, 2007.

CAPANEMA, Walter Aranha. O direito ao anonimato: uma nova interpretação do art. 5º, IV, CF. **A Voz do Cidadão**, [s.d.]. Disponível em: <http://www.avozdocidadao.com.br/images_02/artigo_walter_capanema_o_direito_ao_anonimato.pdf>. Acesso em: 13 mar. 2018.

CAPELAS, Bruno. Até o fim de 2017, Brasil terá um smartphone por habitante, diz FGV. **Link Estadão**, abr. 2017. Disponível em: <http://link.estadao.com.br/noticias/gadget,ate-o-fim-de-2017-brasil-tera-um-smartphone-por-habitante-diz-pesquisa-da-fgv,70001744407>. Acesso em: 20 dez. 2017.

CARDOZO, Nate. Lei e criptografia em 2016. **Actantes**, jan. 2017. Disponível em: <https://actantes.org.br/leis-e-criptografia-em-2016/>. Acesso em: 13 abr. 2018.

CARNEIRO, Luis Sergio F. Criptografia, Hash, Assinatura Digital: Qual a Diferença? **Matera**, fev. 2015. Disponível em: <http://matera.com/br/2015/02/27/criptografia-hash-assinatura-digital-qual-diferenca/>. Acesso em: 13 mar. 2018.

CARVALHO, Luiz Gustavo Grandinetti Castanho de. Direito à Privacidade. **Revista da EMERJ**, v.1, n. 2, p. 55, 1998.

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA. Certificação Digital. **Instituto Nacional de Tecnologia da Informação**, jun. 2017. Disponível em: <http://www.iti.gov.br/perguntas-frequentes/41-perguntas-frequentes/112-sobre-certificacao-digital>. Acesso em 18 mar. 2018.

CASTRO, Daniel. Spring Privacy Series: Consumer Generated and Controlled Health Data. **Center for Data Innovation**, Project No. P145401, 2014. Disponível em: <https://www.ftc.gov/system/files/documents/public_comments/2014/06/00016-90408.pdf>. Acesso em: 10 jan. 2018.

_____. The rise of Data Poverty in America. **Center for Data Innovation**, set. 2014, p. 6. Disponível em: <http://www2.datainnovation.org/2014-data-poverty.pdf>. Acesso em: 10 jan. 2017.

CERVASIO, Daniel Bucar. **Proteção de Dados da Pessoa Humana na Administração Pública**. 2008. Dissertação (Mestrado em Direito Civil) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2008.

CFPB CONSUMER LAWS AND REGULATIONS. Equal Credit Opportunity Act (ECOA). **CFPB**, jun. 2013. Disponível em: <http://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_ecoa-combined-june-2013.pdf>. Acesso em: 08 jan. 2018.

CHAMY, Constanza Hola. Como o FBI conseguiu desbloquear o iPhone de suspeito de ataque à revelia da Apple. **BBC Brasil**, mar. 2016. Disponível em: <http://www.bbc.com/portuguese/noticias/2016/03/160330_fbi_apple_lab>. Acesso em: 18 mar. 2018.

CHANG, Lulu. 5 billion people worldwide now have a mobile device, GSMA data shows. **Digital Trends**, jun. 2017. Disponível em: <https://www.digitaltrends.com/mobile/5-billion-mobile-users/?utm_source=feedly&utm_medium=webfeeds>. Acesso em: 20 dez. 2017.

CIO.COM. Blockchain: o que é e como funciona. **ComputerWorld**, jun. 2016. Disponível em: <http://computerworld.com.br/blockchain-o-que-e-e-como-funciona>. Acesso em: 13 mar. 2018.

CLINTON, William J. Executive Order 13026—Administration of Export Controls on Encryption Products. **The American Presidency Project**, nov. 1996. Disponível em: <http://www.presidency.ucsb.edu/ws/index.php?pid=52252>. Acesso em: 10 abr. 2018.

CLOVER, Charles. China: When big data meets big brother. **Financial Times**, jan. 2016. Disponível em: <https://www.ft.com/content/b5b13a5e-b847-11e5-b151-8e15c9a029fb>. Acesso em: 18 mar. 2018.

COHEN, Fred. A Short History of Cryptography. **All**, 1995. Disponível em: <http://all.net/edu/curr/ip/Chap2-1.html>. Acesso em 13 mar. 2018.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as a Object. **Stanford Law Review**, v. 52, p. 1373-1426, mai. 2000.

COMO FUNCIONA O APP 'ultrasseguro' de mensagens usado por Snowden. **BBC Brasil**, nov. 2016. Disponível em: <http://www.bbc.com/portuguese/geral-37821449>. Acesso em: 18 mar. 2018.

COMO O WAZE funciona? **Suporte do Google**, [s.d.]. Disponível em: <https://support.google.com/waze/answer/6078702?hl=pt-BR>. Acesso em: 20 dez. 2017.

CONSTANTIN, Lucian. LG admite que Smart TVs coletam dados sobre hábitos de usuários. **IDGNow!**, nov. 2013. Disponível em: <http://idgnow.com.br/internet/2013/11/25/lg-admite-que-smart-tvs-coletam-dados-sobre-habitos-de-usuarios/>. Acesso em: 20 dez. 2017.

CONTESINI, Leonardo. GPS integrado pode coletar dados do motorista e do carro e enviá-los para as fabricantes. **Flatout**, jan. 2014. Disponível em: <https://www.flatout.com.br/gps-integrado-pode-coletar-dados-motorista-e-carro-e-envia-los-para-fabricantes/. Acesso em: 20 dez. 2017.

COOLEY, Thomas M. A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract. Chicago: Callaghan, 1879.

CORREIA, Luis Fernando. Medicação com sensor que envia alerta sobre ingestão ao médico é aprovada nos EUA. **CBN**, nov. 2017. Disponível em: <http://cbn.globoradio.globo.com/media/audio/137863/medicacao-com-sensor-que-envia-alerta-sobre-ingest.htm>. Acesso em: 18 jan. 2017.

COSTA JR., Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Editora Revista dos Tribunais, 1995.

CRAWFORD, Kate. The Hidden Biases in Big Data. **Harvard Business Review**, abr. 2013. Disponível em: <https://hbr.org/2013/04/the-hidden-biases-in-big-data>. Acesso em: 08 jan. 2018.

DATA-DRIVEN HEALTHCARE organizations use big data analytics for big gains. New York: IBM, 2013, p. 5.

DATAINFORMED. They Know Who You're Voting For: How Big Data Redefines Political Campaigns' Microtargeting. Disponível em: <http://data-informed.com/they-know-who-youre-voting-for-how-big-data-redefines-political-campaigns-microtargeting/>. Acesso em: 18 dez. 2017.

DE ONDE VÊM as sugestões de Pessoas que você talvez conheça? **Facebook**, [s.d.]. Disponível: <https://pt-br.facebook.com/help/163810437015615?helpref=faq_content>. Acesso em: 10 jan. 2018.

DECISÃO QUE SUSPENDIA WhatsApp em todo o Brasil é derrubada no TJ-PI. **Consultor Jurídico**, fev. 2015. Disponível em: <https://www.conjur.com.br/2015-fev-26/decisao-suspendia-whatsapp-brasil-derrubada-tj-pi>. Acesso em: 19 mar. 2018.

