LGPD NA PRÁTICA

Gabrielle Bezerra Sales Sarlet
Regina Linden Ruaro
Orgs.

Editora Fundação Fênix

No que concerne à proteção de dados, se, por um lado, há a celebração no que toca ao reconhecimento de um bom conjunto de princípios e de direitos referenciados pela autodeterminação informacional, a atuação diligente do Supremo Tribunal Federal (STF) e a criação e atuação exitosa da Autoridade Nacional de Proteção de Dados (ANPD), sobeja ainda uma profusão de discussões e de adequações a serem feitas para que, de fato, a LGPD saia do papel e ganhe o mundo real, emoldurando e assegurando a cidadania digital no compasso da sua regulamentação e implementação.

Diante dessa conjuntura e no intuito de tornar o debate cada vez mais profícuo, sobretudo a partir de um enfoque mais pragmático, o Grupo de Proteção de Dados Pessoais no Estado Democrático de Direito do Programa de Pós-graduação em Direito da PUCRS, expressa nos textos que perfazem esta coletânea, sua contribuição.

Para tanto, alunos e professores, urdiram um somatório de forças para esquadrinhar o estado da arte, ou seja, projetando suas considerações, dúvidas e inquietações, em uma tessitura pautada no zelo e no cuidado, mas, igualmente na pesquisa e na acurácia quanto às bases jurídicas, para descortinar algumas dimensões que ainda carecem de aprofundamento no ambiente doméstico. De mais a mais, importa destacar que se trata de um trabalho afetivo e, nessa sintonia, conjugado e encetado na medida do tempo, na qual as reflexões foram sendo estruturadas a cada encontro.

Editora Fundação Fênix

PUCRS | ESCOLA DE DIREITO

9 786581 110994

LGPD NA PRÁTICA

Série Direito

Gabrielle Bezerra Sales Sarlet
Regina Linden Ruaro
Organizadoras

Oganização executiva
Cristina Baum da Silva

LGPD NA PRÁTICA

Editora Fundação Fênix

Porto Alegre, 2022

Direção editorial: Ingo Wolfgang Sarlet
Diagramação: Editora Fundação Fênix
Concepção da Capa: Editora Fundação Fênix

Este livro foi editado com o apoio financeiro - CAPES/PROEX - Projeto CAPES/PROEX - 0776/2018

Série Direito– 58

Catalogação na Fonte

L525 LGPD na prática [recurso eletrônico] / Gabrielle Bezerra Sales Sarlet, Regina Linden Ruaro Organizadoras. – Porto Alegre : Editora Fundação Fênix, 2022.
286 p. (Série Direito ; 58)

Organização executiva Cristina Baum da Silva.
Disponível em: <http://www.fundarfenix.com.br>
ISBN 978-65-81110-99-4
DOI https://doi.org/10.36592/9786581110994

1. Brasil. Lei geral de proteção de dados pessoais (2018). 2. Direito. 3. Proteção de dados. 4. Direito à privacidade. 5. Inteligência artificial. I. Sarlet, Gabrielle Bezerra Sales (org.). II. Ruaro, Regina Linden (org.).

CDD: 340

Responsável pela catalogação: Lidiane Corrêa Souza Morschel CRB10/1721

SUMÁRIO

APRESENTAÇÃO

Expressão inarredável da pessoa humana no atual contexto marcadamente informacional, em que a identidade se desdobra como uma mercadoria em uma miríade de dados compartilhados de modo contínuo e em rede, o direito à proteção de dados entrou no radar dos juristas desde os anos setenta, ocasião em que a Alemanha, mais especificamente, o estado de Hesse, de forma pioneira, promulgou a sua lei.

De modo exemplar, a União Europeia em 1995 expediu a Diretiva 95/45 que serviu de marco para a incorporação nos regimes jurídicos dos países membros o direito fundamental à proteção de dados pessoais e, mais recentemente, em 2016 aprovou o Regulamento Geral de Proteção de Dados, agora não mais como diretriz e sim como norma cogente. A partir de então, vem sendo constatada uma série geracional de outras leis que foram e prosseguem maturando modos mais efetivos de garantir a integralidade da pessoa humana inserida em um ecossistema compatível com a teoria dos direitos fundamentais.

No Brasil, a despeito da significativa demora, emergiu, com a Lei Geral de Proteção de Dados -Lei nº 13.709/2018, conhecida como LGPD, uma cultura de afirmação de direitos e de garantias que, em síntese, neste ano, completou um quadriênio no qual muito deve ser sublinhado em termos de avanços e, em outro giro, de diversos desafios, dentre muitos, a necessidade de aculturamento e letramento na matéria. De fato, a entrada em vigor da LGPD foi precedida por um intenso trabalho que reuniu esforços da doutrina, da jurisprudência e da sociedade civil para forjar um alinhamento com os demais países que já possuíam uma legislação específica nessa seara, notadamente com a União Europeia.

Tem-se que reconhecer que, muito embora a LGPD em termos de legislação específica tenha tardado a ser promulgada, diversos textos legais já apontavam para o reconhecimento do direito à proteção de Dados Pessoais no Brasil. Neste sentido, o Código de Defesa do Consumidor (Lei 8.078/90, a Lei de Interceptação Telefônica (Lei 9.296/96); Lei de Sigilo Bancário (LC 105/01); Código Civil (Lei 10.406/02); Lei de Acesso à Informação (Lei 12.527/11) e Marco Civil da Internet (Lei 12.965/14)

Desde então, o cenário brasileiro passou e, em razão da complexidade dessa virada digital, continua passando por inúmeras transformações, somente comparáveis ao que se presenciou nos anos noventa, ocasião em que, após a promulgação da Constituição Federal de 1988, e, por meio de diplomas como o Estatuto da criança e do adolescente (ECA) e o Código de defesa do consumidor (CDC), foram forjados parâmetros comportamentais inusitados para a cultura nacional.

No que concerne à proteção de dados, se, por um lado, há a celebração no que toca ao reconhecimento de um bom conjunto de princípios e de direitos referenciados pela autodeterminação informacional, a atuação diligente do Supremo Tribunal Federal (STF) e a criação e atuação exitosa da Autoridade Nacional de Proteção de Dados (ANPD), sobeja ainda uma profusão de discussões e de adequações a serem feitas para que, de fato, a LGPD saia do papel e ganhe o mundo real, emoldurando e assegurando a cidadania digital no compasso da sua regulamentação e implementação.

Diante dessa conjuntura e no intuito de tornar o debate cada vez mais profícuo, sobretudo a partir de um enfoque mais pragmático, o Grupo de Proteção de Dados Pessoais no Estado Democrático de Direito do Programa de Pós-graduação em Direito da PUCRS, expressa nos textos que perfazem esta coletânea, sua contribuição.

Para tanto, alunos e professores, urdiram um somatório de forças para esquadrinhar o estado da arte, ou seja, projetando suas considerações, dúvidas e inquietações, em uma tessitura pautada no zelo e no cuidado, mas, igualmente na pesquisa e na acurácia quanto às bases jurídicas, para descortinar algumas dimensões que ainda carecem de aprofundamento no ambiente doméstico. De mais a mais, importa destacar que se trata de um trabalho afetivo e, nessa sintonia, conjugado e encetado na medida do tempo, na qual as reflexões foram sendo estruturadas a cada encontro.

Certamente, ainda haveriam alinhavos a serem empreendidos, vez que os tempos em curso se superam em vertiginosa mudança e, por vezes, atropelam o intérprete da norma, eclodindo situações impensáveis, sobretudo nessa área do conhecimento. Contudo, espera-se, para além da contribuição cientifica, que o vigor

deste trabalho venha a contagiar o leitor com o entusiasmo e o compromisso que permeiam a nossa ação em prol de um estar no mundo em que a tecnologia seja sempre empregada a favor do ser humano e que Brasil alcance patamares apropriados para a efetivação da proteção multinível, em especial do livre desenvolvimento da personalidade de todos e não somente de alguns poucos.

Gabrielle Bezerra Sales Sarlet e Regina Linden Ruaro.

Porto Alegre, 2022.

1. DADOS PESSOAIS COMO MEIO DE PROVA E A POSSIBILIDADE DE COLETA DE OFÍCIO PELO JUIZ

https://doi.org/10.36592/9786581110994-01

Ana Carolina Squadri[1]

Sumário

1. Considerações iniciais

O Estado Democrático de Direito exige que o processo judicial deva, sobretudo, resultar em decisões justas, sendo adequado e efetivo para o caso concreto levado a juízo[2]. O art. 5º, LIV, da Constituição Federal determina que ninguém será privado da liberdade ou de seus bens sem o devido processo legal, instituindo o direito fundamental ao processo justo, o qual deve servir de base para a organização do processo e condição mínima para obtenção de um resultado justo[3]. Do conteúdo mínimo existencial do processo justo decorre o direito fundamental à prova, cujo pressuposto ético é a apuração da verdade dos fatos, pois o direito à prova somente

---

[1] Doutoranda pela PUCRS, Mestre em Direito Processual pela UERJ, membro do Instituto Brasileiro de Processo, Procuradora Federal.
http://lattes.cnpq.br/3890534188881183; E-mail: acarolinasquadri@gmail.com.

[2] "A jurisdição nasceu historicamente para resolver litígios. O surgimento de conflitos entre os indivíduos remonta às mais primitivas organizações sociais. Assim, a maior parte da atividade jurisdicional está voltada para resolução de litígios; compor a lide significa resolvê-la, solucioná-la. Contudo, a jurisdição deve atuar para a justa composição da lide, ou seja, compor a lide de acordo com o direito, porque é ele que estabelece as regras de comportamento vigentes numa sociedade, recomendando a sua observância a todos os cidadãos. Logo, a justa composição da lide é a solução do conflito de interesses pela aplicação do direito, de acordo com as regras de comportamento que todos devem observar. Assim, não satisfaz qualquer composição da lide, mas apenas aquela que se dê em conformidade com o direito". GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed., Rio de Janeiro: Forense, 2015, p. 75.

[3] MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. Novo Curso de Processo Civil: teoria do processo civil. São Paulo: Editora Revista dos Tribunais, 2015, p. 489

garante a liberdade e a igualdade se tiver o escopo de investigar objetivamente os fatos relevantes para a aplicação correta da norma.

Portanto, o direito probatório no processo civil brasileiro deve ser interpretado e aplicado em consonância com o processo justo, pois o melhor aproveitamento da busca de informações relevantes para os fatos narrados no processo deve estar moldado segundo os ideais democráticos, os quais privilegiam a igualdade processual e a paridade de armas, pressupostos de um Estado Democrático de Direito[4].

Não é possível estudar o direito à prova, sem analisar previamente a igualdade processual, a qual é apresentada em dois aspectos: o primeiro estabelece uma divisão perante a lei, qual seja, a igualdade formal e a igualdade material; e o segundo aspecto que está relacionado ao processo, cabendo distinguir entre igualdade no processo e igualdade pelo processo. Importante salientar que toda a atividade do juiz deve visar à igualdade processual, no que se refere à paridade de armas disponíveis ao longo do trâmite processual, de modo a impossibilitar o tratamento desequilibrado das partes, sobretudo no que diz respeito à produção de prova e à obtenção de um resultado justo[5]. Logo, o processo deve estar estruturalmente organizado para que atenda a igualdade das partes no que se refere à obtenção de prova relevante e suficiente para ser proferida uma decisão mais próxima da verdade.

O direito à prova exercido com a observância da igualdade processual constitui um dos pilares do processo justo, previsto no art. 5º, LIV, da Constituição Federal, sem o qual o processo não estaria organizado conforme os ditames do Estado Democrático de Direito. Sem o equilíbrio real entre as partes no processo, sem a concessão de oportunidades reais de contraditório mediante a produção de provas e sem garantir uma função ativa ao juiz com intuito de exercer o controle da

[4] "Em primeiro lugar, do ponto de vista da 'divisão de trabalho' processual, o processo justo é pautado pela colaboração do juiz com as partes. Daí a razão pela qual o NCPC positivou expressamente o modelo cooperativo de processo civil e o princípio da colaboração (art. 6º do CPC). O juiz é paritário no diálogo e assimétrico apenas no momento da imposição de suas decisões. Em segundo lugar, constitui processo capaz de prestar tutela jurisdicional adequada e efetiva (arts. 5º, XXXV, CF/88, e 3º do CPC), em que as partes participam em pé de igualdade e com paridade de armas, em contraditório (arts. 5º, I e LV, da CF/1988, e 7º, 9º e 10 do CPC), com ampla defesa, com direito à prova, perante juiz natural, em que todos os seus pronunciamentos são previsíveis, confiáveis e motivados (...)". Idem 2, p. 491.

[5] MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. Novo Curso de Processo Civil: teoria do processo civil. São Paulo: Editora Revista dos Tribunais, 2015, p. 499.

regularidade e do desenvolvimento do processo[6], não haveria condição suficiente para a construção de uma decisão justa[7] baseada na verdade dos fatos e não numa verdade fabricada no processo pelas partes [8].

O presente trabalho restringir-se-á à análise da apuração da verdade dos fatos como pilar do processo justo, sem adentrar na questão da correta aplicação da norma jurídica através de artigos de lei e decisões. Em síntese, o processo justo impõe que ocorra uma apuração adequada dos fatos, ou seja, a verdade dos fatos deve ser investigada adequadamente sem, contudo, violar outro direito fundamental.

Avançando o tema, e voltando à questão do princípio da igualdade, o direito processual civil precisou evoluir para garantir a igualdade material no processo, revendo a função do juiz para possibilitar um equilíbrio real entre as partes na defesa de suas alegações, principalmente no que se refere ao direito à prova[9]. Todavia, não se deve afastar a relevância para o processo civil, da igualdade perante a legislação[10], embora não seja suficiente para promover o direito fundamental à igualdade.

Foi adotada no estudo a concepção de prova como resultado, também denominada de concepção metajurídica.[11] Isso significa que o juiz não deve ficar

---

[6] "De qualquer modo, no processo civil, o estado de coisas chamado de ordem pública se expressa pelo controle a regularidade e desenvolvimento de atos e procedimentos, chamando a atenção para a presença de defeitos tidos como graves, intransponíveis, bem como para a necessidade de afastá-los para se garantir a legalidade. (...) Destarte, a ordem processual funciona como elemento regulador da marcha progressiva do processo, podendo atuar como um limite ou com caráter proibitivo, mas também de forma permissiva, autorizando condutas de maior eficiência e possibilitando a superação dos defeitos processuais." CABRAL, Tricia Navarro Xavier. Ordem Pública Processual. Brasília, DF: Gazeta Jurídica, 2015, p. 81 e 83.

[7] "O direito ao processo justo constitui princípio fundamental para organização do processo no Estado Constitucional. É o modelo mínimo de atuação processual do Estado e mesmo dos particulares em determinadas situações substanciais. A sua observação é condição necessária e indispensável para obtenção de decisões justas e para a formação de precedentes". Idem 4, p. 489.

[8] "Já foi salientado pela doutrina que não é possível eleger-se um único critério idôneo para avaliar a justiça da decisão. Pelo menos três critérios foram desenhados, entretanto, como necessários, mas nenhum, sozinho, suficiente para garantir a justiça da decisão. Os critérios são os seguintes: (a) correta escolha e interpretação da regra jurídica; (b) apuração adequada dos fatos relevantes do caso; (c) emprego de um procedimento válido e justo para chegar à decisão." RAMOS, Vitor de Paula. Ônus da prova no processo civil: do ônus ao dever de provar. 2ª ed., São Paulo: Thomson Reuters Brasil, 2018, p. 44 e 45.

[9] ABREU, Rafael Sirangelo. Igualdade e processo: posições processuais equilibradas e unidade do direito. São Paulo: Editora Revista dos Tribunais, 2015, p. 96.

[10] Idem 8, p. 77.

[11] A concepção metajurídica "identifica a prova como um fenômeno humano, utilizado pelo conhecimento em todas as áreas do saber – e não como fenômeno exclusivo e típico do processo judicial". GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed. Rio de Janeiro: Forense, 2015, p. 102.

acomodado aos argumentos das partes, devendo utilizar de métodos disponíveis e legítimos, inclusive pertencente a outras áreas do conhecimento, para instruir o processo e buscar um resultado justo.

Diante do exposto e contextualizando o trabalho com o século XXI, representado pela resistência contrailuminista – movimento que promove a alienação, segundo Steven Pinker [12] – aos avanços científicos e, sobretudo, tecnológicos, visto que tais movimentos sociais refletem em todas as esferas sociais, inclusive a jurídica, a doutrina deve estar atenta a essa nova era, sob pena de o Direito ficar à margem da realidade. Portanto, se vivemos em uma sociedade digital, onde dados pessoais são disponibilizados na internet, sem fronteiras físicas, cabe à teoria da prova enfrentar se o tratamento [13] de dados pessoais pelo juiz ou por sua determinação, é um meio legítimo de prova e quais seriam as limitações impostas pelo ordenamento jurídico brasileiro. O objetivo não é esgotar o debate, mas provocar o estudo do direito processual, sobretudo a teoria da prova para a questão da proteção de dados.

A presente pesquisa teve como abordagem o método hipotético-dedutivo, pois não apresentou um caso concreto como meio para conclusão geral. Como objetivo se buscou a confirmação de que os dados pessoais podem servir como fonte de prova, com a possibilidade de tratamento de ofício pelo juiz. Para tanto, foram utilizadas bibliografias e jurisprudências nacionais como procedimento de pesquisa, realizando então, a intepretação sistemática das informações como forma de conclusão do estudo.

O trabalho está dividido em quatro capítulos. O primeiro aborda o direito fundamental à proteção de dados pessoais no ordenamento brasileiro, bem como a influência do direito alemão e europeu no desenvolvimento desse direito fundamental.

---

[12] PINKER, Steven. O novo iluminismo: em defesa da razão, da ciência e do humanismo. São Paulo: Companhia das Letras, 2018, p. 54.

[13] "Art. 5º. Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração." BRASIL. Lei nº 13.709 de agosto de 2018. Disponível em: <http://www.planalto.gov.br>. Acesso em: 18 de abril de 2022.

O segundo capítulo traça importante distinção entre documento, documento eletrônico e dados pessoais. Superado o período formalista do direito processual civil, cabe à teoria geral da prova rever conceitos derivados da fase em que se exigia uma formalidade exacerbada para a prática de atos processuais, visto que está em desarmonia com o caráter virtual das situações jurídicas no presente momento. Ademais, a exigência de documento escrito como pressuposto para a admissão da prova não corresponde à atual fase metodológica do direito processual civil, em que os valores constitucionais devem ser considerados na interpretação das regras processuais.

O terceiro capítulo avança no estudo do direito probatório e analisa a função instrutória do juiz à luz da Constituição Federal, a qual prevê o princípio do contraditório, cuja compreensão contemporânea abrange o princípio colaborativo, que é a integração do juiz no contraditório para auxiliar as partes na condução do processo, além de outros deveres derivados do princípio. O capítulo também tratou dos limites da função instrutória do juiz, pois os valores constitucionais devem ser respeitados quando aplicados o art. 7º, VI da LGPD e o art. 370, do CPC, como também analisou a jurisprudência do Superior Tribunal de Justiça e do Tribunal Regional Federal da 4ª Região.

Por fim, o quarto e último capítulo, conclui o trabalho, destacando a relevância do avanço no estudo do direito probatório para a busca da verdade dos fatos e, por conseguinte, para a garantia da liberdade e igualdade processuais. Considerando que o acompanhamento do direito probatório com a realidade social é fundamental para a obtenção de um resultado justo, a doutrina e a jurisprudência não podem ignorar o avanço da comunicação pela internet, visto que origina dados de fácil acesso e o seu uso indevido pode acarretar na violação do direito fundamental à proteção de dados pessoais.

2. Direito fundamental à proteção de dados pessoais

A análise sobre o exercício legítimo do juiz no tratamento de dados pessoais para instrução de processo judicial, deve ocorrer a partir da Constituição Federal, principalmente da perspectiva do direito fundamental à proteção de dados pessoais,

pois o direito à prova também possui limitações em decorrência de outros interesses e direitos fundamentais.

Com a promulgação da Emenda Constitucional n.º 115/2022, o direito fundamental à proteção de dados pessoais foi alçado a um direito expressamente positivado na Constituição Federal[14][15].

Embora a proteção de dados pessoais tenha sido expressamente prevista como direito fundamental no ano de 2022, a doutrina e o Supremo Tribunal Federal[16] já consideravam como um direito implicitamente positivado, decorrente do direito à autodeterminação informativa[17][18]. É importante frisar que o direito fundamental à proteção de dados protege todo e qualquer dado, seja físico ou digital, com o intuito de preservar o livre desenvolvimento da personalidade e a autodeterminação informativa, todos esses conectados ao princípio da dignidade da pessoa humana. Desse modo, não existem dados irrelevantes, pois sua concepção integra a formação da personalidade humana, sobretudo na era da sociedade digital, em que milhares de pessoas tornam disponíveis informações pessoais na internet[19].

---

[14] Art. 5º. LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. EC 115/2022. BRASIL. Emenda Constitucional nº 115, de fevereiro de 2022. Disponível em <https://www2.camara.leg.br/legin/fed/emecon/2022/emendaconstitucional-115-10-fevereiro-2022-792285-publicacaooriginal-164624-pl.html>. Acesso em: 18 de abril de 2022

[15] Na lição de Sarlet, a carga positiva deste direito fundamental "assegura à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio", além de ser inquestionável a aplicação do regime constitucional ao direito fundamental em estudo, seja no seu sentido formal, seja no material. SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo *et al*. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 37 e 38.

[16] "Além disso, pela sua subida relevância e atualidade, não se poderia deixar de referir, nesse contexto, o julgamento, pelo Plenário do STF, em 07.05.2020, que confirmou o deferimento, em sede de decisão monocrática proferida em 17.04.2020, pela relatora da ADIn 6387, Ministra Rosa Weber, de medida liminar suspendendo a eficácia da Medida Provisória nº 954, que determinava às empresas de telefonia a fornecer ao IBGE os nomes, endereços e telefones de mais de cem milhões de brasileiros, mediante o argumento de que tal medida representaria uma restrição constitucionalmente ilegítima dos direitos à privacidade, intimidade e sigilo dos dados pessoais, porquanto inconsistente com as exigências da proporcionalidade e razoabilidade". Idem 14, p. 37.

[17] Idem 14, p. 22.

[18] "No que toca à fundamentalidade em sentido formal, esta se traduz na circunstância de que, mesmo não sendo expressamente contido no texto constitucional, o direito à proteção de dados pessoais tem *status* equivalente em termos de hierarquia normativa, sendo igualmente parâmetro para o controle da legitimidade constitucional dos atos normativos infraconstitucionais e de atos (e omissões) do poder público em geral, ademais de sua projeção na esfera das relações privadas, o que também será objeto de maior desenvolvimento". Idem 14, p. 29.

[19] Idem 14, p. 35.

Inspirado no direito alemão, o direito fundamental à proteção de dados foi moldado pelo Tribunal Constitucional, o qual não determinou um controle absoluto sobre os dados pelo cidadão, pois outros interesses permitem limitação à proteção dos dados[20]. Na visão de Hans-Peter Bull, a preocupação do Tribunal Constitucional da Alemanha era proteger o cidadão da repressão do Estado, ou seja, do uso abusivo dos dados pessoais[21].

No âmbito infraconstitucional, diversas leis já disciplinam a proteção de dados, como a Lei nº 12.527/2011 (Lei de Acesso à Informação), a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). Como não poderia deixar de ser, as regras previstas na legislação devem ser interpretadas e aplicadas conforme os direitos fundamentais, de modo que as normas sobre proteção de dados não violem o objeto de proteção de diversos interesses constitucionalmente resguardados.

O conteúdo do objeto de proteção do direito fundamental à proteção de dados não é facilmente definido, podendo ser conceituado como uma liberdade no gerenciamento das informações pessoais, sem a possibilidade do uso dessas informações por outras pessoas contra seu titular[22]. Importante ressaltar que a LGPD, assim como o Regulamento Europeu 2016/679, adotou um conceito amplo para dado, não restringindo a proteção aos sinais e aos símbolos, mas também incluindo as informações pessoais, ou seja, os dados valorados, imbuídos de interpretação contextualizada a determinado tempo e lugar[23]. Logo, é a definição legal de dado que deve ser considerada para fins de proteção.

A LGPD prevê, no seu art. 7º, as hipóteses legais de tratamento de dados pessoais e, no seu art. 11, de dados sensíveis, nas quais, em princípio, não haveria ofensa ao direito fundamental à proteção de dados, sendo a primeira delas, o próprio consentimento do titular (art. 7º, I). Segundo Mario Viola e Chiara Teffé, o rol dos arts.

---

[20] SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo *et al*. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 37 e 38.
[21] Idem 19, p. 31.
[22] Idem 19, p. 39.
[23] VIOLA, Mario; TEFFÉ, Chiara. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo *et al*. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 117.

7º e 11 são taxativos, assim como ocorre no regulamento europeu[24].

Para o presente estudo, será analisada a hipótese legal da LGPD que prevê expressamente o direito ao tratamento de dados pessoais para uso em processo judicial, previsto no art. 7º, VI, da lei[25].

Antes de avançar sobre a possibilidade de tratamento de dados pessoais, de ofício pelo juiz, sem o consentimento do titular, a partir da leitura do art. 370 do CPC combinado com o art. 7º, VI, da LGPD, cabe destacar que a teoria da prova se utiliza do conceito de documento para sua admissão no processo judicial. Desse modo, para interpretar o CPC com a LGPD é preciso compreender os conceitos de dados pessoais e de documentos, sobretudo no contexto atual de uma sociedade digital.

Pode-se afirmar que os dados são uma novidade para a teoria da prova, sendo preciso compreender ambos institutos para garantir o melhor resultado do processo. Nessa esteira, é oportuna a crítica de Vitor de Paula Ramos a respeito do conceito clássico de documento, além de sua advertência para a necessidade de revisão da teoria da prova documental[26].

O estudo dos dados pessoais e da prova documental é de suma relevância para o processo civil, pois deve estar de acordo com a realidade do seu tempo, sob pena de não alcançar a efetiva prestação jurisdicional e o resultado justo, principalmente quando a sociedade está diante de situações cada vez mais complexas que demandam repostas coerentes e adequadas do Direito. Não querer compreender que as relações jurídicas estão sendo estabelecidas mediante a transferência e a análise de dados é fechar os olhos para a complexidade dos fatos

[24] Idem 22, p. 119.

[25] Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) .

[26] "Os primeiros escritos da processualística clássica, como já mencionei à exaustão até aqui, focavam-se nos documentos disponíveis à época, em sua maior parte escritos e em papel. Com o passar do tempo, a doutrina passou a fazer espécies de "adendos" na teoria geral, acrescentando primeiro as chamadas "reproduções mecânicas" e, posteriormente, as chamadas "provas informáticas", ou eletrônicas. A uma, isso tornou cada vez mais confusas as categorias de documentos, fazendo com que especificidades importantes dos tipos de provas documentais ficassem de fora do radar da doutrina, do legislador e dos tribunais. A duas, fez com que se passasse a ver a prova documental como um infinito de particularidades, como se cada documento singular demandasse uma teoria específica". RAMOS, Vitor de Paulo. Prova documental: do documento aos documentos, do suporte à informação. Salvador: Editora Juspodivm, 2021, p. 133 e 134.

e da informação e, por conseguinte, tornar obsoleta a teoria da prova documental[27].

Portanto, é preciso interpretar e aplicar os institutos processuais em conformidade com o direito fundamental à proteção de dados, como também em consonância com a sociedade digital, que desafiam compreensões clássicas do direito probatório.

3. Diferença conceitual entre documento, documento eletrônico e dado pessoal

O documento é um dos meios de prova idôneos e admitidos pelo ordenamento jurídico, com o escopo de levar o conhecimento dos fatos ao processo. Trata-se de um elemento formal que garante a segurança com relação ao conteúdo descrito no documento, atribuindo maior confiabilidade ao fato descrito[28].

Além dos meios legais previstos, como a confissão, a prova documental, a prova testemunhal e a prova pericial, por exemplo, o art. 369 do CPC, que se refere ao direito das partes de empregar todos os meios legais[29], ainda admite meios atípicos de prova, como a comunicação telefônica e a videoconferência[30]. Em geral, toda tecnologia da comunicação capaz de captar fatos é enquadrada como meio atípico de prova, sendo utilizada na instrução do processo, desde que transmita informações com segurança sobre os fatos a serem provados[31].

---

[27] "O fato de um documento ser escrito, portanto, tampouco tem relação com o fato de ser ou não 'em papel', algo que era defendido e sustentado antigamente; o fato de ser em papel ou em meio eletrônico nada diz, por si só, a respeito da confiabilidade ou da qualidade da informação gerada; muito menos serve para contrapor ou agrupar as chamadas 'reproduções mecânicas' a 'documentos informáticos." RAMOS, Vitor de Paulo. Prova documental: do documento aos documentos, do suporte à informação. Salvador: Editora Juspodivm, 2021, p. 138.

[28] "O estudo dos meios de prova permite o conhecimento dos tipos de elementos através dos quais a verdade dos fatos que o juiz tem de apreciar é trazida para o processo. Meios de prova são, então, os tipos de fonte, que transmitem o conteúdo dos fatos ao conhecimento do juiz e das partes, e que, segundo o artigo 332 do Código de Processo Civil, podem ser os meios de prova previstos em lei e os meios atípicos de prova". GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed. Rio de Janeiro: Forense, 2015, p. 116. Cabe destacar que o trecho da obra se refere ao CPC de 1973, que corresponde ao art. 369 do CPC de 2015.

[29] "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz" FUX, Luiz; NEVES, Daniel. Novo CPC Comparado. 3ª ed. Rio de Janeiro: Forense, 2016, p. 369.

[30] GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed. Rio de Janeiro: Forense, 2015, p. 116.

[31] O direito probatório "se trata de um sistema aberto, que recebe o influxo do saber humano originário de todos os quadrantes, que a todo momento está descobrindo novos métodos de investigação de

Na verdade, os meios atípicos de prova enquadram-se, na maior parte das vezes, na definição de prova documental, como o documento eletrônico, ou de prova testemunhal, como a videoconferência[32].

O debate sobre meios atípicos e sobre meios legais de prova tem origem no formalismo processual, pois os requisitos mínimos para a formação de um meio de prova seriam a garantia do exercício regular do direito de prova, sobretudo do juiz, visto que estaria assegurada a ausência de arbitrariedade na condução processual.

No afã de classificar novos meios de prova e verificar sua legitimidade, a doutrina e a jurisprudência esforçam-se para conceituar prova documental, acrescentando novas características ao que seria documento, visando conceder fundamento legal às novas descobertas científicas[33].

O documento eletrônico, por exemplo, foi incorporado à classificação de prova documental, tradicionalmente conceituado como um objeto físico que mantém de forma duradoura o registro de um acontecimento[34]. À medida que a tecnologia evolui, mais esforço é feito para integrá-la aos meios de prova, sobretudo quando se trata da prova documental, averiguando a confiabilidade da sua representação.[35]

No entanto, considerando a velocidade do avanço tecnológico e o incessante desenvolvimento social[36], o qual atribui novos instrumentos de comunicação e

---

que o direito deve fazer uso com o mesmo grau de confiabilidade de que desfrutam nas áreas de conhecimento de que se originam". Idem 29, p. 117.

[32] Idem 29, p. 117.

[33] "Quanto a novas descobertas científicas, não se trata de problema exclusivo das provas atípicas, mas principalmente da prova pericial e da prova documental. Por exemplo, atualmente vivemos o problema da incorporação ao sistema probatório do documento eletrônico". GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed. Rio de Janeiro: Forense, 2015, p. 118.

[34] GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed. Rio de Janeiro: Forense, 2015, p. 187.

[35] Para a concepção de prova documental dois requisitos devem estar presentes: a permanência e a inalterabilidade. Referente à permanência para o autor Leonardo Greco: "A permanência é do suporte físico e do próprio meio de registro para a conservação deste durante todo o período de tempo em que se tornar necessário que ele produza efeitos no processo. (...) A noção de permanência significa que o registro é apto a conservar-se durante todo o tempo necessário para que seja usado no processo, com o exato conteúdo com que foi confeccionado. (...) A inalterabilidade é correlata à permanência. É a imodificabilidade intrínseca do registro efetuado no suporte físico, salvo se for atingido por algum agente especialmente agressivo ou pela deterioração natural incidente durante longo período de tempo". Idem 33, p. 188.

[36] "A cibercultura é vivenciada por milhões de pessoas através de ações práticas com o uso de tecnologias digitais em rede tais como: *home banking*, cartões inteligentes, celulares, *smartphones*, *tablets*, *palm tops*, voto eletrônico, *webcam*, imposto de renda via *internet*. Na parte comunicacional, blogs, *e-mail*, *chats*, fóruns, web jornalismo." MIRANDA, Amli Paula Martins de; GARCIA NETTO, Luiz

armazenamento de dados, a doutrina questiona se a permanência e a inalterabilidade deve ser do documento ou da informação.[37]

Assim sendo, não é a forma ou o formato que valida a prova no processo, mas sim os dados, as informações ou os signos que devem ser admitidos como prova, como também protegidos conforme a ordem constitucional assim determinar. Em sentido contrário, Chiovenda[38] conferia importância para o documento escrito, de modo que a prova era invalidada apenas com a incidência de um procedimento probatório legalmente previsto ou com propositura de uma ação de falsidade. No contexto atual da história, o documento escrito perde a sua relevância e cede lugar aos dados pessoais que circulam aos milhares por diversos meios de comunicação.

Por conseguinte, no que se refere a um dever de não admitir prova documental, o documento deixa de ser requisito formal e essencial para a análise da admissão da prova, de maneira que a nulidade processual não seria decorrente do defeito da forma, ou seja, do documento admitido, mas sim da relevância do fato para o direito material, bem como da violação a algum direito fundamental com relação à informação levada ao processo[39].

Por outro lado, no que se refere ao dever de atuação do juiz ou de colaboração, a admissão da prova para instrução processual independe da existência de um documento formalmente constituído, visto que os dados estão disponíveis em nossa sociedade por meio de diversos sistemas organizacionais. Sendo o fato relevante para o resultado justo, cabe ao juiz obter as informações nos canais responsáveis pelo seu armazenamento, sob pena de violar o direito fundamental à prova.

Em virtude disso, o estudo sobre a admissão da prova documental deve se

---

da Rosa. Geografia do ciberespaço: novos territórios da informação em rede. Curitiba: Appris, 2014, p. 54.

[37] Vitor de Paula Ramos afirma que: "Parece-me carecer de valor a suposta diferença entre documentos escritos, reproduções mecânicas e documentos informáticos; e isso não só porque, na minha opinião, não só não há um critério que possa determinar tal classificação, como essa pode levar a uma série de equívocos". RAMOS, Vitor de Paula. Prova documental: do documento aos documentos, do suporte à informação. Salvador: Editora Juspodivm, 2021, p. 138.

[38] CHIOVENDA, Giuseppe. Instituições de direito processual civil. Campinas: Bookseller, 2009, p. 1098 e 1099.

[39] "Se não devemos (e não podemos) desformalizar totalmente o processo, impende, sim, libertarmo-nos dos 'falsos formalismos', ilusórios, antieconômicos, ineficientes, e que não cumprem nenhuma função, nem de garantia processual, nem de proteção eficiente aos direitos materiais". CABRAL, Antonio do Passo. Nulidades no processo moderno: contraditório, proteção da confiança e validade *prima facie* dos atos processuais. Rio de Janeiro: Forense, 2010, p. 180 e 181.

direcionar para uma análise da informação a ser obtida com o direito material a ser protegido, bem como da confrontação entre direito fundamental à prova e demais direitos fundamentais, como a proteção de dados pessoais, por exemplo.[40]

Para concluir o tópico, frisa-se que o conceito de dados pessoais é o determinado pelo art. 5º, I, da LGPD, sendo o conceito adotado por lei o mais abrangente possível, qual seja, toda informação relacionada a pessoa natural identificada ou identificável[41]. De acordo com Jeffrey Pomerantz, os dados são coletados por diversos instrumentos ou máquinas, podendo ser desde um sinal transmitido pelo celular a um fluxo de bits enviados por uma máquina em Marte para cientistas no planeta Terra[42]. Assim sendo, a investigação dos fatos relevantes pode ser realizada mediante o tratamento de dados, obtidos de formas variadas, dependendo da tecnologia utilizada.

4. Tratamento de ofício de dados pessoais para instrução probatória

Em vista do exposto, é possível afirmar que o juiz poderia obrigar a parte entregar seu celular em juízo para coleta de dados para fins de instrução probatória? Além disso, poderia o juiz de ofício coletar livremente os dados pessoais das partes na internet como fonte de prova?