DEVRIES-VALENTINO, Jennifer; ANGWIN, Julia; STECKLOW, Steve. Tecnologias de espionagem agora são vendidas no varejo. **The Wall Street Journal**, nov. 2011. Disponível em: <https://www.wsj.com/articles/SB10001424052970204531404577050803429174524>. Acesso em: 12 jan. 2018.

DI FÁTIMA, Branco. Primavera Árabe: vigilância e controle na sociedade da informação. **Biblioteca online de ciências da comunicação**, [s.d.]. Disponível em: <http://www.bocc.ubi.pt/pag/fatima-branco-primavera-arabe-vigilancia-e-controle.pdf>. Acesso em: 11 jan. 2018.

DIAS, Guilherme. Cerca de 100 bilhões de buscas são realizadas no Google mensalmente. **TecMundo**, abr. 2014. Disponível em: <https://www.tecmundo.com.br/google/53852-cerca-de-100-bilhoes-de-buscas-sao-realizadas-no-google-mensalmente.htm>. Acesso em: 20 dez. 2017.

DO PORTAL DO GOVERNO. Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. **Portal do Governo de São Paulo**, mai. 2017. Disponível em: <http://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em: 18 jan. 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

EDITORIAL. Facebook em novo caso de manipulação eleitoral. **O Globo**, mar. 2018. Disponível em: <https://oglobo.globo.com/opiniao/facebook-em-novo-caso-de-manipulacao-eleitoral-22513403>. Acesso em: 22 mar. 2018.

EFE. 'WhatsApp tem vulnerabilidade que permite interceptar mensagens'. **Exame**, jan. 2017. Disponível em: <http://exame.abril.com.br/tecnologia/whatsapp-tem-vulnerabilidade-que-permite-interceptar-mensagens/>. Acesso em: 05 mar. 2017.

EPSTEIN, Adam. Facebook's new patent lets lenders reject a loan based on your friends' credit scores—but don't freak out. **Quartz**, ago. 2015. Disponível em: <https://qz.com/472751/facebooks-new-patent-lets-lenders-reject-a-loan-based-on-your-friends-credit-scores-but-dont-freak-out/>. Acesso em: 10 jan. 2018.

ESTADOS UNIDOS DA AMÉRICA. Supreme Court of Wisconsin. State v. Lomis. Disponível em: <http://caselaw.findlaw.com/wi-supreme-court/1742124.html>. Acesso em: 10 jan. 2018.

EUROPEAN COMMISSION. Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Recommendation 3/97: Anonymity on the Internet. **European Commission**, dez. 1997, p. 5. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf>. Acesso em: 10 abr. 2018.

EUROPEAN COUNCIL. European Council meeting (22 and 23 June 2017) – Conclusions. **European Council**, jun. 2017. Disponível em: <http://data.consilium.europa.eu/doc/document/ST-8-2017-INIT/en/pdf>. Acesso em: 13 mar. 2018.

EUROPEAN PARLIAMENT. Reform of the e-Privacy Directive. **European Parliament**, set. 2017. Disponível em: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf>. Acesso em: 18 mar. 2018.

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES. **Big Data And Differential Pricing**. Council of Economic Advisers: [s.l.], 2012. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf>. Acesso em: 08 jan. 2018.

_____. **Big Data**: A Report on Algorithmic Systems, Opportunity, and Civil Rights. The White House: Washington, 2016, p. 13

_____. **Big data**: seizing opportunities, preserving values. Washington: The White House, 2014. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 18 dez. 2017.

FARINACCIO, Rafael. Dark Web revelada: afinal, o que mais existe no canto obscuro da internet? **TecMundo**, set. 2016. Disponível em: <https://www.tecmundo.com.br/internet/109781-dark-web-revelada-existe-canto-obscuro-internet.htm>. Acesso em: 10 mar. 2018.

FEDERAL TRADE COMISSION. **Big Data**: A tool for inclusion or exclusion? Understanding the issues. FTC Report, jan. 2016. Disponível em:

<https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>. Acesso em: 18 dez. 2017.

_____. **Data Brokers**: A Call for Transparency and Accountability. FTC: [s.l.], p. 46. Disponível: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 20 dez. 2017.

FERNANDES, Carlos Henrique de; O.FILHO, Fernando Mario de. A Privacidade na Sociedade da Informação. **Rede Linux IME-USP**, nov. 2003.Disponível em: <https://www.linux.ime.usp.br/~carloshf/0302-mac339/fase1/>. Acesso em: 22 dez. 2017.

FERNANDES, Carol. O que é cloud computing. **TechTudo**, mar. 2012.Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/03/o-que-e-cloud-computing.html>. Acesso em: 20 dez. 2017.

FESTAS, David de Oliveira. **Do conteúdo patrimonial do direito à imagem**: Contributo para um Estudo do seu Aproveitamento Consentido e Inter Vivos. Coimbra: Coimbra Editora, 2009.

FITZPATRICK, Jason. If You're Not Paying for It; You're the Product. **LifeHacker**, nov. 2010. Disponível em: <https://lifehacker.com/5697167/if-youre-not-paying-for-it-youre-the-product>. Acesso em: 18 dez. 2017.

FRANCIS, Bob. User confidence takes a Net loss. **InfoWorld**, jul. 2005. Disponível em:<https://www.infoworld.com/article/2670085/security/user-confidence-takes-a-net-loss.html>. Acesso em: 20 dez. 2017.

FRIEDMAN, Barry; KERR, Orin. The Fourth Amendment. **Constitution Center**, [s.d.]. Disponível em: <https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv>. Acesso em: 10 jan. 2018.

FROTA, Hidemberg Alves da. A proteção da vida privada, da intimidade e do segredo no direito brasileiro e comparado. **Revista Jurídica da UNIJUS**, v. 29, n. 11, p. 79, 2006.

FUTURE ATTRIBUTE SCREENING Technology. **DHS Science and Technology Directorate**, nov. 2014. Disponível em: <https://www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST-508_0.pdf>. Acesso em: 10 jan. 2018.

G1 SÃO PAULO. Deputado diz que Exército admitiu ter colocado militar em ato em SP nas Olimpíadas. **G1**, dez. 2016.Disponível em: <https://g1.globo.com/sao-paulo/noticia/exercito-admite-militar-infiltrado-em-ato-em-sp-nas-olimpiadas-diz-deputado.ghtml>. Acesso em: 10 jan. 2018.

G1. Documentos da NSA apontam Dilma Rousseff como alvo de espionagem. **G1**, set. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html>.Acesso em: 10 fev. 2018.

_____. Em dois dias, Facebook perde quase US$ 50 bilhões em valor de mercado. **G1**, mar. 2018. Disponível em: <https://g1.globo.com/economia/noticia/em-dois-dias-facebook-perde-quase-us-50-bilhoes-em-valor-de-mercado.ghtml>. Acesso em: 20 mar. 2018

_____. Ministério de Minas e Energia foi alvo de espionagem do Canadá. **G1**, out. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/10/ministerio-de-minas-e-energia-foi-alvo-de-espionagem-do-canada.html>. Acesso em: 10 fev. 2018.

_____. Mulheres são maioria entre usuários de internet no Brasil, diz pesquisa. **G1**, fev. 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/02/mulheres-sao-maioria-entre-usuarios-de-internet-no-brasil-diz-pesquisa.html>. Acesso em: 20 dez. 2017.

GEARY, Brandon. Data Is The New Commodity. **Brand Quaterly**, [s.d.]. Disponível em: <http://www.brandquarterly.com/data-new-commodity>. Acesso em: 08 jan. 2018.

GIANNOTTI, Edoardo. **A tutela constitucional da intimidade**. Rio de Janeiro: Forense, 1987.

GIBBINS, Nicholas. How what's on your credit report can affect job applications. **Experian**, jan. 2015. **Disponível em: <**http://www.experian.co.uk/blogs/consumer-advice/credit-report-affect-job-application/>. Acesso em: 10 jan. 2018.

GIBBS, Samuel. What is 'safe harbour' and why did the EUCJ just declare it invalid? **The Guardian**, out. 2015. Disponível em: <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>. Acesso em: 15 fev. 2018.

GOMES, Helton Simões; LAPORTA, Taís. Entenda o que é blockchain, a tecnologia por trás do bitcoin. **G1**, fev. 2018. Disponível em: <https://g1.globo.com/economia/noticia/entenda-o-que-e-blockchain-a-tecnologia-por-tras-do-bitcoin.ghtml>. Acesso em: 13 mar. 2018.

_____. Brasil supera marca de 100 milhões de internautas, diz IBGE. **G1**, São Paulo, nov. 2016. Dispnível em: <http://g1.globo.com/tecnologia/noticia/2016/11/brasil-supera-marca-de-100-milhoes-de-internautas-diz-ibge.html>.Acesso em: 20 dez. 2017.

GOMES, Rodrigo Dias de Pinho Gomes. 2017. **Big data**: desafios à tutela da pessoa humana na sociedade da informação. Dissertação (Mestrado em Direito) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017.

GRANDELLE, Renato. Desastres naturais forçam migrações de 60 mil por dia. **O Globo**, out. 2015. Disponível em: <https://oglobo.globo.com/sociedade/sustentabilidade/desastres-naturais-forcam-migracoes-de-60-mil-por-dia-17680284>. Acesso em: 20 dez. 2017.

GREEN, Jon. Facebook knows you're gay before you do. **American Blog**, mar. 2013. Disponível em: <http://americablog.com/2013/03/facebook-might-know-youre-gay-before-you-do.html>. Acesso em: 10 jan. 2018.

GREEN, Matthew. Why can't Apple decrypt your iPhone? **Cryptography Engineering**, out. 2014. Disponível em: <https://blog.cryptographyengineering.com/2014/10/04/why-cant-apple-decrypt-your-iphone/>. Acesso em: 18 abr. 2018.

GREENBERG, Andy. Apple's 'Differential Privacy' is About Collecting Your Data—But Not *Your* data. **Wired**, jun. 2016. Disponível em: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>. Acesso em: 31 mar. 2018.

GREENWALD, Gleen; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, jun. 2013. Disponível em:<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 10 fev. 2018.

GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. **The Guardian**, jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. Acesso em: 10 fev. 2018.

GREENWALD, Glenn. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo americano. Tradução de: Fernanda Abreu. Rio de Janeiro: Sextante, 2014 (ePub).

GRESCHBACH, Benjamin; KREITZ, Gunnar; BUCHEGGER, Sonja. The devil is in the metadata — New privacy challenges in Decentralised Online Social Networks. In: **Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on Pervasive Computing and Communications Workshops**, 2012, p. 333-339. Disponível em: <https://ieeexplore.ieee.org/document/6197506/>. Acesso em: 16 abr. 2018.

GUERREIRO, Yan. você Sabia Que o Bilhete Único Utiliza a Tecnologia RFID?**RFID Brasil**, out. 2017. Disponível em: <https://rfidbrasil.com/blog/bilhete-unico-com-rfid/>. Acesso em: 05 jan. 2018.

HAITI EARTHQUAKE 2010. **Flowminder**, [s.d.]. Disponível em: <http://www.flowminder.org/case-studies/haiti-earthquake-2010>. Acesso em: 20 dez. 2017.

HARADA, Eduardo. Tor: entenda como esta rede garante o seu anonimato na internet. **TecMundo**, mai. 2016. Disponível em: <https://www.tecmundo.com.br/seguranca/104364-tor-entenda-rede-garante-anonimato-internet.htm>. Acesso em: 10 abr. 2018.

HARRIS, John. The tyranny of algorithms is part of our lives: soon they could rate everything we do. **The Guardian**, mar. 2018. Disponível em: <https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data>. Acesso em: 10 mar. 2018.

HICKMAN, Leo. How Algorithms Rule the World. **The Guardian**, jul. 2013. Disponível em: <https://www.theguardian.com/science/2013/jul jan. how-algorithms-rule-world-nsa>. Acesso em: 11 jan. 2018.

HIGA, Paulo. Ransomware WannaCry já infectou 200 mil computadores em 150 países. **Tecnoblog**, [s.d.]. Disponíel em: <https://tecnoblog.net/214656/wannacry-ataque-disseminacao-150-paises/>. Acesso em: 13 abr. 2018.

HISTORY AND SCOPE of the Amendment. **Justia US Law**, [s.d.]. Disponível em: <https://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html>. Acesso em: 10 jan. 2018.

HISTORY SNIFFING. **Schott's Vocab**, jun. 2011. Disponível em: <https://schott.blogs.nytimes.com/2010/12/08/history-sniffing/>. Acesso em: 20 dez. 2017.

HODGE, Mark. Real Black Mirror. **The Sun**, mar. 2018. Disponível em: <https://www.thesun.co.uk/news/5730910/china-social-credit-rating-blacklists-citizens/>. Acesso em: 10 mar. 2018.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. **Big Data no Sul Global**: Relatório sobre estudos de caso. Rio de Janeiro: ITS, 2016, p. 9. Disponível em: <https://itsrio.org/wp-content/uploads/2017 fev. ITS_Big-Data_PT-BR_v4.pdf>. Acesso em: 22 dez. 2017.

JACOBSON, Ralph. IBM. 2.5 quintillion bytes of data created every day. How does CPG & Retail manage it? **IBM**,abr. 2013. Disponível em:<https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/>. Acesso em: 20 dez. 2017.

JORNAL DO BRASIL. PNAD: número de internautas cresce 143,8% em seis anos, **Jornal do Brasil**, mai. 2013. Disponível em: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2013/05/16/pnad-numero-de-internautas-cresce-1438-em-seis-anos/>. Acesso em: 10 jan. 2018.

JULINHO DE ADELAIDE, 24 anos depois. **Sanatório Geral**, [s.d.]. Disponível em: <http://www.chicobuarque.com.br/sanatorio/julinho.htm>. Acesso em: 10 abr. 2018.

KALVEN JR., Harry. Privacy in Tort Law - Were Warren and Brandeis Wrong? **Law and Contemporary Problems**, v. 31, p. 326-341, 1966.

KANELLOS, Michael. A Big Data App That Helps You Find A Parking Spot. **Forbes**, jun. 2015. Disponível em: <https://www.forbes.com/sites/michaelkanellos/2015/06/03/a-big-data-app-that-helps-you-find-a-parking-spot/#4b23e23c43ba>. Acesso em: 20 dez. 2017.