Para responder o questionamento supramencionado, deve-se partir da premissa que a verdade é um valor fundamental da democracia e que o principal escopo da jurisdição é a tutela dos direitos[43], embora seja admitido no ordenamento brasileiro ritos, cujo objetivo seja a resolução do conflito, como ocorre nos juizados

[40] Também crítico à corrente tradicional, Vitor de Paula Ramos destaca que "a doutrina costuma sustentar que os critérios para admissão da prova documental ligam-se exclusivamente à tempestividade de sua juntada, ao fato de se tratar de um documento novo, ou à inexistência de impugnação pela parte contrária a respeito da chamada 'falsidade material' (aquela que incidiria no elemento extrínseco do documento) ou à chamada 'autenticidade' (no sentido dado pela doutrina tradicional, ligado exclusivamente à autoria)". RAMOS, Vitor de Paula. Prova documental: do documento aos documentos, do suporte à informação. Salvador: Editora Juspodivm, 2021, p. 266.

[41] Cabe ressaltar não haver um consenso entre os cientistas da informação sobre o conceito de dado, sendo importante a definição em lei para fins de proteção. "*We will start by trying to understand what data is. This is, unfortunately, leaping into deep end of the pool: data is such nebulous concept that even information scientists, who have devoted their entire careers to this phenomenon, don´t always agree*". POMERANTZ, Jeffrey. Metadata. Cambridge: The MIT Press, 2015, p. 19 e 20.

[42] POMERANTZ, Jeffrey. Metadata. Cambridge: The MIT Press, 2015, p. 20.

[43] TARUFFO, Michele. La vertitá nel processo. Revista de Processo, v. 235, p. 51-67, 2014, 53.

especiais e nos métodos de solução consensual de conflito[44].

Michele Taruffo leciona que o modelo de processo civil, denominado adversarial[45], prevalecente nos Estados Unidos, designa a investigação dos fatos às partes, pois o processo é considerado uma competição ou um jogo, onde os participantes devem esforçar-se para vencer. Nesse caso, o juiz possui uma função passiva, sem muito interferir na instrução processual.

A crítica a esse modelo é que não garante a concretização dos valores democráticos na prestação jurisdicional, visto que a verdade não é o escopo do processo nessa hipótese. Contudo, na Inglaterra, cuja tradição jurídica é similar à dos Estados Unidos, há uma tendência no direito processual civil de reforçar o poder do juiz com relação à investigação dos fatos, contrariando o sistema processual clássico[46].

Por outro lado, em outros modelos processuais comuns na Europa e presente na Alemanha[47], por exemplo, há previsão legal do poder instrutório do juiz, que, no entendimento de Taruffo, impede a prevalência da ideologia autoritária, pois o autoritarismo não é aliado da verdade, mas sim da manipulação dos instrumentos disponíveis, justamente para impedir a busca da verdade dos fatos[48].

Além da atuação do juiz ser mais passiva, outra característica do processo adversarial, é que a qualidade da decisão final do processo é irrelevante[49]. Sendo o escopo o fim da controvérsia entre as partes, o conteúdo da decisão final deverá

---

[44] "Nesse sentido, na mediação não se busca uma decisão que ponha um ponto final na controvérsia, até mesmo porque o mediador não tem poder decisório, o que, desde logo, o difere do árbitro. O que se procura é a real pacificação do conflito por meio de um mecanismo de diálogo (discurso racional), compreensão e ampliação da cognição das partes sobre os fatos que as levaram àquela disputa." PINHO, Humberto; DURÇO, Karol. A mediação e a solução de conflitos no Estado Democrático de Direito. O 'juiz Hermes' e a nova dimensão da função jurisdicional [online]. Disponível em <www.academia.edu>. Acesso em: 03 de maio de 2022.

[45] Idem 42, p. 53.

[46] TARUFFO, Michele. Poteri probatori delle parti e del giudice in Europa. Revista de Processo, v. 133, p. 239-266, 2006, p. 249.

[47] "*Un secondo modelo, al quale si ispira la maggior parte degli ordinamenti attuali – tra i quali si possono prendere ad esempio l´Italia e la Germania – prevede che al giudice vengano attibuiti alcuni poteri di iniziativa istruttoria. Naturalmente questi poteri possono essere più o meno numerosi e più o meno ampi a seconda dei casi. Emerge tuttavia uma tendenza piuttosto netta all´incremento dei potere istuttori del giudice che si manifesta anche in Italia, ad es. Com la recente introduzione dell´art. 281-ter.*" Idem 45, p. 242 e 243.

[48] Idem 42, p. 52.

[49] TARUFFO, Michele. Poteri probatori delle parti e del giudice in Europa. Revista de Processo, v. 133, p. 239-266, 2006, p. 246.

corresponder somente àquilo que as partes apresentaram ao processo e a sua qualidade com relação à verdade dos fatos não poderá ser questionada.

De acordo com Taruffo, o rito processual legitima a decisão judicial, não importando o grau de profundidade da instrução probatória ocorrida no processo, muito menos se foi suficiente para provar os fatos mencionados pelas partes ou relevantes para o julgamento da causa[50]. No entanto, se a qualidade da decisão é um valor democrático e integra o direito fundamental ao processo justo[51], é preciso primar por um resultado condizente com a verdade, bem como justificar a decisão com base em critérios objetivos de investigação dos fatos, ocorrendo somente com a possibilidade de investigação de ofício pelo juiz[52].

Nessa mesma linha, seguindo o modelo que prioriza a busca da verdade dos fatos, destaca-se a previsão do art. 370 do CPC de 2015[53]. Todavia, não se trata de um poder absoluto, que não encontre limitações em outros interesses também garantidos pela Constituição Federal.

A verdade dos fatos deve ser investigada pelo juiz, visando a um resultado justo, contudo, sem ultrapassar o objetivo de colaboração entre os sujeitos do processo, para que não seja violado algum direito corolário do princípio da dignidade da pessoa humana. Outra limitação à investigação incessante da verdade é o direito à duração razoável do processo, o qual não permite a prolongação desnecessária da fase instrutória em busca de esclarecimentos de fato que já se encontram minimamente comprovados[54].

---

[50] Idem 48, p. 247.

[51] "Pelo menos três critérios foram desenhados, entretanto, como necessários, mas nenhum sozinho, suficiente para garantir a justiça da decisão. Os critérios são os seguintes: (a) correta escolha e interpretação da regra jurídica; (b) apuração adequada dos fatos relevantes do caso; (c) emprego de um procedimento válido e justo para chegar à decisão." RAMOS, Vitor de Paula. Ônus da prova no processo civil: do ônus ao dever de provar. São Paulo: Thomson Reuters Brasil, 2018, p. 44 e 45.

[52] "*Se l áccertamento della veritá non interessa, e quindi il processo non deve essere orientato verso questo obbiettivo, e se neppure releva la qualità della decisione, allora è difficile comprendere perché mail e parti e il giuduce debbano perder tempo a dedurre e ad assumere le prove*". Idem 48, p. 247.

[53] "Caberá ao juiz, de ofício ou a requerimento da parte, determinar as provas necessárias ao julgamento do mérito" BRASIL. Lei nº 13.105 de março de 2015. Disponível em: < http://www.planalto.gov.br>. Acesso em 04 de maio de 2022.

[54] "Diante do direito brasileiro, pois, há necessidade de encontrar-se um 'ponto de equilíbrio' entre o direito à prova e o direito a um processo com duração razoável. Sendo o processo um ponto de encontro de direitos fundamentais, todos atendíveis em maior ou menor medida por exigência constitucional, é imprescindível que se ponderem os valores subjacentes às normas a fim de que se consiga propor uma justa solução para o problema (art. 8º do CPC/2015)." MITIDIERO, Daniel.

O art. 370 do CPC/2015 tem como propósito possibilitar a igualdade substancial das partes no processo, visando ao exercício do direito fundamental à prova, que pode estar sendo obstaculizado por fatores externos ao processo, como a complexidade do caso ou mesmo a desigualdade na defesa técnica das partes[55]. O poder de ofício do juiz para instrução processual corresponde ao ideal de um processo justo, porém, enquanto colabora para a obtenção de um resultado de qualidade, sem ferir direitos fundamentais.

Ao contrário do direito processual civil predominante no século XX[56], caracterizado pelo impulso processual feito pelas partes, atualmente é esperada uma postura ativa do juiz no andamento do processo, com o intuito de obter um resultado justo, garantindo um equilíbrio entre as partes e colaborando na investigação dos fatos, pois seu papel no processo judicial é a busca da verdade[57]. A doutrina fundamenta o poder de direção do juiz no princípio da colaboração, oriundo do princípio constitucional ao contraditório, o qual também deve abranger o juiz e não somente as partes[58].

Colaboração no processo civil: pressupostos sociais, lógicos e éticos. 3ª ed. São Paulo: Editora Revista dos Tribunais, 2015, p. 142.

[55] "A participação ativa do órgão jurisdicional no processo é uma premissa importante para a construção de um modelo adequado às exigências próprias da realidade contemporânea. Sendo as tensões decorrentes do aumento das diferenças sociais e culturais entre as partes cada vez mais fortes, o reforço dos poderes do juiz serve como instrumento para minimizar a influência exercida por fatores preexistentes ao próprio debate processual. A atribuição ao juiz de poderes relacionados à direção material do processo serve como meio para a realização de um processo inspirado pelo critério da igualdade substancial, como norte a regular as relações entre as partes, destinado à obtenção de justiça social, livre de amarras formalistas". REICHELT, Luis Alberto. O direito fundamental à prova e os poderes instrutórios do juiz. Revista de Processo, v. 281, p. 171-185, 2018, p. 172.

[56] "A doutrina tradicional, principalmente do século XX, tinha, primeiramente, como já destacado, a ideia de que a verdade não era assunto para o processo civil. Afinal, aquilo que ocorria dentro desse, ou a "verdade" (com aspas) que lá se produzia, não necessariamente tinha relação com o mundo exterior, ou seja, com a 'verdade' externa ao processo. (...) Assim, as provas serviriam para 'convencer o juiz da verdade." RAMOS, Vitor de Paula. Ônus da prova no processo civil: do ônus ao dever de provar. São Paulo: Thomson Reuters Brasil, 2018, p. 74 e 75.

[57] "O juiz, no desenvolvimento do diálogo, coloca-se no mesmo nível das partes, e sua atividade é tendente à busca da verdade". ABREU, Rafael Sirangelo. Igualdade e processo: posições processuais equilibradas e unidade do direito. São Paulo: Editora Revista dos Tribunais, 2015, p. 97.

[58] "Na doutrina brasileira, a colaboração foi pela primeira vez invocada a propósito da divisão do trabalho entre o juiz e as partes no processo civil por José Carlos Barbosa Moreira. Em duas oportunidades, Barbosa Moreira alude à colaboração: em primeiro lugar, como 'lema' do processo civil em tema de repartição das iniciativas probatórias; em segundo, como meio de 'resolver, em acorde harmonioso, a tradicional contraposição entre o modelo 'dispositivo' e o modelo 'inquisitivo' do processo civil. (...) Nada obstante a lembrança da colaboração pela doutrina na década de oitenta dos Novecentos, apenas posteriormente o tema foi introduzido de maneira efetiva entre nós por Alvaro de Oliveira. Partindo de seus estudos dos anos noventa sobre o direito ao contraditório, Alvaro de Oliveira

Nesse sentido, não apenas está legitimado, como passa a ser um dever do juiz exercer sua função, sobretudo a atividade probatória, com o máximo empenho no uso de medidas disponíveis na ordem jurídica para o alcance de uma decisão justa. Com base no princípio colaborativo, o juiz estaria sendo parcial na hipótese de não exercer um papel ativo na investigação dos fatos, em razão da ausência de paridade de armas entre as partes, comum nas disputas judiciais, como também por possuir experiência acerca das fontes de prova idôneas a comprovar situação específica. Esse *know how* adquirido pelo exercício da magistratura não deve ser omisso na fase instrutória do processo, sob pena de violar o princípio colaborativo e, por conseguinte, a igualdade processual, pilar do Estado Democrático de Direito. Portanto, a função ativa no desenvolvimento do processo, no que se refere à atividade probatória, não deveria ser subsidiária à iniciativa das partes, mas sim concomitante e integrado definitivamente como um papel do juiz.

Embora o direito processual civil muito tenha evoluído, principalmente, a partir de sua perspectiva colaborativa, a doutrina tradicional que estuda o direito probatório ainda compreende o ônus da prova como uma medida ideal para a adequada apuração das provas, considerado como critério de instrução, com o intuito de estimular a reunião de provas relevantes e necessárias para corroborar as alegações das partes.[59] Resumidamente, haveria apenas um ônus das partes de submeterem provas ao processo judicial. Ao invés do dever de provar, haveria tão somente um risco de perder a demanda. Caso o autor, por exemplo, não anexasse as provas correspondentes aos fatos alegados na petição inicial, provavelmente o seu pedido seria julgado improcedente[60].

---

propôs uma 'visão cooperativa' para o processo civil: em síntese, propôs uma direção efetiva do processo pelo juiz, porém, não em uma posição dominante e superior, mas pautada pelo diálogo a respeito do material fático-jurídico e probatório recolhido no processo, com a consequente relativização dos brocardos '*Iura novit curia*' e '*Da mihi factum, dabo tibo ius*." MITIDIERO, Daniel. Colaboração no processo civil: pressupostos sociais, lógicos e éticos. 3ª ed. São Paulo: Editora Revista dos Tribunais, 2015, p. 101 e 102.

[59] "Partindo da ideia de que o processo lida, via de regra, com versões contraditórias dos fatos (exemplo, alguém alega a ocorrência de dano moral e a parte contrária alega sua existência), o legislador incumbe a cada uma das partes a tarefa de aportar aos autos provas dos fatos que, caso resultassem provados, lhes beneficiariam." RAMOS, Vitor de Paula. Ônus da prova no processo civil: do ônus ao dever de provar. São Paulo: Thomson Reuters Brasil, 2018, p. 53.

[60] Todavia, não será aprofundado o debate acerca do ônus da prova como um critério de instrução e julgamento ou se a partir da leitura colaborativa do processo, a produção de prova torna-se um dever das partes, visto que fugiria do objeto do trabalho.

Conforme supramencionado, o adequado desenvolvimento processual requer uma instrução ativa do juiz, a qual possui fundamento legal no Código de Processo Civil de 2015, ao conceder amplos poderes probatórios ao magistrado [61]. Combinando o avanço da teoria da prova no processo civil com a evolução da tecnologia da comunicação, não é de se estranhar que no século XX quando a informação não era disseminada em comparação aos dias atuais e no Brasil a internet ainda não era popularmente utilizada, fazia sentido compreender um processo judicial hermético, cuja instrução dependia somente das partes e cujo objetivo era convencer o juiz[62].

Todavia, num contexto atual, caracterizada pela terceira revolução industrial[63], em que um volume enorme de dados circula livremente pela web[64], a investigação de ofício pelo juiz não se resume à juntada de documentos ao processo, sendo possível diversos meios para obter as informações necessárias ao resultado justo.

Logo, se a busca da verdade é uma das funções principais do processo e se o resultado da instrução tem o potencial de elevar a qualidade da prestação jurisdicional[65], o avanço da internet da comunicação e da disponibilidade de dados pessoais não pode ser ignorado pela teoria da prova, de modo que, se existem novos meios legítimos de obtenção de prova, o direito processual civil deve integrá-los ao sistema jurídico, sob pena de obstar uma das principais funções do Estado-juiz.

---

[61] MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. Comentários ao Código de Processo Civil: artigos 369 ao 380. São Paulo: Editora Revista dos Tribunais, 2016, p. 173.

[62] RAMOS, Vitor de Paula. Ônus da prova no processo civil: do ônus ao dever de provar. São Paulo: Thomson Reuters Brasil, 2018, p. 75.

[63] "A ideia global é que estamos vivendo uma terceira revolução industrial, e o núcleo dessa terceira revolução industrial é o que chamamos de NBIC. N de nanotecnologias, B de biotecnologias, particularmente o sequenciamento do genoma humano e a ferramenta de edição do DNA que se chama Crispr-Cas9. Depois o I, de informática, os *big data* e a internet dos objetos. E o C é o cognitivismo, isto é, a inteligência artificial (IA), o coração do coração dessas quatro inovações." FERRY, Luc. A revolução transumanista. Barueri, SP: Manole, 2018, p. 8.

[64] "(...) é realmente a infraestrutura da *web* que dá origem a novos modos de relações humanas, a começar pelas redes sociais em que, a cada dia, centenas de milhões de indivíduos trocam todo tipo de mensagens, fotos, músicas, filmes e opiniões – sistema aparentemente gratuito, mas que, como veremos, permite coletar continuamente dados privados (os famosos *big data*) cuja venda a outra empresas gera lucros propriamente inacreditáveis, sendo o gratuito, na realidade, uma magnífica cortina de fumaça, um fascinante meio de ganhar dinheiro". FERRY, Luc. A revolução transumanista. Barueri, SP: Manole, 2018, p. 84.

[65] MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. Novo Curso de Processo Civil: teoria do processo civil. São Paulo: Editora Revista dos Tribunais, 2015, p. 244.

Ressalta-se que não se trata da busca de uma verdade absoluta, completamente idêntica à realidade, mas sim de uma verdade cognoscível mediante meios legítimos de investigação ou algumas vezes limitados por outros direitos igualmente protegidos pela Constituição Federal[66]. Também não pertence à noção da verdade, os fatos demonstrados mediante argumentação das partes[67], a qual é elaborada por um discurso lógico, visando ao convencimento ao juiz (função retórica da prova)[68]. Na lição de Greco, a natureza argumentativa da prova não é adequada para um processo justo[69].

Portando, a verdade é aquela obtida mediante informações cognoscíveis por instrumentos tecnológicos e científicos disponíveis na sociedade. Logo, em princípio, poderia o juiz colher informações a partir do aparelho celular de uma das partes para fins de obtenção da verdade dos fatos. Contudo, seria um poder ilimitado? Em qualquer hipótese, poderia o juiz utilizar-se de dados pessoais, sem o consentimento das partes, para julgamento de uma demanda?

A limitação ao poder de ofício pelo juiz vai além das regras processuais que

---

[66] "Por isso, observa Giovanni Verde, que no processo as regras sobre prova não regulam apenas os meios de que o juiz pode servir-se para 'descobrir a verdade', mas também traçam limites à atividade probatória, tornando inadmissíveis certos meios de prova, resguardando outros interesses (como a intimidade, o silencia etc.) ou ainda condicionando a eficácia do meio probatório à adoção de certas formalidades (como o uso do instrumento público)." Idem 64, p. 245 e 246.

[67] "Para Perelman o objetivo de toda argumentação é provocar ou aumentar a adesão dos ouvintes à tese defendida, utilizando da argumentação eficaz, na qual consegue aumentar a intensidade de adesão, como forma de desencadeamento de ideias nos ouvintes no mesmo sentido daquela proferida pelo orador. Dessa feita, os efeitos da argumentação se mostram de grande valia ao discurso, pois o processo argumentativo considera-se aquele em que a prova da verdade ou a probabilidade de que sua tese é verdadeira e deve ser administrada no campo formal ou científica, em comum acordo com os interlocutores da tese." PESSENHA, Jackelline. Chaïm Perelman e o combate à retórica da eficácia dos sofistas. Opinion Jurídica, v. 13, n. 25, 2014.
Disponível em: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-25302014000100012.>. Acesso em 02 de abril de 2022.

[68] Idem 64, p. 248.

[69] "Seria ingênuo acreditar que esse sentido lógico de prova – como resultado da dialética, dos argumentos, da oratória – era capaz de assegurar rigorosa objetividade ao julgamento dos fatos. A ora mencionada concepção lógica da prova ainda é muito prestigiada na atualidade, porque a certeza de que o juiz fez todo o esforço para transpor para o processo a realidade da vida exige que seu convencimento não seja puramente íntimo e subjetivo, mas que se funde em argumentos e razões que podem ser aceitos ou reconhecidos como razoáveis por todos. Contudo, a adoção dessa concepção é perigosa, insuficiente, porque nela se superestimam, na avaliação das provas, a estratégia e os argumentos dos advogados, desprezando a busca da verdade e havendo, assim, o risco de comprometer todas as suas conclusões. " GRECO, Leonardo. Instituições de processo civil: introdução ao direito processual civil. 5ª ed. Rio de Janeiro: Forense, 2015, p. 101.

disciplinam o direito probatório[70], sendo sua atuação mais ativa ou menos ativa dependendo de fatores externos ao processo, como o direito a ser tutelado, envolvendo questões de família, ou mesmo desigualdades econômicas e sociais entre as partes, que dificultariam o acesso à prova. Também pode servir de critério para a obtenção de dados sem o consentimento das partes, para os casos mais complexos e de difícil comprovação, cuja abstenção na investigação dos fatos poderia prejudicar uma das partes, resultando num processo injusto.

O mecanismo de avaliação para a medida da atuação judicial está na confrontação dos direitos fundamentais envolvidos. De um lado está o direito à prova, que exige uma instrução séria e objetiva na busca da verdade, e de outro lado, o direito fundamental à proteção de dados pessoais, que visa a proteger a autodeterminação informativa, como também o livre desenvolvimento da personalidade. Por essa razão, não é qualquer caso concreto que possibilita a coleta de dados pessoais de um *smartphone* ou mesmo da web, pois haveria uma desproporção entre aquilo que o indivíduo construiu como sua personalidade e o que se quer investigar no processo.

É preciso uma justificativa com base em critérios objetivos para o tratamento de dados pessoais sem o consentimento da parte. Tal justificativa, conforme referido anteriormente, transcende as regras processuais, devendo referir-se ao direito material, à ausência de paridade de armas ou à complexidade do caso, por exemplo. Por conseguinte, mesmo a LGPD estabelecendo no art. 7º, VI, que é possível ocorrer o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, é preciso interpretar essa regra e a do art. 370 do CPC conforme a Constituição Federal, sobretudo com o direito fundamental à proteção de dados pessoais.

A jurisprudência do Superior Tribunal de Justiça firmou entendimento pela discricionariedade do juiz de determinar de ofício a produção de prova[71] e a partir dela

[70] REICHELT, Luis Alberto. O direito fundamental à prova e os poderes instrutórios do juiz. Revista de Processo, v. 281, p. 171-185, 2018, p. 173.

[71] "Processual civil. Agravo interno no agravo em recurso especial. Contrato de seguro. Negativa de prestação jurisdicional. Não ocorrência. Responsabilidade contratual. Falha na prestação do serviço. Reexame do conjunto fáticoprobatório dos autos. Inadmissibilidade. Incidência das súmulas n. 5 e 7 do STJ. Princípio da persuasão racional. Decisão mantida. (...) 4. O CPC/2015, em seus artigos 370 e 371, manteve o princípio da persuasão racional, reafirmando que compete ao magistrado dirigir a

é importante notar que o STJ entende pela existência de discricionariedade do juiz para avaliar a necessidade de produção de prova, embora o processo justo exija o uso de critérios objetivos pelo juiz para decidir acerca da produção da prova de ofício. Se a verdade dos fatos é essencial para garantir um processo pautado nos ideais democráticos, a apuração pelo juiz deve ser coerente com essa busca pela verdade, seguindo uma lógica racional e não meramente discricionária[72].

No processo AgInt no AREsp 1628617/RS, o STJ julgou importante questão sobre a interpretação do art. 370 do CPC, pois ao negar provimento ao recurso da parte, entendeu que a investigação de ofício pelo juiz não é somente complementar ou subsidiária à produção de prova iniciada pelas partes.[73]

Todavia, o pedido de indenização por danos morais foi julgado improcedente, pois o juiz, de ofício, consultou o cadastro de devedores, cujo resultado culminou na aplicação do entendimento da Súmula nº 385/STJ, que veda indenização por dano moral no caso de existência de anotações anteriores.

A autora recorreu ao STJ alegando que restou vencida exclusivamente em razão da prova produzida pelo juiz em favor do réu. Além disso, a autora alegou que

---

instrução probatória. Assim, cabe ao juiz (sempre em decisão fundamentada): (i) determinar, até mesmo de ofício, a produção das provas que entender necessárias ao julgamento de mérito, (ii) rejeitar as diligências inúteis ou protelatórias, e (iii) apreciar a prova, indicando os motivos de seu convencimento. Precedentes. 5. Agravo interno a que se nega provimento" (AgInt no AREsp 1.581.285/RJ, Rel. Ministro ANTONIO CARLOS FERREIRA, QUARTA TURMA, julgado em 18/02/2020, DJe 02/03/2020). "Processual civil e administrativo. Recurso especial. Prestação de contas. Anulação da sentença. Determinação, de ofício, pela instância recursal de realização de prova pericial. ARTIGO 370 DO CPC (130 DO CPC/73). Possibilidade. Precedentes. Acórdão em consonância com a jurisprudência do Superior Tribunal de Justiça. Súmula 83/STJ. (...) 2. O juiz tem o poder de iniciativa probatória, inclusive para determinar a produção das provas que julgar necessárias à solução da lide. Esta prerrogativa pode ser utilizada em qualquer fase do processo. Precedentes: AgRg no AgRg no AREsp 416.981/RJ, Rel. Ministro Antônio Carlos Ferreira, Quarta Turma, DJe 28.05.2014; REsp 382.742/PR, Rel. Ministro Francisco Peçanha Martins, Segunda Turma, DJ 26.04.2006; AgRg no Ag 1.345.439/RJ, Rel. Ministro Sidnei Beneti, Terceira Turma, DJe 07.06.2011. 3. O acórdão recorrido está em sintonia com o atual entendimento do Superior Tribunal de Justiça, razão pela qual não merece prosperar a irresignação. Incide, *in casu,* o princípio estabelecido na Súmula 83/STJ: 'Não se conhece do Recurso Especial pela divergência, quando a orientação do Tribunal se firmou no mesmo sentido da decisão recorrida.' 4. Recurso Especial não conhecido." (REsp 1.818.766/AM, Rel. Ministro HERMAN BENJAMIN, SEGUNDA TURMA, julgado em 20/08/2019, DJe 18/10/2019).

[72] SQUADRI, Ana Carolina. Tutela jurisdicional efetiva e imediatidade do juiz em relação à prova. Revista de Direito, Universidade Federal de Viçosa, v. 13, n. 1, 2021.

[73] No caso concreto, a autora ajuizou ação declaratória de indébito e de indenização por danos morais, julgado parcialmente procedente pelo juiz de primeiro grau de jurisdição, visto que "a parte ré não se desincumbiu de seu ônus probatório, consistente em demonstrar a contratação dos serviços cobrados, de modo que foi reconhecida a inexigibilidade do débito questionado". RIO GRANDE DO SUL. Superior Tribunal de Justiça. AgInt no AREsp 1628617 / RS, 3ª Turma, Rel. Ricardo Villas, DJe 07/05/2021. Disponível em: < www.stj.jus.br>. Acesso em: 14 de maio de 2022.

o STJ compreende que a produção de prova de ofício somente ocorre após todos os esforços realizados pelas partes. Por sua vez, o STJ decidiu que o magistrado de primeiro grau possui discricionariedade para expedir ofício junto aos órgãos de proteção ao crédito, para verificar a existência de outros apontamentos em nome da autora, quando for decidir pedido de danos morais[74].

No Tribunal Regional Federal da 4ª Região há exemplo de caso concreto em que o tribunal negou a admissão de prova pericial numa ação de improbidade administrativa, pois entendeu que a prova era irrelevante para o julgamento da causa, bem como em razão da proibição de acesso aos dados dos pacientes de determinada unidade hospitalar, com fundamento na LGPD[75]. Vale destacar que, ao contrário do que foi decidido, o magistrado pode requerer, justificadamente, os dados pessoais de pacientes, sem o consentimento dos titulares, com base no art. 11, II, e, da LGPD, se for a hipótese de não haver alguma violação a direito fundamental. Ademais, a produção de prova de ofício pelo juiz atende ao processo justo, de modo que a não sua admissão deve ser em decorrência de violação de outros direitos fundamentais.

5. Considerações finais

O direito à prova tem como propósito a apuração da verdade dos fatos, de modo a garantir a liberdade e igualdade processual das partes, como também um resultado justo. Conforme exposto, sem a participação ativa do juiz na instrução processual, não é possível conferir um contraditório efetivo, em que as partes consigam se defender provando, visto que, por razões diversas e exteriores ao

---

[74] "Agravo interno no agravo em recurso especial. Produção de provas. Determinação de ofício. Possibilidade. Artigo 370 do CPC/2015. Reexame. Súmula nº 7/STJ. Cadastro de devedores. Inscrição indevida. Outros apontamentos. Dano moral. Impossibilidade. Súmula nº 385/STJ. 1. Recurso especial interposto contra acórdão publicado na vigência do Código de Processo Civil de 2015 (Enunciados Administrativos nºs 2 e 3/STJ). 2. O magistrado pode determinar, de ofício, a realização das provas que julgar necessárias à instrução do processo, nos termos do artigo 370 do CPC/2015. 3. O juízo acerca da produção da prova compete soberanamente às instâncias ordinárias (Súmula nº 7/STJ). 4. A existência de outros apontamentos em nome da autora no cadastro de devedores impede a procedência do pedido indenizatório. Súmula nº 385/STJ. 5. Agravo interno não provido". RIO GRANDE DO SUL. Superior Tribunal de Justiça. AgInt no AREsp 1628617 / RS, 3ª Turma, Rel. Ricardo Villas, DJe 07/05/2021. Disponível em: < www.stj.jus.br>. Acesso em: 14 de maio de 2022.

[75] RIO GRANDE DO SUL. Tribunal Federal Regional da 4ª região. 5038459-02.2021.4.04.0000/ RS. 4ª Turma, Rel. Luís Alberto D´Azevedo Aurvalle, 24/09/21. Disponível em: <www.tr4.jus.br>. Acesso em: 14 de maio de 2022.

processo judicial, não conseguem demonstrar suas alegações sem a colaboração do juiz.

Todavia, o direito fundamental à prova somente irá efetivamente cumprir seu papel caso acompanhe o avanço social, o qual vem se mostrando cada vez mais tecnológico e interconectado pela *web*. Essa interação social no meio cibernético resulta na disponibilização de dados pessoais, utilizados muitas vezes de forma indevida, como por exemplo, a sua comercialização para empresas. Por esse motivo, o ordenamento jurídico procura proteger os dados, tanto com a previsão expressa de um direito fundamental, quanto com a regulação da matéria por lei.

O direito fundamental à proteção de dados tem como objeto a liberdade e o controle sobre os dados e informações pessoais, pois fazem parte do desenvolvimento da personalidade e da autodeterminação informativa, não podendo ser utilizados contra o próprio titular, principalmente como forma de repressão do Estado ou de arbitrariedade judicial. O uso de dados pessoais pelo Estado deve ter como justificativa a proteção de outro interesse resguardado constitucionalmente, como o processo justo, por exemplo.

Para o estudo da proteção de dados pessoais com o direito à prova, é preciso, porém, avançar alguns paradigmas, como a necessidade de formação de um documento para sua utilização como fonte de prova. Considerando que as informações estão disponíveis e acessíveis na sociedade digital e que a exigência de uma formalidade na produção de prova documental não atende seu propósito atualmente, qual seja, a permanência e a estabilidade da forma, é preciso interpretar e aplicar as regras do processo civil de acordo com essa realidade.

Sendo assim, os requisitos para a admissão da prova documental não seriam de natureza formal, como a autenticidade do documento, por exemplo, mas sim fazendo referência a não violação de algum outro direito fundamental. Desse modo, para o uso de dados pessoais com base no art. 7º, VI, da LGPD, é preciso justificar o tratamento de dados com elementos do direito material, sem a necessária aprovação do seu titular. Portanto, se um juiz determinar como fonte de prova o uso do diálogo de uma das partes por alguma rede social, deve fundamentar a decisão analisando os interesses em questão e os direitos fundamentais correspondentes. O controle da atividade jurisdicional não ocorre somente com a verificação de cumprimentos de

ritos e formas, é preciso sopesar os direitos fundamentais intrínsecos às decisões, sobretudo, no que diz respeito à instrução processual.

Ademais, a regra do art. 7º, VI, da LGPD, deve ser interpretada conjuntamente com a do art. 370 do CPC, a qual a prevê a produção de prova de ofício pelo juiz. Ela deve ser interpretada conforme o modelo cooperativo de processo civil, sistema organizacional que estabelece o processo como uma comunidade de trabalho.

Nessa comunidade o juiz não exerce sua atividade arbitrariamente, sem considerar a iniciativa das partes, mas deve estar atento para que sua atuação passiva não prejudique eventual desigualdade processual. Por isso, o art. 370 não confere um direito absoluto ao juiz de investigar qualquer fato e de utilizar qualquer meio de prova, pois sua atuação deve ser coerente com os fatos alegados pelas partes e a medida da atividade probatória de ofício requer uma justificativa no campo do direito material ou mesmo extraprocessual, como a desigualdade econômica entre as partes ou a facilidade do magistrado de obter a prova em relação às partes.

Por conseguinte, o tratamento de dados pessoais pelo juiz, conforme previsto no art. 7º, VI, da LGPD c/c o art. 370 do CPC, é um meio legítimo de prova, que possibilita coletar informações a partir dos meios tecnológicos disponíveis, podendo ocorrer sem o consentimento do titular, quando outros direitos fundamentais estiverem ameaçados, como por exemplo, quando não houver paridade de armas, quando a natureza do direito material a ser tutelado permite atuação mais ativa do juiz ou quando a complexidade do caso requer iniciativa do juiz para superar a dificuldade do contraditório efetivo por uma das partes.

Referências bibliográficas

ABREU, Rafael Sirangelo. **Igualdade e processo: posições processuais equilibradas e unidade do direito.** São Paulo: Editora Revista dos Tribunais, 2015.

BRASIL. Emenda Constitucional nº 115, de fevereiro de 2022. Disponível em: <https://www2.camara.leg.br/legin/fed/emecon/2022/emendaconstitucional-115-10-fevereiro-2022-792285-publicacaooriginal-164624-pl.html>. Acesso em 18 de abril de 2022.

BRASIL. Lei nº 13.105 de março de 2015. Disponível em: <http://www.planalto.gov.br>. Acesso em 04 de maio de 2022.

BRASIL. Lei nº 13.709 de agosto de 2018. Disponível em: <http://www.planalto.gov.br>. Acesso em 18 de abril de 2022.

BRASIL. Superior Tribunal de Justiça. AgInt no AREsp 1628617 / RS, 3ª Turma, Rel. Ricardo Villas, DJe 07/05/2021. Disponível em: <www.stj.jus.br>. Acesso em: 14 de maio de 2022.

CABRAL, Antonio do Passo. **Nulidades no processo moderno: contraditório, proteção da confiança e validade *prima facie* dos atos processuais.** Rio de Janeiro: Forense, 2010.

CABRAL, Tricia Navarro Xavier. **Ordem Pública Processual.** Brasília, DF: Gazeta Jurídica, 2015.

CHIOVENDA, Giuseppe. **Instituições de direito processual civil.** Campinas: Bookseller, 2009.

FERRY, Luc. **A revolução transumanista**. Barueri, SP: Manole, 2018.

FUX, Luiz; NEVES, Daniel. **Novo CPC Comparado**. 3ª ed. Rio de Janeiro: Forense, 2016.

GRECO, Leonardo. **Instituições de processo civil: introdução ao direito processual civil.** 5ª ed. Rio de Janeiro: Forense, 2015.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. Novo **Curso de Processo Civil: teoria do processo civil.** São Paulo: Editora Revista dos Tribunais, 2015.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Comentários ao Código de Processo Civil: artigos 369 ao 380.** São Paulo: Editora Revista dos Tribunais, 2016.

MIRANDA, Amli Paula Martins de; GARCIA NETTO, Luiz da Rosa. **Geografia do ciberespaço: novos territórios da informação em rede.** Curitiba: Appris, 2014.

MITIDIERO, Daniel. **Colaboração no processo civil: pressupostos sociais, lógicos e éticos.** 3ª ed. São Paulo: Editora Revista dos Tribunais, 2015.

PINKER, Steven. **O novo iluminismo: em defesa da razão, da ciência e do humanismo**. São Paulo: Companhia das Letras, 2018.

PINHO, Humberto; DURÇO, Karol. **A mediação e a solução de conflitos no Estado Democrático de Direito. O 'juiz Hermes' e a nova dimensão da função jurisdicional** [online]. Disponível em:<www.academia.edu>. Acesso em: 03 de maio de 2022.