KATO, Rafael. Big Data contra o crime. **Exame**, abr. 2014. Disponível em: <https://exame.abril.com.br/tecnologia/big-data-contra-o-crime>. Acesso em: 11 jan. 2018.

KAYE, David. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/29/32). **Human Rights Council**, mai. 2015. Disponível em: <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>. Acesso em: 10 abr. 2018.

KAYYALI, Dia. Why Fusion Centers Matter: FAQ. **Electronic Frontier Foundation**, abr. 2014. Disponível em: <https://www.eff.org/deeplinks/2014/04/why-fusion-centers-matter-faq>.Acesso em: 10 jan. 2018.

KEHL, Danielle; GUO, Priscilla; KESSLER, Samuel. Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. **Harvard Law School**, jul.

2017. Disponível em: <https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf?sequence=1>. Acesso em: 10 jan. 2018.

KERR, Orin S. Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't. 97 **Northwestern University Law Review**, v, 97, n. 2, p. 607-674, 2003.

KLEIN, Gisiela Hasse; NETO, Pedro Guidi; TEZZA, Rafael. Big Data e mídias sociais: monitoramento das redes como ferramenta de gestão. **Saúde Soc. São Paulo**, v. 26, n. 1, p. 208-217, 2017.

KOPFSTEIN, Janus. É assim que o FBI destravará o iPhone de San Bernardino sem a ajuda da Apple. **Motherboard**, mar. 2016. Disponível em: <https://motherboard.vice.com/pt_br/article/kb34kz/e-assim-que-o-fbi-destravar-o-iphone-de-san-bernardino-sem-a-ajuda-da-apple>. Acesso em: 18 mar. 2018.

KOSINSK, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits & attributes are predictable from digital records of human behaviour. **PNAS**, v. 110, n. 5, p. 5802-5805, abr. 2013.

LARSON, Jeff et al. How We Analyzed the COMPAS Recidivism Algorithm. **ProPublica**, mai. 2016. Disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Acesso em: 10 jan. 2018.

LAZER, D. M. et al.The Parable of Google Flu: Traps in Big Data Analysis. **Science**, v. 343, n. 6176, p. 1203-1205, mar. 2014.

LEMOS, Ronaldo et al. Estudo sobre a regulamentação jurídica do spam no Brasil. Trabalho comissionado pelo Comitê Gestor da Internet no Brasil ao Centro de Tecnologia e Sociedade (CTS), da Escola de Direito do Rio de Janeiro/Fundação Getúlio Vargas, Fundação Getulio Vargas, Rio de Janeiro, 2007. Disponível em: <https://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 22 dez. 2017.

LESKOVEC, Jure; MILLIWAY, Anand R.; ULLMAN, Jeffrey D. **Mining of Massive Datasets**. Disponível em: <http://infolab.stanford.edu/~ullman/mmds/book.pdf>. Acesso em: 08 jan. 2017.

LI, Li et al. Identification of type 2 diabetes subgroups through topological analysis of patient similarity. **Science Translational Medicine**, v. 7, n. 311, p. 311 e ss., out. 2015.

LIMA, Glaydson de Farias. **Manual de Direito Digital**: Fundamentos Legislação e Jurisprudência. Curitiba: Apris, 2016.

LINK PREDICTION BY De-anonymization: How We Won the Kaggle Social Network Challenge.**33 Bits of Entropy**, mar. 2011. Disponível em: <https://33bits.wordpress.com/2011/03/09/link-prediction-by-de-anonymization-how-we-won-the-kaggle-social-network-challenge/>. Acesso em: 08 jan. 2018.

LIRA, Isadora Teixeira de. Hacktivistas e Cypherpunks: A Resistência à Militarização e Vigilância do Ciberespaço na Sociedade de Controle. In: **40º Encontro Anual de Anpocs**, Caxambu, out. 2016. Disponível em: <http://www.anpocs.com/index.php/papers-40-

encontro/st-10/st05-8/10169-hacktivistas-e-cypherpunks-a-resistencia-a-militarizacao-e-vigilancia-do-ciberespaco-na-sociedade-de-controle/file>. Acesso em: 18 mar. 2018.

LOHR, Steve. Google Flu Trends: The Limits of Big Data.**Bits**, mar. 2014. Disponível em: <https://bits.blogs.nytimes.com/2014/03/28/google-flu-trends-the-limits-of-big-data/>. Acesso em: 20 dez. 2017.

LOMAS, Natasha. What Apple's differential privacy means for your data and the future of machine learning. **TechCrunch**, jun. 2016. Disponível em: <https://techcrunch.com/2016/06/14/differential-privacy/>. Acesso em: 13 abr. 2018.

LOTT, Diana. Brasil é sétimo país do mundo em número de jornalistas assassinados. **Folha**, São Paulo, out. 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2017/10/1930121-brasil-e-o-setimo-pais-do-mundo-em-numero-de-jornalistas-assassinados.shtml>. Acesso em: 18 mar. 2018.

LUENGO-OROZ, Miguel. Big Data for Development in Action: The Global Pulse Project Series. **United Nations Global Pulse**, jul. 2015. Disponível em: <https://www.unglobalpulse.org/blog/big-data-development-action-global-pulse-project-series. Acesso em: 08 jan. 2017.

LYON, David. Cyberespace: Beyond the Information Society? In: ARMITAGE, John Armitage; ROBERTS, Joanne (Eds.). **Living With Cyberspace**. New York: Bloomsbury Academic, 2002, p. 21-33.

MACCARINI, Juarez Lencioni. O Gmail agora é todo criptografado. **Tecnoblog**, 2010. Disponível em: <https://tecnoblog.net/14260/o-gmail-agora-e-todo-criptografado/>. Acesso em: 10 abr. 2018.

MAIEROVITCH, Wálter. Os "Cinco Olhos" e os cegos. **Carta Capital**, out. 2013. Disponível em: <https://www.cartacapital.com.br/revista/774/os-201ccinco-olhos201d-e-os-cegos-9894.html>. Acesso em: 10 fev. 2018.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática**: uma abordagem jurídica sobre a criptografia, São Paulo: Forense, 2010.

MARTEL, Letícia de Campos Velho. Indisponibilidade de Direitos Fundamentais: Conceito lacônico, consequências duvidosas. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coords.). **Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica. Rio de Janeiro: Lumen Juris, 2011, p. 75-112.

MASCARENHAS, Gabriel. Polícia Federal recorreu a infiltrado para obter dados de grupo suspeito. **Folha de São Paulo**, Brasíia, jul. 2016. Disponível em: <http://www1.folha.uol.com.br/esporte/olimpiada-no-rio/2016/07/1794611-policia-federal-recorreu-a-infiltrado-para-obter-dados-de-grupo-suspeito.shtml>. Acesso em: 17 abr. 2018.

MATHEWS, Jud; SWEET, Alec Stone. All Things in Proportion? American Rights Doctrine and the Problem of Balancing. **Emory Law Journal**, v. 60, n. 4, p. 799-875, mar. 2010.

MAYER-SCHONBERER, Viktor; CUKIER, Kenneh. **Big Data**: A Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mffin Hartcourt, 2013.

MCCULLAGH, Declan. FBI taps cell phone mic as eavesdropping tool.**CNET**, dez. 2006. Disponível em: <https://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/>. Acesso em: 18 jan. 2018.

MELO, Mariana Cunha e. Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil. **ITS Rio**, mar. 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf>. Acesso em: 13 mar. 2018.

MELTZER, Joshua P. The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment. **Global Economy & Development**,working papern. N. 79, out. 2014.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2008.

MENEZES, Alfred J.; OORSCHOT, Paul C. van.; VANSTONE, Scott A. (Eds.). **Handbook of applied cryptography**. New York: CRC Press Book.

MILLER, Claire Cain. When Algorithms Discriminate. **The New York Times**, jul. 2015. Dispon'vel em: <https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html>. Acesso em: 08 jan. 2018.

MOBILE PHONE DATA to Understand Climate Change and Migration Patterns in Bangladesh. **Flowminder**, [s.d.]. Disponível em: <http://www.flowminder.org/case-studies/mobile-phone-data-to-understand-climate-change-and-migration-patterns-in-bangladesh>. Acesso em: 20 dez. 2017.

MORE ABOUT FUSION Centers. **American Civil Liberties Union**, [s.d]. Disponível em: <https://www.aclu.org/other/more-about-fusion-centers>. Acesso em: 10 jan. 2018.

MOREIRA, Matheus. O que é a deep web e por que ela está encolhendo. **Nexo Jornal**, mar. 2017. Disponível em:<https://www.nexojornal.com.br/expresso/2017/03/17/O-que-%C3%A9-a-deep-web-e-por-que-ela-est%C3%A1-encolhendo>. Acesso em: 13 mar. 2018.

MORETTO, Julia. Qual é a diferença entre a deep web e dark web? **Jornal Ciência**, nov. 2016. Disponível em: <http://www.jornalciencia.com/qual-e-a-diferenca-entre-a-deep-web-e-dark-web/>. Acesso em: 10 mar. 2018.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets. **The University of Texas at Austin**, [s.d.]. Disponível em: <http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>. Acesso em: 08 jan. 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Big Data Interoperability Framework**: Volume 1, Definitions. [s.l.]: NIST, 2015. Disponível em: <https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf>. Acesso em: 20 dez. 2017.

NEPAL EARTHQUAKE 2015. **Flowminder**, [s.d.]. Disponível em: <http://www.flowminder.org/case-studies/nepal-earthquake-2015>. Acesso em: 20 dez. 2017.

O BIG DATA antecipa a morte do currículo. **Fabramires**, out. 2013. Disponível em: <https://fabramires.wordpress.com/2013/10/30/o-big-data-antecipa-a-morte-do-curriculo/>. Acesso em: 10 jan. 2018.

O GLOBO COM AGÊNCIAS INTERNACIONAIS. Entenda o caso do escândalo de dados no Facebook e saiba como proteger sua privacidade. **O Globo**, mar. 2018. Disponível em: <https://oglobo.globo.com/economia/entenda-caso-do-escandalo-de-dados-no-facebook-saiba-como-proteger-sua-privacidade-22511997>. Acesso em: 22 mar. 2018.

O GLOBO. Big Data já substitui currículos na seleção de candidatos. **O Globo**, jul. 2014. Disponível em: <https://oglobo.globo.com/economia/emprego/big-data-ja-substitui-curriculos-na-selecao-de-candidatos-13225088>. Acesso em: 10 jan. 2018.

O GLOBO/AGÊNCIAS INTERNACIONAIS. 'Estamos indo para o Brasil', diz diretor da Cambridge Analytica. **O Globo**, mar. 2018. Disponível em: <https://oglobo.globo.com/mundo/estamos-indo-para-brasil-diz-diretor-da-cambridge-analytica-22510961>. Acesso em: 21 mar. 2018.

O QUE SÃO metadados. **Metadados**, [s.d.]. Disponível em: <http://www.metadados.pt/oquesaometadados>. Acesso em: 11 jan. 2018.

OEA. Comunicado de Imprensa R80/2015. **OEA**, jul. 2015. Disponível em: <http://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=998&lID=4>. Acesso em: 12 fev. 2018.

_____. Declaração Conjunta sobre Programas de Vigilância e seu Impacto na Liberdade de Expressão. **OEA**, jun. 2013. Disponível em:<http://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=926&lID=4>. Acesso em: 08 jan. 2018.

OHM, Paul. Broken Promises of Privacy Responding to the Surprising Failure of Anonymization. **UCLA Law Review**, v. 57, p. 1758, 2010.

OI, Mariko. As cicatrizes do confinamento de descendentes de japoneses nos EUA durante a 2ª Guerra. **BBC Brasil**, jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38440118>. Acesso em: 10 jan. 2018.

OLIVEIRA, Arize. O que é proxy? Descubra o significado desse termo.**TechMundo**, mai. 2011. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2011/05/o-que-e-proxy-descubra-o-significado-desse-termo.html>. Acesso em: 10 abr. 2018.

ORWELL, George. **1984**. Tradução de: Alexandre Hubner e Heloísa Jahn. São Paulo: Companhia das Letras, 2009.

OSBORNE, Charlie. As devastating as KRACK: New vulnerability undermines RSA encryption keys. **ZDNet**, out. 2017. Disponível em: <http://www.zdnet.com/article/as-

devastating-as-krack-new-vulnerability-undermines-rsa-encryption-keys/>. Acesso em: 18 mar. 2018.

PATAILLE, J. Sargent c. Defonds, Trib. Civ. Seine. **Annales de la proprieté industrielle artistique et littéraile**, n. 1860, nov. 1859.

PAVÃO, Samantha. Entenda o que é criptomoeda e saiba como usar. **PSafe Blog**, nov. 2017. Disponível em: <http://www.psafe.com/blog/o-que-criptomoeda/>. Acesso em: 17 dez. 2017.

PEREIRA, Jane Reis Gonçalves. Os imperativos da proporcionalidade e da Razoabilidade: Um panorama da discussão atual e da jurisprudência do STF. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Orgs.). **Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica. Rio de Janeiro: Lumen Juris, 2011, p. 167-206.

_____. Quem não deve teme apenas a injustiça. **Estado de Direitos**, set. 2012. Disponível em: <https://estadodedireitos.com/2012/09/03/quem-nao-deve-teme-apenas-a-injustica/>. Acesso em: 10 jan. 2018.

PERKINS, Kleiner. **Internet Trends 2017** – Code Conference, p. 14. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 20 dez. 2017.

PETTYPIECE, Shannon; ROBERTSON, Jordan. Hospitals are mining patients' credit card data to predict who will get sick. **InfoWars**, jul. 2014. Disponível em: <https://www.infowars.com/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick/>. Acesso em: 20 dez. 2018.

PIMENTA, Ricardo M. Big Data e Controle da Informação na Era Digital: Tecnogênese de uma Memória a Serviço do Mercado e do Estado. **Tendências da Pesquisa Brasileira em Ciência da Informação**, v. 6, n. 2, p. 15, jul./dez. 2013.

PRADO, Eduardo. Medicina personalizada: Big Data no combate ao Câncer [Parte 02]. **Saúde Business**, out. 2015. Disponível em: <http://saudebusiness.com/medicina-personalizada-big-data-no-combate-ao-cancer-parte-02/>. Acesso em: 20 dez. 2017

PROSSER, William. Privacy. **California Law Review**, v 48, n. 3, p. 383-423, 1960.