PESSENHA, Jackelline. Chaïm Perelman e o combate à retórica da eficácia dos sofistas. Opinion Jurídica, v. 13, n. 25, 2014. Disponível em:

<http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-25302014000100012>. Acesso em: 02 de abril de 2022.

POMERANTZ, Jeffrey. Metadata. Cambridge: The MIT Press, 2015.

RAMOS, Vitor de Paula. **Ônus da prova no processo civil: do ônus ao dever de provar**. São Paulo: Thomson Reuters Brasil, 2018.

RAMOS, Vitor de Paulo. **Prova documental: do documento aos documentos, do suporte à informação**. Salvador: Editora Juspodivm, 2021.

REICHELT, Luis Alberto. **O direito fundamental à prova e os poderes instrutórios do juiz.** Revista de Processo, v. 281, p. 171-185, 2018.

RIO GRANDE DO SUL. Tribunal Federal Regional da 4ª região. 5038459 02.2021.4.04.0000/ RS. 4ª Turma, Rel. Luís Alberto D´Azevedo Aurvalle, 24/09/21. Disponível em: <www.tr4.jus.br>. Acesso em: 14 de maio de 2022.

SARLET, Ingo**. Fundamentos constitucionais: o direito fundamental à proteção de dados.** In: DONEDA, Danilo *et al*. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

SQUADRI, Ana Carolina. **Tutela jurisdicional efetiva e imediatidade do juiz em relação à prova.** Revista de Direito, Universidade Federal de Viçosa, v. 13, n. 1, 2021. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/12086>. Acesso em: 14 de abril de 2022.

TARUFFO, Michele. **La vertitá nel processo.** Revista de Processo, v. 235, p. 51-67, 2014. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2014;1001020719>. Acesso em: 18 maio de 2022.

TARUFFO, Michele. **Poteri probatori delle parti e del giudice in Europa**. Revista de Processo, v. 133, p. 239-266, 2006. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2006;1000760732>. Acesso em: 19 maio de 2022.

2. COMPLIANCE DIGITAL NA EDUCAÇÃO: UMA VISÃO OBRIGACIONAL SOB O ENFOQUE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

https://doi.org/10.36592/9786581110994-02

Ana Cláudia Miranda Lopes Assis[1]

Sumário

1. Introdução

Diante da plasticidade do conceito de privacidade, mister distinguir privacidade informacional da privacidade tradicional, figurando a última como gênero das espécies vida privada, particular e íntima, vista como direito de estar só, sem intromissão ou percepção alheia. Por sua vez, a privacidade informacional se liga aos novos desafios que ecoam na era digital em relação à proteção de dados pessoais, percebendo-se o indivíduo como um ser informacional, representado por meio de dados cuja privacidade se vê, muitas vezes, ameaçada diante da não identificação de todas as dimensões no ciclo dos conhecimentos[2] e possibilidade de colidir com conceitos ligados, dentre muitos, à transmissão e utilização dos dados. É essa distinção que possibilita entender a atribuição de uma valoração jurídico-constitucional própria[3] para os interesses envolvidos.

---

[1] Doutoranda do Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e do Doutorado Interinstitucional (DINTER) da Faculdade Católica de Rondônia (FCR). Membro do Grupo de Estudos em Proteção de Dados do PPGD da PUCRS. E-mail: ackreu@gmail.com Lattes: http://lattes.cnpq.br/6517350158770001.

[2] Cf. SPIECKER, Indra. Wissensverarbeitung in Öffentlichen Recht. Rechtswissenschaft, [*s.l.*], n.3, p. 247-282, jan. 2010, p. 247.

[3] No Direito alemão, o direito à proteção de dados é visto como um direito fundamental à autodeterminação informativa.

O direito à proteção de dados refere-se a uma parcela do direito à informação, cujo interesse foi desperto a partir de 1970 na Alemanha e, em 1990, no restante da Europa, quando despontaram as primeiras legislações, por isso é considerado um direito relativamente recente[4]. Não se olvide, contudo, que o marco fundamental e mundial em matéria de proteção de dados pessoais foi o documento "Diretrizes para Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", publicado em 1980 pela Organização para Cooperação e Desenvolvimento Econômico (OCDE) — em inglês, *Organization for Economic Co-operation and Development* (OECD)[5].

No Brasil, a fim de tornar o ambiente digital mais seguro e democrático, foi elaborado o "Marco Civil da Internet"[6] pela Lei n.º 12.965, de 23 de abril de 2014[7], fundamentada nos pilares da liberdade de expressão, da neutralidade da rede e da privacidade, legislação essa que norteia todo o processo de aplicação da internet, cuja forma e conteúdo diz respeito à tutela dos direitos fundamentais consagrados na Constituição Federal de 1988[8], delegando a proteção de dados pessoais a uma legislação específica, posteriormente conhecida como Lei Geral de Proteção de Dados, Lei n.º 13.709, de 14 de agosto de 2018, doravante denominada LGPD[9].

Nesse contexto, as reflexões globais quanto ao progresso e quanto à evolução tecnológica propiciar maior acesso à informação evidenciam a problemática desse

---

[4] Em levantamento realizado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, 2022) constatou-se que 132 dos 194 países possuem legislação direcionada a garantia da proteção de dados pessoais. Cf. UNCTAD. Data Protection and Privacy Legislation Worldwide. UNCTAD, 2022.

[5] Cf. OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD, 2022. Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyand transborderflowsofpersonaldata.htm>. Acesso em: 20 mai. 2022.

[6] Legislação de cunho principiológico consistente em uma espécie de "Constituição da Internet".

[7] Cf. BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União de 24.4.2014. Brasília, DF: 2014.

[8] Cf. BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Diário Oficial da União de 05.10.1988. Brasília, DF: 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 16 ago. 2022.

[9] A Lei n.º 13.709/2018 foi alterada pela Lei n.º 13.583, de 8 de junho de 2019. Cf. BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União de 15.8.2018, republicado parcialmente em 15.8.2018 - Edição extra. Brasília, DF: 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 16 ago. 2022.

novo cotidiano informacional e "algoritmizado", porquanto revela a emulação das novas *commodities,* figurando em primeira ordem os dados pessoais, que passam a ser a principal moeda de troca, o que, por conseguinte, avulta a necessidade de coibir excessos e resguardar os direitos fundamentais.

Nesse sentir, por meio do método hipotético-dedutivo, com uma investigação bibliográfica e exploratória, acercando-se de considerações sobre a aplicação crescente das tecnologias digitais no âmbito educacional, procurou-se na presente pesquisa demonstrar a necessidade da adoção de condutas e/ou procedimentos direcionados a um padrão valorativo e comportamental das organizações e instituições quanto ao uso de plataformas digitais, aplicativos e demais tecnologias, aptos em preservar o direito fundamental da privacidade, garantir a segurança e a proteção de dados pessoais de crianças e adolescentes. Para tanto, serão apontadas características ou elementos de um programa de integridade relacionado hodiernamente a ideia do "*compliance* digital".

Nesse desiderato, inicialmente direcionar-se-á a atenção da pesquisa para questões afetas à aplicação prática do *compliance* no ambiente ciberespacial e sua adequação à normatização que envolve a proteção de dados [10], privacidade informacional e segurança informática na promoção de boa governança e gestão de riscos[11], passando-se a adotar a nomenclatura "*compliance* digital" por mais se adequar à temática proposta, acercando-se de considerações sobre os princípios indicados na LGPD.

E, considerando que o direito à proteção de dados se inicia no campo da prevenção[12], sendo um trabalho de evolução de pessoas, processos e cultura

[10] Interessa destacar que a Convenção 108 (Convenção para a Proteção das Pessoas a respeito do Tratamento Automatizado de Dados de Caráter Pessoal), instituída pelo *Tratado de Estrasburgo* de 1981, é considerada um dos mais relevantes instrumentos de identificação da relação entre privacidade, proteção de dados e algoritmos. E, adequando-se às novas tecnologias e diante do exponencial crescimento no compartilhamento de dados pessoais, o Conselho da Europa promoveu sua atualização de modo a convergir com as atuais legislações de proteção de dados, tal como a LGPD, recebendo nova titulação como "Convenção 108+", cuja vigência depende, em primeira ordem, de sua ratificação por todas as partes da Convenção, ou, quando as partes signatárias a ratificaram até 11 de outubro de 2013. Cf. NATARAJAN, Aishwarya; RINKE, Franziska; WEISE, Sebastian. Dawn of a new era of global data protection?. Völkerrechtsblog, 02.03.2021. DOI: 10.17176/20210302-153629-0

[11] Cf. LÓSSIO, Claudio Joel Brito. Proteção de Dados e Compliance Digital. São Paulo: Almedina, 2021.

[12] Indra Spiecker (2019, p. 28) destaca que "as próprias exposições do *BVerfG* (Tribunal Constitucional Alemão) na decisão sobre o censo populacional tornam evidente que se tratava de acompanhar

organizacional na adoção de medidas para alcance da conformidade[13] ligada à proteção de dados pessoais, no segundo momento da pesquisa adentrar-se-á na questão afeta ao direito à proteção de dados pessoais de crianças e adolescentes que, por meio de um maior adensamento na Doutrina da Proteção Integral, enfatiza a importância em observar a criação de um sistema dinâmico de políticas, procedimentos e controles internos visando sempre adequação à lei para, ao fim e ao cabo, direcionar o estudo em relação ao *compliance* digital no âmbito escolar.

Nas considerações finais destacar-se-á a necessidade do estabelecimento de medidas de segurança adequadas nas instituições educacionais, enaltecendo a sensibilização quanto a temática da proteção de dados de crianças e adolescentes, a preservação da privacidade e a Doutrina da Proteção Integral; mormente, se considerada a previsão constitucional quanto ao dever da família, do Estado e da sociedade, inclua-se, por corolário lógico, organizações e instituições educacionais, em garantir e preservar os direitos daqueles titulares frente aos desafios trazidos pelas tecnologias, sendo o *compliance* digital uma das formas de enfrentamento, de modo que não basta apenas evitar o dano, mas demonstrar o que está sendo adotado para evitá-lo.

2. *Compliance* Digital: conceito e princípios

Originário do verbo em língua inglesa "*to comply*", em tradução para o português significa "cumprir", "executar" ou "agir" consoante com a legislação, regulamentos internos e externos, comandos ou determinadas imposições perante as atividades de uma instituição e/ou organização, o termo "*compliance*" deve ser entendido, então, de forma mais abrangente e sistêmica como um gerenciamento dos riscos dentro de uma instituição, seja pública ou privada, de modo a mitigar e/ou evitá-los, com predominância de relações éticas e transparentes, assim como com

preventivamente, no âmbito do direito, as vastas consequências de um novo tipo de tecnologia – qual seja, o processamento automatizado de dados". Cf. SPIECKER, Indra. O direito à proteção de dados na internet em caso de colisão. Revista Brasileira de Direitos Fundamentais & Justiça, [*s.l.*], v. 12, n. 38, p. 17-33, 2019. DOI: https://doi.org/10.30899/dfj.v12i38.709.

[13] LÓSSIO, 2019, p. 28.

o cumprimento de leis e normas[14] capazes de impulsionar o "*branding valuation*"[15], porquanto ligados à atividade exercida e gestão reputacional.

Desse modo, trata-se, pois, de um sistema geral complexo e organizado que pode ser compreendido como programa de *compliance* ou de integridade, cujas diretrizes para o seu estabelecimento, desenvolvimento e implantação foram primeiramente indicadas pela ISO 19600:201416, que se baseia nos princípios da boa governança, proporcionalidade, transparência e sustentabilidade. A referida ISO foi substituída pela ISO 37301:202117, que estabelece os requisitos para um sistema de gestão de conformidade funcional, erigida sobre uma abordagem do "*risk based approaching*" [18] e baseada nos princípios da integridade, boa governança, proporcionalidade, transparência, responsabilidade e sustentabilidade. É, portanto, uma norma certificável cuja adoção dos programas de *compliance* passou a assumir *status* de exigência mundial a fim de aumentar as responsabilidades de conformidade.

No tocante à segurança da informação, os pilares da ISO 27001/201319 são imprescindíveis para o atendimento da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), enquanto abrange confidencialidade, integridade e disponibilidade, evidenciando o compromisso da instituição para administrar e controlar os riscos de informação. Baseado no entendimento da adoção de padrões, políticas e controles, vislumbra-se a finalidade preventiva do *compliance* que, no contexto da sociedade da informação com coleta, gerenciamento e tratamento de dados pessoais, tem-se como certa e necessária conformação com os regramentos que contém pontos ligados à matéria digital[20], mormente se considerado o contexto atual da utilização

---

[14] Cf. MANZI, Vanessa Alessi. Compliance no Brasil: consolidação e perspectivas. São Paulo: Saint Paul, 2008, p. 15.
[15] Em tradução livre: "valorização da marca".
[16] Conhecida como "ISO *Compliance*".
[17] Designada e publicada pela International Organization for Standardization (ISO) em 13 de abril de 2021.
[18] Em tradução livre: "abordagem baseada em risco".
[19] Publicada primeiramente em 2005 e revisada e atualizada em 2013. O Anexo A da ISO/IEC 27001 está sendo atualizado de acordo com as evoluções do cenário atual para abranger temas como: computação em nuvem, trabalho remoto e privacidade de dados. A ISO 27001 é utilizada em conjunto com a ISO 27002, que fornece orientação quanto a implementação de controles de segurança, valendo o destaque que em fevereiro de 2022 foi publicada a atualização desse padrão.
[20] Considerando que o desenvolvimento tecnológico e suas evoluções demandam a adequação no campo jurídico para responder a situações que podem advir do desequilíbrio de poderes gerados pela

crescente das Tecnologias da Informação e Comunicação (TIC) e suas diversas afetações em relação à pessoa humana, o que redundou na composição de medidas legais de proteção e prevenção, consoante a LGPD.

Após a sanção da LGPD[21], desponta a relevância em se discutir a adoção de programas de *compliance* concernente a questão de comportamentos éticos capazes de estabelecer prioridades quanto ao correto uso dos dados pessoais e promoção da privacidade informacional, o que deve ser encarado de maneira abrangente, diante do contexto de uma economia baseada em dados que utiliza *big data, deep learning, data mining* e suas variadas formas de coleta, análise, vinculação, anonimização e pseudoanonimização das informações; notadamente se considerada a hiperconectividade da sociedade em rede, em que os megadados físicos e digitais são convertidos em informações[22].

Nesse sentido, a proteção de dados tem direta ligação com a preservação da privacidade das pessoas, cuja importância do conhecimento de como proceder para o alcance da prevenção e proteção de direitos fundamentais no contexto do espaço cibernético ou digital é atribuída à constelação principiológica norteadora da adequação jurídico-organizacional[23] na perspectiva da LGPD[24], valendo o destaque da convergência, total ou parcial, com as Diretrizes da OCDE:

I – Princípio da finalidade: define os propósitos para o tratamento de dados pessoais, os quais devem ser legítimos, específicos, explícitos, assim como informados ao titular, restando proibido um tratamento posterior não condizente com as finalidades indicadas ao titular. A legitimidade do propósito equivale ao bom senso, legalidade e boa-fé. A especificidade decorre da preocupação em direcionar o objetivo do tratamento à finalidade indicada. Por sua vez, entende-se como propósitos explícitos aqueles que demonstram de forma inequívoca e delineada, sem qualquer ambiguidade, o conteúdo da finalidade. Esses objetivos devem ser

ubiquidade da computação. Cf. HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital: transformação digital: desafio para o Direito. Rio de Janeiro: Forense, 2021, p. 13.

[21] Vigente a partir de 16 de agosto de 2020, alteração promovida pela Lei n.º 13.853/2019.

[22] LÓSSIO, 2019, op. cit.

[23] A esse respeito, o próprio prefácio do documento "Diretrizes para a Proteção da Privacidade dos Fluxos Transfronteiriços de Dados Pessoais" ressalta a importância dos princípios, diante de sua "clareza e flexibilidade de aplicação e pela formulação, suficientemente ampla para possibilitar a adaptação às mudanças tecnológicas" (OECD, 2022, n.p.).

[24] Também indicados como *Fair Information Privacy Principles* (FIPP).

informados ao titular de dados para que, havendo concordância, delimite o objeto do tratamento. Importante ainda destacar que a alteração da finalidade requer novo consentimento do titular.

II – Princípio da adequação: informa a necessária congruência/compatibilidade do tratamento com as finalidades informadas ao titular, devendo o tratamento ser condizente com a atividade fim para a qual foi destinada, necessitando de um nexo de pertinência (relação) lógica de conformidade do tratamento dos dados com a finalidade e a informação previamente repassada ao titular.

III – Princípio da necessidade da coleta de dados pessoais: a coleta de dados deve ocorrer de forma restritiva, estando o tratamento limitado às finalidades informadas ao titular, abrangendo somente os dados pertinentes, proporcionais e não excessivos. Tal princípio possibilita que, mediante a necessidade, seja realizada uma revisão na estrutura de armazenamento e segurança de informação para fins de adequação à finalidade pretendida, sendo imperiosa sua especificação quanto aos dados imprescindíveis e relevantes para o tratamento, cabendo-se ainda observar a proporcionalidade na manipulação desses dados, para evitar extensão inapropriada em relação ao alcance do tratamento.

IV – Princípio do livre acesso: aos titulares deve ser facilitada gratuitamente a consulta em relação à forma, duração do tratamento e a integralidade de seus dados, o que poderá ocorrer por meio físico ou eletrônico, cujo repasse das informações solicitadas deve ser simplificado e imediato, podendo se dar por meio de declaração completa e clara, com indicação das informações referentes ao tratamento de dados, devendo ocorrer no prazo de até 15 (quinze) dias, a partir da solicitação pelo titular[25].

V – Princípio da qualidade dos dados: os dados pessoais tratados devem ser exatos, relevantes e atualizados, com observância da necessidade e para o cumprimento da finalidade de seu tratamento, com possibilidade de correção daqueles dados incompletos, desatualizados e inexatos, assim como o direito do

[25] Art. 19 da LGPD, Lei n.º 13.709/2018: "A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I – em formato simplificado, imediatamente; ou II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de 15 (quinze) dias, contada da data do requerimento do titular" (BRASIL, 2018, n.p.).

titular a ser informado em relação ao compartilhamento dos dados pelas entidades (públicas ou privadas), sendo-lhe ainda assegurado o não consentimento das alterações[26] e as consequências daí advindas.

VI – Princípio da transparência: aos titulares dos dados pessoais devem ser repassadas informações claras, certas e de fácil acesso acerca do tratamento e os respectivos agentes responsáveis do tratamento, observando-se, contudo, os segredos comercial e industrial. Assim, o titular tem o direito de ser informado ("*Right to be informed*")[27] quanto a coleta, uso e finalidade para o processamento de seus dados, assim como o tempo de retenção e o seu compartilhamento.

VII – Princípio da segurança: para garantir a proteção de dados pessoais devem ser adotadas medidas técnicas e administrativas aptas a protegê-los, de modo que devem ser adotadas atitudes preventivas em relação a possíveis inconsistências quanto a proteção de dados pessoais. Tais medidas devem ser realizadas em todos os momentos (antes, durante e após o tratamento dos dados), demandando atualização e aprimoramento constante, eis que irrelevante que as intercorrências sejam decorrentes de conduta voluntária ou acidental.

VIII – Princípio da prevenção: tem-se nesse princípio a reiteração expressa quanto a importância da adoção de medidas preventivas para evitar danos quando do tratamento de dados pessoais.

IX – Princípio da não discriminação: sendo vedado o tratamento de dados pessoais com finalidade discriminatória, ilícita ou abusiva; e, conquanto não seja especificado o que se pode entender por "tratamento abusivo de dados pessoais", há que se entender pelo manuseio excessivo ou imoderado de dados, ultrapassando a relação lógica do trinômio dado-tratamento-finalidade[28].

---

[26] Art. 8º, parágrafo 6º, da LGPD, Lei n.º 13.709/2018: "Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração" (BRASIL, 2018, n.p.).

[27] Nas palavras de Paul Siehgart (1976, p. 76), o "*right data are used by the right people for the right purposes*". Desse modo, a garantia da autodeterminação informativa da pessoa em exercer o controle em relação aos seus dados pessoais, possibilitando-lhe decidir se a informação a seu respeito poderá ser coletada, usada ou transferida por terceiros.

[28] Cf. PESTANA, Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). CONJUR, 2018. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 20 mai. 2022.

X – Princípio da responsabilização e da prestação de contas: o agente de tratamento de dados pessoais, seja controlador ou operador, deve demonstrar a adoção de medidas eficazes e aptas a comprovar a observância e cumprimento das normas de proteção dos dados pessoais. Tal princípio parte do pressuposto que as medidas adotadas no tratamento de dados estejam em conformidade com os regramentos e preceitos estabelecidos, mormente se considerada a rastreabilidade dos procedimentos e atos praticados, por meio da fiscalização e auditoria pela Autoridade Nacional de Proteção de Dados (ANPD).

A compreensão desses 10 princípios equivale reconhecer o caminho para a conformidade na preservação dos direitos do titular dos dados, sendo parâmetros para determinar a aplicação efetiva do *compliance* digital.

3. O tratamento de dados pessoais de crianças e adolescentes na LGPD: O melhor interesse e o consentimento

A LGPD protege amplamente os dados pessoais, ou seja, toda informação relacionada a pessoa natural identificada ou identificável. Proteção essa aplicável também ao dado pessoal sensível, referente a origem racial ou étnica, convicção religiosa, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

A Lei n.º 13.709/2018 tem por escopo proteger os dados pessoais tratados por qualquer pessoa natural ou jurídica, de direito público ou privado, independente do país de sua sede ou em que estejam localizados os dados, desde que o tratamento de dados seja realizado no território nacional, objetive ofertar ou fornecer bens ou serviços de dados de indivíduos localizados em referido território e nele tenham sido coletados[29]. Esse direito encontra previsão constitucional e se relaciona diretamente com a democracia, reconhecido pelo Supremo Tribunal Federal como direito

[29] Art. 3º da LGPD, Lei n.º 13.709/2018: "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (...)" (BRASIL, 2018, n.p.).

fundamental[30].

Em relação ao tratamento de dados pessoais de crianças e adolescentes, diante do cenário atual de ampliação exponencial do desenvolvimento tecnológico e, considerando que crianças e jovens são os maiores apreciadores do circuito integrado que as novidades tecnológicas e midiáticas proporcionam, os quais vivem praticamente interligados e/ou abraçados aos dispositivos eletrônicos e digitais[31], que, por sua vez, não são recursos neutros e não propiciam a necessária confiabilidade e segurança da informação coletada, mormente diante da capacidade em propagar variados efeitos na conexão em redes informatizadas, fazendo com que as vidas privadas sejam rastreadas e monetizadas por plataformas digitais cujas atividades e interesses não são transparentes, a LGPD reservou capítulo especial quanto à proteção de dados pessoais desses titulares, trazendo o princípio do melhor interesse das crianças e adolescentes[32] em relação ao uso, coleta e tratamento de seus dados pessoais, primando de maneira absoluta para sua proteção, de modo que nem mesmo o poder familiar, a Administração Pública ou qualquer outra atividade possa se sobrepor àquele princípio.

O princípio do melhor interesse é uma consequência da Doutrina da Proteção Integral[33], acompanhando a lógica protetiva do Estatuto da Criança e do Adolescente (ECA) — Lei n.º 8.069, de 13 de julho de 1990[34]. Não é demais lembrar que em relação à referida Doutrina, no plano internacional, tem-se a Convenção Internacional sobre

[30] Cf. MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. JOTA, 10 mai. 2020, 09h36m. Disponível em:<https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dadospessoais-10052020>. Acesso em: 20 mai. 2022.

[31] Cf. SIBILIA, Paula. Rede ou paredes: a escola em tempos de dispersão. Tradução Vera Ribeiro. Rio de Janeiro: Contraponto, 2012.

[32] Art. 14 da LGPD, Lei n.º 13.709/2018: "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente" (BRASIL, 2018, n.p.).

[33] Para Bruno Ricardo Bioni e Maria Luciano (2021, p. 150), o melhor interesse é visto como uma regra jurídica e não como princípio, não estando sujeita "à mitigação ou atenuação em casos de colisão com os direitos fundamentais de outros indivíduos ou mesmo coletividades".

[34] Cf. BRASIL. Lei n.º 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União de 16.7.1990, retificado em 27.9.1990. Brasília, DF: 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 16 ago. 2022.

os Direitos da Criança[35], de 1989; as Regras Mínimas das Nações Unidas para a Administração dos Direitos dos Menores — Regras de Beijing, de 1985; Regras das Nações Unidas para a Proteção dos Menores Privados de Liberdade, de 1990; Diretrizes das Nações Unidas para a Prevenção da Delinquência Juvenil — Diretrizes de Riad, de 1990; Regras Mínimas das Nações Unidas para a elaboração de Medidas Não-Privativas de Liberdade e Regras de Tóquio, ambas de 1990[36].

Registre-se, por oportuno, que diante da necessária observância à Convenção Internacional sobre os Direitos da Criança, com fins de ressaltar as imposições e realidades do mundo digital, foi produzido pelo Comitê dos Direitos da Criança da Organização das Nações Unidas (ONU), o Comentário Geral n.º 25, em 2021, que detalha normativamente como aplicar a Convenção, interpretando-a em relação ao ambiente digital, assim como especifica os direitos e o que corresponde ao melhor interesse das crianças e adolescentes frente às particularidades desse ambiente pan-óptico[37].

No âmbito nacional, a Doutrina da Proteção Integral foi inaugurada pela Constituição Federal que, fundamentada no princípio da Dignidade da Pessoa Humana, trouxe o reconhecimento quanto a ser criança e adolescente como prioridade absoluta e detentores de direitos e garantias fundamentais[38], ganhando

---

[35] Cf. MÉNDEZ, Emílio Garcia. Adolescentes e Responsabilidade Penal: um debate latino-americano. Por uma reflexão sobre o Arbítrio e o Garantismo na Jurisdição Socioeducativa. Porto Alegre: AJURIS; Escola Superior do Ministério Público; FESDEP, 2000, p. 7-10.

[36] Para Gabrielle Bezerra Sales e Ana Paula Motta Costa (2021, n.p.), ocorrera a "consolidação na legislação internacional, com influência gradativa nas Constituições dos vários países, da 'Doutrina das Nações Unidas de Proteção Integral à Criança'".

[37] Mendes, 2020, op. cit.

[38] Ao mencionar sobre a consolidação dos direitos da criança e do adolescente no texto constitucional, Olympio de Sá Sotto Maior Neto (apud MELO, 2021, n.p.) faz a seguinte colocação a respeito do art. 227 da CF/88: "Esse texto absorve o preconizado na doutrina da proteção integral, cuja tese fundamental é no sentido de que cabe à lei assegurar às crianças e aos adolescentes a possibilidade de exercício de seus direitos fundamentais. Esse conceito, base teórica para todos os documentos e tratados internacionais da área, deu suporte também à Convenção Internacional dos Direitos da Criança e do Adolescente, que estava sendo elaborada na mesma época pela Organização das Nações Unidas (ONU). Por isso, o artigo 227 da CF prevê que 'é dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão'. Com isso, indica quais são os direitos fundamentais da infância e juventude. Então, o que faltava no Código de Menores passa a ser assegurado na Carta Magna.".

expressividade posterior com o ECA[39] e quando ratificado pelo Congresso Nacional a Convenção Internacional.

Em razão da situação peculiar das crianças e adolescentes, a LGPD impôs requisitos específicos para todo e qualquer tratamento de dados pessoais desses titulares, cuja proteção deve garantir-lhes absoluta prioridade, direitos previstos no sistema jurídico, promoção da dignidade, bem como convergência com os princípios gerais enunciados pela legislação, motivo da necessidade do tratamento dos dados exigir o consentimento específico e, em destaque, dado por pelo menos um dos pais ou responsável legal, em razão da condição específica de pessoa em desenvolvimento, evidenciando seu melhor interesse e proteção integral e diferenciada, permitindo a identificação da similitude de proteção com os dados sensíveis[40].

Concernente ao consentimento para o tratamento dos dados de crianças[41], devem ser adotadas as mesmas exigências referentes aos dados pessoais sensíveis, consolidando-se, ainda, a necessidade de uma manifestação específica, livre, informada e destacada para determinada finalidade, de modo a evidenciar a transparência quanto ao consentimento.

Sobreleva ressaltar uma aparente dicotomia em relação ao consentimento do tratamento de dados de adolescentes, na medida em que a legislação não menciona a necessidade do consentimento específico e destacado dos pais e/ou responsáveis, o que, contudo, não retira a obrigação quanto ao tratamento ocorrer com base no "melhor interesse" para garantir a integralidade dos direitos desses titulares, demandando interpretação do dispositivo em referência com a Constituição Federal e o Código Civil, mormente se considerada a estruturação do sistema de capacidade dessa última legislação que estabelece a necessária representação pelos

[39] Art. 4º do ECA, Lei n.º 8.069/1990: "É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária" (BRASIL, 1990, n.p.).

[40] Cf. SARLET, Gabrielle Bezerra Sales; COSTA, Ana Paula Motta. A perspectiva da proteção de dados pessoais em face dos direitos das crianças e adolescentes no sistema normativo brasileiro. *In*: REDECKER, Ana Cláudia *et al*. (Coord.). Proteção de Dados: temas controvertidos. Indaiatuba: Editora Foco, 2021. E-book.

[41] De acordo com o art. 2º do ECA, Lei n.º 8.069/1990, "Considera-se criança, para os efeitos desta Lei, a pessoa de até 12 anos incompletos, e adolescente aquela entre doze e dezoito anos de idade" (BRASIL, 1990, n.p.).

responsáveis desses titulares até os 16 (dezesseis) anos, e, após, até os 18 (dezoito) anos, o fato de serem assistidos, o que por certo, dirime a dúvida quanto ao consentimento[42].

Em suma, tais explanações permitem interpretar que até os 16 (dezesseis) anos de idade há necessidade de um consentimento expresso, específico e destacado pelos responsáveis legais das crianças e adolescentes e, dos 16 (dezesseis) aos 18 (dezoito) anos, deverá haver o consentimento de ambos e não apenas do responsável.

É oportuno evidenciar que a redação do art. 14, parágrafo 1.º, da LGPD foi inspirada no art. 8º da *General Data Protection Regulation* (GPDR), a qual estabelece a obrigatoriedade do consentimento parental até os 16 (dezesseis) anos para o tratamento de dados pessoais de crianças e adolescentes, todavia, possibilita que os Estados Membros da União Europeia estipulem, por lei, idade inferior para tratamento dos dados pessoais sem autorização do responsável legal, apenas limitando essa exigência a 13 (treze) anos de idade. Diante disso, vislumbra-se a proximidade com o texto da LGPD.

Portanto, a Doutrina da Proteção Integral e o melhor interesse são anteparos capazes de justificar uma maior preocupação no tratamento de dados de crianças e adolescentes, notadamente se considerado o arcabouço jurídico-normativo internacional e nacional que emoldura a prioridade absoluta da proteção e promoção dos direitos de referidos titulares, o que demanda ampla discussão e interpretação rigorosa e transversal sobre o passado, presente e futuro daqueles que se encontram em uma peculiar situação, seres em formação, cabendo ao Estado, à sociedade e à família garantir-lhes segurança em qualquer ambiente. Assim sendo, não se olvide da posição diferenciada e emblemática que o consentimento assume, de modo que não deve ser em hipótese alguma negligenciado, mormente se considerado os fundamentos indicados na LGPD em relação aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

---

[42] Em sentido contrário, Viviane Maldonado Nóbrega e Renato Opice Blum (2019, p. 209) apontam a limitação textual do parágrafo 1.º do art. 14 da LGPD, Lei n.º 13.709/2018, porquanto bastar o "consentimento ordinário" para os titulares a partir dos 13 anos.

Nesse sentido, são nesses aspecto que a LGPD enuncia caber ao controlador dos dados pessoais verificar se o consentimento foi dado pelo responsável ou por ambos, assim como dar conhecimento acerca dos tipos de dados coletados, como serão utilizados e os procedimentos para o exercício dos direitos nessa seara, valendo destacar a impossibilidade de condicionar a participação dos titulares dos dados pessoais em jogos, aplicações de internet e atividades outras que demandam o fornecimento de informações que não as estritamente necessárias à atividade[43], na medida em que o objetivo maior do consentimento é garantir que o tratamento de dados somente ocorra se for consentido.

Entrementes, conquanto deva prevalecer o melhor interesse da criança, não se olvide que a indispensabilidade do consentimento é aplicável ao tratamento de dados pessoais de crianças e adolescentes nas hipóteses enunciadas na legislação[44].

4. Desafios da implementação do *compliance* digital nas escolas: mudança de cultura e de educação digital

Partindo da ideia da ampliação exponencial do desenvolvimento tecnológico, inclusive em relação à Educação Escolar, já que os padrões geracionais exigem constante adaptação[45], cujos limites podem ser definidos pelas *affordances*[46] de

[43] Vide redação do art. 14, parágrafo 4º, da LGPD, Lei n.º 13.709/2018, em consonância com a Resolução n.º 163, de 13 de março de 2014, do Conselho dos Direitos da Criança e do Adolescente (CONANDA), que dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Cf. CONANDA. Resolução n.º 163, de 13 de março de 2014. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Diário Oficial da União n. 65, de 04.04.2014, Seção 1, p. 4. Brasília, DF: 2014. Disponível em: <https://crianca.mppr.mp.br/pagina-1635.html#resolucao_163>. Acesso em: 16 ago. 2022.

[44] Cf. Art. 11, II, da LGPD, Lei n.º 13.709/2018 (BRASIL, 2018).

[45] Cf. JONES, Chris. Students, the net generation, and digital natives: accounting for educational change. *In*: THOMAS, Michael. Deconstructing digital natives: young people, technology and the new literacies. New York: Routledge, 2011, p. 30-48.

[46] A Teoria das *Affordances* foi desenvolvida por James Gibson (1986) no livro *The ecological approach to visual perception*, cujo termo "*affordance*" foi definido, no contexto da Ecologia, como sendo aquilo que o meio ambiente fornece aos seres vivos, independentemente de sua utilização para o bem ou o mal. Seguindo a extensão de tal conceito, entende-se como sendo as diversas percepções de utilização/uso de um determinado objeto. E, para melhor utilização do termo, partindo da observação de Dong-Hee Shin (2017, p. 1828. Tradução livre), de que as "*Affordances* devem ser adequadamente percebidas pelo usuário para que se reconheça o potencial de ação", de modo que determinado objeto poderá ser utilizado dependendo das percepções de suas *affordances,* sejam elas

ferramentas digitais, com base na utilização de *softwares* direcionados a atender ao direito fundamental da Educação e, sendo certo que o tema da proteção de dados pessoais está na agenda do dia, mormente se considerado o aumento das ferramentas tecnológicas educacionais impostas pela urgência do momento ocasionado pela pandemia causada pelo vírus Sars-Cov-2 (Covid-19)[47] e a vigência da LGPD, foram impulsionadas discussões quanto a adoção de um programa de *compliance* digital direcionado ao contexto educacional, uma vez que o uso de dados pessoais se mostra fundamental para uma adequada prestação dos serviços neste setor.

No âmbito educacional a prestação de serviços requer constante tratamento de dados pessoais de alunos (as), professores (as), pais e mães ou responsáveis legais, assim como corpo técnico envolvido com o sistema. Tendo em vista que tais dados e informações privadas e pessoais são importante produção de conhecimento da comunidade escolar, como as coletadas pelo Censo Escolar anual do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INPE)[48] com dados sobre o perfil dos alunos (as), é certa a necessidade de haver uma proteção e correta administração desses dados para evitar violações aos direitos fundamentais do titular, mormente se considerado que estes, em sua grande maioria, são menos ciente dos riscos, consequências e cautelas relacionados ao uso dos seus dados.

Para melhor identificação da preocupação em relação ao tratamento de dados pessoais de crianças e adolescentes, já que qualquer operação como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

---

qualitativa ou quantitativamente. Cf. BROCH, José Carlos. O conceito de affordance como estratégia generativa no design de produtos orientado para a versatilidade. 2010. 100 f. Dissertação (Mestrado em Design e Tecnologia) – Programa de Pós-graduação em Design, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/25510/000752864.pdf>. Acesso em: 16 ago. 2022.

[47] Cf. LEAL, Kariny. Big Techs superam estimativas de balanços e consolidam crescimento durante a pandemia. Forbes, 30 abr. 2021. Disponível em: <https://forbes.com.br/forbes-money/2021/04/big-techs-superam-stimativas-de-balancos-e-consolidam-crescimento-durante-a-pandemia>. Acesso em: 20 abr. 2022.