RAMPELL, Catherine. Your Next Job Application Could Involve a Video Game. **The New York Times Magazine**, jan. 2014. Disponível em: <https://www.nytimes.com/2014/01/26/magazine/your-next-job-application-could-involve-a-video-game.html>. Acesso em: 10 jan. 2018.

REDAÇÃO ÉPOCA COM AGÊNCIA EFE. Casa Branca admite que monitora telefonemas de cidadãos americanos. **Época**, jun. 2013. Disponível em: <http://revistaepoca.globo.com//Mundo/noticia/2013/06/casa-branca-admite-que-monitora-telefonemas-de-cidadaos-americanos.html>. Acesso em: 21 jan. 2018.

REDAÇÃO. "Signal" é consenso na comunidade científica, diz professor da Universidade de Washington. **Crypto ID**, jun. 2017. Disponível em: <https://cryptoid.com.br/banco-de-noticias/signal-e-consenso-na-comunidade-cientifica-diz-professor-da-universidade-de-washington/>. Acesso em: 13 abr. 2018.

REDAÇÃO. Apple se nega a hackear iPhone de atirador de San Bernardino. **Época**, fev. 2016. Disponível em: <https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/apple-se-nega-hackear-iphone-de-atirador-de-san-bernardino.html>. Acesso em: 18 mar. 2018.

REDAÇÃO. Coleta de dados de usuário era rotina, diz ex-funcionário do Facebook a jornal. **Folha de São Paulo**, mar. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/coleta-de-dados-de-usuario-era-rotina-diz-ex-funcionario-do-facebook-a-jornal.shtml>. Acesso em: 22 mar. 2018.

REDAÇÃO. Criptografia e anonimato são centrais para liberdade de opinião e expressão na era digital, diz ONU. **Nações Unidas no Brasil**, jul. 2015. Disponível em: <https://nacoesunidas.org/criptografia-e-anonimato-sao-centrais-para-liberdade-de-opiniao-e-expressao-na-era-digital-diz-onu/>. Acesso em: 10 abr. 2018.

REDAÇÃO. Elena Ferrante: suposta revelação da identidade da autora causa polêmica. **G1**, out. 2016. Disponível em: <http://g1.globo.com/pop-arte/noticia/2016/10/elena-ferrante-suposta-revelacao-da-identidade-da-autora-causa-polemica.html>. Acesso em: 10 abr. 2018.

REDAÇÃO. Entenda as questões legais envolvendo o escândalo de dados do Facebook. **Folha de São Paulo**, mar. 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/03/escandalo-de-dados-do-facebook-as-questoes-legais.shtml>. Acesso em: 22 mar. 2018.

REDAÇÃO. Jungmann diz que mandado coletivo de busca e apreensão pode ser medida extra. **Isto É**, fev. 2018.Disponível em: <https://istoe.com.br/jungmann-diz-que-mandado-coletivo-de-busca-e-apreensao-pode-ser-medida-extra/>. Acesso em: 20 fev. 2018.

REDAÇÃO. Maior manifestação antigoverno da era Mubarak deixa 3 mortos no Egito. **Estadão**, jan. 2011. Disponível em: <http://internacional.estadao.com.br/noticias/geral,maior-manifestacao-antigoverno-da-era-mubarak-deixa-3-mortos-no-egito-imp-,671222>. Acesso em: 18 mar. 2018.

REDAÇÃO. O que são cookies? **Super Interessante**, out. 2016. Disponível: <https://super.abril.com.br/tecnologia/o-que-sao-cookies/>. Acesso em: 18 dez. 2017.

REDAÇÃO. WhatsApp chega a 120 milhões de usuários no Brasil. **Estadão**, mai. 2017. Disponível em: <http://link.estadao.com.br/noticias/empresas,whatsapp-chega-a-120-milhoes-de-usuarios-no-brasil,70001817647>. Acesso em: 19 mar. 2018.

REDAÇÃO. WhatsApp tem vulnerabilidade que permite interceptar mensagens, diz jornal. **Época Negócios**, jan. 2017. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2017/01/whatsapp-tem-vulnerabilidade-que-permite-interceptar-mensagens-diz-jornal.html>. Acesso em: 13 abr. 2018.

REDAÇÃO. Who is harmed by a "Real Names" policy?.**Geek Feminism Wiki**, [s.d.]. Disponível em: <http://geekfeminism.wikia.com/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F>. Acesso em: 10 mar. 2018.

RIBEIRO, Bruno; LEITE, Fabio. Após 2 anos, sistema Detecta da polícia não identifica crimes, diz TCE. **Estadão**, ago. 2016. Disponível em: <http://sao-paulo.estadao.com.br/noticias/geral,apos-2-anos-sistema-detecta-da-policia-nao-identifica-crimes-diz-tce,10000069080>. Acesso em: 18 jan. 2018.

RICHARDS, David. The Ebola Crisis and Where Big Data Can Help.**Recode**, out. 2014. Disponível em: <https://www.recode.net/2014/10/24/11632210/the-ebola-crisis-and-where-big-data-can-help>. Acesso em: 20 dez. 2017.

RICHARDS, Neil M.; SOLOVE, Daniel J. Prosser's Privacy Law: A Mixed Legacy. **California Law Review**, v. 98, n. 6, p. 1895, 2010.

RICO.COM.VC O Que é Bitcoin e Como Funciona: Guia Atualizado. **Rico**, set. 2017. Disponível em: <https://blog.rico.com.vc/bitcoin-o-que-e>. Acesso em: 13 mar. 2018.

RISEN, James; LICHTBLAUDEC, Eric. Bush Lets U.S. Spy on Callers Without Courts. **The New York Times**, dez. 2005. Disponível em: <http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html>. Acesso em: 10 fev. 2018.

RIZZO, Alana; MONTEIRO, Tânia. Abin monta rede para monitorar internet. **Estadão**, jun. 2013. Disponível em: http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500>. Acesso em: 18 mar. 2018.

ROBEIRO, Rafael de Souza. Bitcoin dispara após bolsa de Chicago confirmar lançamento de contratos futuros da moeda. **InfoMoney**, dez. 2017. Disponível em: <http://www.infomoney.com.br/mercados/bitcoin/noticia/7119990/bitcoin-dispara-apos-bolsa-chicago-confirmar-lancamento-contratos-futuros-moeda>. Acesso em: 13 mar. 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** - a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROOSENDAAL, Arnold. Facebook Tracks and Traces Everyone: Like This! **Tilburg Law School Legal Studies**, Research Paper Series No. 03, p. 1-10, 2011.

ROTH, Aaron. The Algorithmic Foundations of Differential Privacy. **Foundations and Trends in Theoretical Computer Science**, v. 9, n. 3–4, p. 211-407, 2014. Disponível em: <https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf>. Acesso em 31 mar. 2018.

ROVER, Tadeu. Juiz determina bloqueio do WhatsApp a partir das 14h desta segunda. **Consultor Jurídico**, mai. 2016. Disponível em: <https://www.conjur.com.br/2016-mai-02/juiz-determina-bloqueio-whatsapp-partir-14h-segunda>. Acesso em: 17 mar. 2018.