[48] Autarquia Federal vinculada ao Ministério da Educação (MEC) responsável pelas evidências educacionais, atuando nas áreas de avaliações e exames educacionais, pesquisas estatísticas e indicadores educacionais, assim como gestão do conhecimento e estudos educacionais. Cf. INEP. Institucional > Sobre. Gov.br, 01 jul. 2022. Disponível em: <https://www.gov.br/inep/pt-br/acesso-a-informacao/institucional/sobre>. Acesso em: 16 ago. 2022.

distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração são ações consideradas tratamento de dados, as quais, diga-se, não se relacionam apenas ao uso no formato digital, mas também engloba o formato físico/analógico na identificação dos dados abrangidos.

Nesse contexto, exemplifica-se: identidade, histórico escolar, informações médicas, telefone, endereço, e-mail, registro de aluno, carteira estudantil, Número de Identificação Social (NIS), indicadores de performance escolar, gravações de imagens geradas por uso de aplicativos educacionais ou câmeras de segurança, coleta do IP do dispositivo móvel utilizado, *cookies*[49] e até mesmo a voz. Por sua vez, identificam-se como dados sensíveis, abrangidos no ambiente escolar, dentre outros: informações médicas, religião, dados biométricos e imagens, sendo estas consideradas dados sensíveis quando houver inferência sobre cor/raça e outros dados cuja utilização abusiva permite práticas discriminatórias.

Proporcionalmente ao aumento dos dados pessoais incluídos no setor educacional, premente a adoção de medidas de segurança, procedimentos e boas práticas direcionadas ao *compliance* digital, aptas a garantir a privacidade e proteção de dados, devendo-se atentar para as finalidades de utilização de tais informações, o que perpassa, necessariamente, em observar as hipóteses [50] (bases legais) indicadas pela LGPD que autorizam o tratamento de dados, as quais se diferenciam conforme o tipo de informação/dado, cabendo ao gestor educacional identificar as bases legais aplicáveis, o que implica dizer que, não obstante, se considere tais parâmetros gerais, inexistem aplicações específicas destinadas ao setor educacional, entrementes, há que se considerar a primazia do direito à Educação, levando ao entendimento de que quando certas situações assim o exigirem, tal como um dever legal para o tratamento de dados, é prescindível o consentimento[51].

O consentimento deve ocorrer de maneira livre, informada e inequívoca, sendo

[49] Geralmente a utilização de *cookies* envolve a coleta de dados pessoais capazes de identificar ou que possa vir a identificar um indivíduo.
[50] Artigos 7.º e 11 da LGPD, Lei n.º 13.709/2018 (BRASIL, 2018).
[51] Nesse sentido, cita-se a obrigatoriedade do Poder Público quanto ao recenseamento de educandos no Ensino Fundamental, chamada e zelar pela frequência escolar (art. 208, § 3º, da Constituição Federal); Censo escolar do INEP; Políticas Assistenciais e aquelas relacionadas ao transporte escolar, dentre outras (BRASIL, 1988).

uma base legal subsidiária/secundária por demandar análise preliminar das demais, assim como perscrutar o tipo de dado a ser fornecido, já que envolvendo dado sensível, mister o consentimento de um dos pais ou responsável legal até os 16 anos de idade, ou dos 16 aos 18 anos, com o consentimento de ambos, tais como casos de biometria, fotos em redes sociais e sítio eletrônico da escola[52].

Assinale-se, outrossim, ser desnecessário o consentimento parental quando houver necessidade de contatar os pais ou responsável legal, cujos dados deverão ser utilizados uma única vez e sem armazenamento ou quando para proteção da criança, estando vedado, em qualquer hipótese, repasse dessas informações a terceiro, situação que evidencia a consonância com o ECA diante do dever de assegurar com prioridade absoluta os direitos das crianças e adolescentes.

Quanto ao legítimo interesse[53], por ser a mais genérica das bases legais, é inaplicável à hipótese dos dados pessoais sensíveis, pois, conquanto se observe sua aplicação para situações concretas relacionadas ao apoio, promoção de atividades do controlador, proteção de direitos do titular e prestação de serviços que o beneficiem, é necessário que o tratamento de dados seja direcionado para atividades diárias.

Destaque-se, ainda, a necessidade de haver um canal de interação para viabilizar o exercício dos direitos do titular de dados, de modo a repassar informações sobre dados coletados, local de armazenamento, finalidade na utilização no processo educacional, tempo de armazenamento (temporalidade), compartilhamento dos dados e com quais entidades públicas e/ou privadas[54], bem como garantir o acesso ao titular, pais ou responsável legal, correção de dados incompletos, inexatos ou desatualizados[55], resguardar o direito de anonimização[56], bloqueio e eliminação de dados desnecessários, excessivo ou tratados em

---

[52] Cf. BORELLI, Alessandra. É pra já! A proteção de dados de crianças e adolescentes não pode esperar. São Paulo: OPEE Educação, 2020. Disponível em: <https://opee.com.br/wp-content/pra-ja%CC%81-18-agosto-FINAL.pdf>. Acesso em: 25 mai. 2022.

[53] Art. 10 da LGPD, Lei n.º 13.709/2018 (BRASIL, 2018).

[54] O compartilhamento, seja com entidades públicas ou privadas, deve almejar o interesse público e sob uma justificativa lícita e legítima. Com o poder público decorre de obrigação legal ou para execução de políticas públicas. Com o setor privado, para execução de políticas públicas ou com o consentimento dos titulares.

[55] Art. 18 da LGPD, Lei n.º 13.709/2018 (BRASIL, 2018).

[56] Nessa hipótese, deve-se certificar que a técnica aplicada foi capaz de não mais revelar a identidade do titular, de modo a deixar de ser um dado pessoal.

desacordo com a legislação, devendo-se ainda possibilitar o direito à portabilidade[57], eliminar dados tratados com base no consentimento quando solicitado pelo titular, assim como lhe informar sobre a possibilidade de não oferecer consentimento ou o direito de sua revogação e revisão das decisões automatizadas. Para tanto, mister uma estruturação (técnica ou de comunicação) adequada e capaz de permitir respostas de imediato ou em até 15 (quinze) dias da data da solicitação.

E, por ser a coleta de dados uma atividade diária no meio escolar, premente a adoção de práticas capazes de salvaguardar e garantir a segurança das informações, o que perpassa pela elaboração de um eficiente e personalizado programa de adequação de política interna de controle de acessos (restrição) e de segurança de dados, com abrangência de questões relativas à retenção dos dados com indicação dos períodos[58] de armazenamento para cada tipo de informação, evitando-se, assim, a utilização indevida, devendo ainda haver conscientização do corpo técnico e colaboradores com abordagens educacionais sobre o tema da privacidade e proteção de dados pessoais, e ainda elaboração de Relatórios de Impactos de Proteção de Dados[59] com avaliação do uso das ferramentas disponíveis no ambiente escolar e medidas de mitigação, não se olvidando da obrigatória elaboração de planos de resposta a incidentes com dados e indicação de remediação[60] (gestão de crise).

Frisa-se, ademais, que a criação de uma estrutura de governança em proteção de dados pessoais requer a disponibilização da Política de Privacidade aos titulares e/ou familiares e responsáveis, com enunciação dos impactos da utilização desses dados, a finalidade, ciclo de vida (temporalidade), graus de precaução, informação quanto a criação de perfis para acompanhamento pedagógico, existência de tratamento automatizado (se houver), medida essa que demonstra a procura pela

[57] Necessário formato interoperável para facilitar a comunicação e utilização por novo controlador, o que demanda padrões e linguagens passíveis de comunicação com tecnologias diversificadas. Observando-se, ainda, que dados anonimizados não são incluídos na portabilidade.
[58] Inexiste parâmetro capaz de identificar objetivamente o tempo de armazenamento dos dados, de modo a caber à instituição (pública ou privada) a justificativa quanto ao motivo, observando-se, contudo, a finalidade e a natureza da informação. Cf. CNIL. La vidéosurveillance – vidéoprotection dans les établissements scolaires. CNIL, 03 dez. 2019. Disponível em: <https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaire>. Acesso em: 25 mai. 2022.
[59] Art. 38 da LGPD, Lei n.º 13.709/2018 (BRASIL, 2018).
[60] Art. 50, parágrafo 2º, "g", da LGPD, Lei n.º 13.709/2018 (BRASIL, 2018).

integridade da instituição escolar e enuncia um compromisso permanente com a privacidade e proteção de dados.

Diante do grande fluxo de dados pessoais em um ambiente escolar, mostra-se ideal a utilização de ferramentas direcionadas ao atingimento dos objetivos relacionados a salvaguarda da privacidade e proteção de dados, sendo o *compliance* digital importante, significativa e transformadora ferramenta de regulação capaz de minimizar riscos e possibilitar maior compreensão acerca do funcionamento das tecnologias e/ou ferramentas de comunicação na sociedade informacional.

Importa registrar, contudo, que no contexto do ambiente digital não há como se garantir a segurança plena, porquanto inexistir segurança absoluta e risco zero na realidade tecnológica, uma vez que as redes se mantêm instável a todo momento, bem como pelo fato de sempre surgirem novos ataques no ciberespaço, impossibilitando identificar com acurácia as vulnerabilidades[61], o que, de qualquer forma, confirma a necessidade da constante busca pela boa governança e gestão de riscos.

5. Considerações finais

A perspectiva universalizante da LGPD direcionada à proteção de dados pessoais engloba os direitos das crianças e adolescentes, cuja interpretação perpassa pela intersecção dos demais conjuntos normativos relacionados a esse contingente em estágio de desenvolvimento que, em razão de suas peculiaridades, justifica um tratamento especial dentro e fora do ambiente digital.

Diante do grande fluxo de informações no ambiente educacional, urge a adoção de uma Educação que considere não somente o aspecto pedagógico, mas todo o contexto do meio digital em que está compulsoriamente inserida, eis que certo ser a proteção de dados essencial para assegurar a manutenção do direito fundamental à Educação, o que, seja qual for o âmbito, necessita de um processo de educação digital que enfatize a mudança de comportamento aliada a valores éticos e morais capazes de proporcionar uma evolução naquele ambiente e garantir o

[61] Cf. COHEN, Fred. Dr. Fred Cohen, 2022. Disponível em: <http://fc0.co/>. Acesso em: 23 mai. 2022.

direito fundamental de liberdade, privacidade e de personalidade das crianças e adolescentes.

Desse modo, com os desafios impostos pela LGPD, tem-se a possibilidade de criar relações transparentes e um canal de comunicação permanente com os envolvidos, por isso premente a adoção de técnicas de segurança da informação e reestruturação organizacional no sentido de observar a legislação, a boa governança e a tecnologia da informação[62] no ambiente educacional, priorizando a transparência e ética digital, para, consequentemente, garantir um tratamento de dados adequado e em conformidade com as legislações concernentes às questões de segurança no ambiente cibernético e aos padrões ISO internacionais, sendo o *compliance* digital a medida adequada para esse desiderato, de modo a expandir a cultura de proteção de dados das crianças e adolescentes no ambiente escolar, sempre com a observância quanto ao tratamento de dados ocorrer no melhor interesse destes seres em formação.

Referências bibliográficas

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel *et al*. **Tratado de proteção de dados pessoais**. São Paulo: Forense: 2021, p. 149-162.

BORELLI, Alessandra. **É pra já! A proteção de dados de crianças e adolescentes não pode esperar**. São Paulo: OPEE Educação, 2020. Disponível em: <https://opee.com.br/wp-content/uploads/2020/08/E%CC%81-pra-ja%CC%81-18-agosto-FINAL.pdf>. Acesso em: 25 mai. 2022.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União de 05.10.1988. Brasília, DF: 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 16 ago. 2022.

BRASIL. **Lei n.º 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União de 16.7.1990, retificado em 27.9.1990. Brasília, DF: 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 16 ago. 2022.

[62] LÓSSIO, 2019, op. cit.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União de 24.4.2014. Brasília, DF: 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 ago. 2022.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União de 15.8.2018, republicado parcialmente em 15.8.2018 - Edição extra. Brasília, DF: 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.>. Acesso em: 16 ago. 2022.

BROCH, José Carlos. **O conceito de affordance como estratégia generativa no design de produtos orientado para a versatilidade**. 2010. 100 f. Dissertação (Mestrado em Design e Tecnologia) – Programa de Pós-graduação em Design, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/25510/000752864.pdf.> Acesso em: 16 ago. 2022.

CNIL. La vidéosurveillance – vidéoprotection dans les établissements scolaires. **CNIL**, 03 dez. 2019. Disponível em: <https://www.cnil.fr/fr/la-videosurveillance-videoprotection-dans-les-etablissements-scolaire.>. Acesso em: 25 mai. 2022.

COHEN, Fred. **Dr. Fred Cohen**, 2022. Disponível em:<http://fc0.co/>. Acesso em: 23 mai. 2022.

CONANDA. **Resolução n.º 163, de 13 de março de 2014**. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Diário Oficial da União n. 65, de 04.04.2014, Seção 1, p. 4. Brasília, DF: 2014. Disponível em: <https://crianca.mppr.mp.br/pagina-1635.html#resolucao_163>. Acesso em: 16 ago. 2022.

GIBSON, James. **The ecological approach to visual perception**. New York: Psychology Press, 1986.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**: transformação digital: desafio para o Direito. Rio de Janeiro: Forense, 2021.

INEP. Institucional > Sobre. **Gov.br**, 01 jul. 2022. Disponível em: <https://www.gov.br/inep/pt-br/acesso-a-informacao/institucional/sobre.> Acesso em: 16 ago. 2022.

JONES, Chris. Students, the net generation, and digital natives: accounting for educational change. *In*: THOMAS, Michael. **Deconstructing digital natives**: young people, technology and the new literacies. New York: Routledge, 2011, p. 30-48.

LEAL, Kariny. Big Techs superam estimativas de balanços e consolidam crescimento durante a pandemia. **Forbes**, 30 abr. 2021. Disponível em: <https://forbes.com.br/forbes-money/2021/04/big-techs-superam-stimativas-de-balancos-e-consolidam-crescimento-durante-a-pandemia>. Acesso em: 20 abr. 2022.

LÓSSIO, Claudio Joel Brito. **Proteção de Dados e Compliance Digital**. São Paulo: Almedina, 2021.

MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **JOTA**, 10 mai. 2020, 09h36m. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dadospessoais-10052020>. Acesso em: 20 mai. 2022.

MÉNDEZ, Emílio Garcia. **Adolescentes e Responsabilidade Penal**: um debate latino-americano. Por uma reflexão sobre o Arbítrio e o Garantismo na Jurisdição Socioeducativa. Porto Alegre: AJURIS; Escola Superior do Ministério Público; FESDEP, 2000.

MELO, Ana Paula Branco de. Uma breve jornada dos direitos da criança e do adolescente e o MPPR: história, conquistas, COVID-19. **Memorial - MPPR**, 15 out. 2021. Disponível em: <https://memorial.mppr.mp.br/modules/conteudo/conteudo.php?conteudo=279>. Acesso em: 16 ago. 2022.

NATARAJAN, Aishwarya; RINKE, Franziska; WEISE, Sebastian. Dawn of a new era of global data protection?. **Völkerrechtsblog**, 02.03.2021. DOI: 10.17176/20210302-153629-0

NÓBREGA, Viviane Maldonado; OPICE BLUM, Renato (Coord.). **LGPD — Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, 2019.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. **OECD**, 2022. Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyand%20transborderflowsofpersonaldata.htm>. Acesso em: 20 mai. 2022.

PESTANA, Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). **CONJUR**, 2018. Disponível em:<https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 20 mai. 2022.

SARLET, Gabrielle Bezerra Sales; COSTA, Ana Paula Motta. A perspectiva da proteção de dados pessoais em face dos direitos das crianças e adolescentes no sistema normativo brasileiro. *In*: REDECKER, Ana Cláudia *et al.* (Coord.). **Proteção de Dados**: temas controvertidos. Indaiatuba: Editora Foco, 2021. E-book.

SHIN, Dong-Hee. The role of affordance in the experience of virtual reality learning: Technological and affective affordances in virtual reality. **Telematics and Informatics**, [*s.l.*], v. 34, n. 8, p. 1826-1836, 2017. DOI: https://doi.org/10.1016/j.tele.2017.05.013.

SIBILIA, Paula. **Rede ou paredes**: a escola em tempos de dispersão. Tradução Vera Ribeiro. Rio de Janeiro: Contraponto, 2012.

SIEHGART, Paul. **Privacy and Computer**. Londres: Latimer, 1976.

SPIECKER, Indra. Wissensverarbeitung in Öffentlichen Recht. **Rechtswissenschaft**, [*s.l.*], n.3, p. 247-282, jan. 2010. DOI: https://doi.org/10.5771/1868-8098-2010-3-247.

SPIECKER, Indra. O direito à proteção de dados na internet em caso de colisão. **Revista Brasileira de Direitos Fundamentais & Justiça**, [*s.l.*], v. 12, n. 38, p. 17-33, 2019. DOI: https://doi.org/10.30899/dfj.v12i38.709.

UNCTAD. Data Protection and Privacy Legislation Worldwide. **UNCTAD**, 2022. Disponível em:<https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>. Acesso em: 22 mai. 2022.

3. O DIREITO À DESINDEXAÇÃO À LUZ DA PROTEÇÃO DOS DADOS PESSOAIS

https://doi.org/10.36592/9786581110994-03

Ana Luiza Liz dos Santos[1]

Sumário

1. Introdução. 2. As bases para a proteção de dados pessoais no Brasil e o seu reconhecimento como direito fundamental 3. O estado da arte do direito à desindexação no ordenamento jurídico brasileiro 4. A proteção de dados pessoais como fundamento do direito à desindexação 5. Considerações Finais. Referências bibliográficas.

1. Introdução

O advento da Era Digital e da Sociedade da Informação, baseados no superinformacionismo, tem promovido significativas transformações nas relações pessoais e institucionais, tornando-as mais complexas. Por decorrência disso, surge a postulação de uma necessária transformação também do Direito.

Nesse cenário, a partir da capacidade cada vez mais crescente de um acúmulo infindável de informações sobre tudo e sobre todos, em um ambiente social de verdadeiro superinformacionismo, surgiu a necessidade de ampliação do tradicional conceito de privacidade. Com o passar do tempo, contudo, as demandas passaram a suplicar o desenvolvimento de novos e distintos direitos, não sendo suficiente, pois, a ampliação do escopo compreendido pelo direito à privacidade.

Efetivamente, no ambiente virtual, em específico, tornou-se manifesta a necessidade de desenvolvimento de mecanismos aptos a tutelar os dados pessoais, a partir, inclusive, da elaboração de um adequado sistema de gestão destas informações, de modo a garantir a consolidação da dignidade da pessoa humana, do

[1] Mestre em Direito pela FMP-RS. Especialista em Direito Público pela PUC-RS. Especialista em Direito Civil e Processo Civil pelo IDC. Aluna do LLM em Proteção de Dados: LGPD e GDPR - Curso Binacional com dupla titulação (FMP-RS e Faculdade de Direito da Universidade de Lisboa). Graduada em Direito pela PUC-RS. Assessora Jurídica no Tribunal de Justiça do Estado do Rio Grande do Sul. Currículo Lattes: http://lattes.cnpq.br/1213105149446784. E-mail: analuizaliz.s@hotmail.com.

livre desenvolvimento da personalidade, da proteção dos dados pessoais, da autodeterminação informativa e, ainda, de outras liberdades individuais.

Para todos estes direitos, a partir de um viés mais específico, os dados pessoais atuam em posição de centralidade, sendo tutelados, por isso, de forma cada vez mais enfática pelos principais ordenamentos jurídico-constitucionais ao redor do mundo. O Brasil, felizmente, também tem caminhado neste sentido. A bem da verdade, em que pese o caráter inaugural e inovador exposto em alguns ordenamentos jurídicos, bem como o certo retardo de outros, fato é que nunca antes esta temática foi tão protagonista como agora.

O direito à desindexação, que tem sua origem fortemente associada ao desenvolvimento tecnológico, assume também a atenção do pensamento jurídico na temática da proteção de dados pessoais. Trata-se de um direito que objetiva a possibilidade de bloqueio nas ferramentas de pesquisa que estão disponíveis na internet, com vistas, ao final, à tutela dos direitos associados à privacidade, à autodeterminação informativa e, especialmente, à proteção dos dados pessoais.

É neste contexto, pois, que está inserida a problemática da presente investigação, a qual se propõe a estudar a possibilidade de realização do direito à desindexação sob o fundamento do direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro. A atualidade do problema e a sua necessidade de resolução justificam a presente pesquisa, uma vez que, por meio do direito à desindexação, consolida-se mais uma possibilidade de tutela do direito fundamental à proteção de dados pessoais, especialmente quando este é considerado à luz do superinformacionismo e da Era Digital.

Para tanto, o estudo se desenvolve em três capítulos, cuja abordagem é formulada a partir do método hipotético-dedutivo, tomando por base a utilização de material bibliográfico, jurisprudencial e legislativo para fundamentar sua essência e construir seu arrazoado.

Por estas considerações, o presente ensaio se propõe, em um primeiro momento, a fazer um breve apanhado sobre as bases para a proteção dos dados pessoais no Brasil, a partir, especialmente, da promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), bem assim e, sobretudo, do seu reconhecimento como direito fundamental expressamente positivado no texto da Constituição

Federal, a partir da Emenda Constitucional nº 115/2022. Na sequência, objetiva adentrar no estudo específico do direito à desindexação, a partir da análise do estado da arte deste instituto no ordenamento jurídico brasileiro. Ao final, pretende analisar o direito à proteção de dados pessoais como um fundamento específico para concretização do direito à desindexação, mormente no contexto que decorre do superinformacionismo da Era Digital e da Sociedade da Informação.

2. As bases para a proteção de dados pessoais no Brasil e o seu reconhecimento como direito fundamental

O sistema jurídico da proteção de dados pessoais vem sendo desenvolvido, ao redor do mundo, há pelo menos cinco décadas. Sua origem, como tal, no início dos anos 1970, está relacionada com o crescimento exponencial do tratamento de dados dos cidadãos, primeiro pelos órgãos estatais, e logo em seguida também pelas instituições privadas.

A primeira legislação específica envolvendo a temática data de 1970, quando foi concebida a *Hessisches Datenschutzgesetz* no *land* alemão de Hesse. A partir daquele momento, cada vez mais passaram a ser desenvolvidos leis e regramentos sobre a proteção dos dados pessoais, os quais, também cada vez mais, foram sendo aperfeiçoados em termos de abrangência e eficácia.

No Brasil, a introdução da expressão "proteção de dados pessoais" é consideravelmente recente, mas sua essência, por certo, não é nova. Quer dizer, questões que hoje são diretamente associadas à proteção de dados pessoais, não eram estranhas à práxis jurídica brasileira, uma vez que eram relacionadas a questões referentes ao direito à privacidade e aos direitos dos consumidores, além de outras liberdades individuais[2].

Tem-se, assim, que os direitos hoje associados diretamente à noção de proteção de dados pessoais não eram, de qualquer forma, desprotegidos. Sua tutela era fundamentada, especialmente, a partir do texto constitucional, bem assim do

[2] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel *et al.* (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 10.

Código de Defesa do Consumidor[3], da Lei do Habeas Data[4], do Código Civil[5], da Lei do Cadastro Positivo[6], da Lei de Acesso à Informação[7] e, mais recentemente, do Marco Civil da Internet[8].

Em razão, contudo, do crescimento cada vez maior do tratamento de dados pessoais, em muito potencializado, ressalta-se, pelo exponencial avanço tecnológico, passou a surgir a necessidade de uma sólida sistematização do arcabouço de proteção dos dados pessoais no Brasil, à semelhança do que já vinha sendo desenvolvido em importantes ordenamentos jurídicos ao redor do mundo. Quer dizer, a necessidade crescente da proteção dos dados pessoais, e de tudo que envolve o uso destes dados, advém muito fortemente da reestruturação e do surgimento de novos modelos de relações nas sociedades, quando começaram a se organizar em torno dos fluxos de conhecimento e de informação[9].

E isso em muito porque, o direito fundamental à privacidade, em que pese sua forte relação com o que hoje se tem por direito à proteção dos dados pessoais, mesmo que com seu efetivo desenvolvimento e aplicação, não chegou a formular, especificamente, um arcabouço apto a fazer frente às novas situações que passaram a surgir a partir da introdução das novas tecnologias, com significativos efeitos nas

[3] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 22 jun. 2022.

[4] BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 22 jun. 2022.

[5] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 22 jun. 2022.

[6] BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 22 jun. 2022.

[7] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de dezembro de 1990; revoga a Lei 11.111, de 5 maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 22 jun. 2022.

[8] BRASIL. Lei nº 12.965, de 23 de abril 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 jun. 2022.

[9] GUTIÉRREZ, Ileana. América Latina ante la sociedad del riesgo. Disponível em: <https://www.oei.es/historico/salactsi/gutierrez.htm>. Acesso em: 22 jun. 2022.

relações pessoais e institucionais[10].

É preciso considerar, para a bem da verdade, que o interesse por uma regulamentação específica do uso de bancos de dados no Brasil iniciou no ano de 1999 – de forma tardia para o cenário internacional, mas há mais tempo do que se imagina, quando considerado o cenário pátrio atual – com o Projeto de Lei do Senado Federal nº 268/1999[11] (Projeto de Lei nº 3.494/2000, na Câmara dos Deputados[12]), dispondo sobre a estrutura e o uso de bancos de dados e garantindo a tomada de medidas de segurança contra o acesso não autorizado a dados pessoais e informações deles derivadas. Após mais de 20 anos de tramitação, contudo, o Projeto aguarda parecer do Relator na Comissão de Constituição e Justiça da Câmara.

Na sequência, diversos outros projetos de lei começaram a tramitar no Congresso Nacional, porém, sem sucesso, seja por decorrência de arquivamento ou de rejeição do inteiro teor e, mais recentemente, pela declaração de prejudicialidade em consequência da promulgação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Em assim sendo, é possível afirmar que, apesar de disposições esparsas e fragmentadas na Constituição Federal e em leis federais, bem como apesar das diversas tentativas inexitosas de criação de uma lei específica para a regulamentação dos bancos de dados e para a proteção dos dados pessoais, apenas no ano de 2018, com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), é que o Brasil adentrou no rol de países dotados de um sistema normativo voltado à proteção dos dados pessoais. A compreensão sobre o papel e o alcance da Lei Geral de Proteção de Dados, pois, é essencial e de suma importância para a tutela dos dados pessoais em nosso país.

A Lei Geral de Proteção de Dados brasileira tem por principal objetivo a

[10] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel *et al.* (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 11.
[11] BRASIL. Projeto de Lei nº 268, de 1999, do Senado Federal. Dispõe sobre a estruturação e o uso de bancos de dados sobre a pessoa e disciplina o rito processual do habeas data. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/40242>. Acesso em: 22 jun. 2022.
[12] BRASIL. Projeto de Lei nº 3.494, de 2000, da Câmara dos Deputados. Dispõe sobre a estruturação e o uso de bancos de dados sobre a pessoa e disciplina o rito processual do habeas data. Disponível em: <https://www.camara.leg.br/propostas-legislativas/19753>. Acesso em: 22 jun. 2022.

proteção dos direitos fundamentais de liberdade e de privacidade, bem assim o livre desenvolvimento da personalidade da pessoa natural. Ademais, tem por fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e, ainda, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Tem-se, ainda, que, para garantir a consumação do seu rol de fundamentos, a Lei é especialmente voltada para as operações de tratamento de dados, inclusive nos meios digitais, ou seja, para as operações realizadas com os dados pessoais, desde a sua coleta, até a sua eliminação, passando pelas possibilidades de utilização, reprodução, distribuição e armazenamento. Isso significa dizer que toda e qualquer operação que se reflita em algum tipo de manuseio (tratamento) de dados pessoais, deverá passar pelo crivo da Lei Geral de Proteção de Dados, excetuadas, por certo, as expressas disposições em sentido contrário.

De mais a mais, uma vez que, no contexto da Sociedade da Informação e da Era Digital, não existem dados que possam ser considerados insignificantes, a garantia decorrente do rol de fundamentos da LGPD é primordial para a conscientização das instituições públicas e privadas no sentido de que os dados que em uma determinada circunstância podem não acarretar riscos ou danos, em algum momento futuro, e/ou a partir da combinação com outros dados, podem o ser.

Por estas considerações, importante esclarecer que a Lei não pretende a inviabilização do uso de dados pessoais – o que sequer seria possível, à bem da verdade, em termos práticos –, mas sim a regulamentação do uso destes dados de forma equilibrada, possibilitando a inovação e o desenvolvimento dos setores que se utilizam dos dados, sem que haja violação dos direitos dos seus titulares. Tem-se, nesse sentido, que a Lei Geral de Proteção de Dados apresenta mecanismos idealizados tanto para a tutela do titular, quanto para que as instituições públicas e privadas possam dispor destes dados, dentro dos parâmetros e limites para sua

utilização[13].

Fato é que, em verdade, mais do que inaugurar a ideia de proteção de dados pessoais no ordenamento jurídico brasileiro – nesses termos – a Lei Geral de Proteção de Dados estabelece uma base normativa específica para que valores e princípios já existentes em nosso ordenamento jurídico sejam orientados em torno de uma disciplina de caráter geral, a partir de uma noção uniforme e padronizada no encaminhamento das diversas situações que decorrem do tratamento de dados pessoais[14], com vistas ao desenvolvimento de uma política nacional de proteção de dados. Relevante considerar, ainda, que trata-se de uma Lei com perfil de código, ou microssistema, dotada de regras e procedimentos, os quais, repita-se, devem passar a estar presentes em qualquer instituição que promova o tratamento de dados pessoais[15].

Daí decorre, pois, sua importância e essencialidade para o ordenamento jurídico brasileiro. Sobre este ponto, em que pese o considerável retardo no que tange ao desenvolvimento da primeira legislação específica sobre o tema da proteção de dados pessoais no Brasil – isso considerando a posição dos demais países ao redor do mundo –bem assim as demandas da sociedade pátria, fato é que a Lei Geral de Proteção de Dados brasileira, em seu inteiro teor, e uma vez representando um eixo legislativo central e sistematizado, foi capaz de alcançar aspectos fulcrais para a proteção dos dados pessoais em nosso país.

Ademais, para além da importância da Lei Geral de Proteção de Dados, relevante se faz a avaliação do caminho percorrido pelo direito à proteção de dados pessoais, até alcançar condição de direito fundamental no ordenamento jurídico-

---

[13] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor. São Paulo, v. 120, nov./dez. 2018, p. 585.

[14] DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). Lei geral de proteção de dados (lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters do Brasil, 2020, p. 245.

[15] Antônio Carlos Negrão, ao discorrer sobre a Lei Geral de Proteção de Dados brasileira, afirma que "a LGPD é um novo código ou um novo microssistema, possuindo 350 dispositivos, se considerados os artigos, incisos e parágrafos. Apenas para comparar, o CDC possui 367 dispositivos". NEGRÃO, Antônio Carlos. Economia digital, proteção de dados e competitividade. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). Lei geral de proteção de dados (lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters do Brasil, 2020, p. 30.

constitucional brasileiro, primeiro de forma implícita e, mais recentemente, de forma expressamente positivada no texto da Constituição Federal.

Sobre este ponto, por primeiro, calha ressaltar o ensinamento de Ingo Sarlet[16], no sentido de que o conceito materialmente aberto dos direitos fundamentais remete-nos à percepção de que existem dois grandes grupos de direitos fundamentais: os direitos fundamentais positivados em diversos pontos do texto constitucional e em tratados internacionais, bem como os direitos fundamentais não escritos, tanto implícitos nas normas do catálogo, quanto decorrentes do regime e dos princípios. As três fontes estabelecidas pelo artigo 5º, § 2º, da Constituição Federal, em conjunto, correspondem aos fundamentos para uma conceituação material dos direitos fundamentais no cenário brasileiro, instituindo, por consequência, as bases para a abertura aos direitos fundamentais atípicos.

No que tange ao direito fundamental à proteção de dados, em um primeiro momento, era possível considerá-lo como materialmente fundamental, implicitamente previsto, a partir da abertura do texto constitucional para tal, e por decorrência de sua dimensão subjetiva, na medida em que, na atualidade, não parece ser demasiadamente árdua a demonstração da relevância relativa aos valores, princípios e direitos fundamentais associados à proteção dos dados – dentre os quais destacam-se a dignidade da pessoa humana, a cláusula geral do livre desenvolvimento da personalidade e o direito à privacidade –, tanto, por certo, para a esfera individual, quanto para o interesse coletivo, traduzido pela sociedade organizada e pelo Estado[17].

Além deste, que já é fator apto a consolidar a proteção dos dados pessoais como direito fundamental, o Supremo Tribunal Federal, em decisão histórica de relatoria da Ministra Rosa Weber, posteriormente referendada pelo Plenário da Corte, reconheceu de forma expressa, nos autos da Ação Direta de Inconstitucionalidade nº 6.387/2020[18], a existência de um direito fundamental autônomo, positivado de forma

[16] SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018, p. 72.
[17] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel *et al.* (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 28.
[18] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6.387/2020. Relatora: Ministra Rosa Weber. Brasília, DF, 24/04/2020. Disponível em:

implícita. Na ocasião, a Relatora reconheceu, fundamentadamente, que os dados pessoais integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual, da privacidade e do livre desenvolvimento da personalidade e, por isso, sua manipulação e tratamento devem observar os limites delineados pela proteção constitucional.

Somando-se a isso, desde o ano de 2019 começaram a ser promovidos esforços, de modo a fazer constar, formalmente no texto constitucional brasileiro, a proteção dos dados pessoais do cidadão como direito expressamente positivado, a partir da Proposta de Emenda à Constituição nº 17/2019[19], originária do Senado Federal. Após três anos de trâmite, finalmente, em 10 de fevereiro de 2022, restou promulgada a Emenda Constitucional nº 115/2022, que acrescenta o inciso LXXIX ao artigo 5º da Constituição Federal, de modo a assegurar o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Por todos estes movimentos e reconhecimentos, da Lei Geral de Proteção de Dados à Emenda Constitucional, passando pela importante decisão do Supremo Tribunal Federal, tem-se que, finalmente, o Brasil está dedicando a devida atenção à temática da proteção dos dados pessoais, o que é essencial quando considerada a realidade extremamente "dataficada", isto é, baseada em dados, que a sociedade contemporânea vivencia. Agora, compete-nos a observância e a fiscalização quanto à aplicabilidade prática das disposições legais e constitucionais estabelecidas no ordenamento jurídico brasileiro, com vistas à consolidação de uma cultura da proteção de dados pessoais.

<http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 22 jun. 2022.

[19] Proposta de Emenda à Constituição nº 17/2019, de iniciativa dos Senadores Eduardo Gomes, Ângelo Coronel, Antônio Anastasia, Chico Rodrigues, Eduardo Braga, Eliziane Gama, Flávio Arns, Humberto Costa, Irajá, Jean Paul Prates, Jorge Kajuru, Lasier Martins, Leila Barros, Luiz do Carmo, Mailza Gomes, Marcos Rogério, Marcos do Val, Maria do Carmo Alves, Mecias de Jesus, Nelsinho Trad, Paulo Paim, Randolfe Rodrigues, Rodrigo Pacheco, Rogério Carvalho, Telmário Mota, Veneziano Vital do Rêgo, Wellington Fagundes, Weverton e Zequinha Marinho. "Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria". BRASIL. Proposta de Emenda à Constituição nº 17, de 2019. Assegura o direito à proteção de dados pessoais, inclusive nos meios digitais; inclui entre as competências da União legislar sobre proteção e tratamento de dados pessoais. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 22 jun. 2022.

3. O estado da arte do direito à desindexação no ordenamento jurídico brasileiro

A Era Digital e a Sociedade da Informação surgem como reflexo das transformações que impactam as mais diversas relações em todo o mundo, tornando-as mais complexas. Estas transformações, efetivamente, estão ancoradas especialmente no fato de que, neste contexto, as informações fluem em níveis expressivos de quantidade e velocidade, de modo que assumem fundamentais valores sociais, econômicos e, por consequência, jurídicos. Em contrapartida, e por decorrência disso, surgem também novas formas de violação de bens jurídicos, o que, por sua vez, postula também uma renovação do Direito.

Quer dizer, o superinformacionismo decorre da digitalização do mundo, ao passo que esta digitalização potencializa o superinformacionismo. É como um ciclo.

A internet, como elemento central deste cenário, promoveu – e segue promovendo – uma revolução nas formas como são armazenadas, acessadas e compartilhadas as informações, fazendo com que registros que antes eram restritos a um pequeno e/ou delimitado grupo de pessoas, sejam capazes de alcançar o mundo inteiro em apenas alguns segundos e a partir de poucos cliques. Somado a isso, tem-se que, no campo da internet, as informações se mantêm registradas *ad aeternum*, o que faz com que elas tenham potencial para se tornarem inoportunas ou inapropriadas em algum momento futuro[20].

Além do mais, é imprescindível considerar que o uso da internet teve seu crescimento e desenvolvimento potencializados a partir da utilização dos serviços de mecanismos de busca[21], que atuam como ferramentas aptas a facilitar a localização de conteúdos na rede[22]. De mais a mais, em termos práticos, a tecnologia dos mecanismos de busca na internet é orientada para potencializar as informações

[20] XAVIER, José Tadeu Neves. A problemática do direito ao esquecimento no direito brasileiro. Tese (Pós-Doutorado) - Santiago de Compostela (ES): Universidade de Santiago de Compostela, 2018, p. 38.

[21] "Um mecanismo de busca é um conjunto de programas de computador que executa diversas tarefas com o objetivo de possibilitar a localização de arquivos e *web sites* que contenham ou guardem relação com a informação solicitada pelo usuário". LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo: Juarez de Oliveira, 2005, p. 16.

[22] OLIVEIRA, Caio César de. Eliminação, desindexação e esquecimento na internet. São Paulo: Revista dos Tribunais, 2020, p. 125.

mais acessadas, o que, por consequência, acaba por atrair mais acessos para aquela mesma página.

Em assim sendo, no ambiente virtual, tornou-se manifesta a necessidade de desenvolvimento de mecanismos aptos a tutelar os dados pessoais, a partir do gerenciamento do tratamento destes dados, a ser realizado com base na elaboração de um adequado sistema de gestão destas informações. Isso para, ao final, garantir a tutela da dignidade da pessoa humana, do direito fundamental à proteção de dados pessoais, da autodeterminação informativa, do livre desenvolvimento da personalidade e da privacidade.

Foi este cenário, então, que fez surgir o assim chamado direito à desindexação. Quer dizer, é no contexto da Era Digital e da Sociedade da Informação que está inserido o direito à desindexação, justamente pelo fato de que este é um direito próprio do sistema de informação, que tem forte relação com a divulgação de dados e de informações no âmbito da internet, especialmente por meio dos provedores de busca e pesquisa.

A origem do direito à desindexação (*Recht auf Nicht-indexierung*) remonta à doutrina alemã, a partir da proposta conceitual desenvolvida por Oskar Josef Gstrein, tendo sido desenvolvida, ao menos em um primeiro momento, por decorrência da percepção de necessidade de ampliação do escopo de especificação e proteção do direito a ser esquecido[23]. Esta definição, porém, não nos permite concluir que o direito ao esquecimento e o direito à desindexação são sinônimos, ou, ainda, que o direito à desindexação se confunde com a ideia de um direito ao esquecimento na internet.

Efetivamente, o direito à desindexação decorre do sistema de proteção de dados pessoais[24], uma vez que o titular dos dados pode apresentar oposição ao tratamento de dados realizado sem uma base legal que o sustente, nos termos do que dispõem o artigo 7º e o artigo 18, § 2º, da LGPD, ou, ainda, quando o titular de dados se oponha, de modo a revogar o consentimento anteriormente manifestado de

[23] SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. O direito ao "esquecimento" na sociedade da informação. Porto Alegre: Livraria do Advogado, 2019, p. 65-66.
[24] LIMA, Cíntia Rosa de. O direito à desindexação em uma perspectiva civil-constitucional. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coord.). Proteção de dados: temas controvertidos. Indaiatuba: Editora Foco, 2021, p. 39.

forma expressa e inequívoca, com base no disposto no artigo 8º, § 5º, também da LGPD.

Por esta ideia, o direito à desindexação objetiva determinar que as informações tuteladas sejam arquivadas – e não excluídas ou eliminadas – a fim de garantir que o acesso ao seu conteúdo seja impossibilitado, com o consequente impedimento de que as informações sejam resgatadas dos sistemas informatizados[25]. Nesses termos, o pedido de desindexação pretende uma espécie de diálogo com a empresa responsável por um provedor de busca, a partir do pedido de rompimento do vínculo entre determinado conteúdo – defasado, incompleto ou irrelevante – e o nome ou outros dados que possam identificar um indivíduo[26].

O direito à desindexação, assim, visa preservar o quadro informacional do seu titular, a partir de mecanismos de bloqueio nas ferramentas de busca da internet, de modo que, uma vez bloqueadas, as plataformas obrigam-se a desvincular determinados dados e informações de seus bancos[27]. Soma-se a isso o fato de que, para a efetivação do direito à desindexação, a questão temporal não é relevante, de sorte que este direito pode tutelar tanto os acontecimentos pretéritos, quanto os atuais[28].

Por tais considerações, oportuno citar os elementos que, pela doutrina de Caio César de Oliveira[29], perfazem a essência do direito à desindexação: (I) a ação de desindexar não garante a remoção total do conteúdo, pois ele permanece disponível no site original; (II) a desindexação incide sobre a busca realizada pelo nome do titular da informação, porém, a informação continua podendo ser localizada a partir de outros parâmetros; e (III) a desindexação não garante o esquecimento e, tampouco, pode ser considerada como sinônimo de um direito ao esquecimento.

---

[25] SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. O direito ao "esquecimento" na sociedade da informação. Porto Alegre: Livraria do Advogado, 2019, p. 66.
[26] MEDEIROS, Carlos Henrique Garcia de. O direito ao esquecimento na atual era digital. In: CAMARGO, Coriolano Almeida; SANTOS, Cleórbete. Direito digital: novas teses jurídicas. Rio de Janeiro: Lumem Juris, 2018, p. 53.
[27] SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. O direito ao "esquecimento" na sociedade da informação. Porto Alegre: Livraria do Advogado, 2019, p. 66.
[28] XAVIER, José Tadeu Neves. A problemática do direito ao esquecimento no direito brasileiro. Tese (Pós-Doutorado) - Santiago de Compostela (ES): Universidade de Santiago de Compostela, 2018, p. 39.
[29] OLIVEIRA, Caio César de. Eliminação, desindexação e esquecimento na internet. São Paulo: Revista dos Tribunais, 2020, p. 126.

Metaforicamente, é interessante considerar que a medida de desindexar figura como suprimir o sumário de um livro, isto é, o conteúdo permanece existindo e, se se sabe onde está o trecho desejado, será possível acessá-lo[30]. Quer dizer, o trecho continua no livro – não é excluído – mas, sem o índice, o seu acesso imediato será dificultado.

De mais a mais, por ter sua origem, como inicialmente exposto, com o direito ao esquecimento, o direito à desindexação, inevitavelmente, se tornou objeto de debates e questionamentos no que tange à sua validade, por decorrência da tese jurídica fixada pelo Supremo Tribunal Federal sobre o direito ao esquecimento, no ano de 2021, quando do julgamento, em repercussão geral, do Recurso Extraordinário nº 1.010.606/RJ (Tema 786)[31].

Sobre este ponto, de imediato é preciso voltar à consideração de que o direito ao esquecimento e o direito à desindexação não se confundem, o que resulta, por consequência lógica, na inaplicabilidade do Tema 786 do STF à temática do direito à desindexação. Para demonstrar esta conjuntura, dois pontos, em especial, merecem destaque.

Primeiro que, quanto ao direito ao esquecimento, em que pese a parte inicial da tese jurídica fixada pelo STF, reconhecendo a incompatibilidade do direito ao esquecimento para com a ordem jurídico-constitucional brasileira, fato é que a própria Corte não fechou por completo as portas para a temática – ainda que sejam discutíveis as questões de nomenclatura –, pois excetuou expressamente (*distinguishing facts*) as situações de excesso no exercício das liberdades comunicativas e as expressas previsões legais nos âmbitos penal e cível.

Segundo que o referido paradigmático julgamento não alcançou a temática do direito à desindexação, não tendo o STF excluído a possibilidade deste direito em sua

---

[30] LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2012, p. 293.

[31] "É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais – especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral – e as expressas e específicas previsões legais nos âmbitos penal e cível". BRASIL. Supremo Tribunal Federal (Plenário). Recurso Extraordinário nº 1.010.606/RJ. Relator: Ministro Dias Toffoli. Brasília, DF, 11/02/2021. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15346473757&ext=.pdf>. Acesso em: 22 jun. 2022.

decisão. Quer dizer, se especificamente quanto ao direito ao esquecimento a Suprema Corte apresentou consideráveis ressalvas, quanto ao direito à desindexação não há falar em alcance da decisão.

A nível legislativo, duas importantes leis se destacam na compreensão do direito à desindexação.

O Marco Civil da Internet, em vigor desde o ano de 2014, foi a primeira lei brasileira a definir as aplicações de internet como conjunto de funcionalidades, além de estabelecer princípios e garantias aptos a assegurar os direitos e os deveres dos usuários e das empresas provedoras de acesso e serviços on-line, o que é de fundamental relevância para a temática do direito à desindexação. Relativamente à questão da responsabilidade civil, contudo, que também impacta fortemente na temática do direito à desindexação, é preciso atentar-se para o fato de que, no âmbito do Supremo Tribunal Federal, foi reconhecida repercussão geral relativa à (in) constitucionalidade do artigo 19 [32], suscitada no Recurso Extraordinário nº 1.037.396/SP, de relatoria do Ministro Dias Toffoli (Tema 987)[33], o qual ainda não foi julgado no mérito.

[32] Art. 19, Lei 13.709/2018. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal. § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação. BRASIL. Lei nº 12.965, de 23 de abril 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 jun. 2022.

[33] Tema 987, STF: "Discussão sobre a constitucionalidade do art. 19 da Lei nº 12.965/2014 (Marco Civil da Internet) que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, *websites* e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros". BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.037.396/SP. Relator: Ministro Dias Toffoli. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em: 22 jun. 2022.

A Lei Geral de Proteção de Dados, por sua vez, dispõe, em seu artigo 18, inciso IV, que o titular dos dados pessoais tem o direito de obter, mediante requisição, a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei. O artigo 15, inciso I, no mesmo sentido, dispõe que o tratamento de dados pessoais terá seu fim quando verificado que a finalidade foi alcançada, ou quando apurado que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

Nesse sentido, nos termos do que dispõe a LGPD, se uma informação desatualizada causar dano ao seu titular, bem como se não houver interesse público no sentido de que continue sendo veiculada, a informação terá cumprido sua finalidade, qual seja, a de informar, tornando-se, na sequência, possivelmente desnecessária e excessiva, razão pela qual o titular poderá requerer a eliminação da informação, inclusive aos provedores de pesquisa, "haja vista que estes também realizam tratamentos de dados"[34].

No âmbito jurisprudencial, é notório que as demandas envolvendo o direito à desindexação e o bloqueio nas ferramentas de pesquisa na internet estão, cada vez mais, sendo levadas à apreciação do Poder Judiciário, o qual, por consequência, também com mais frequência, tem tido a oportunidade de se manifestar sobre a temática. E, ressalta-se, para além dos paradigmáticos julgamentos comumente estudados sobre a temática[35], fato é que os Tribunais de Justiça Estaduais, reiterada e cotidianamente, têm sido chamados a apreciar as demandas que envolvem a matéria no dia a dia da comunidade[36].

---

[34] EHRHARDT JR., Marcos; MODESTO, Jéssica Andrade. Direito ao esquecimento e direito à desindexação: uma pretensão válida? Comentários ao acórdão proferido pelo STJ no REsp nº 1.660.168-RJ. Revista do Programa de Pós-Graduação em Direito da UFBA, v. 30, nº 1, jan./jun. 2020, p. 99.

[35] No Superior Tribunal de Justiça, o REsp 1.660.168/RJ. BRASIL. Superior Tribunal de Justiça (3ª Turma). Recurso Especial nº 1.660.168/RJ. Relatora: Ministra Nancy Andrighi. Redator para o acórdão: Ministro Marco Aurélio Bellizze. Brasília, DF, 08/05/2018. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1628798&num_registro=201402917771&data=20180605&peticao_numero=-1&formato=PDF>. Acesso em: 22 jun. 2022. Na Europa, o processo C-131/12. EUROPEAN UNION. European Union Court of Justice. Sentencia C-131/12, may 13, 2014. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=152065&text=&dir=&doclang=ES&part=1&occ=first&mode=DOC&pageIndex=0&cid=2842945>. Acesso em: 22 jun. 2022.

[36] Vide Apelação Cível nº 1033284-17.2016.8.26.0100. BRASIL. Tribunal de Justiça do Estado de São Paulo (1ª Câmara de Direito Privado). Apelação Cível nº 1033284-17.2016.8.26.0100. Relator: Desembargador Enéas Costa Garcia. São Paulo, SP, 12/12/2019. Disponível em:

Fato é, então, que a temática do direito à desindexação, apesar de relativamente nova no ordenamento jurídico brasileiro, tem pleno – e necessário – campo para desenvolvimento, especialmente porque representa uma essencial e inevitável evolução, hábil a tutelar as novas possibilidades de violação que alcançam o fundamento da dignidade da pessoa humana, mormente no contexto que decorre do superinformacionismo da Era Digital.

4. A proteção de dados pessoais como fundamento do direito à desindexação

O direito à proteção de dados pessoais percorreu uma trajetória de exponencial crescimento e evolução, tanto em termos de tutela, quanto em termos de alcance, desde a sua concepção como tal, no cenário europeu da década de 1970, até sua consolidação como direito fundamental, no Brasil – agora, inclusive, de forma expressamente positivada no texto constitucional, a partir da Emenda Constitucional nº 115/2022 – e em outros importantes ordenamentos jurídicos ao redor do mundo. Trata-se, inegavelmente, de um desenvolvimento constante e progressivo, com vistas a uma maior efetividade.

Por este processo de ascensão, o direito fundamental à proteção de dados pessoais, atualmente, no ordenamento jurídico-constitucional pátrio, figura como um direito autônomo e de aplicabilidade imediata, independendo, portanto, de outros direitos fundamentais para sua consagração. Esta constatação, em contrapartida, não exclui a possibilidade de associação do direito fundamental à proteção de dados pessoais para com outros princípios e direitos fundamentais de caráter geral e

---

<https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=13177002&cdForo=0>. Acesso em: 22 jun. 2022. Apelação Cível nº 1050428-67.2017.8.26.0100. BRASIL. Tribunal de Justiça do Estado de São Paulo (4ª Câmara de Direito Privado). Apelação Cível nº 1050428-67.2017.8.26.0100. Relator: Desembargador Fábio Quadros. São Paulo, SP, 12/08/2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14926581&cdForo=0>. Acesso em: 22 jun. 2022. Apelação Cível nº 1053176-04.2019.8.26.0100. BRASIL. Tribunal de Justiça do Estado de São Paulo (7ª Câmara de Direito Privado). Apelação Cível nº 1053176-04.2019.8.26.0100. Relator: Desembargador José Rubens Queiroz Gomes. São Paulo, SP, 18/08/2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14930624&cdForo=0>. Acesso em: 22 jun. 2022. Apelação Cível nº 1086490-77.2015.8.26.0100. BRASIL. Tribunal de Justiça do Estado de São Paulo (9ª Câmara de Direito Privado). Apelação Cível nº 1086490-77.2015.8.26.0100. Relator: Desembargador Edson Luiz de Queiroz. São Paulo, SP, 13/07/2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14809469&cdForo=0>. Acesso em: 22 jun. 2022.

especial, como, por exemplo, a dignidade da pessoa humana e o livre desenvolvimento da personalidade, bem como o direito à autodeterminação informativa[37].

Especificamente sobre a temática do direito à autodeterminação informacional, importante considerar que este, com muita frequência, e cada vez mais – a partir de uma nomenclatura que vem se popularizando –, está presente nos estudos e debates sobre a proteção dos dados pessoais, podendo-se concluir que ambos estão estreitamente vinculados, não por dependência, mas por complementação. Em verdade, ressalta-se, o direito à autodeterminação informativa em muitas vezes é utilizado para assegurar o direito à proteção de dados pessoais.

Com origem na jurisprudência alemã, uma das principais noções a alicerçar o direito à autodeterminação informativa está na constatação "precoce e cirúrgica"[38] desenvolvida pelo Tribunal Constitucional Federal da Alemanha, segundo a qual nas circunstâncias modernas do processamento automatizado de dados, não mais existem dados pessoais que possam ser considerados insignificantes, menos importando, por isso, o tipo de dado que é tratado, mais importando a finalidade e as possibilidades de processamento[39].

No ordenamento jurídico-constitucional brasileiro, o direito à autodeterminação informativa está, de igual forma, intimamente atrelado ao direito fundamental à proteção de dados pessoais. Isso porque, quando o Supremo Tribunal Federal reconheceu, pela primeira vez no cenário pátrio, a existência de um direito fundamental autônomo e implicitamente positivado no texto constitucional, relativo à proteção dos dados pessoais, no julgamento da Ação Direta de Inconstitucionalidade nº 6.387/DF, em 2020, restou afirmado, de igual forma, o direito à autodeterminação informativa, apto a assegurar o controle do cidadão para com o tratamento de seus dados.

---

[37] SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como direito fundamental I. 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental.> Acesso em 22 jun. 2022.

[38] COÊLHO, Marcus Vinicius Furtado. O direito à proteção de dados e a tutela da autodeterminação informativa. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa>. Acesso em 22 jun. 2022.

[39] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Pensar: Revista de Ciências Jurídicas, v. 25, n. 4, out./dez. 2018, p. 11.

Em termos legislativos, a Lei Geral de Proteção de Dados, sancionada em 2018 e vigente desde 2020, dispõe expressamente que a disciplina da proteção de dados pessoais – tutelada, pois, de forma específica tanto na via constitucional, quanto na via infraconstitucional – tem como um de seus fundamentos a autodeterminação informativa[40]. Nesse sentido, o titular do dado pessoal, no cenário brasileiro, por força de lei, é dotado de um poder de escolha, caracterizado pela autorização, ou não, do tratamento de seus dados – observadas, por certo, as hipóteses legais que prescindem de consentimento –, bem como da configuração e das circunstâncias do tratamento, em caso de autorização.

Somado a isso, tem-se que o rol de direitos do titular, exposto na LGPD, não é taxativo, isto é, a Lei não exaure as posições jurídicas associadas à proteção de dados pessoais. Isso significa que, por decorrência de sua condição no ordenamento jurídico-constitucional brasileiro, o direito fundamental à proteção de dados pessoais pode atuar como fundamento para o reconhecimento implícito de outras posições subjetivas dotadas de relevância jurídica e social, de modo que, a partir do texto constitucional, bem assim, especificamente, do direito fundamental à proteção de dados pessoais, podem ser reconhecidas implicitamente novas e diferentes posições subjetivas merecedoras de tutela.

O direito à desindexação, conforme defendido no presente estudo, figura como uma dessas possibilidades. Quer dizer, o direito à desindexação representa um exemplo possível de direito do titular dos dados pessoais – sujeito e destinatário do direito fundamental à proteção de dados pessoais –, que não consta do rol de direitos da Lei Geral de Proteção de Dados brasileira, mas que, em contrapartida, pode ser deduzido do ponto de vista constitucional da proteção de dados pessoais, pois, efetivamente, o direito à desindexação, por sua essência, visa à proteção dos dados e das informações pessoais do seu titular.

De fato, o direito à desindexação está intimamente ligado ao direito fundamental à proteção de dados pessoais e ao direito à autodeterminação

[40] Art. 2º, Lei 13.709/2018. A disciplina da proteção de dados pessoais tem como fundamentos: [...] II. A autodeterminação informativa. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 jun. 2022.

informativa[41], especialmente porque, conceber a autodeterminação informativa, externalizada na proteção de dados pessoais, é particularmente desafiador quando se leva em consideração a realidade tecnológica atualmente vigente, bem assim, e por consequência, a arquitetura da internet[42]. Assume, pois, a atenção do pensamento jurídico a importância e a aplicabilidade do direito à desindexação, de modo que passa-se a estudar não só a necessária vinculação entre o direito à proteção de dados pessoais e o direito à autodeterminação informativa, mas também a vinculação entre ambos, e cada um, com o direito à desindexação.

Efetivamente, por decorrência do papel desempenhado pelos motores de pesquisa da internet, especificamente no acesso e na divulgação das informações, está-se diante de um momento histórico em que é imperativo o fortalecimento do direito à autodeterminação informativa, sendo importante, para tal, a utilização de uma prerrogativa de natureza jurídica mais específica[43]. Parte-se, assim, do reconhecimento de que o direito de escolher a indexação de dados pessoais em motores de pesquisa e busca[44], relaciona-se com a garantia efetiva do direito à autodeterminação informacional[45], assim como, por certo, do direito à proteção de dados pessoais.

---

[41] LIMA, Cíntia Rosa de. O direito à desindexação em uma perspectiva civil-constitucional. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coord.). Proteção de dados: temas controvertidos. Indaiatuba: Editora Foco, 2021, p. 39.

[42] VIEIRA, Laísa Fernanda Alves. O direito à desindexação na sociedade *googlelizada*: autodeterminação informativa como expressão na construção da personalidade. 2020. Dissertação (Mestrado) - Universidade Federal do Paraná, Curitiba, 2020, p. 68.

[43] CERDÁN, Tábata Andrea Romero. Desindexación de datos personales: fortaleciendo el derecho a la autodeterminación informativa y el olvido digital. Revista de investigación en Derecho, Criminología y Consultoría Jurídica, v. 11, n. 22, out. 2017. Disponível em: <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/531/440>. Acesso em: 22 jun. 2022, p. 236.

[44] De fato, como bem dispõe Tábata Andrea Romero Cerdán, "*La intromisión a nuestra vida privada no siempre es negativa ni mucho menos ilícita, sin embargo, al percibirlo como una amenaza potencial es un argumento legítimo de los titulares de los datos personales, para elegir los medios de divulgación y [...] sobre la autorización respecto a la indexación de tales datos en los motores de búsqueda*". CERDÁN, Tábata Andrea Romero. Desindexación de datos personales: fortaleciendo el derecho a la autodeterminación informativa y el olvido digital. Revista de investigación en Derecho, Criminología y Consultoría Jurídica, v. 11, n. 22, out. 2017. Disponível em: <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/531/440>. Acesso em: 22 jun. 2022, p. 236.

[45] CERDÁN, Tábata Andrea Romero. Desindexación de datos personales: fortaleciendo el derecho a la autodeterminación informativa y el olvido digital. Revista de investigación en Derecho, Criminología y Consultoría Jurídica, v. 11, n. 22, out. 2017. Disponível em: <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/531/440>. Acesso em: 22 jun. 2022, p. 236.

Tem-se, pois, que, uma vez considerados o contexto que decorre da Era Digital e do superinformacionismo, bem assim a relevância da proteção dos dados pessoais e da autodeterminação informativa em face das atividades desempenhadas pelos provedores de pesquisa da internet, o direito à desindexação pode – e, em muito, deve – ser reconhecido como um importante instrumento jurídico, decorrente, ressalta-se, do momento histórico que a sociedade contemporânea vivencia.

Não se desconhece, por certo, a necessidade do desenvolvimento de uma adequada sistematização da temática que alcança o direito à desindexação. Critérios de aplicação e efetividade, os quais envolvem alcances e limites complexos, precisam ser mais profundamente delineados. Tal pode – e deve – ocorrer a partir de contribuições doutrinárias, o que não exclui, em contrapartida, a necessidade e a importância de regulamentação por meio de lei ou, ainda, de decisão judicial com repercussão geral.

O direito à desindexação, em verdade, em que pese dotado de inegáveis complexidades e indefinições, bem como passível de necessário desenvolvimento, aporta em terreno mais sólido quando analisado sob o viés que decorre do sistema de proteção de dados pessoais. Trata-se, pois, de fornecer uma possibilidade de controle do titular para com os seus dados que são divulgados na internet, de modo a, por meio do direito à desindexação – sempre analisado casuisticamente – ser efetivada a garantia ao livre desenvolvimento da personalidade, à dignidade da pessoa humana, à proteção dos dados pessoais e à autodeterminação informativa.

5. Considerações finais

Na sociedade contemporânea, a realização das relações pessoais e institucionais está intimamente associada ao constante fornecimento de dados e de informações pessoais, tanto em ambientes físicos, quanto, principalmente, em ambientes digitais. Soma-se a isso o fato de que a tecnologia, em sentido amplo, e a internet, em sentido mais específico, na rápida medida em que foram sendo desenvolvidas, passaram a permitir a transferência e o acesso a dados e a informações em poucas frações de segundos e mediante poucos cliques.

Está realidade já está fortemente consolidada na sociedade e nas relações contemporâneas, de modo que dela não há como se afastar.

A instituição e a solidificação da tecnologia, bem assim a sociedade cada vez mais "dataficada", isto é, baseada em dados, por sua vez, justifica a necessária preocupação com a proteção dos dados pessoais, com a realização da autodeterminação informacional e, ainda, com a tutela da vida privada. Assim, as novas possibilidades que decorrem do superinformacionismo fizeram – e seguem fazendo – surgir novas formas de violação a bens jurídicos, fazendo surgir, de igual forma, novos direitos passíveis de tutela e novos institutos jurídicos aptos a assegurar estes direitos.

O direito à desindexação surgiu e tem sido disseminado nos cenários jurídicos por decorrência desta realidade. Quer dizer, o contexto do superinformacionismo da Era Digital fez surgir o direito à desindexação. Trata-se, especificamente, de, por meio da desindexação, dificultar o acesso a uma determinada informação que está disponível na internet, por interesse do titular, com vistas a assegurar seu direito fundamental à proteção de dados pessoais.

Uma vez estudada, pois, a ascensão e a consolidação do direito à proteção de dados pessoais no ordenamento jurídico brasileiro, à nível infraconstitucional e constitucional, ambos de forma expressa, bem assim o estado da arte do direito à desindexação no cenário pátrio, ao final do presente ensaio demonstrou-se a importância da reunião de ambas as temáticas para, então, embasar a compreensão do direito fundamental à proteção de dados pessoais, em sua dimensão subjetiva, como um fundamento do direito à desindexação, sendo este, por sua vez, decorrente do sistema de proteção de dados pessoais.

A temática do direito à desindexação, em que pese relativamente nova, especialmente no ordenamento jurídico brasileiro, além de passível de uma adequada sistematização, é dotada de pleno e necessário campo para desenvolvimento, tendo em vista que retrata uma evolução com capacidade para tutelar as possibilidades contemporâneas de violação a bens jurídicos fundamentais, diante das avassaladoras transformações que vêm ocorrendo em razão do advento da Era Digital e da Sociedade da Informação.

Referências bibliográficas

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 22 jun. 2022.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 22 jun. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 22 jun. 2022.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 22 jun. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de dezembro de 1990; revoga a Lei 11.111, de 5 maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 22 jun. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 jun. 2022.

BRASIL. **Projeto de Lei nº 268, de 1999, do Senado Federal**. Dispõe sobre a estruturação e o uso de bancos de dados sobre a pessoa e disciplina o rito processual do habeas data. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/40242>. Acesso em: 22 jun. 2022.

BRASIL. **Projeto de Lei nº 3.494, de 2000, da Câmara dos Deputados**. Dispõe sobre a estruturação e o uso de bancos de dados sobre a pessoa e disciplina o rito processual do habeas data. Disponível em: <https://www.camara.leg.br/propostas-legislativas/19753>. Acesso em: 22 jun. 2022.

BRASIL. **Proposta de Emenda à Constituição nº 17, de 2019**. Assegura o direito à proteção de dados pessoais, inclusive nos meios digitais; inclui entre as

competências da União legislar sobre proteção e tratamento de dados pessoais. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 22 jun. 2022.

BRASIL. Tribunal de Justiça do Estado de São Paulo (1ª Câmara de Direito Privado). **Apelação Cível nº 1033284-17.2016.8.26.0100**. Relator: Desembargador Enéas Costa Garcia. São Paulo, SP, 12/12/2019. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=13177002&cdForo=0>. Acesso em: 22 jun. 2022.

BRASIL. Tribunal de Justiça do Estado de São Paulo (4ª Câmara de Direito Privado). **Apelação Cível nº 1050428-67.2017.8.26.0100**. Relator: Desembargador Fábio Quadros. São Paulo, SP, 12/08/2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14926581&cdForo=0>. Acesso em: 22 jun. 2022.

BRASIL. Tribunal de Justiça do Estado de São Paulo (7ª Câmara de Direito Privado). **Apelação Cível nº 1053176-04.2019.8.26.0100**. Relator: Desembargador José Rubens Queiroz Gomes. São Paulo, SP, 18/08/2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14930624&cdForo=0>. Acesso em: 22 jun. 2022.

BRASIL. Tribunal de Justiça do Estado de São Paulo (9ª Câmara de Direito Privado). **Apelação Cível nº 1086490-77.2015.8.26.0100**. Relator: Desembargador Edson Luiz de Queiroz. São Paulo, SP, 13/07/2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14809469&cdForo=0>. Acesso em: 22 jun. 2022.

BRASIL. Superior Tribunal de Justiça (3ª Turma). **Recurso Especial nº 1.660.168/RJ**. Relatora: Ministra Nancy Andrighi. Redator para o acórdão: Ministro Marco Aurélio Bellizze. Brasília, DF, 08/05/2018. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1628798&num_registro=201402917771&data=20180605&peticao_numero=-1&formato=PDF>. Acesso em: 22 jun. 2022.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387/2020**. Relatora: Ministra Rosa Weber. Brasília, DF, 24/04/2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 22 jun. 2022.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.037.396/SP**. Relator: Ministro Dias Toffoli. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em: 22 jun. 2022.

BRASIL. Supremo Tribunal Federal (Plenário). **Recurso Extraordinário nº 1.010.606/RJ**. Relator: Ministro Dias Toffoli. Brasília, DF, 11/02/2021. Disponível

em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15346473757&ext=.pdf>. Acesso em: 22 jun. 2022.

CERDÁN, Tábata Andrea Romero. Desindexación de datos personales: fortaleciendo el derecho a la autodeterminación informativa y el olvido digital. **Revista de investigación en Derecho, Criminología y Consultoría Jurídica**, v. 11, n. 22, p. 223-244, out. 2017. Disponível em: <http://www.apps.buap.mx/ojs3/index.php/dike/article/view/531/440>. Acesso em: 22 jun. 2022.

COÊLHO, Marcus Vinicius Furtado. **O direito à proteção de dados e a tutela da autodeterminação informativa**. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa>. Acesso em 22 jun. 2022.

DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters do Brasil, 2020, p. 243-255.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel *et al.* (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 3-20.

EHRHARDT JR., Marcos; MODESTO, Jéssica Andrade. Direito ao esquecimento e direito à desindexação: uma pretensão válida? Comentários ao acórdão proferido pelo STJ no REsp nº 1.660.168-RJ. **Revista do Programa de Pós-Graduação em Direito da UFBA**, v. 30, nº 1, p. 78-105, jan./jun. 2020.

EUROPEAN UNION. European Union Court of Justice. **Sentencia C-131/12**, may 13, 2014. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=152065&text=&dir=&doclang=ES&part=1&occ=first&mode=DOC&pageIndex=0&cid=2842945>. Acesso em: 22 jun. 2022.

GUTIÉRREZ, Ileana. **América Latina ante la sociedad del riesgo**. Disponível em: <https://www.oei.es/historico/salactsi/gutierrez.htm>. Acesso em: 22 jun. 2022.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LIMA, Cíntia Rosa de. O direito à desindexação em uma perspectiva civil-constitucional. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo

Neubarth; MELGARÉ, Plínio (Coord.). **Proteção de dados**: temas controvertidos. Indaiatuba: Editora Foco, 2021, p. 29-46.

MEDEIROS, Carlos Henrique Garcia de. O direito ao esquecimento na atual era digital. In: CAMARGO, Coriolano Almeida; SANTOS, Cleórbete. **Direito digital**: novas teses jurídicas. Rio de Janeiro: Lumem Juris, 2018.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar: Revista de Ciências Jurídicas**, v. 25, n. 4, p. 1-18, out./dez. 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**. São Paulo, v. 120, p. 555-687, nov./dez. 2018.

NEGRÃO, Antônio Carlos. Economia digital, proteção de dados e competitividade. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). **Lei geral de proteção de dados (lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters do Brasil, 2020, p. 29-37.

OLIVEIRA, Caio César de. **Eliminação, desindexação e esquecimento na internet**. São Paulo: Revista dos Tribunais, 2020.

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como direito fundamental I**. 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental>. Acesso em 22 jun. 2022.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel *et al.* (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 21-59.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. **O direito ao "esquecimento" na sociedade da informação**. Porto Alegre: Livraria do Advogado, 2019.

VIEIRA, Laísa Fernanda Alves. **O direito à desindexação na sociedade *googlelizada***: autodeterminação informativa como expressão na construção da personalidade. 2020. Dissertação (Mestrado) - Universidade Federal do Paraná, Curitiba, 2020.

XAVIER, José Tadeu Neves. **A problemática do direito ao esquecimento no direito brasileiro**. Tese (Pós-Doutorado) - Santiago de Compostela (ES): Universidade de Santiago de Compostela, 2018.

4. O CONSENTIMENTO NO TRATAMENTO DE DADOS NEURAIS

https://doi.org/10.36592/9786581110994-04

Cíntia Teresinha Burhalde Mua[1]

Sumário

1. Introdução

No contexto da medicina baseada em evidências[2], os avanços disruptivos da

---

[1] Doutoranda em Direito pela PUCRS. Mestre em Instituições de Direito do Estado (Pontifícia Universidade Católica do Rio Grande do Sul, 2006). Especialista em Direito Ambiental Nacional e Internacional (UFRGS, 2015).Especialista em Direito Processual Civil (PUCRS,1998). Bacharel em Ciências Jurídicas e Sociais pela UNISINOS (1995). Juíza de Direito desde 1998. Docente, Pesquisadora e Conteudista ENFAM (Escola Nacional de Formação de Magistrados). Docente convidada no PPGD da PUCRS. Docente no PPGD da FMP/RS. Coordenadora dos Núcleos de Estudos sobre Processo Coletivo (desde 2008) e Neurociência Aplicada ao Direito (desde 2018), ambos na Escola Superior da Magistratura da AJURIS. Membro do Núcleo de Inovação e Administração Judiciária da ESM/AJURIS. Assessora da Presidência da AJURIS. Membro do Departamento de Direitos Humanos da AJURIS. Membro do Grupo de Trabalho em Planejamento estratégico da Diretoria de Aposentados da AJURIS. Membro do LIODS CNJ – JUSClima. Membro do Fórum Gaúcho de Combate aos Efeitos dos Agrotóxicos -FGCIA Membro do Instituto Brasileiro de Direito Processual -IBDP. Membro do grupo de pesquisa CNPq - Interpretação Constitucional e Direito Administrativo, da Pontifícia Universidade Católica do Rio Grande do Sul. Autora de livros e artigos Jurídicos. http://lattes.cnpq.br/9922069811486300;
https://orcid.org/0000-0002-3478-1840. cintia.mua@edu.pucrs.br; cintia.mua@gmail.com

[2] Conforme FARIA, Lina; OLIVEIRA-LIMA, José Antonio de; ALMEIDA-FILHO, Naomar; Medicina baseada em evidências: breve aporte histórico sobre marcos conceituais e objetivos práticos do cuidado, Disponível em: <https://doi.org/10.1590/S0104-59702021000100004>. Acesso em 18/06/2022. a expressão medicina baseada em evidências refere-se *"(...) à utilização de pesquisas na tentativa de ampliar o conhecimento (expertise) médico e diminuir incertezas no processo clínico (diagnóstico/terapêutica/prognóstico), mediante permanente consulta às informações produzidas (e validadas) em pesquisas de epidemiologia clínica(...)"*. O método, mesmo apresentando registros mais antanho, desenvolveu-se a partir do trabalho de Archibald Cochrane e David Sackett. Para aprofundamento do tema: SACKETT, David L. Using Evidence-based medicine to help physicians keep up-to-date. Serials, v.9, n.2, p.178-181, 1996; Disponível em: < http://doi.org/10.1629/09178>. Acesso em 18/06/2022. SACKETT, David L. William M C Rosenberg, J A Muir Gray, R Brian Haynes, W Scott Richardson. Evidence-based medicine: what it is and what it isn't. BMJ, v.13, n.312, p.71-72, 1996, Disponível em: < https://doi.org/10.1136/bmj.312.7023.71.>. Para uma reflexão sobre os desafios da medicina baseada em evidências (BEM), veja: WORSHAM, Christopher; JENA, Anupam B.. The Art of Evidence-Based Medicine. Harward Business Review, January 30, 2019, Disponível em: <https://hbr.org/2019/01/the-art-of-evidence-based-medicine>. Acesso em 19/06/2022

biotecnologia[3] pautam a urgência da proteção de dados neurais.