RUGGIERI, Ruggero. VPN e Criptografia. **Crypto ID**, dez. 2015. Disponíel em: <https://cryptoid.com.br/banco-de-noticias/vpn-e-criptografia/>. Acesso em: 18 mar. 2018.

RUIJTER, Tom. **A big data view of on-street parking**. 2015. Thesis (Master in Computer Science) -Radboud University, Nijmegen, 2015.

SAISSE, Renato. Big Data Contra o Crime: Efeito Minority Report. **Direito & TI**, Porto Alegre, v. 1, p. 5, 2017.

SARAIVA, Adriana R. et al. Device Fingerprinting: Conceitos e Técnicas, Exemplos e Contramedidas. Minicursos do XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Sociedade Brasileira de Computação, 2014. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2014/0035.pdf>. Acesso em: 20 dez. 2017.

SARMENTO, Daniel. A vinculação dos particulares aos direitos fundamentais: o debate teórico e a jurisprudência do STF. In: _____; SARLET, Ingo Wolfgang (Orgs.). **Direitos fundamentais no Supremo Tribunal Federal**: balanço e crítica. Rio de Janeiro: Lumen Juris, 2011, p. 142.

_____. **Dignidade da pessoa humana**: conteúdo, trajetória e metodologia. Belo Horizonte: Fórum, 2016.

_____. Liberdades comunicativas e "Direito ao Esquecimento" na ordem constitucional brasileira. **Revista Brasileira de Direito Civil**, v. 7, p. 190-232, jan./mar. 2016.

SCHAUER, Frederick. Fear, Risk and the First Amendment: Unraveling the Chilling Effect. **Faculty Publications**, Paper 879, 1978.

SCHNEIER, Bruce. 'Stalker economy' here to stay. **CNN**, nov. 2013. Disponível em: <https://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html>. Acesso em: 22 mar. 2018.

SCHNEIER, Bruce. The Public-Private Surveillance Partnership. **Bloomberg**, jul. 2013. Disponível em: <https://www.bloomberg.com/view/articles/2013-07-31/the-public-private-surveillance-partnership>. Acesso em: 10 jan. 2018.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. Reconciling Personal Information in the United States and European Union. **California Law Review**, v. 102, n. 4, p. 877, 2014.

SCRIVANO, Roberta. 'Não é possível interceptar', afirma especialista sobre dados do WhatsApp'. **O Globo**, jul. 2016. Disponível em: <http://oglobo.globo.com/economia/nao-possivel-interceptar-afirma-especialista-sobre-dados-do-whatsapp-19750758>. Acesso em: 05 mar. 2017.

SGARRO, Andrea. **Codigos Secretos**. Madrid: Ediciones Parámide, 1990.

SHAMPAN'ER, Kristina; ARIELY, Dan. Zero as a special price: The true value of free products. **MIT**, [s.d]. Disponível em: <http://web.mit.edu/ariely/www/MIT/Papers/zero.pdf>. Acesso em: 10 jan. 2018.

SHAYWITZ, David. New Diabetes Study Shows How Big Data Might Drive Precision Medicine. **Forbes**, out. 2015. Disponível em: <https://www.forbes.com/sites/davidshaywitz/2015/10/30/new-diabetes-study-shows-how-big-data-might-drive-precision-medicine/#63d1637e44b0>. Acesso em: 20 dez. 2017.

SISTEMA AVISA QUANDO carro precisa de manutenção. **Autoo**, jul. 2012. Disponível em: <https://www.autoo.com.br/sistema-avisa-quando-carro-precisa-de-manutencao/>. Acesso em: 20 dez. 2017.

SMITH, Mitch. In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. **New York Times**, jun. 2016. Disponível em: <https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html>. Acesso em: 20 dez. 2017.

SOFTWARE ESTILO 'MINORITY Report' ajuda polícia a prever crimes. **Terra**, jan. 2013. Disponível em: < https://www.terra.com.br/noticias/mundo/estados-unidos/software-estilo-minority-report-ajuda-policia-a-prever-crimes,f957183d48a2c310VgnVCM5000009ccceb0aRCRD.html>. Acesso em: 10 jan. 2018.

SOGHOIAN, Chris. Keeping the Government Out of Your Smartphone. **ACLU**, set. 2012. Disponível em: <https://www.aclu.org/blog/national-security/keeping-government-out-your-smartphone?redirect=blog/technology-and-liberty-national-security-free-speech/keeping-government-out-your-smartphone>. Acesso em: 18 abr. 2018.

SOLON, Olivia. You are Facebook's product, not customer. **Wired**, set. 2011. Disponível em: <http://www.wired.co.uk/article/doug-rushkoff-hello-etsy>. Acesso em: 18 fev. 2018.

SOLOVE, Daniel J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. **San Diego Law Review**, v. 44, p. 745, 2007.

_____. Conceptualizing Privacy. In: CANNATACI, Joseph A. (Ed.). **The Individual and Privacy**. V. I. London and New York: Routledge, 2015.

_____. **Nothing to Hide**: The false tradeoff between privacy and security. New Haven: Yale University Press, 2013.

_____. **The Digital Person**: Technology and Privacy in the information Age. New York: New York University Press, 2004.

_____. **Understanding Privacy**. London & Cambridge: Harvard University Press, 2009, p. 125.

SARLET, Ingo; MARINONI, Luiz Guilherme; MITIDIERO, Daniel *et al*. Curso de Direito Constitucional. 5. ed. rev. e atual. São Paulo: Saraiva, 2016.

SOUZA NETO, Cláudio Pereira de; SARMENTO, Daniel. **Direito constitucional**: teoria, história e métodos de trabalho. Belo Horizonte: Forum, 2013.

STATE AND MAJOR Urban Area Fusion Centers. **Homeland Security**, [s.d.]. Disponível em: <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>. Acesso em: 10 jan. 2018.

STATE OF UTAH. Adult Sentencing & Release Guidelines. **Utah Sentencing Comission**, 2015. Disponível em: <https://www.utah.gov/pmn/files/172049.pdf>. Acesso em: 10 jan. 2018.

STORNI, Eduardo. LinkedIn: o que é e para que serve? **WSI**, mar. 2017. Disponível em: <https://wsidm.com.br/blog/linkedin-o-que-e-e-para-que-serve>. Acesso em: 10 jan. 2018.

SUMARES, Gustavo. França e Alemanha querem leis para limitar criptografia. **Olhar Digital**, ago. 2016. Disponível em: <https://olhardigital.com.br/pro/noticia/franca-e-alemanha-querem-leis-para-limitar-criptografia/61501>. Acesso em: 18 mar. 2018.

SWEENEY, Latanya. Discrimination in Online Ad Delivery.**Harvard University**. Disponível em: <https://dataprivacylab.org/projects/onlineads/1071-1.pdf>. Acesso em: 08 jan. 2017.

TAMBURRO, Paul. Theresa May's Plan to Stop Online Extremism Would Require an Impossible Encryption Ban. **Mandatory**, jun. 2017. Disponível em: <http://www.mandatory.com/living/1273027-theresa-mays-plan-stop-online-extremism-require-impossible-encryption-ban#P2phMksU3fH6lVJ0.99>. Acesso em: 18 mar. 2018.

TASHEA, Jason. Courts are using AI to sentence criminals. That must stop now. **Wired**, abr. 2017. Disponível em: <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/>. Acesso em: 10 jan. 2018.