Os dados neurais são o último baluarte da privacidade humana; seu tratamento, por conseguinte, reclama uma regulação mais incisiva que a destinada aos dados pessoais sensíveis na Lei Geral de Proteção de Dados[4].

Neurodados a partir de pesquisas genéticas, imagéticos (para registro ou estimulação) e provenientes de neurotecnologias estão sendo coletados a todo o tempo, ubiquamente, sendo imperativa a proteção da (1) identidade e da autonomia pessoal; (2) da neuroprivacidade.

Ademais, há que garantir (3) acesso equitativo às neurotecnologias e às interfaces cérebro-computador (BCIs); (4) a proteção contra os vieses (bias) e a (5) autodeterminação informativa.

Este conjunto de bens jurídicos conformam, plasticamente, os denominados neurodireitos, que já foram reconhecidos como direitos fundamentais explícitos na recente alteração da Constituição Chilena[5].

Cediço que, para além da proteção da privacidade - tendo o consentimento papel central -, outros neurodireitos, como a agência (autonomia e autodeterminação informativa) e sua correção com a preservação da identidade pessoal; o acesso

---

[3] Conforme DE OLIVEIRA, Vanessa Kelly Silva; COSTA, Lorena Faria; Cristiane Alves da Fonseca. Principais Aplicações da Biotecnologia na Medicina. Revista Eletrônica de Farmácia, Suplemento Vol 3 (2), 42-43, 2006, Disponível em: <https://revistas.ufg.br/REF/article/download/2106/2041/9094> Acesso 18/06/2022: "*No Campo da saúde, a biotecnologia pode levar à descoberta de novas formas de diagnosticar, tratar e prevenir doenças. O Diagnóstico pode ser feito através de técnicas desenvolvidas como anticorpos monoclonais, biosensores, sondas de DNA, chips de DNA, polimorfismo de fragmentos de restrição e reação em cadeia da polimerase.*" Outrossim, consoante DINIZ, Mariana de Oliveira; FERREIRA, Luís Carlos de Souza. Biotecnologia aplicada ao desenvolvimento de vacinas. Dossiê Biotecnologia, nº 24 , v. 70, 2010, Disponível em: <https://doi.org/10.1590/S0103-40142010000300003>. Acesso em 18/09/2022: "*A biotecnologia tem contribuído de forma decisiva para o aprimoramento de processos relacionados ao desenvolvimento e à produção de novas vacinas ou ao aprimoramento de vacinas já existentes para que se tornem mais seguras e eficazes. A disponibilização de vacinas profiláticas e a perspectiva de desenvolvimento de vacinas com efeito terapêutico para tumores associados ao HPV ilustram de forma clara o impacto que a biotecnologia moderna traz para o campo da pesquisa vacinal.*"

[4] Artigo 11, da LGPD.

[5] A Lei nº 21.383/2021 alterou a redação do artigo 19, item 1, da Constituição chilena, estabelecendo: *"El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella;"* Tradução livre: "*O desenvolvimento científico e tecnológico estará ao serviço das pessoas e será realizado com respeito pela vida e pela integridade física e mental. A lei regulará os requisitos, condições e restrições para seu uso em pessoas, e deve proteger especialmente a atividade do cérebro, bem como as informações dele.*". Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=1166983>. Acesso em 25/08/2022.

equitativos às tecnologias de integração cérebro-máquina; a proteção contra os vieses e a não-discriminação são dignatários de proteção especial.

Outrossim, a responsabilidade dos controladores e operadores quanto ao tratamento dos dados neurais também se revela como de assaz importância.

Este ensaio restringe-se a analisar a tessitura do consentimento no tratamento dos dados neurais, tendo por norte paradigmas éticos-jurídicos aplicáveis a órgãos, tecidos e biotecnologias, à luz da Magna Carta brasileira, documentos convencionais e da Lei Geral Proteção de dados.

2. Contextualização do problema

Hodiernamente, há plataforma interativa [6] "para comparar a morfologia cerebral derivada de qualquer amostra atual ou futura de dados de ressonância magnética[7].

BETHLEHEM e SEIDLITZ detalham os objetivos principais da ferramenta:

> (1) definir de forma robusta os processos normativos de mudanças relacionadas à idade e estratificadas por sexo em vários fenótipos derivados de ressonância magnética; (2) identificar marcos de crescimento cerebral não relatados anteriormente; (3) aumentar a sensibilidade para detectar efeitos ambientais genéticos e precoces na estrutura cerebral; e (4) fornecer tamanhos de efeito padronizados para quantificar a atipicidade neuroanatômica de varreduras cerebrais coletadas em vários distúrbios clínicos.[8]

Na Austrália, estudos científicos descobrem que "*Medir a atividade elétrica da retina em resposta ao estímulo de luz pode ser um biomarcador para TDAH e autismo*"[9]

---

[6] Criada por BETHLEHEM, R.A.I.; SEIDLITZ, J.; WHITE, S.R. et al. Brain charts for the human lifespan. **Nature,** nº 604, p. 525–533, 2022. Disponível em: <https://doi.org/10.1038/s41586-022-04554-y>. Acesso em 19/06/2022.

[7] Os quais podem ser consultados no seguinte endereço eletrônico: https://brainchart.shinyapps.io/brainchart/, acesso em 25/08/2022.

[8] Ob cit., vide nota 6

[9] Sobre o tema, ver a reportagem Disponível em: <https://neurosciencenews.com/adhd-asd-retina-20848/, acesso em 20/06/2022.

*Pesquisadores de Ronchester publicaram artigo no qual "um novo mecanismo neural(...) que ajuda o c*érebro a detectar o movimento do objeto durante o automovimento"[10].

Salientam que o estudo apresenta "novos insights sobre como o cérebro interpreta as informações sensoriais e pode ter aplicações no projeto de dispositivos de inteligência artificial e no (...) tratamentos e terapias para tratar distúrbios cerebrais."

Na Universidade do Texas, uma pesquisa apresenta uma "simulação dinâmica molecular de todos os átomos da fusão de vesículas sinápticas"[11].

Estudiosos da Universidade da Califórnia em Berkeley adaptaram fones de ouvido para "detectar sinais neurais e retransmitindo os dados de volta para smartphones via Bluetooth"[12].

Segundo os pesquisadores, a biotecnologia (earEEG) será transformada em plataforma, "para dar suporte a aplicativos de monitoramento de saúde e consumidores."

Pesquisadores da Northwestern University anunciam que algoritmos de aprendizado de máquinas identificaram "padrões de fala em crianças no espectro do autismo que são consistentes entre diferentes idiomas.[13]"

Enquanto isso, cientistas da Universidade da Califórnia em Los Angeles afirmam que a inteligência artificial "pode entender palavras e conceitos complexos, representando o significado das palavras de uma maneira semelhante [aos] julgamentos humanos."[14]

Estudantes da Universidade de Bristol apresentaram, em junho deste ano, no Congresso Internacional do Royal College, pesquisa a demonstrar que o tabagismo "*aumenta significativamente o risco de uma pessoa desenvolver esquizofrenia ou*

[10] Reportagem Disponível em: <https://neurosciencenews.com/motion-perception-movement-20879/>. Acesso em 20/06/2022.
[11] Ver em https://neurosciencenews.com/synaptic-transmission-20875/ , acesso em 20/06/2022
[12] Confira em https://neurosciencenews.com/eeg-earbuds-17975/, acesso em 20/06/2022.
[13] Ver a reportagem Disponível em: < https://neurosciencenews.com/ai-asd-language-20867/, acesso em 20/06/2022
[14] Sobre o assunto, ver https://neurosciencenews.com/ai-complex-words-20861/ ,acesso em 20/06/2022

depressão."[15]

Cientistas da Universidade de Columbia tem advertido para os efeitos colaterais do uso de interfaces cérebro computador, inclusive, v.g., experiência de despersonalização[16] pós estimulação elétrica transcraniana.[17]

No contexto do quadro pandêmico, a ausência de notificação compulsória das sequelas – e aqui vamos nos deter apenas àquelas que tenham sido constatadas por neurotecnologias, tais como a ressonância nuclear magnética -, representa um vazio epidemiológico relevante. Além disto, há que se perguntar como, por quem e para o quê os dados neurais coletados serão utilizados, mormente num contexto de compartilhamento – nacional e internacional – destas informações, para usos direitos e indiretos, por terceiros que nunca tiveram contato com o paciente.

Esta resenha indica a importância e a complexidade da proteção de dados neurais, tema objeto deste ensaio.

Analisaremos, em prosseguimento, o problema à luz do cenário internacional.

3. Tratamento do tema em âmbito internacional

A Declaração Universal Sobre Bioética e Direitos Humanos, celebrada em

[15] Ver a reportagem Disponível em: < https://neurosciencenews.com/smoking-schizophrenia-depression-20870/, acesso em 22/06/2022

[16]Conforme relatam YUSTE, R., Goering, S., ARCAS, B. *et al.* Four ethical priorities for neurotechnologies and AI. **Nature,** nº 551, p. 159–163, 2017. Disponível em: < https://doi.org/10.1038/551159a, acesso em 18/06/2022: "Some people receiving deep-brain stimulation through electrodes implanted in their brains have reported feeling an altered sense of agency and identity. In a 2016 study, a man who had used a brain stimulator to treat his depression for seven years reported in a focus group that he began to wonder whether the way he was interacting with others — for example, saying something that, in retrospect, he thought was inappropriate — was due to the device, his depression or whether it reflected something deeper about himself. He said: "It blurs to the point where I'm not sure ... frankly, who I am." Tradução livre: Algumas pessoas que receberam estimulação cerebral profunda por meio de eletrodos implantados em seus cérebros relataram sentir uma sensação alterada de agência e identidade. Em um estudo de 2016, um homem que usou um estimulador cerebral para tratar sua depressão por sete anos relatou em um grupo focal que começou a se perguntar se a maneira como estava interagindo com os outros – por exemplo, dizendo algo que, em retrospecto, ele pensava ser inapropriado - era devido ao dispositivo, sua depressão ou se refletia mais profundamente sobre ele. Ele disse: "Isso se confunde ao ponto de eu não ter certeza... francamente, quem eu sou."

[17] Sobre o tema, ver ROSA, Moacyr Alexandro. Eletroconvulsoterapia e estimulação magnética transcraniana: semelhanças e diferenças, **Scielo Brasil**. Disponível em: < https://doi.org/10.1590/S0101-60832004000500008, acesso em 10/06/2022; WASSERMANN, Eric M. Side effects of repetitive transcranial magnetic stimulation Anxiety e Depression Association of America, 2000. Disponível em: < https://doi.org/10.1002/1520-6394(2000)12:3<124::AID-DA3>3.0.CO;2-E. Acesso em 22/06/2022.

Paris, em 2005, pondera a preocupação com o crescimento exponencial das tecnologias, que paulatinamente ressignifica nossa autocompreensão e a percepção da biosfera em que vivemos, "resultando em uma forte exigência de uma resposta global para as implicações éticas de tais desenvolvimentos".

O documento convencional considera que as aplicações tecnológicas devem respeitar a dignidade da pessoa humana, os direitos humanos e a liberdades fundamentais, declinando-os expressamente no artigo 2º, IV[18], que trata dos objetivos do tratado.

Neste contexto, exorta a comunidade científica internacional a pautar-se por *standards* universais "que proporcionarão uma base para a resposta da humanidade aos sempre crescentes dilemas e controvérsias que a ciência e a tecnologia apresentam à espécie humana e ao meio ambiente".

A dignidade humana e os Direitos Humanos compõem o conjunto principiológico do documento, merecendo destaque o artigo 3º, alínea (b), *verbis*: "Os interesses e o bem-estar do indivíduo devem ter prioridade sobre o interesse exclusivo da ciência ou da sociedade."

O artigo 4º[19] da normativa trata da relação de proporcionalidade entre o benefícios direitos e indiretos a pacientes e os potenciais danos.

O artigo 5º da Convenção em testilha trata da autonomia e responsabilidade individuais e da representação dos incapazes para dar o consentimento, cuja disciplina é objeto do artigo 6º.

A alínea "a" do artigo trata do consentimento no caso de intervenções médicas -e de profissionais de outras áreas da saúde, por analogia -, no caso de intervenções preventivas ou terapêuticas.

---

[18] *Verbis* (grifamos): *"reconhecer a importância da liberdade da pesquisa científica e os benefícios resultantes dos desenvolvimentos científicos e tecnológicos, evidenciando, ao mesmo tempo,* ***a necessidade de que tais pesquisas e desenvolvimentos ocorram conforme os princípios éticos dispostos nesta Declaração e respeitem a dignidade humana, os direitos humanos e as liberdades fundamentais".***

[19] *Cuja redação é a seguinte: Os benefícios diretos e indiretos a pacientes, sujeitos de pesquisa e outros indivíduos afetados devem ser maximizados e qualquer dano possível a tais indivíduos deve ser minimizado, quando se trate da aplicação e do avanço do conhecimento científico, das práticas médicas e tecnologias associadas*.

Tais condutas dependerão de consentimento "prévio, livre e esclarecido do indivíduo envolvido, baseado em informação adequada", revogável a qualquer tempo.

No âmbito da pesquisa científica (artigo 6º, "b"), o consentimento terá a mesma conformação, ou seja, deverá ser prévio, livre, expresso e esclarecido, baseado em informação adequada, erigida numa linguagem compreensível, incluindo o protocolo para a revogação da aquiescência.

No caso do artigo 6º, "b", a exceção ao modelo será excepcional e desde que fundada em "(...) padrões éticos e legais adotados pelos Estados, consistentes com as provisões da presente Declaração, particularmente com o Artigo 27[20] e com os direitos humanos."

Em ambas as situações, a revogação do consentimento não pode gerar qualquer desvantagem ou preconceito a pacientes.

A Declaração Universal Sobre Bioética e Direitos Humanos (artigo 6º, "c") ainda regula a situação do consentimento, no caso de pesquisas científicas em grupos de indivíduos ou comunidades estabelecendo que nada pode substituir a aquiescência individualizada, com todos os predicados já destacados, mesmo que o representante do grupo ou da comunidade possa manifestar um consentimento adicional.

A Convenção sobre Direitos Humanos e Biomedicina do Conselho da Europa, adotada em 1997 e que entrou em vigor em 1999 e seus protocolos adicionais tratam do consentimento no artigo 5º[21]. A regra geral está estruturada no mesmo arquétipo principiológico da Declaração Universal Sobre Bioética e Direitos Humanos à qual nos reportamos. A exceção, no artigo 8º[22], relative à situações de urgência da

---

[20] Declaração Universal Sobre Bioética e Direitos Humanos, artigo 27: *"Limitações à Aplicação dos Princípios. Se a aplicação dos princípios da presente Declaração tiver que ser limitada, tal limitação deve ocorrer em conformidade com a legislação, incluindo a legislação referente aos interesses de segurança pública para a investigação, constatação e acusação por crimes, para a proteção da saúde pública ou para a proteção dos direitos e liberdades de terceiros. Quaisquer dessas legislações devem ser consistentes com a legislação internacional sobre direitos humanos."*

[21] Convenção sobre Direitos Humanos e Biomedicina do Conselho da Europa, artigo 5: *"Regra geral. Qualquer intervenção no domínio da saúde só pode ser efectuada após ter sido prestado pela pessoa em causa o seu consentimento livre e esclarecido. Esta pessoa deve receber previamente a informação adequada quanto ao objectivo e à natureza da intervenção, bem como às suas consequências e riscos. A pessoa em questão pode, em qualquer momento, revogar livremente o seu consentimento."*

[22] Convenção sobre Direitos Humanos e Biomedicina do Conselho da Europa, artigo 8: *"Situações de urgência Sempre que, em virtude de uma situação de urgência, o consentimento apropriado não puder*

intervenção médica.

O artigo 6º[23] do Documento convencional em testilha trata da "Protecção das pessoas que careçam de capacidade para prestar o seu consentimento"; o artigo 7º[24], a seu turno, cuida da "Protecção das pessoas que sofram de perturbação mental"; o artigo 9º[25], da consideração da vontade anteriormente manifestada para o suprimento do consentimento daquele que, no momento da intervenção, não esteja em condições de consentir.

No âmbito da OCDE, a Recomendação do Conselho de Inovação Responsável em Neurotecnologia traz importantes diretivas, dentre elas a proteção de "dados pessoais do cérebro e outras informações obtidas por meio da neurotecnologia", prescrevendo ações a seres adotadas pelos controladores e operadores[26].

---

ser obtido, poder-se-á proceder imediatamente à intervenção medicamente indispensável em benefício da saúde da pessoa em causa."

[23] Convenção sobre Direitos Humanos e Biomedicina do Conselho da Europa, artigo 6: *"Protecção das pessoas que careçam de capacidade para prestar o seu consentimento 1. Sem prejuízo dos artigos 17.º e 20.º, qualquer intervenção sobre uma pessoa que careça de capacidade para prestar o seu consentimento apenas poderá ser efectuada em seu benefício directo. 2. Sempre que, nos termos da lei, um menor careça de capacidade para consentir numa intervenção, esta não poderá ser efectuada sem a autorização do seu representante, de uma autoridade ou de uma pessoa ou instância designada pela lei. A opinião do menor é tomada em consideração como um factor cada vez mais determinante, em função da sua idade e do seu grau de maturidade. 3. Sempre que, nos termos da lei, um maior careça, em virtude de deficiência mental, de doença ou por motivo similar, de capacidade para consentir numa intervenção, esta não poderá ser efectuada sem a autorização do seu representante, de uma autoridade ou de uma pessoa ou instância designada pela lei. A pessoa em causa deve, na medida do possível, participar no processo de autorização. 4. O representante, a autoridade, a pessoa ou a instância mencionados nos nºs 2 e 3 recebem, nas mesmas condições, a informação citada no artigo 5.º 5. A autorização referida nos nºs 2 e 3 pode, em qualquer momento, ser retirada no interesse da pessoa em questão."*

[24] Convenção sobre Direitos Humanos e Biomedicina do Conselho da Europa, artigo 7: *"Protecção das pessoas que sofram de perturbação mental. Sem prejuízo das condições de protecção previstas na lei, incluindo os procedimentos de vigilância e de controlo, bem como as vias de recurso, toda a pessoa que sofra de perturbação mental grave não poderá ser submetida, sem o seu consentimento, a uma intervenção que tenha por objectivo o tratamento dessa mesma perturbação, salvo se a ausência de tal tratamento puser seriamente em risco a sua saúde."*

[25] Convenção sobre Direitos Humanos e Biomedicina do Conselho da Europa, artigo 9: *"Vontade anteriormente manifestada. A vontade anteriormente manifestada no tocante a uma intervenção médica por um paciente que, no momento da intervenção, não se encontre em condições de expressar a sua vontade, será tomada em conta."*

[26] *Trata-se um conjunto de dez diretrizes, a saber: "a)Fornecer informações claras ao público e aos participantes da pesquisa sobre a coleta, armazenamento, processamento e uso potencial de dados cerebrais pessoais coletados para fins de saúde; b)Garantir a existência de meios de obtenção de consentimento adequados para proteger a autonomia dos indivíduos, incluindo a consideração de casos especiais de capacidade limitada de tomada de decisão; c)Promova oportunidades para que os indivíduos escolham como seus dados são usados e compartilhados, incluindo opções para acessar, alterar e excluir dados pessoais; d)Promover políticas que protejam os dados cerebrais pessoais de serem usados para discriminar ou excluir inadequadamente certas pessoas ou populações, especialmente para fins comerciais ou no contexto de processos legais, emprego ou seguro;*

A Declaração de Helsink[27], que estabelece os princípios éticos para as pesquisas médicas em seres humanos, remonta a 1964 e passou por sete revisões, a última no Brasil, em 2013, bem como duas alterações[28].

A principiologia básica da Declaração original, composta por cinco diretrizes, foi incrementada para doze, tendo por escopo principalmente a pesquisa clínica terapêutica e a pesquisa biomédica puramente científica.

Desde 1982, a Declaração incorporou as Diretrizes Éticas Internacionais para Pesquisas Biomédicas Envolvendo Seres Humanos do Conselho das Organizações Internacionais de Ciências Médicas (CIOMS) em colaboração com a Organização Mundial da Saúde (OMS)[29].

Na revisão de 1983, o foco foi a normatização do consentimento dos incapazes[30]; em 1989, a Declaração definiu a função e estrutura de um comitê de ética independente do pesquisador[31].

---

e)Proteger as informações obtidas por meio da aplicação de neurotecnologia contra uso não autorizado, inclusive por meio do uso de acordos de acesso a dados, quando apropriado. f)Promova a confidencialidade e a privacidade e reduza as violações de segurança, inclusive por meio da implementação de padrões de segurança rigorosos. g)Garantir não apenas a rastreabilidade dos dados coletados e processados, mas também dos atos médicos em que a neurotecnologia é utilizada."

[27]Declaração de Helsink Disponível em: <https://www.fcm.unicamp.br/fcm/sites/default/files/declaracao_de_helsinque.pdf>. Acesso em 20/06/2022.

[28] Primeira revisão ocorrida por ocasião da 29ª Assembleia Médica Mundial, em Tóquio, no Japão, em 1975; a segunda, na 35ª Assembleia, em Veneza, na Itália, em 1983; a terceira, na 41ª Assembleia, em Hong Kong, em 1989; a quarta, na 48ª Assembleia em Sommerset West, na África do Sul, em 1996; a quinta, na 52ª Assembleia, em Edimburgo, na Escócia, em outubro de 2000; a sexta, na 59ª Assembleia, em Seul, Coreia do Sul, em outubro de 2008; a sétima, na 64ª Assembleia, em Fortaleza, Brasil, em outubro de 2013; Além das revisões, ocorreram duas alterações: alteração ocorrida na 53ª Assembleia, em Washington, Estados Unidos, em 2002 (Nota no parágrafo 29); Alteração ocorrida na 55ª Assembleia, em Tóquio, Japão, em 2004 (Nota no parágrafo 30).

[29] Diretrizes Éticas Internacionais para Pesquisas Biomédicas Envolvendo Seres Humanos do Conselho das Organizações Internacionais de Ciências Médicas (CIOMS). Disponível em: <https://cioms.ch/wp-content/uploads/2018/11/CIOMS-final-Diretrizes-Eticas-Internacionais-Out18.pdf>.Acesso em 20/06/2022.

[30] Objeto dos §§ 24 e 25 do item B (Princípios básicos para toda pesquisa clínica): *24. Para sujeitos de pesquisa que forem legalmente incompetentes, incapazes física ou mentalmente de dar o consentimento ou menores legalmente incompetentes, o pesquisador deverá obter o consentimento informado do representante legalmente autorizado, de acorde com a legislação apropriada. Esses grupos não devem ser incluídos em pesquisas, a menos que sejam necessárias para promover a saúde da população representada e não podem, em seu lugar, ser realizadas em indivíduos legalmente competentes; 25. Quando um sujeito considerado legalmente incompetente, como uma criança menor, é capaz de aprovar decisões sobre a participação no estudo, o pesquisador deve obter esta aprovação, além do consentimento, do representante legalmente autorizado.*

[31] Conforme dos §§ 13 e 14 do item B das Diretrizes Éticas Internacionais para Pesquisas Biomédicas Envolvendo Seres Humanos do Conselho das Organizações Internacionais de Ciências Médicas

A revisão de 2000 estabelece que "Os benefícios, riscos, encargos e eficácia de um novo método devem ser testados comparativamente com os melhores métodos atuais profiláticos, diagnósticos e terapêuticos existentes"[32].

A Declaração em tela prescreve a indeclinabilidade do consentimento prévio, informado, livre, espontâneo, devidamente esclarecido, revogável a qualquer tempo[33], como *conditio sine qua non* para qualquer pesquisa científica envolvendo seres humanos. Horrorizada com o caso Tuskegee[34], a comunidade científica reagiu com

---

(Princípios básicos para toda pesquisa clínica): "*13. O desenho e a realização de cada procedimento experimental envolvendo seres humanos devem ser claramente discutidos no protocolo experimental. Esse protocolo deve ser submetido à análise, com comentários, orientações e, quando apropriado, à aprovação de um comitê de ética médica especialmente indicado, que deve ser independente do pesquisador e do patrocinador de estudo ou qualquer outro tipo de influência indevida. Esse comitê de ética independente deve estar de acordo com as regulações e leis do país no qual a pesquisa clínica será conduzida; 14. O comitê tem o direito de monitorar estudos em andamento. O pesquisador tem obrigação de fornecer informações de monitoração ao comitê, especialmente qualquer evento adverso sério. O pesquisador deve também submeter ao comitê, para revisão, informações sobre financiamento, patrocinador, afiliações institucionais, outros conflitos de interesses em potencial e incentivos aos sujeitos.*"

[32] *C. Princípios adicionais para pesquisa clínica combinada a cuidados médicos. 29. Os benefícios, riscos, encargos e eficácia de um novo método devem ser testados comparativamente com os melhores métodos atuais profiláticos, diagnósticos e terapêuticos existentes. Isso não inclui o uso de placebo ou de não-tratamento em estudo que não existam métodos profiláticos, diagnósticos ou terapêuticos comprovados.*

[33] Conforme dicção do § 22 do item B (Princípios básicos para toda pesquisa clínica) das Diretrizes Éticas Internacionais para Pesquisas Biomédicas Envolvendo Seres Humanos do Conselho das Organizações Internacionais de Ciências Médicas, *verbis*: "*Em qualquer pesquisa envolvendo seres humanos, cada paciente em potencial deve estar adequadamente informado dos objetivos, métodos, fontes de financiamento, quaisquer possíveis conflitos de interesse, aflições institucionais do pesquisador, os benefícios antecipados e riscos em potencial do estudo e qualquer desconforto a que possa estar vinculado. O sujeito deverá ser informado da liberdade de se abster de participar do estudo ou de retirar seu consentimento para sua participação em qualquer momento, sem retaliação. Após assegurar-se de que o sujeito entendeu toda a informação, o médico deverá então obter seu consentimento informado espontâneo, preferencialmente por escrito. Se o consentimento não puder ser obtido por escrito, o consentimento não-escrito deve ser formalmente documentado e testemunhado.*"

[34] Conforme descrito por GOLDIM, José Roberto, Disponível em: < https://www.ufrgs.br/bioetica/tueke2.htm>. Acesso em 20/06/2022: *"De 1932 a 1972 o Serviço de Saúde Pública dos Estados Unidos da América realizou uma pesquisa, cujo projeto escrito nunca foi localizado, que envolveu 600 homens negros, sendo 399 com sífilis e 201 sem a doença, da cidade de Macon, no estado do Alabama. (...) Não foi dito aos participantes do estudo de Tuskegee que eles tinham sífilis, nem dos efeitos desta patologia. O diagnóstico dado era de "sangue ruim". (...) A contrapartida pela participação no projeto era o acompanhamento médico, uma refeição quente no dia dos exames e o pagamento das despesas com o funeral. Durante o projeto foram dados, também, alguns prêmios em dinheiro pela participação. (...) A inadequação foi omitir o diagnóstico conhecido e o prognóstico esperado. (...) A inadequação do estudo foi seguindo o padrão conhecido como "slippery slope", isto é, uma inadequação leva a outra e o problema vai se agravando de forma crescente. Da omissão do diagnóstico se evoluiu para o não tratamento, e deste para o impedimento de qualquer possibilidade de ajuda aos participantes.(...) Em 1969, a imprensa noticiou a confirmação de que já tinham ocorrido 28 mortes no estudo. (...) a repórter Jean Heller, da Associated Press, publicou no New York Times, em 26/7/72, uma matéria denunciando este projeto, que houve uma forte*

o Relatório de Belmont, o qual compila dos princípios éticos básicos para a pesquisa biomédica com seres humanos: respeito às pessoas; beneficência; justiça.

O Relatório de Belmont prima pelo consentimento guarnecido por três elementos: informação, compreensão e voluntariedade, os quais são minudentemente descritos no item 1, relativo ao consentimento informado[35].

Nos casos de emergência epidemiológica, prevalece o Regulamento Sanitário Internacional (RSI 2005), incorporado ao direito pátrio pelo Decreto Legislativo nº 395/2009 e promulgado pelo Decreto nº 10.212, de 30 de janeiro de 2020.

O RSI 2005 fixa diretrizes a serem observadas pelos Estados-parte quando do tratamento de dados pessoais, em situações especiais, *ex vi* do artigo 45, § 2º[36].

A conferência de Asilomar, havida em 2017, na Califórnia, trata dos princípios éticos aplicáveis ao desenvolvimento da inteligência artificial. Abstraindo a restrição do espectro protetivo apenas aos dados gerados pelo titular - inaplicável no Brasil, pois a LGPD abrange o tratamento como um todo, envolvendo a lista não exaustiva dos verbos nucleares do artigo 5º, X; da Lei nº 13.709/2018[37] -, no que toca ao consentimento (objeto do 12º princípio[38] do Documento em tela), acompanha em

---

repercussão social e política sobre o mesmo. Após 40 anos de acompanhamento dos participante, ao término do projeto, somente 74 sobreviveram. Mais de 100 participantes morreram de sífilis ou de complicações da doença. A instituição responsável pela condução do projeto, na suas últimas etapas, foi o Centro de Controle de Doenças (CDC) de Atlanta. Em 1997 existiam apenas 8 pessoas ainda vivas. O governo norte-americano decidiu fazer um pedido de desculpas formais a todos os que foram enganados durante o experimento de Tuskegee."

[35] U.S. Department of Health and Human Services (HHS). Office for Human Research Protections. Belmont Report Disponível em: <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>. Acesso em 20/06/2022, *verbis*: *1. Consentimento informado. -- O respeito pelas pessoas exige que os sujeitos, na medida em que sejam capazes, tenham a oportunidade de escolher o que deve ou não acontecer com eles. Esta oportunidade é fornecida quando os padrões adequados para o consentimento informado são satisfeitos. Embora a importância do consentimento informado seja inquestionável, prevalece a controvérsia sobre a natureza e a possibilidade de um consentimento informado. No entanto, há um consenso generalizado de que o processo de consentimento pode ser analisado como contendo três elementos: informação, compreensão e voluntariedade.*

[36] Que tem a seguinte redação: "*(a) processados de modo justo e legal, e sem outros processamentos desnecessários e incompatíveis com tal propósito; (b) adequados, relevantes e não excessivos em relação a esse propósito; (c) acurados e, quando necessário, mantidos atualizados; todas as medidas razoáveis deverão ser tomadas a fim de garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e (d) conservados apenas pelo tempo necessário*".

[37] Cujo teor é o seguinte: "*Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;*"

[38] *Verbis*: "12) Personal Privacy: People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data." Tradução livre: As pessoas

linhas gerais a tessitura vista nos demais documentos internacionais mencionados, devendo ser prévio e explícito, revogável a qualquer tempo[39].

Dentre os 23 princípios, destacamos também a diretiva segundo a qual a "superinteligência só deve ser desenvolvida a serviço de ideias éticos amplamente compartilhados e para o benefício de toda a humanidade."

A Resolução do Parlamento Europeu 2020/2012 aborda, dentre outros aspectos[40] éticos da inteligência artificial, centrada em parâmetros antropocêntricos e antropogênicos, considerando o respeito à dignidade humana, à autonomia e à autodeterminação; a prevenção de danos, a promoção da equidade, a inclusão e a transparência, a proteção contra os vieses e a discriminação; a limitação das externalidades negativas da tecnologia utilizada, a explicabilidade das tecnologias e seu caráter instrumental para aumentar o bem-estar para todos os seres humanos.

Passemos ao exame do estado da arte no Brasil.

4. Estado da arte no brasil

No Brasil, a elevação do direito à proteção de dados ao *status* de direito fundamental explícito (artigo 5º, LXXIX, *in fine*), por meio da Emenda Constitucional nº 115/2022[41], representa um grande avanço para a densificação de seu âmbito de proteção, sua substancialidade formal e material, os direitos autônomos e as posições subjetivas decorrente.

Antes mesmo da dicção do Poder Constituinte derivado, o plenário do Supremo Tribunal Federal já tinha consolidado a proteção de dados e a autodeterminação informativa como direitos fundamentais autônomos, em decisão célebre, havida nos autos da Medida Cautelar na ADI 6393 MC[42], sob a relatoria da

devem ter o direito de acessar, gerenciar e controlar os dados que geram, dado o poder dos sistemas de IA de analisar e utilizar esses dados.

[39] Cujo inteiro teor consta no sítio oficial da Future of Life Institute (FLI). Disponível em: <https://futureoflife.org/2017/08/11/ai-principles/>. Acesso em 22/06/2022.

[40] Responsabilidade civil e propriedade intelectual.

[41] Que também introduz o inciso XXVI ao *caput* do art. 21 e o inciso XXX ao *caput* do art. 22 ambos da Constituição Federal.

[42] Que foi julgada conjuntamente com as ADIs 6.387, 6.388, 6.389, 6.390.

Ministra ROSA WEBER[43].

No centro da controvérsia, o compartilhamento de dados pessoais ao IBGE, especificamente dos dados dos usuário dos serviços de telefonia móvel e fixa, pelas respectivas operadoras, supostamente para dar "suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus", autorizado pela Medida Provisória nº 954/2020[44] e regulamentado pela Instrução Normativa IBGE nº 2/2020[45].

A decisão da composição plenária do Sodalício referendou a liminar concedida[46]. No legislativo, tramita o projeto de lei nº 522/2022, de autoria do

---

[43] BRASIL, Supremo Tribunal Federal. ADI-MC 6393, Relatora: Ministra Rosa Weber. Tribunal Pleno, julgado em 07/05/2020, DJU-e 12/11/2020.

[44] BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Diário Oficial da União: 17/4/2020. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em: 20/06/2022.

[45]BRASIL, IBGE. Instrução Normativa nº 2, de 17/04/2020, Disponível em: <http://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-17-de-abril-de-2020-253341223>. Acesso em 20/06/2022.

[46] Em acórdão assim ementado (grifamos): (...) 1. Decorrências dos direitos da personalidade, foram positivados, o respeito à privacidade e o respeito à autodeterminação informativa, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança quanto a esses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

deputado federal Carlos Henrique Gaguim (REPUBLIC-TO), que "modifica a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção."

Conforme a proposta, a redação do artigo 5º da LGPD seria alterada para albergar os dados neurais como dados sensíveis (inciso II), conceituar esta categoria semântica, introduzindo o inciso XX, a interface cérebro-computador (inciso XXI) e a neurotecnologia (inciso XXII).

Dados neurais, conforme o texto propositivo, seria a informação acedida, direta ou indiretamente "da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador, ou qualquer outra tecnologia, invasivas ou não-invasivas".

A conceituação telada pretendeu atingir um conjunto de situações em que dados neurais possam ser coletados, optando pela técnica clausular aberta ("ou qualquer outra tecnologia"), o que é adequado, pois propicia abertura dialógica com o movimento incremental da tecnologia.

Outrossim, possibilita compreender que a neuroplasticidade[47], que ocorre tanto em nível celular como macroestrutural[48], está inserida no âmbito protetivo, que teria, então, tessitura analítico-comportamental.

Partindo do pressuposto de que esta premissa está correta, a proteção dos

[47] Conforme ORTU, D.; VAIDYA, M.. The Challenges of Integrating Behavioral and Neural Data: Bridging and Breaking Boundaries Across Levels of Analysis. Behav Anal, 2016, nº 40(1), p. 209/224. Disponível em: <10.1007/s40614-016-0074-5>. Acesso em 20/06/2022: *"(...)neuroplasticidade é uma perspectiva de ponte de fronteira consistente com a ideia de que o cérebro é um sistema flexível e em constante mudança. Mais especificamente, a pesquisa em neuroplasticidade se concentra na relação entre mudanças no nível comportamental e alterações correspondentes no nível neural, mostrando como a atividade e as estruturas cerebrais podem variar ao longo do tempo em função da exposição a variáveis ambientais. Descobriu-se que as alterações neurais relacionadas à contingência envolvem várias áreas do cérebro, incluindo os córtices cerebrais visuais e auditivos, anteriormente considerados estáveis após as primeiras janelas críticas de aprendizado."*

[48] idem .

dados neurais interage com a neurociência[49] analítico-comportamental[50] e incorpora os desafios neuroéticos[51].

Temos que ter em mente que não há neutralidade científica, pois a ciência é conduzida por seres humanos, que são suscetíveis a idiossincrasias, vieses e preconceitos.

Neste contexto, circunstanciando a profundidade dos desafios éticos de que trata, podemos citar a transformação de dados neurais em informações digitais para propósitos bélicos ou como instrumento de eugenia. Neurociências e engenharia genética tem grande afinidade e são moduladas por mecanismos de contenção similares.