TATE, Ryan. AMID NSA Outrage, Big Tech Companies Plan To Track You Even More Aggressively. **Wired**, nov. 2013. Disponível em: <https://www.wired.com/2013/10/private-tracking-arms-race/>. Acesso em: 22 mar. 2018.

THE EVOLUTION OF Privacy on Facebook. **Mattmckeon**, [s.d.]. Disponível em: <http://mattmckeon.com/facebook-privacy/>. Acesso em: 22 mar. 2018.

THE USA PATRIOT Act: Preserving Life and Liberty. **Department of Justice Website**, [s.d]. Disponível em: <https://www.justice.gov/archive/ll/highlights.htm>. Acesso em: 10 jan. 2018.

THE WORLD'S MOST valuable resource is no longer oil, but data. **The Economist**, may. 2017. Disponível em: <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>. Acesso em: 22 dez. 2017.

THIRANI, Vasudha; GUPTA, Arvind. The value of data. **World Economic Forum**, set. 2017. Disponível em: <https://www.weforum.org/agenda/2017/09/the-value-of-data/>. Acesso em: 22 dez. 2017.

TRACKING COOKIE. **Symantec**, jul. 2014. Disponível em: <https://www.symantec.com/security_response/writeup.jsp?docid=2006-080217-3524-99&tabid=2>. Acesso em: 22 dez. 2017.

UCHOA, Pablo. Dilma usará discurso na ONU para criticar espionagem dos EUA. **BBC Brasil**, set. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/09/130923_dilma_onu_pu_dg>. Acesso em: 10 fev. 2018.

UN GLOBAL PULSE. Analyzing Attitudes Towards Contraception & Teenage Pregnancy Using Social Data. **Global Pulse Project Series**, n. 8, 2014. Disponível em: <https://www.unglobalpulse.org/projects/UNFPA-social-data>. Acesos em: 20 dez. 2017.

_____. Data Visualisation and Interactive Mapping to Support Response to Disease Outbreak. **Global Pulse ProjectSeries**, n. 20, 2015. Disponível em: <https://www.unglobalpulse.org/projects/mapping-infectious-diseases>. Acesso em: 20 dez. 2017.

_____. Nowcasting Food prices in Indonesia using Social Media Signals. **Global Pulse Project Series**, n. 1, 2014. Disponível em: <https://www.unglobalpulse.org/projects/nowcasting-food-prices>. Acesso em: 20 dez. 2017.

_____. Understanding Public Perceptions of Immunisation Using Social Media. **Global Pulse Project Series**, n. 19 2015. Disponível em: <http://www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Perception_Immunisation_2014_0.pdf>. Acesso em: 20 dez. 2017.

_____. Using Mobile Phone Data and Airtime Credit Purchases to Estimate Food Security. **Global Pulse Project Series**, n. 14, 2015. Disponível em: <http://www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Airtimecredit_Food_2015.pdf>. Acesso em: 20 dez. 2017.

UNITED NATIONS. Report of the Special Rapporteur of the Human Rights Council on the right to privacy. A/72/43103, out 2017, p. 10. Disponível em: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>. Acesso em: 20 dez. 2017.

UNITED STATES OF AMERICA. United States Court of Appeals, Ninth Circuit. Bernstein v. United States Department of Justice. No. 97-16686. Disponível em: <http://caselaw.findlaw.com/us-9th-circuit/1317290.html>. Acesso em: 18 mar. 2018.

_____. Electronic Code of Federal Regulations. **Government Publishing Office**, abr. 2018. Disponível em: <https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=36613dec83f28e22c86fd9a4c9c7f632&mc=true&n=pt15.2.740&r=PART&ty=HTML>. Acesso em: 12 abr. 2018.

UNIVERSITY OF WASHINGTON. Who's a CEO? Google image results can shift gender biases. **EurekAlert!**, abr. 2015. Disponível em: <https://www.eurekalert.org/pub_releases/2015-04/uow-wac040915.php>. Acesso em: 08 jan. 2018.

VALENTE, Rubens. Ditadura "fichou" 308 mil, revelam arquivos do SNI. **Folha de São Paulo**, dez. 2008. Disponível em: <http://www1.folha.uol.com.br/fsp/brasil/fc1412200805.htm>. Acesso em: 08 jan. 2018.

VALENTINO-DEVRIES, Jennifer; SINGER-VINE, Jeremy; SOLTANI, Ashkan. Websites Vary Prices, Deals Based on Users' Information. **The Wall Street Journal**, dez. 2012. Disponível em:

<https://www.wsj.com/articles/SB10001424127887323777204578189391813881534>. Acesso em: 10 jan. 2018.

VELOSO, Thássius. Justiça americana proíbe financeira de cobrar dívida pelo Facebook. **Tecno Blog**, 2011.Disponível em: <https://tecnoblog.net/59137/justica-americana-proibe-empresa-de-cobrar-conta-via-facebook/>. Acesso em: 22 jul. 2017.

VIANA, Tulio Lima. **Transparência pública, opacidade privada**: o Direito como instrumento de limitação do poder na sociedade de controle. 2006. Dissertação (Mestrado em Direito) - Universidade Federal do Paraná, Curitiba, 2006.

VITORINO, Fabricio. Facebook reforça luta contra o fake news e diz que mudança no algoritmo é só o começo. **G1**, mar. 2018. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/facebook-reforca-luta-contra-o-fake-news-e-diz-que-mudanca-no-algoritmo-e-so-o-comeco.ghtml>. Acesso em 31/03/2018.

VPN, entre outros. CRAIG, Cristina. Device Fingerprinting the tracking we can't avoid. **Nordvpn**, abr. 2017. Disponível em: <https://nordvpn.com/blog/device-fingerprinting-the-tracking-we-cant-avoid/>. Acesso em: 20 dez. 2017.

WALL, Matthew. Ebola: Can big data analytics help contain its spread? **BBC News**, out. 2014. Disponível em: <http://www.bbc.com/news/business-29617831>. Acesso em: 20 dez. 2017.

WARREN, Samuel; BRANDEIS Louis. The right to privacy, **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890.

WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. **Congressional Research Service**, mai. 2016. Disponível em: <https://fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 18 dez. 2018.

WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 1967.

WHAT YOU SHOULD Know About History Sniffing. **Krebs on Security**, dez. 2010. Disponível em:<https://krebsonsecurity.com/2010/12/what-you-should-know-about-history-sniffing/>. Acesso em: 20 dez. 2017.

WHITAKER, Reginald. **The End of Privacy**: How Total Surveillance Is Becoming a Reality. New York: Paw Prints, 2008.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, v. 113, p. 1202-1211, 2004.

WHY MACHINES DISCRIMINATE—and How to Fix Them. **Sciency Friday**, nov. 2015. Disponível em: <https://www.sciencefriday.com/segments/why-machines-discriminate-and-how-to-fix-them/>. Acesso em: 08 jan. 2018.

WORLD ECONOMIC FORUM. **Big Data, Big Impact**: New Possibilities for International Development. WEF: [s.e.], 2012. Disponível em:

<http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf>. Acesso em: 20 dez. 2017.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. **Revista Brasileira de Direito Civil**, v. 3, p. 13, jan./mar 2015.

ZUBOFF, S. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology**, v. 30, p. 75-89, 2015.