Outrossim, não se pode olvidar as aplicações da epigenétic[52-53],especialmente

---

[49] TONINATO, Maria Alice Dittert. Desafios éticos e bioéticos da neurociência. Bioética. Disponível em: <http://www.saocamilo-sp.br/pdf/bioethikos/57/Desafios_eticos_e_bioeticos_da_neurociencia.pdf>. Acesso em 20/06/2022: *"(...)a neurociência estuda o modo como funcionam os neurônios e a importância das restantes células do tecido nervoso, as células da glia, o equilíbrio funcional desse tecido, buscando compreender os mecanismos da memória, o modo como se geram as emoções e os mecanismos da neurodegenerescência, que ocorrem em doenças como, por exemplo, a de Alzheimer e a de Parkinson."*

[50] ORTU a VAIDYA apresentam o conceito funcional da neurociência analítico-comportamental, *verbis*: *"A neurociência analítico-comportamental (...) está preocupada em entender sob quais condições as respostas cerebrais podem ser consideradas comportamento e interpretadas apenas dentro de uma estrutura comportamental.(...) alguns sistemas de medição neurocientíficos podem ser considerados simplesmente como ferramentas extras à disposição do analista do comportamento."*

[51] TONINATO, ob cit.: *"A ética da neurociência e a neurociência da ética compõem a neuroética em si e equivale à bioética, considerando-se a especificidade do sistema nervoso e os impactos dos estudos sobre as estruturas sociais e legais."*

[52] Segundo LEITE, Michel Lopes; COSTA, Fabricio F. Epigenômica, epigenética e câncer. Rev Pan-Amaz Saude, Ananindeua, v. 8,n. 4,p. 23-25, dez. 2017. Disponível em: < http://dx.doi.org/10.5123/s2176-62232017000400006>. Acesso em 26/06/2022, epigenética respeita "aos mecanismos baseados na cromatina importantes na regulação da expressão gênica que não envolvem alterações na sequência de DNA.(...) a epigenética foi considerada o epicentro da biomedicina moderna, devido ao estudo da hereditariedade não relacionada à sequência de DNA que pode ajudar a explicar a relação entre a origem genética de um indivíduo, do meio ambiente, envelhecimento e de uma doença."

[53] MARCHIORO, Mariana et al. Relação entre Doença de Parkinson e Modulação Epigenética. Revista Neurociências, 27, 2019. p. 1/16. Disponível em: <https://periodicos.unifesp.br/index.php/neurociencias/article/download/9615/7365/40177as>. Acesso em 20/06/2022, "O termo epigenética refere-se a modificações na expressão gênica que ocorrem independentemente de mudanças na sequência primária do DNA e são adquiridas ao longo da vida. Este processo pode ser decorrente de fatores ambientais, tais como estilo de vida como a dieta, prática de exercício físico e exposição a toxinas, resultando em mudanças fenotípica."

a neuro-epigenética cognitiva[54], que apenas robustecem a indeclinabilidade da proteção eficiente e segura dos dados neurais.

Conceituando *brain-computer interface* (BCI)[55], o projeto de lei a concebe como "qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático".

Numa acepção alternativa, a proposta legislativa inclui no espectro conceitual da BCI a substituição, a restauração, a complementação ou melhoramento "da atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo."

As neurotecnologias[56], a seu turno, seriam um "conjunto de dispositivos, métodos ou instrumentos não farmacológicos que permitem uma conexão direta ou indireta com o sistema nervoso."

Neste nicho, merecem destaque as neuropróteses[57], as técnicas de neuroimagem[58].

Por fim, a proposta acrescenta a seção II-A ao capítulo II da Lei n° 13.709/2018, sobre o tratamento dos dados neurais, que somente será admitido se

---

[54] Sobre o tema, Cf.: MARSHALL, P.; BREDY, T. Neuroepigenética cognitiva: a próxima evolução em nossa compreensão dos mecanismos moleculares subjacentes à aprendizagem e memória? **Nature**, 2016. Disponível em: < https://doi.org/10.1038/npjscilearn.2016.14>. ,Acesso em: 20.09/2022.

[55] *Sobre o tema, cf. HINOJOSA, Alfredo Quiñones, Brain-Computer Interfacing: Prospects and Technical Aspects of Functional Cranial Implants. Science Direct, 2022. Disponível em: < https://www.sciencedirect.com/topics/neuroscience/brain-computer-interface>. Acesso em: 20/06/2022.*

[56] Conforme Estudo de Tendências Tecnológicas Neurociência e Neurotecnologia da BRAIN (Brazilian Institute of Neuroscience and Neurotechnology), Disponível em: <https://www.brainn.org.br/wp-content/uploads/2018/11/CEPID-BRAINN-Estudo-de-Tend%C3%AAncias-em-Neurotecnologias-2018> Acesso em 20/06/2022, um exemplo de neurotecnologia é o *"dispositivo de fibra ótica para medição clínica, que auxilia as avaliações diagnósticas de pacientes que sofreram um AVC. De maneira simplificada, a luz no infravermelho próximo consegue atravessar a pele e o crânio e interage com as moléculas de hemoglobina no nosso sangue. Assim é possível podemos enxergar, em tempo real, o que está acontecendo no cérebro de pacientes que sofreram um AVC."*

[57] Sobre o assunto: DE OLIVEIRA, José Oswaldo Júnior; CORRÊA, Cláudio Fernandes; FERREIRA, Jânio Alves. Tratamento invasivo para o controle da dor neuropática. **Scielo**, Disponível em: <https://www.scielo.br/j/rdor/a/VbzLfkxjWJyTwq4mXJ8v38M/?lang=pt>. Acesso em 20/06/2022.

[58] Como muito bem apanhado pelo autor do projeto de lei, *"Existe, hoje em dia, uma quantidade muito grande de técnicas de neuroimagem. Apenas para ficar em alguns exemplos, podemos citar a tomografia computadorizada, que se baseia em técnicas de hemodinâmica, medindo e deduzindo a atividade cerebral do fluxo sanguíneo, a tomografia por emissão de pósitrons (PET), a tomografia computadorizada por emissão de fóton único (SPECT), e, mais importante, a ressonância magnética funcional (fMRI) e a eletroencefalografia (EEG), que se vale de métodos para a coleta de atividades de dados sobre atividades eletromagnéticas do cérebro. Tudo isso é tecnologia que vem avançando e pode implicar problemas futuros para o tratamento de dados neurais*".

o titular ou seu representante legal consentir, específica e destacadamente, mesmo em circunstâncias clínicas (artigo 13-A, I)[59], com o expresso esclarecimento sobre os possíveis efeitos físicos, cognitivos e emocionais de sua aplicação, as contraindicações (Artigo 13-A, §único)[60].

As hipótese de tratamento de dados neurais sem o consentimento do titular são especificadas no artigo 13-A, II[61], tendo por nota comum a indispensabilidade do tratamento para estudos por órgãos de pesquisa, proteção da vida e da incolumidade física do titular ou de terceiro, tutela da saúde.

A proteção à identidade individual do titular dos dados neurais é peremptória[62]; a vedação absoluta da comunicação ou uso compartilhado dos dados neurais, com fins econômicos[63]; é dever do Estado assegurar acesso equitativo a neurotecnologias (artigo 13-E); inaplicam-se aos dados neurais as exceções previstas no inciso I e inciso II, alínea 'a', do art. 4º (artigo 13-D).

A ausência de neutralidade ou insignificância em processamento de dados é a premissa basal da justificativa da proposta, sendo sempre iminente potencial, latente, iminente ou concreto o risco à intimidade, mormente em se tratando de dados neurais.

Se para a pegada digital já fora reconhecido que a proteção dos dados pessoais é direito fundamental autônomo (STF, ADI 6393; EC 115/2022), a questão

---

[59] Cujo teor é o seguinte (grifamos): "*Seção II-A Do Tratamento de Dados Neurais. Art. 13-A O* ***tratamento de dados neurais somente ocorrerá*** *quando: I - o titular ou o responsável legal* ***consentir, de forma específica e destacada****, para* ***finalidades específicas****, mesmo em circunstâncias clínicas ou nos casos em que a interface cérebro-computador tenha a capacidade de tratar dados com o titular inconsciente".*

[60] Cujo teor é o seguinte (grifamos): "*Parágrafo único. O* ***pedido de consentimento para o tratamento de dados neurais deve indicar, de forma clara e destacada, os possíveis efeitos físicos, cognitivos e emocionais de sua aplicação, as contraindicações*** *bem como as normas sobre privacidade e as medidas de segurança da informação adotadas".*

[61] Cujo teor é o seguinte (grifamos): "*II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) realização de estudos por órgão de pesquisa, garantida a anonimização dos dados pessoais sensíveis; b) proteção da vida ou da incolumidade física do titular ou de terceiro; c) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;"*

[62] Conforme dicção do artigo 13-B, *verbis* (grifamos): **É vedado o uso de qualquer interface cérebro computador ou método que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua integridade psicológica**.

[63] Na forma do artigo 13-C (grifamos): ***"É vedada a comunicação ou o uso compartilhado entre controladores de dados neurais com objetivo de obter vantagem econômica."***

hipertrofia-se no caso dos dados neurais, que são a última instância da intimidade, da autonomia e da identidade humanas.

Não por acaso, a tessitura do consentimento para o tratamento dos dados neurais vem erigida de maneira mais detalhada se comparada ao regime dos dados sensíveis. Afinal, acessar dados neurais significa o poder de "revelar lembranças, pensamentos, padrões comportamentais, emoções, sonhos e mesmo os desejos mais íntimos."

Há que se ter em conta que o indivíduo participa ativamente da construção do seu rastro digital. Atua conscientemente, por meio de *cookies e likes*, v.g., muito embora não se possa negligenciar a comunicação subliminar na *internet* e seu papel persuasivo[64], assunto que exorbita destas linhas.

Na coleta de dados neurais poderão vir à tona "pensamentos que jamais viriam a ser comunicados ou transformados em ações, ou mesmo podem ser registradas informações do nosso subconsciente."

O subscritor da proposta sustenta que "Os dados neurais não se confundem com dados biométricos pois não constituem órgãos ou tecidos corporais.".

Não obstante, o projeto de lei veda o uso comercial de dados neurais (artigo 13-C), tal qual a disciplina destinada a órgãos e tecidos[65].

O tratamento dos dados neurais, tal como modulados na proposta legislativa, vais na direção da proteção dos neurodireitos fundamentais, quais sejam: "a) o direito à privacidade mental; b) o direito à identidade e autonomia pessoal; c) o direito ao livre arbítrio e autodeterminação; d) o direito ao acesso equitativo ao aumento cognitivo; e e) o direito à proteção contra a discriminação algorítmica ou as decisões tomadas."

---

[64] Sobre o tema, vide MUA, Cíntia Teresinha Burhalde. Publicidade comportamental e assédio de consumo dos hipervulneráveis, com foco na criança e no idoso: aportes neurocientíficos para superação da ineficiência da contrapropaganda na internet. In: MUA, Cíntia Teresinha Burhalde; SILVA, Ângelo Roberto Ilha da.; CARDOSO, Renato César. (Orgs). Neurociências aplicadas ao Direito. Porto Alegre, RS: Editora Fundação Fênix, 2022.

[65] Lei nº 9434/1997, que dispõe sobre a remoção de órgãos, tecidos e partes do corpo humano para fins de transplante e tratamento e dá outras providências e Decreto nº 2.268/1997, que regulamenta a Lei nº 9.434, de 4 de fevereiro de 1997, que dispõe sobre a remoção de órgãos, tecidos e partes do corpo humano para fim de transplante e tratamento, e dá outras providências.

Feita esta breve revista ao cenário brasileiro, passemos a algumas conclusões propositivas.

5. Conclusões propositivas

O presente ensaio pretendeu demonstrar que a tessitura do consentimento, no âmbito da proteção dos dados neurais, é diferenciada, fulcrada em paradigmas relativos à bioética.

O consentimento real, previamente esclarecido, realmente livre e espontâneo, é *conditio sine qua non* para o tratamento dos dados neurais.

A contextualização do problema e seu manejo no âmbito internacional, assim como a abordagem do estado da arte no Brasil, demonstram a relevância e a complexidade do tema, que reclama tratamento urgente e eficiente.

O modelo protetivo do Projeto de Lei nº 522/2022, sem prejuízo do mérito da proposta, desponta insuficiente para a o tratamento dos dados neurais, na tessitura, complexidade, dimensões e alcance exigíveis, precisando de aperfeiçoamentos, o que foi tangenciado no texto.

Ademais, independentemente da tramitação da proposta legislativa e seus possíveis melhoramentos, o tratamento dos dados neurais é imperativo atual, aqui e agora.

A substancialidade material do direito fundamental à proteção de dados permite considerar os dados neurais como uma de suas múltiplas declinações. E consabido tratar-se de norma de eficácia direta e imediata. A eficácia objetiva do direito fundamental em causa vincula o Estado, em quaisquer de suas funções.

Neste diapasão, para o tratamento dos danos neurais, incide o dever de máxima proteção, decorrente do mandado de otimização que emana da dimensão objetivo dos direitos fundamentais em causa.

Vale dizer: o tratamento de dados neurais somente poderá ser realizado em consonância com a proteção aos neurodireitos.

A proteção da privacidade (e da intimidade) determina a interpretação restritiva do artigo 5º, inciso XII, da LGPD, para a consubstanciação do *consentimento real,* vedadas as configurações meramente ficcionais ou contextuais.

O consentimento do titular deverá ser prévio, verbalizando manifestação *efetivamente* livre, informada e inequívoca, revogável a qualquer tempo e vinculada à finalidade específica, sem analogias, *devendo ser renovado a cada novo escopo*.

Por isso, a opção de exclusão (*opt out*) deverá ser o basal (*default*) para qualquer aplicação que requeira consentimento para o tratamento de dados neurais.

O consentimento deverá ser formalizado por escrito, *obrigatoriamente*, e deverá conter *claramente* os *efeitos físicos, cognitivos e emocionais que dada neurotecnologia possa causar* ao titular dos dados.

A agência (autonomia e autodeterminação informativa) o uso de qualquer interface cérebro-maquínica que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua integridade psicológica.

Ademais, o acesso às tecnologias de integração cérebro-máquina deverá ser equitativo; a proteção contra os vieses e a não-discriminação são valores peremptórios, condicionantes inderrogáveis para o desenvolvimento e aplicação de neurotecnologias.

A exegese do artigo 11, I, da LGPD segue a mesma toada: o consentimento, no caso do tratamento dos dados neurais, deverá atender a rigidez formal e material compatível com a máxima proteção dos neurodireitos em causa.

Por outro lado – e aqui justificamos o porquê da qualificação dos *dados neurais como dados sensibilíssimos* -, as *hipóteses do artigo 11, II, alíneas (a) a (g)* da Lei 13.709/2018[66] *são inaplicáveis*, à exceção da proteção à vida do próprio titular (alínea "e", parte inicial).

Por consequência, igualmente inincidentes os §§ 1º a 3º do artigo 11 da

[66] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019); g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

normativa em tela[67].

São vedados a comunicação ou o compartilhamento de dados neurais, não incidindo à espécie as exceções previstas nos incisos I e II do §4º do artigo 11 da LGPD[68].

Ademais, é expressamente proscrita a cessão onerosa de dados neurais, devendo incidir, na espécie, a disciplina dada a órgãos e tecidos humanos, pela Lei nº 9434/1997.

Por derradeiro, a proibição do § 5 º do artigo 11 da LGPD[69], em se tratando de dados neurais, apresenta-se ainda mais incisiva e peremptória.

Sob o ponto de vista convencional, seria recomendável que a proteção de dados neurais fosse incluída na Declaração Universal dos Direitos Humanos.

Outrossim, concordamos com a escola da Universidade de Columbia, no sentido de ser necessária e urgente a edição de uma convenção internacional específica sobre o tema, que defina quais são as condutas proibidas no âmbito das neurotecnologias e da inteligência artificial.

Entrementes, para proscrever o uso de interfaces cérebro-computador que possa causar despersonalização e outros prejuízos à identidade humana, é possível aplicar, analogicamente a Convenção Internacional para Proteção de Todas as

---

[67] § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica. § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei. § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

[68] § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)

[69] § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Pessoas contra o Desaparecimento Forçados, que foi promulgada entre nós pelo Decreto nº 8.767/2016[70].

Considerando que a bioética preside as pesquisas científicas envolvendo seres humanos, bem como que a disciplina proposta para o tratamento de dados neurais dela aproxima-se, não existe tensionamento entre proteção de dados neurais e evolução da ciência.

Não existe ciência sem a observância de padrões éticos. No caso dos dados neurais, último fronteira da privacidade, da intimidade e da autonomia humanas, estes padrões precisam arrimar-se nos parâmetros mais rígidos quanto possível.

Proteger os dados neurais é proteger, em última instância, o que faz de cada ser humano uma criatura única. Protegendo este relicário de singularidades, o Direito, a Ciência e a Tecnologia ombrearão esforços para os mais lídimos ideais democráticos.

Referências bibliográficas

ADAM, Barbara; BECK Ulrich; VAN, Joost. **The Risk Society and Beyond: Crítical Issues for Social Theory**. London: SAGE Ltd., 2000.

ALCES, Petera. **The Moral Conflict of Law and Neuroscience**. Chicago Press, 2018.

BENASAYAG, Miguel. **The Tiranny of the Algorithms: Freedom, Democracy and the Challenge of AI**. Europa Compass, 2019.

BETHLEHEM, R.A.I.; SEIDLITZ, J.; WHITE, S.R. et al. Brain charts for the human lifespan. **Nature,** nº 604, p. 525–533, 2022. Disponível em: <https://doi.org/10.1038/s41586-022-04554-y>. Acesso em 19/06/2022.

BIONDI, Bruno Ricardo e LUCIANO, Maria. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: MULHOLLAND, CAITLIN; FRAZÃO, ANA. **Inteligência artificial e Direito**. São Paulo: Revista dos Tribunais, 2ª ed., 2020, 205-226.

BIONDI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2ª edição, 2020.

[70] BRASIL, Decreto nº 8.767, de 11 de maio de 2016. Brasília, 11 de maio de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8767.htm>. Acesso em 22/06/2022.

BOTELHO, Martinho Martins. A eficiência e o efeito Kaldor-Hicks: a questão da compensação social**. Revista de Direito, Economia e Desenvolvimento Sustentável**, v. 2, n. 1 (2016), p. 1-19. Disponível em: <https://www.indexlaw.org/index.php/revistaddsus/article/download/1595/PDF>. Acesso em 06/04/2022.

BRAIN (Brazilian Institute of Neuroscience and Neurotechnology), **Estudo de Tendências Tecnológicas Neurociência e Neurotecnologia**. Disponível em <https://www.brainn.org.br/wp-content/uploads/2018/11/CEPID-BRAINN-Estudo-de-Tend%C3%AAncias-em-Neurotecnologias-2018>. Acesso em 20/06/2022.

BRASIL, Poder Executivo. IBGE. **Instrução Normativa nº 2/2020**. Disponível em: <http://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2-de-17-de-abril-de-2020-253341223>. Acesso em 20/06/2022.

BRASIL, Poder Executivo. Planalto. **Decreto 8.767/2016**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8767.htm>. Acesso em 22/06/2022.

BRASIL, Poder Executivo. Planalto. **Medida Provisória nº 954/2020**. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em 20/06/2022 .

BRASIL, Supremo Tribunal Federal. **ADI-MC 6393**, Relatora: Ministra Rosa Weber. Tribunal Pleno, julgado em 07/05/2020, DJU-e 12/11/2020.

COELHO, Amanda Carmen Bezerra**. A lei geral de proteção de dados pessoais brasileira como meio de efetivação dos direitos da personalidade**. 2019. Disponível em:<https://repositorio.ufpb.br/jspui/bitstream/123456789/14305/1/ACBC05052019.pdf>. Acesso: 06/04/2022.

D'ALOIA, Antonio; ERRIGO, Maria Chiara. **Neuroscience and Law Complicated Crossings and New** Perspectives. Springer. ISBN 978-3-030-38839-3 ISBN 978-3-030-38840-9 (eBook). Disponível em: <https://doi.org/10.1007/978-3-030-38840-9>. Acesso em 20/09/2022.

DE OLIVEIRA, José Oswaldo Júnior; CORRÊA, Cláudio Fernandes; FERREIRA, Jânio Alves. Tratamento invasivo para o controle da dor neuropática. **Scielo**, Disponível em: <https://www.scielo.br/j/rdor/a/VbzLfkxjWJyTwq4mXJ8v38M/?lang=pt>. Acesso em 20/06/2022.

DE OLIVEIRA, Vanessa Kelly Silva; COSTA, Lorena Faria; Cristiane Alves da Fonseca. Principais Aplicações da Biotecnologia na Medicina. **Revista Eletrônica de Farmácia**, Suplemento Vol 3 (2), 42-43, 2006. Disponível em: <https://revistas.ufg.br/REF/article/download/2106/2041/9094>. Acesso 18/06/2022.

DI MAJO, Adolfo. Il tratamento dei dati personali tra diritto sostanziale e modelli di tutela. In: CUFFARO, Vicenzo et alli (org.). **Tratamento dei dati e tutela dela persona**. Milão: Giuffrè, 1999, p. 225-247.

DINIZ, Mariana de Oliveira; FERREIRA, Luís Carlos de Souza. Biotecnologia aplicada ao desenvolvimento de vacinas. **Dossiê Biotecnologia**, nº 24 , v. 70, 2010. Disponível em: <https://doi.org/10.1590/S0103-40142010000300003>. Acesso em 18/09/2022.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais**. 2ed. São Paulo: Revista dos Tribunais, 2019.

DOWD, Rebekah. **The Birth of Digital Human Rights Digitized Data Governance as a Human Rights Issue in the EU**. **Information Technology and Global Governance** ISBN 978-3-030-82968-1 ISBN 978-3-030-82969-8 (eBook). Disponível em: <https://doi.org/10.1007/978-3-030-82969-8>. Acesso em 20/06/2022.

DRUCKER, P.F. **The age of discontinuity: Guidelines to our changing society**. New Brunswick: Transaction Publishing, 1969.

FARIA, Lina; OLIVEIRA-LIMA, José Antonio de; ALMEIDA-FILHO, Naomar; **Medicina baseada em evidências: breve aporte histórico sobre marcos conceituais e objetivos práticos do cuidado**, Disponível em: <https://doi.org/10.1590/S0104-59702021000100004>. Acesso em 18/06/2022.

FEDYK, Anastassia. How to Tell If Machine Learning Can Solve Your Business Problem. **Harvard Business Review**, Nov/2016, p. 20/23. Disponível em: <https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper2/hbr-next-analytics-age-machine-learning-108855.pdf>. Acesso em 20/05/2022.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Trad. Raquel Ramalhete. Petrópolis, Vozes, 1987. 288p.

FREITAS, Juarez**. Sustentabilidade: Direito ao Futuro**. Belo Horizonte: Fórum, 2019.

FREITAS, Juarez. **Interpretação Sistemática do Direito**. 5ª. ed. São Paulo: Malheiros Editores, 2010, 312p; 3ª. ed. São Paulo: Malheiros Editores, 2010.

FREITAS, Juarez; FREITAS, Thomas Bellini. **Direito e Inteligência Artificial: em defesa do Humano**. Belo Horizonte: Fórum, 2020.

FUNTOWICZ Silvio O.; RAVETZ Jerome R. Science for the post-normal age, **Futures**. V 25-7, 1993, p. 739-755. Disponível em: <http://www.sciencedirect.com/science/article/pii/001632879390022L>. Acesso: 20/03/2022.

GEOFFREY, S.; HOLTZMAN, Elisabeth Hildt. **Does Neuroscience Have Normative Implications? The International Library of Ethics, Law and Technology** (eBook). Disponível em: <https://doi.org/10.1007/978-3-030-56134-5>. Acesso em 20/06/2022.

GIDDENS, Antony; LASH, Scott; BECK, Ulrich. **Modernização Reflexiva: política, tradição estética na ordem social moderna.** Trad. Magda Lopes. 2.ed. São Paulo: UNESP, 2012.

GOLDIM, José Roberto. **Verbete bioética**. Disponível em: <https://www.ufrgs.br/bioetica/tueke2.htm>. Acesso em 20/06/2022.

GOLDSCHMIDT, Ronaldo Ribeiro. **Inteligência Computacional**. Rio de Janeiro: IST-Rio, 2010, p. 9.

HANS-W. Micklitz et al. **Constitutional Challenges in the Algorithmic Society**. Cambridge University Press, 2022.

HILDEBRAND, Diogo; SHIRAISHI, Guilherme de Farias et al. O livre arbítrio no comportamento do consumidor. In: CARDOSO, Renato C.; MALLOY-DINIZ, Leandro F. et al**. Livre-arbítrio: uma abordagem interdisciplinar**. Belo Horizonte: Artesã, 2017, p. 147/160.

HINOJOSA, Alfredo Quiñones, Brain-Computer Interfacing : Prospects and Technical Aspects of Functional Cranial Implants. **Science Direct**, 2022. Disponível em: <https://www.sciencedirect.com/topics/neuroscience/brain-computer-interface>. Acesso em 20/06/2022.

HITACHI-UTokyo Laboratory. **Society 5.0: A people-centric super-smart society.** Tokyo: Springer Open, 2018.

KALPOKAS, Ignas. **Algorithmic Governance: Politics and Law in the Post-Human Era**. Palgrave Macmillan. (eBook). Disponível em: <https://doi.org/10.1007/978-3-030-31922-9>. Acesso em 22/06/2022.

KNOERR, Fernando Gustavo; ABAGGE, Yasmine de Resende; DA MOTTA, Ivan Dias. A Lei Geral de Proteção de Dados: Os Dados Pessoais Podem Ser Considerados Direitos Da Personalidade? **Revista Economic Analysis of Law Review**, V. 10, nº 2, p.278-302. Mai-Ago/2019. Disponível em: <https://portalrevistas.ucb.br/index.php/EALR/article/download/11907/pdf>. Acesso:06/04/2022.

KNUTH, Donald E. **The art of computer programming: fundamental algotithms**, 3 ed. Cidade: Addin Wesley Longman, 1997.

LEITE, Michel Lopes; COSTA, Fabricio F. Epigenômica, epigenética e câncer. **Rev Pan-Amaz Saúde**, Ananindeua. v. 8,n. 4,p. 23-25, dez. 2017. Disponível em: <http://dx.doi.org/10.5123/s2176-62232017000400006>. Acesso em: 26/06/2022.

MARCHIORO, Mariana et al. Relação entre Doença de Parkinson e Modulação Epigenética. **Revista Neurociências**, nº 27, 2019, p. 1/16. Disponível em: <https://periodicos.unifesp.br/index.php/neurociencias/article/download/9615/7365/40177as>. Acesso em 20/06/2022.

MARSHALL, P.; BREDY, T. Neuroepigenética cognitiva: a próxima evolução em nossa compreensão dos mecanismos moleculares subjacentes à aprendizagem e memória? **Nature**, 2016. Disponível em: <https://doi.org/10.1038/npjscilearn.2016.14>. Acesso em 20.09/2022.

McAFEE, A.; BRYNJOLFSSON, E. Big data: The management revolution**. Harvard Business Review**, v. 90, n. 10, p. 60, 2012.

MULHOLLAND, CAITLIN; FRAZÃO, ANA. **Inteligência artificial e Direito**. São Paulo: Revista dos Tribunais, 2ª ed., 2020.

ORTU, D.; VAIDYA, M.. The Challenges of Integrating Behavioral and Neural Data: Bridging and Breaking Boundaries Across Levels of Analysis**. Behav. Anal**, 2016, nº 40(1), p. 209/224. Disponível em: <https://10.1007/s40614-016-0074-5>. Acesso em 20/06/2022.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, 10:1, 40-81, 2018 Disponível em <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176>. Acesso em 07/04/2022.

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

ROSA, Moacyr Alexandro. Eletroconvulsoterapia e estimulação magnética transcraniana: semelhanças e diferenças, **Scielo Brasil**. Disponível em: <https://doi.org/10.1590/S0101-60832004000500008>. Acesso em 10/06/2022.

ROSSETTI, Regina; ANGELUCI, Alan. Ética Algorítmica: questões e desafios éticos do avanço tecnológico da sociedade da informação. São Caetano do Sul. (SP), Brasil. **Galáxia** (São Paulo, online), Nº 46, 2021, pp.1-18. Disponível em <http://dx.doi.org/10.1590/1982-2553202150301>. Acesso em 22/06/20/22.

RUBEL, Alan et al. **Algorithms and Autonomy: The Ethics of Automated.** Disponível em: <https://www.cambridge.org/core>. Acesso em 22/06/2022.

SACKETT, David L. William M C Rosenberg, J AMuir Gray, R Brian Haynes, W Scott Richardson. Evidence-based medicine: what it is and what it isn't. **BMJ**, v.13, n.312, p.71-72, 1996. Disponível em: <https://doi.org/10.1136/bmj.312.7023.71>. Acesso 19/06/2022.

SACKETT, David L. Using Evidence-based medicine to help physicians keep up-to-date. **Serials**, v.9, n.2, p.178-181, 1996. Disponível em<http://doi.org/10.1629/09178>. Acesso em 18/06/2022.

SARLET, INGO W. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF? **Conjur**. Disponível em: <https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf>. Acesso: 09-04-2021.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados. In: **Tratado de Proteção de Dados Pessoais**. Danilo Donena et al(coord.). Rio de Janeiro: Forense, 2020, p. 319 e ss.

SUNSTEIN, Cass. **Laws of Fear: beyond the precautionary principle**. New York: Cambridge Press, 2005.

WASSERMANN, Eric M. **Side effects of repetitive transcranial magnetic stimulation**. Anxiety e Depression Association of America, 2000. Disponível em: <https://doi.org/10.1002/1520-6394(2000)12:3<124::AID-DA3>3.0.CO;2-E>. Acesso em 22/06/2022.

WORSHAM, Christopher; JENA, Anupam B.. The Art of Evidence-Based Medicine. **Harward Business Review**, January 30, 2019, Disponível em: <https://hbr.org/2019/01/the-art-of-evidence-based-medicine>. Acesso em 19/06/2022

YUSTE, R., Goering, S., ARCAS, B. et al. Four ethical priorities for neurotechnologies and AI. **Nature**, nº 551, p. 159–163, 2017. Disponível em: <https://doi.org/10.1038/551159a>. Acesso em 18/06/2022.

ZUBOFF, Shoshana. **In the age of the smart machine**. London: Heinemann, 1988.

_____. **The age of Surveillance Capitalism: The fight for the future at the new frontier of power**. [e-book], p. 134. London: Profile Books Ltda, 2019.

5. ASPECTOS CONCEITUAIS E PRÁTICOS DO DIREITO À EXPLICAÇÃO E A NECESSÁRIA TRANSPARÊNCIA DO AGENTE DE TRATAMENTO

https://doi.org/10.36592/9786581110994-05

Edson Pontes Pinto[1]

Sumário

1. Introdução

A relação jurídica entre titular de dados e o agente de tratamento é hoje influenciada pelo recente reconhecimento do direito fundamental à proteção de dados pessoais, agora presente na Constituição Federal do Brasil (art. 5º, LXXIX).

Essa condição cristaliza a qualidade de direito fundamental da proteção de dados pessoais, ao mesmo tempo em que encerra as discussões até então travadas acerca da existência de tal direito, mesmo que implicitamente, elevando o *status* jurídico dos direitos do titular na perspectiva constitucional.

Porém, reconhecer a proteção de dados pessoais como direito fundamental do cidadão vai muito além de se exigir determinadas práticas de gestão de dados e instrumentos de *compliance*, mas acima de tudo visa garantir a autodeterminação informativa do titular, e da mesma forma o acesso às informações que estão na sua esfera de privacidade.

[1] Doutorando em Direito (Pontifícia Universidade Católica de Rio Grande do Sul). Mestre em Direito (Pontifícia Universidade de São Paulo). Professor Universitário (Faculdade Católica de Rondônia). Membro do conselho consultivo da The AI Robotics Ethics Society – AIRES/PUC-RS. Diretor Executivo da Escola Superior da Advocacia da OAB/RO. Presidente da Comissão de Proteção de Dados da OAB/RO. Advogado.
E-mail: edson.pinto@fcr.edu.br. Lattes: http://lattes.cnpq.br/7151311768492887.

Trata-se de colocar o titular de dados no centro axiológico da relação jurídica informativa, exigindo posturas ativas e passivas do agente de tratamento no respeito aos princípios da proteção de dados pessoais – em especial, para este trabalho, o princípio da transparência.

No entanto, é evidente que a relação jurídica entre o titular de dados e o agente de tratamento é marcada pela assimetria de informação, visto que os detalhes da operação de tratamento não são de conhecimento do cidadão na mesma proporção que do agente, o que se agrava quando se encontram presentes algoritmos de decisão automatizada na operação de processamento.

Nesse contexto, surge o direito à explicação do titular de dados, que tem por objetivo provocar o agente de tratamento para que responda quais os critérios e procedimentos são utilizados pelos algoritmos de decisão automatizada no processamento dos dados e na estruturação de seus resultados.

Trata-se de direito do titular correlato ao direito de acesso à informação, visto que nos dois casos há a provocação do agente de tratamento para que responda com as informações solicitadas.

Com isso, o direito à explicação se mostra importante na concretização da transparência na relação jurídica informativa, oportunizando ao titular que tenha acesso às informações de processamento das decisões automatizadas que lhe afetem, ao mesmo tempo em que reduz a assimetria de informação entre eles.

Ressaltam-se, assim, os seguintes problemas ao objeto da pesquisa: Quais os elementos do direito à explicação? Evidenciado o princípio da transparência, como deve o agente de tratamento garantir o direito à explicação ao titular de dados?

Para resolver tais questões, inicia-se o trabalho trazendo a conceituação e fundamentação do direito à explicação, descrevendo os dispositivos nacionais e europeus nos quais se funda o referido direito, além de tratar dos princípios que o norteiam, em especial da transparência, a qual será objeto de detalhamento de seus aspectos e conteúdo, bem como de boas práticas no exercício e na concretização do referido direito.

Assim, o presente trabalho estrutura-se na análise legislativa, constitucional e regulatória dos institutos aqui descritos, bem como no conjunto doutrinário que até o presente momento tratou dos temas direta ou indiretamente relacionados. Por tal

motivo, o método bibliográfico é, juntamente com o método comparativo, utilizado para a investigação da presente problemática, baseando-se, por sua vez, nos métodos interpretativos sistemático e teleológico.

Por fim, serão tratados de elementos práticos ao se garantir o direito à explicação do titular de dados, avançando nos conceitos de explicabilidade e interpretabilidade, e como deve se manifestar o agente de tratamento, e seu respectivo encarregado de dados, ao responder o requerimento do titular, dando-lhe concretude.

2. O direito à explicação: conceito e fundamentação legal no Brasil e na Europa

Do momento em que se reconheceu, no julgamento do caso censitário alemão de 1983 (*Volkszählungsurteil*),[2] o direito à autodeterminação individual (*Individuelle Selbstbestimmung*) dos dados por parte do titular frente ao agente de tratamento, surgem direitos e deveres que decorrem necessariamente dessa relação jurídica informativa.

Prevista aqui como fundamento da própria Lei Geral de Proteção de Dados em seu art. 2º, inciso II, a autodeterminação informativa é o reconhecimento do direito do titular aos seus dados, e em como são ou serão utilizados pelos agentes de tratamento, exigindo-se ao agente de tratamento uma postura transparente e explicativa de como agirá perante o titular no processamento desses dados.[3]

Considerando este cenário de opacidade algorítmica e fragilidade na transparência do mecanismo de funcionamento dos algoritmos,[4] sejam públicos ou privados, a autodeterminação informativa se apresenta como um direito do titular a provocar o agente de tratamento a dar explicações satisfativas e suficientes acerca de diversas questões do tratamento de dados pessoais.

---

[2] ALEMANHA, Bundesverfassungsgericht (BVerfG). BvR 209/83. Volkszählungsurteil. Absatz 146.

[3] Outra não é a lição de Renato Ópice Blum, ao descrever a autodeterminação informativa como "o direito de controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo" (BLUM, Renato Ópice. LGPD Comentada. 2ª Ed. São Paulo: RT, 2021).

[4] PINTO, Edson Pontes. Precedentes e algoritmos: uma abordagem de *law and economics*. In: BECKER, Daniel. et. al. Litigation 4.0: O futuro da justiça e do processo civil vis-à-vis as novas tecnologias. Thomson Reuters, 2021.

A autodeterminação informativa[5] pode ser vista sob dois prismas diferentes, porém complementares. Em um primeiro momento individual é descrita como a liberdade do cidadão decidir sobre os seus dados pessoais, seu uso e tratamento, já em uma perspectiva coletiva, se firma como uma questão democrática,[6] a partir do momento em que representa uma faceta da liberdade comunicacional e informativa do cidadão, e também um comando negativo à opacidade do tratamento de dados que se revela, pois, como instrumento incompatível com o princípio democrático.[7]

Torna-se imperioso, assim, reconhecer o direito do cidadão/titular de dados de exigir as razões e explicações acerca dos procedimentos automatizados (ou que se utilizem de agentes artificiais) no tratamento dos seus dados pessoais.

É uma questão, como dito, de participação democrática.[8]

---

[5] "O conceito de autodeterminação refere-se à capacidade de uma pessoa de moldar sua vida de acordo com suas próprias ideias, bem como ao exercício real dessa habilidade e uma forma de vida apresentada como ideal. [...] No que se refere à autodeterminação, o contexto social deve ser levado em conta. Neste contexto, ser livre e ser capaz de agir de forma independente significa, ao menos, a possibilidade realista de preservar e moldar a própria identidade e de responder às próprias ações perante si e os outros.24 Isso requer padrões confiáveis e justos de ação enquanto bases do Estado de Direito" (SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de *big data*. In: Direitos Fundamentais & Justiça. n. 41. jul./dez., 2019. p. 201-202).

[6] "Não há sobreposição, contudo, entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar uma dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre acesso, uso e difusão dos seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*)". (SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal Brasileira de 1988: Contributo para a construção de uma dogmática constitucionalmente adequada. In: Direitos Fundamentais & Justiça. Belo Horizonte, ano 14, n. 42, jan./jun. 2020).

[7] "[...] o espírito hermenêutico que deve guiar esta Corte Constitucional no tratamento da matéria em exame deve ser o de renovar o compromisso de manter viva a força normativa da Constituição Federal de 1988, nela encontrando caminhos e não entraves para a proteção jurídica da intimidade enquanto garantia básica da ordem democrática" (BRASIL, Supremo Tribunal Federal (STF). ADI 6389 MC-REF / DF, Voto do Min. Gilmar Mendes).

[8] "Questo confidare negli algoritmi ne determina una presenza sempre più pervasiva, che sembra non conoscere confini. L'algoritmo disegna le modalità di funzionamento di larghe aree delle nostre organizzazioni sociali, e così redistribuisce poteri. Incarna anzi le nuove forme del potere e ne modifica la qualità. E tutto questo suscita diverse domande. Saremo sempre più intensamente alla mercé delle macchine? Quali sono gli effetti su libertà e diritti, quali le conseguenze sullo stesso funzionamento democratico di una società?" (RODOTÀ, Stefano. Il mondo nella rete: Quali i diritti, quali i vincoli. Roma: Laterza, 2014. p. 41).

Daí surge e deriva, portanto, o direito à explicação dos titulares de dados presente na legislação brasileira e, de forma controversa, no ordenamento europeu.

A legislação europeia de proteção de dados, *General Data Protection Regulation* (GDPR), dispõe em seu art. 22, item 3, que nos casos de decisão tomada exclusivamente com base no tratamento automatizado, o responsável pelo tratamento deverá aplicar medidas de salvaguarda dos direitos e liberdades dos titulares dos dados, incluindo o de se manifestar e/ou contestar a decisão proferida.[9]

Esse *tratamento automatizado* (ou *tomada de decisão automatizada*) já foi definido pelo grupo de trabalho *Article 29 data protection working party* (*A29WP*)[10] como a habilidade de tomar decisões por meios tecnológicos sem a intervenção humana, e podem ser baseadas em diversos tipos de dados, como por exemplo, os dados fornecidos diretamente pelo indivíduo ou que deles foram derivados ou inferidos.[11]

Complementando a fundamentação do art. 22, item 3, o Considerando 71 do GDPR dispõe que no caso de tratamento automatizado, o procedimento "deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão".

É relevante ressaltar que os considerandos (*Recitals*) no ordenamento europeu não tem caráter normativo e, portanto, não podem revogar ou derrogar dispositivos legais previstos na legislação europeia, pois "tem por objetivo motivar, de forma concisa, as disposições essenciais do articulado, sem dele reproduzir, ou

---

[9] Art. 22, 3, GDPR: "Nos casos a que se referem o n.o 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão".

[10] Conselho europeu independente na matéria de proteção de dados e privacidade. Criado sob a égide da Diretiva 95/46/EC e tinha função consultiva, cf. art. 29 da referida norma.

[11] "*Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example: data provided directly by the individuals concerned (such as responses to a questionnaire); data observed about the individuals (such as location data collected via an application); derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score)". (UE, União Europeia. A29WP. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation* 2016/679. p. 8).

parafrasear, a redação", sem utilizar linguagem imperativa, e sem que isso implique em disposições com efeitos normativos, ou mesmo com pretensões e finalidades políticas.[12]

Todavia, os considerandos fundamentam os atos a que se referem, e trazem as razões de existência e validade do ato sem que para tanto repliquem o seu conteúdo textual, se preocupando, de fato, em fundamentar de forma concisa o dispositivo em questão.[13]

Embora haja discordância quanto a existência de um direito à explicação na legislação europeia,[14] deve ser considerado que a interpretação combinada do princípio da transparência previsto no art. 5º, item 1, alínea a,[15] e o disposto no art. 22, item 3, garante ao titular de dados na Europa o direito de questionar e exigir do agente de tratamento de dados, uma explicação acerca do resultado do processamento dos algoritmos de decisão automatizada naquilo que lhe interessa e que derive da sua titularidade dos dados.

Além disso, o art. 13, item 2, alínea f,[16] prevê que quando do tratamento dos dados pessoais, o agente de tratamento informará ao titular a existência de decisões automatizadas existentes nesse processo, incluindo questões que tratam da sua *lógica subjacente*, demonstrando, assim, a existência de uma obrigatoriedade de explicação e resposta do agente de tratamento perante o titular dos dados, objeto da

[12] UE, União Europeia. Guia Prático Comum do Parlamento Europeu, do Conselho e da Comissão para as pessoas que contribuem para a redação de textos legislativos da União Europeia, 2013.

[13] "Os considerandos devem fundamentar de forma concisa as disposições essenciais do dispositivo do ato. Os considerandos devem constituir uma verdadeira fundamentação. Tal exclui a menção das bases jurídicas (que devem figurar nas citações) ou a repetição do teor de uma disposição mencionada como base jurídica que confira competência para agir. Além disso, os considerandos são inúteis ou não correspondem à sua finalidade caso se limitem a indicar o objeto do texto ou a reproduzir, ou parafrasear, as disposições do ato, sem mencionar os motivos." (UE, União Europeia. Guia Prático Comum do Parlamento Europeu, do Conselho e da Comissão para as pessoas que contribuem para a redação de textos legislativos da União Europeia, 2013).

[14] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. In: International Data Privacy Law, Volume 7, Issue 2, May 2017.

[15] GDPR: Art. 5º, 1. Os dados pessoais são: a) objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ("licitude, lealdade e transparência").

[16] Art. 13, item 2, f, GDPR: "quando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente: f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22, n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados".

decisão automatizada.[17]

Assim sendo, como estabelecido pelo Considerando 58 do GDPR, "o princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado", fato é que a ausência dele faz surgir necessariamente o direito ao titular de contestar e de requerer explicação acerca da utilização dos seus dados, ou de questionar o uso de algoritmos e do resultado das decisões automatizadas.[18]

Tendo a legislação europeia como exemplo, a Lei Geral de Proteção de Dados no Brasil (LGPD) disciplina o direito à explicação do titular de dados ao determinar ao agente de tratamento a obrigação de fornecer *informações claras e adequadas* acerca dos procedimentos, atributos e elementos utilizados na tomada de decisão dos agentes automatizados (art. 20, §1º).

De forma mais elucidativa, o direito à explicação no ordenamento brasileiro é o direito do titular de dados de requerer ao agente de tratamento a prestação de informações com a finalidade de obter uma explicação sobre os critérios e procedimentos utilizados no tratamento de dados em que há decisões automatizadas que afetem seus interesses, para o titular possa compreendê-las.[19]

No entanto, o direito à explicação vai além da revisão de cadastro ou *score* de crédito; ele exige que o agente de tratamento forneça respostas transparentes e suficientes acerca da utilização dos dados do titular, de modo a lhe garantir efetiva e materialmente o conhecimento e a compreensão dos critérios utilizados pelo algoritmo de decisão automatizada.

---

[17] SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. In: International Data Privacy Law, Volume 7, Issue 4, November 2017.

[18] Outro não é o entendimento firmado pelo já citado *Article 29 data protection working party*: "*The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision*"

[19] MAGRANI, Eduardo. SOUZA; Carlos Affonso; PERRONE, Christian. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: SARLET, Ingo Wolfgang; et. al. Tratado de Proteção de Dados Pessoais. Editora Forense, 2021. p. 275.

3. Explicação e transparência como elementos de mitigação da assimetria informativa

Explicar as decisões automatizadas deriva da dificuldade de compreensão do funcionamento dos algoritmos computacionais, não só tecnicamente, mas quanto aos seus resultados – principalmente quando se analisa na perspectiva do homem médio.

Tal dificuldade é denominada de *opacidade algorítmica*, que pode ser conceituada como a inexistência de transparência capaz de dificultar, ou impossibilitar, a compreensão do funcionamento de um algoritmo de automação ou inteligência artificial, tanto intrinsicamente (parâmetros, elementos, *dataset*),[20] como extrinsecamente em relação aos seus resultados e decisões.

A opacidade algorítmica é caracterizada por uma intensa assimetria informativa entre o agente de tratamento e o titular de dados, visto que aquele possui conhecimento e domínio sobre o funcionamento de seus algoritmos de decisão automatizada, enquanto este é muitas vezes incapaz de compreender sequer o resultado do processamento de seus dados.[21]

Assim, o direito à explicação se mostra importante como forma de garantir ao interessado, e à sociedade, a presença de mecanismos de redução da opacidade algorítmica com o incremento da transparência dos algoritmos de decisão automatizada e de inteligência artificial, abrindo, com isso, as *caixas pretas*.

Neste cenário de *algoritmos como caixas pretas*,[22] a transparência é, para além de um princípio da lei, uma característica essencial dos sistemas computacionais, que permite ao titular de dados compreender e inspecionar os parâmetros e resultados do algoritmo ao decidir de forma automatizada (ou

[20] "Algorithmic opacity is defined as the lack of visible processes to scrutinize the inner workings and resulting applications of algorithms." (LU, Sylvia. Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial intelligence. In: Vanderbilt Journal of Entertainment & Technology Law, vol. 99, 2021).

[21] "We have no clear idea of just how far much of this information can travel, how it is used, or its consequences" (PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press, 2015).

[22] EBERS, Martin. Regulating AI and Robotics: Ethical and legal challenges. In: EBERS, Martin; NAVAS, Susana. Algorithms and Law, 2020. p. 48.

utilizando inteligência artificial).[23]

Com isso, o princípio da transparência visto na perspectiva de agentes de decisão automatizada, bem como de inteligência artificial estabelece a necessidade de informar os critérios e parâmetros que orientam o funcionamento dos sistemas computacionais, bem como os riscos advindos do seu funcionamento e processamento.[24]

A transparência assume, assim, diversas faces, a depender da obrigação que recai sobre o agente que se encontra na condição de revelar e explicar a informação.

Chama-se de *transparência ativa* o dever do agente de divulgar, de forma contínua e organizada, as informações que se encontram em seu poder, seja por ato voluntário ou por obrigação da regulação.[25]

Esta espécie de transparência independe da provocação do cidadão ou titular de dados (no contexto aqui trabalhado), sendo uma ação ou obrigação do agente de tratamento.

Com este enfoque, a transparência ativa exige do agente que deliberadamente torne pública e/ou disponível as informações, com o objetivo de também prestar contas da sua atividade e funcionamento, alinhando os valores protegidos por este princípio àqueles derivados do princípio da responsabilização e prestação de contas (*accountability*), conforme se verifica no art. 6º, inciso X, da LGPD.

Considerando o cenário em que o tratamento de dados se realizará com a utilização de agentes de automação, é obrigatório, pois determinado pela lei, e necessário, por ser boa prática, a estruturação de instrumentos que evidenciem as características da sua utilização e de seus mecanismos de decisão.

Diante disso, a LGPD traz um instrumento denominado Relatório de Impacto de Proteção de Dados, doravante denominado RIPD.

---

[23] É imperioso ressaltar que o Projeto do Marco Legal da Inteligência Artificial, em tramitação no Congresso Nacional, dispõe em seu art. 5º, inciso V que é o direito das pessoas de serem informadas de maneira clara, acessível e precisa sobre a utilização das soluções de inteligência artificial, salvo disposição legal em sentido contrário e observados os segredos comercial e industrial.

[24] Neste sentido, a recomendação de Dubai com as linhas gerais e princípios éticos da inteligência artificial determina que: "AI operator organisations should inform AI subjects when a significant decision affecting them has been made by an AI system" (EMIRADOS ÁRABES UNIDOS, Smart Dubai: AI Ethics principles & Guidelines. 2018. p. 27).

[25] RODRIGUES, Karina Furtado. Desvelando o conceito de transparência: seus limites, suas variedades e a criação de uma tipologia. Cad. EBAPE.BR, v. 18, nº 2, Rio de Janeiro, Abr./Jun. 2020.

O RIPD é o documento do agente de tratamento que descreverá toda a rotina de tratamento de dados pessoais, bem como descreverá os possíveis riscos dessa atividade, e as medidas de mitigação.[26]

Assim sendo, o RIPD é um instrumento previsto na regulação que objetiva o controle da atividade do agente de tratamento, com a descrição dos riscos e impactos dela oriundos, bem como das medidas de mitigação desses efeitos, quando presentes.[27] Dito de outro modo, o referido relatório traz o dever de transparência ativa ao agente de tratamento que, por determinação legal, *sinaliza* (*signaling*)[28] as informações necessárias ao titular de dados para compreender se algum aspecto do tratamento de dados impactará em seus direitos fundamentais e liberdades civis.[29]

Por outro lado, a *transparência passiva* se refere à obrigação do agente de tratamento de garantir acesso à informação sempre que o titular de dados a requisitar, seja exercendo seu direito de acesso *lato sensu* ou o direito à explicação previstos legislação de proteção de dados.[30]

O dever do agente de tratamento é, nos casos de transparência passiva, possibilitar o acesso e estruturar meios de seu exercício material aos titulares de dados, disponibilizando todas as informações pertinentes, e explicando todos os detalhes relativos à utilização de seus dados – respeitados os casos em que a lei afasta a obrigação, como se verifica nos sigilos, por exemplo.

---

[26] Art. 5º, inciso XVII, LGPD: "relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

[27] PECK, Patrícia. Proteção de dados pessoais: Comentários à Lei n. 13.709/2018 (LGPD). Saraiva, 2021. p. 100.

[28] "Asymmetric information motivates not only some public policy but also some individual behavior that otherwise might be hard to explain. Markets respond to problems of asymmetric information in many ways. One of them is signaling, which refers to actions taken by an informed party for the sole purpose of credibly revealing his private information". (MANKIW. N. Gregory. Principles of Economics. Cengage, 2021. p. 450.

[29] A lei europeia em seu art. 35 determina que quando um tratamento de dados for suscetível de acarretar um alto risco a direitos e liberdade das pessoas naturais, deverá o agente de tratamento realizar uma avaliação de impacto do tratamento com a descrição sistemática das operações de tratamento, a avaliação dos riscos, e o detalhamento das medidas de segurança e salvaguardas.

[30] RODRIGUES, Karina Furtado. Desvelando o conceito de transparência: seus limites, suas variedades e a criação de uma tipologia. Cad. EBAPE.BR, v. 18, nº 2, Rio de Janeiro, Abr./Jun. 2020.

A presença de um encarregado de dados e de uma gestão da informação pautada na transparência, com os consequentes mecanismos de proteção, integração e cibersegurança de dados, são alguns dos requisitos que podem compor a estrutura do agente de tratamento lhe permitindo executar um planejamento de *compliance* de dados orientado pelos valores e objetivos da transparência passiva.

Todavia, é necessário ressaltar que a simples disponibilização das informações, ou até mesmo da resposta ao direito à explicação, não pode se dar sem que compreensão do titular de dados seja efetivamente assegurada, ou seja, a apresentação deve ser aderente à situação material e fática do titular de dados.

Por isso, é imprescindível preencher as duas condições essenciais da transparência: visibilidade da informação e capacidade de inferência.

A informação deve estar disponível (transparência ativa), ou ser colocada à disposição quando solicitada pelo titular (transparência passiva), porém, isso por si só não garante que a informação seja considerada *visível*. É necessário que a informação tenha completude, e possa ser encontrada com facilidade pelo interessado.[31]

Não há transparência se a informação estiver incompleta, dificultando a compreensão do homem-médio, ou evitando que ele consiga enxergar e entender o todo. A completude exige a disponibilização da informação desejada por completo, incluindo outros dados e informações adicionais que possam, para uma maior compreensão, complementar o objeto a ser transparente.[32]

Do mesmo modo, a transparência tem em seu núcleo a informação capaz de permitir ao interessado realizar inferências – o que se denomina de *inferabilidade* (*inferability*).[33]

Inferência estatística é a generalização de uma conclusão para além dos conjuntos de dados observados. [34] Inferir é, portanto, tirar conclusões sobre informações, inclusive sobre parâmetros desconhecidos, desde que implícitos a um

[31] MICHENER, Greg; BERSCH, Katherine. Identifying transparency. In: Information Polity 18 (2013). p. 238.
[32] MEIJER, Albert. Transparency. In: BOVENS, Mark; GOODIN, Robert E. et. al. The Oxford Handbook of Public Accountability, 2014.
[33] MICHENER, Greg; BERSCH, Katherine. Identifying transparency. In: Information Polity 18 (2013). p. 238.
[34] WITTE, Robert S.; WITTE, John S. Statistics. 11th Ed. Wiley, 2017. p. 404.

modelo estatístico.

Para se permitir a conclusão sobre determinada informação, mesmo que seja ela visível, é necessário que tenha uma qualidade mínima, evitando-se informações imprecisas, obscuras, desestruturadas e dissociadas do contexto fático e adaptadas ao receptor.[35]

Sendo assim, a transparência só será concretizada se a informação apresentada pelo agente de tratamento for suficiente, em qualidade e quantidade, a permitir a compreensão do titular de dados e, por consequência, que dela possa ele retirar suas conclusões.

Tais classificações, por óbvio, não são independentes, mas sim características de um mesmo valor, e que no final possuem os mesmos objetivos, sendo uma delas a redução da assimetria informativa. Afinal, uma das funções da transparência é permitir o compartilhamento do estoque informacional entre os agentes relacionados, reduzindo-se com isso a diferença ou vão informativo entre eles – ou, simplesmente, a sua assimetria.

Na relação jurídica em que impera a igualdade de condições, pressupõe-se que as partes detenham a mesma quantidade de informação acerca dos fatos e dos aspectos técnicos e jurídicos a ela correspondentes. Em um caso assim caracterizado não há prevalência de uma parte sobre a outra, pois inexiste diferença do estoque informativo entre elas.

A assimetria informativa é, justamente, a situação inversa: trata-se de um fenômeno econômico no qual uma das partes da relação jurídica possui mais estoque informacional do que a outra,[36] como é o caso dos algoritmos de decisão automatizada, situação em que o desenvolvedor conhece e compreende os parâmetros que estruturam o modelo em questão, e o titular de dados, por sua vez, desconhece e não é capaz de entendê-los completamente.

---

[35] "The institutional frameworks of Southern countries must be taken into account as we consider what impact AI might have on the South. Freedom depends not just on political and civil rights but also on other social and economic arrangement such as education and health care" (ARUN, Chinmayi. AI and Global South: Designing for Other Worlds. In: PASQUALE, Frank; et. al. The Oxford Handbook of Ethics of AI. Oxford Press, 2020. p. 602).

[36] RIBEIRO, Marcia Carla Pereira; MARTINS, João Victor Ruiz. Economia do compartilhamento, assimetria informacional e regulação econômica consumerista. In: Revista de Direito, Economia e Desenvolvimento Sustentável. V.2. N.2. Jul/Dez.2016. p. 37.

A existência de um cenário no qual os envolvidos não se encontram em um mesmo patamar informativo, caracterizando uma relação não equânime e assimétrica, determina e fundamenta o direito do titular de dados de exigir explicações. Afinal, não há como se permitir a presença de uma discrepância do titular frente ao agente de tratamento que, se utilizando ou não de mecanismos de automatização, pode ampliar situações em que se mostre presente falhas de mercado, como a seleção adversa ou o risco moral.[37]

Naturalmente, portanto, os sistemas computacionais utilizados para auxiliar ou direcionar o tratamento automatizado de dados trazem um aumento dos custos de transação na relação jurídica, o que pode ser reduzido com a implementação de sistemas dotados de mecanismos de explicabilidade e interpretabilidade de suas decisões e resultados.

4. Explicabilidade e interpretabilidade: a implementação do direito à explicação e os deveres correlacionados do agente de tratamento

Delimitado o conteúdo do direito à explicação, e evidenciada a exigência da conduta passiva e ativa de transparência por parte do agente de tratamento, é imperioso então descrever como deve o controlador garantir ao titular as explicações necessárias.

Sabe-se que o encarregado é o responsável pela comunicação do controlador com os titulares e demais interessados (art. 41, LGPD), e, especificamente sobre o direito à explicação dos titulares, o encarregado tem por função ser a interface do agente de tratamento, e receber as reclamações e quaisquer outras manifestações dos titulares de dados, dando-lhes as devidas resposta e encaminhamentos.[38]

Vale ressaltar que na recente Resolução n. 2 da Autoridade Nacional de Proteção de dados (ANPD), os agentes de tratamento de pequeno porte[39] estão

[37] FREITAS, Jurez; FREITAS, Thomas Beillini. Direito e Inteligência Artificial: Em defesa do humano. Belo Horizonte: Editora Fórum, 2020. p. 59.

[38] A equivalência no GDPR se verifica no art. 38, item 4: "Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento".

[39] Art. 2º, inciso I, da Resolução n. 2 da ANPD: "Art. 2º Para efeitos deste regulamento são adotadas as seguintes definições: I - agentes de tratamento de pequeno porte: microempresas, empresas de

desobrigados da nomeação de um encarregado, por força do art. 11, porém, isso não exclui a obrigação do controlador de disponibilizar um canal de comunicação com o titular de dados (§1º), o que demonstra a existência da mesma obrigação acerca da sua conduta passiva de transparência, e de resposta ao direito à explicação dos titulares.

A explicação pressupõe então um agir do titular de dados, ao requisitar informações acerca do tratamento de seus dados, o funcionamento dos algoritmos de decisão automatizada, os detalhes, e as consequências do seu processamento. Do mesmo modo, o exercício desse direito faz surgir uma obrigação de resposta que preencha materialmente as exigências de informação e compreensão, nas diversas perspectivas da transparência já tratadas acimas.

O questionamento que se coloca é sobre o conteúdo necessário dessa explicação, haja vista que a opacidade algorítmica é, como descrito acima, um fenômeno caracterizado pelo desconhecimento de resultados (*outputs*) dentro de um determinado contexto computacional, justamente por não se ter certeza de como o algoritmo se comportará ao processar determinado conjunto de dados (*datasets*).[40]

O Considerando 39, apoiando a fundamentação da legislação europeia ao tratar da transparência, dispõe que o controlador deve assegurar que o tratamento "seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados".

E mais, dispõe também que "as pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento".

---

pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador".

[40] "Tanto o GDPR quanto a LGPD, ambos lege lata, possuem o direito à explicação previsto em seus textos. Sabe-se que entender o processo decisório e a programação de algoritmos probabilísticos e autoprogramáveis é tarefa hercúlea. Diz-se que programar um algoritmo de *machine learning* é muito difícil; a única coisa reputada como mais difícil do que programá-lo, é auditá-lo e explicá-lo." (BECKER, Daniel; FERRARI, Isabela. O direito à explicação sobre decisões automatizadas: uma análise comparativa entre a união europeia e o brasil. In: Revista de Direito e as Novas Tecnologias, vol. 1. São Paulo: Thomson Reuters/RT, Out-Dez/2018).

O grupo de trabalho europeu A29WP dispõe no seu documento *linhas gerais para as decisões automatizadas*, que o agente de tratamento, ao ser questionado pelo titular, deverá informá-lo em qual atividade ele está envolvido, fornecendo informações relevantes sobre a lógica envolvida no sistema de decisão automatizada,[41] adentrando, principalmente, na explicação do resultado e das consequências do processamento/tratamento de dados.[42]

Do mesmo modo, o Projeto do Marco Legal da Inteligência Artificial além de descrever o princípio da transparência, dispõe nas alíneas, do inciso V, do art. 5º que o questionamento do titular de dados sobre a utilização de sistemas de inteligência artificial, poderá ser realizado em três hipóteses: 1. sobre o fato de estarem se comunicando diretamente com sistemas de inteligência artificial; 2. sobre a identidade da pessoa natural, quando ela operar o sistema de maneira autônoma e individual; 3. sobre critérios gerais que orientam o funcionamento do sistema de inteligência artificial.[43]

Consequentemente, e valendo-se da mesma interpretação para a LGPD, quando instado a explicar acerca do funcionamento e do resultado obtido pela utilização de algoritmos de decisão automatizada, o agente de tratamento deve descrever o procedimento de tomada de decisão do algoritmo, seu funcionamento, mas, ao mesmo tempo, deve ele trazer as razões ou justificações para o resultado obtido (*output*).

Além disso, caso o agente de tratamento não esteja em conformidade, e não tenha ainda estruturado seu relatório de impacto (RIPD), deverá a resposta à explicação trazer também a descrição dos processos de tratamento que podem ser

---

[41] "*The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm.40 The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.*" (UE, União Europeia. A29WP. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. p. 25).

[42] "*This term suggests that information must be provided about intended or future processing, and how the automated decision-making might affect the data subject.*" (UE, União Europeia. A29WP. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. p. 26).

[43] "*An important dimension of transparency relates to the quality of the data used, including its accuracy, completeness, timeliness and update frequency, and uncertainty*". (DIAKOPOULOS, Nicholas. Transparency. In: PASQUALE, Frank; et. al. The Oxford Handbook of Ethics of AI. Oxford Press, 2020. p. 202).

fonte de riscos ao titular de dados, descrevendo da mesma forma as medidas de mitigação de tais situações.

Em resumo: explicar é ser transparente, mas não necessariamente ser transparente significa, ou garantirá, o direito à explicação.[44]

O direito à explicação no seu conteúdo prático, deve ir além da simples descrição do procedimento algorítmico, ou de apenas se ater a detalhar o funcionamento do sistema computacional, mas determina uma obrigação ao agente de tratamento de trazer uma informação explicável e interpretável ao cidadão não especializado na tecnologia, ou na ciência da computação.[45]

Conforme os especialistas da área da ciência da computação, que estudam os sistemas de inteligência artificial explicáveis (*explainable artificial intelligence* – XAI),[46] a interpretabilidade é a característica do modelo de inteligência artificial que assegurará resultados compreensíveis ao humano, lhe permitindo tirar conclusões de causa e efeito;[47] a explicabilidade é, por sua vez, a característica que garantirá a explicação *post hoc* para os modelos existentes,[48] detalhando como se dá o funcionamento do modelo computacional.

Logo, trazendo o primeiro conceito para uma análise combinada com o princípio da transparência na proteção de dados, é possível afirmar que um resultado interpretável é aquele compreensível em seus termos pelo ser humano, ou seja, é a habilidade do sistema computacional de fornecer uma justificativa do resultado em termos suficientes para a compreensão humana.[49]

---

[44] "*It is important to note explanation is not the same as transparency, for being able to understand the process by which a decision was made is not the same as knowing every step taken*" (MENDES, Laura Schendel; MATTIUZZO, Marcela. Algorithms and Discrimination: The case of credit scoring in Brazil. In: ALBERS, Marion; SARLET, Ingo Wolfgang (org.). Personality and Data Protection Rights on the Internet: Brazilian and German Approaches. Springer Verlag, 2022. p. 433).

[45] PINTO, Edson Pontes; CÔRREA, Nicolas Kruge. et. al. Worldwide AI Ethics: a review of 200 guidelines and recommendations for AI governance. Arxiv. Preprint. Disponível em: < https://arxiv.org/abs/2206.11922 >. Acesso em 27 de junho de 2022.

[46] KAMATH, Uday; LIU, John. Explainable Artificial Intelligence: Na introduction to interpretable Machine Learning. Springer Verlag, 2021.

[47] MARCINKEVICS; Ricard, VOGT, Julia E. Interpretability and Explainability: A Machine Learning Zoo Mini-tour. Preprint. Disponível em: < https://arxiv.org/abs/2012.01805>. Acesso em: 21 de junho de 2022.

[48] RUDIN, Cynthia. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. In: Nature Machine Intelligence, 1(5). p. 206–215.

[49] ARRIETA, Alejandro Barredo. DÍAZ-RODRÍGUEZ, Natalia. et. al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. In: Information Fusion, vol. 58, 2020. p. 85.

Interpretabilidade e explicabilidade embora possam parecer sinônimos, demonstram uma diferença sutil: uma inteligência artificial que se considere explicável deve ser capaz de fornecer uma explicação sobre seus resultados; no entanto, uma inteligência artificial que seja interpretável dará uma resposta compreensível (interpretável) ao homem-médio, concretizando materialmente.

É necessário, pois, que a resposta ao direito à explicação do titular de dados garanta a ele interpretabilidade, visto que é um elemento essencial para a sua compreensão acerca do resultado obtido, e de como seus dados foram de fato utilizados pelo sistema algorítmico – incidindo aqui a carga valorativa da autodeterminação informativa.

Esses dois elementos do direito à explicação conversam com a transparência e sua condição de inferabilidade e, portanto, são imprescindíveis para se ter materialmente uma manifestação que permita ao titular de dados compreender como seus dados são efetivamente utilizados, e quais os riscos podem advir dessa atividade de tratamento.

Para trazer exemplo prático, e em contributo ao paralelo entre a legislação brasileira e europeia, a autoridade de proteção de dados da Suécia (*Integritetsskyddsmyndigheten*) em decisão de março de 2022, multou uma instituição financeira em €730.000,00 (setecentos e trinta mil euros) por não fornecer informações adequadas sobre seu tratamento de dados, incluindo os casos de decisão automatizada, visto que se constatou que nesses casos nenhuma informação foi fornecida sobre a lógica nesses procedimentos, nem quanto à qualidade e utilização dos dados, e os eventuais riscos aos titulares de dados.[50]

Outro ponto que merece atenção nessa relação entre *explicação e resposta*, é a profundidade e o conteúdo caracterizado como essencial e suficiente para que se considere cumprida a obrigação de responder à exigência de explicação do titular de dados.

O direito à explicação não abrange o direito a acessar o código-fonte do sistema de decisão automatizada, nem mesmo informações correlacionadas que de

[50] SUÉCIA, Integritetsskyddsmyndigheten (IMY). DI-2019-4062. Disponível em: <https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf. > Acesso em 22 de junho de 2022.

alguma forma se referem à estrutura tecnológica, haja vista que, por permissivo previsto na própria legislação de proteção de dados pessoais, se afasta a necessidade de adentrar em questões técnicas que de alguma forma atinja a propriedade industrial do agente de tratamento.

Sugere-se, neste ponto, a inversão da interpretação dos princípios da boa-fé e da necessidade, vistos aqui na perspectiva do agente de tratamento, e sua obrigação de fornecer uma resposta ao pedido de explicação.

A imposição da boa-fé como princípio da relação entre agente de tratamento e titular de dados, afasta comportamentos abusivos, condutas desviadas, e ressalta a lealdade como característica imprescindível em uma relação justa e equânime[51] entre titular de dados e agente de tratamento.[52]

Já o princípio da necessidade tem como característica nuclear a limitação do tratamento de dados ao mínimo necessário para a execução e preenchimento de sua finalidade.[53] É o denominado *data minimisation*[54] previsto na legislação europeia, e segundo tal princípio, deve ser evitado o excesso de dados tratados pelo agente de

---

[51] *"Specifically, fairness could be assessed based on two components: 'good faith' of the data controller and 'significant imbalance' between the controller and the data subject"* (VRABEC, Helena. Data Subject Rights under the GDPR. Oxford Press, 2021).

[52] Vale ressaltar que o DPA espanhol (*Agencia Española de Protección de Datos - AEPD*) decidiu no *Procedimiento n. E/00739/2021* que o pedido de acesso por parte do titular era abusivo, levando em conta o contexto e os antecedentes da relação entre ele e o controlador. O titular em questão havia previamente apresentado várias reclamações e ações judiciais contra o responsável pelo tratamento em outros campos da lei. Nos seus fundamentos argumentou que a conduta do titular estava em desacordo com a boa-fé: "*La buena fe es un principio general del derecho incorporado al Derecho positivo que se traduce en la imposición de una serie de deberes a quien ostenta la titularidad de un derecho. A su vez, la consideración de que un derecho se ha ejercitado de manera abusiva se ha de apoyar en datos objetivos, rigurosos y ciertos, de manera que conste probado que el titular del derecho ha sobrepasado manifiestamente los límites normales de este con ocasión de su ejercicio*". Ver inteiro teor: ESPANHA, Agencia Española de Protección de Datos (AEPD). Procedimiento n. E/00739/2021. Disponível em: <https://www.aepd.es/es/documento/e-00739-2021.pdf>. Acesso em 20 de junho de 2022.

[53] Em um caso analisado pelo DPA português (Comissão Nacional de Proteção de Dados - CNPD), Deliberação 2021/622, foi decidido pela proibição de uso, por parte de uma instituição de ensino, de um software de avaliação de estudantes, além de excluir todos os dados coletados durante sua utilização. Segundo a CNPD, o software coletava dados além do necessário (*data minimisation*) para a sua finalidade, ferindo assim os princípios da finalidade, necessidade, dentre outros. Ver inteiro teor: PORTUGAL, Comissão Nacional de Proteção de Dados (CNPD). Deliberação 2021/622. Disponível em: < https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887 >. Acesso em 20 de junho de 2022.

[54] GDPR, Art. 5. 1. c.: *"Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* ('data minimisation')".

tratamento, restringindo-se somente àqueles que de fato importam à finalidade,[55] limitando o propósito do agente de tratamento (*purpose limitation*)[56].

Invertendo a interpretação, e focando na resposta fornecida pelo agente de tratamento ao pedido de explicação do titular de dados, tem-se que tal resposta, em seu aspecto qualitativo, deverá trazer os elementos necessários à compreensão do titular, mas em relação ao aspecto quantitativo, deverá o agente de tratamento, calcado na boa-fé, fornecer os dados suficientes a responder os questionamentos, sem ser excessivo quanto aos elementos que integram a resposta, e sem ser obrigado a trazer dados além daqueles necessários à finalidade, ou seja, o mínimo necessário para atingir e cumprir com a obrigação.

Por conseguinte, a concretização material de uma resposta suficiente à explicação exigida pelo titular de dados, passa pela compreensão dos elementos necessários (explicabilidade e interpretabilidade) a garantir a compreensão *de facto* do titular, e como tal resposta concretizará, além dos princípios previstos na LGPD, especialmente o princípio da transparência em todas as suas faces.

5. Conclusão

A presença de algoritmos de decisão automatizada concede ao titular de dados a possibilidade de questionar suas características e seus critérios de processamento e, por consequência, seus resultados.

Em outras palavras, o reconhecimento do direito do titular à autodeterminação de seus dados lhe permite provocar o agente de tratamento para que tenha uma

---

[55] "*Data minimisation is the direct consequence of the legal principle of purpose limitation, which requires that personal data only be processed for specified, explicit and legitimate purposes and not further processed in a manner incompatible with these purposes.*" (BIEGA, Asia J. et al. Operationalizing the Legal Principle of Data Minimization for Personalization In: SIGIR '20, July 25–30, 2020. Preprint. Disponível em: < https://arxiv.org/pdf/2005.13718.pdf.>. Acesso em 05 de maio de 2022.

[56] "*This principle requires data to be collected for specified, explicit and legitimate purposes (the 'purpose specification' dimension) and not further processed in a manner that is incompatible with those purposes (the 'compatible use' dimension). Purposes for processing personal data should be determined from the very beginning, at the time of the collection of the personal data. The processing of personal data for undefined or unlimited purposes is unlawful since it does not enable the scope of the processing to be precisely delimited.*" (DE TERWANGNE, Cecile. Principles relating to processing of personal data. In: KUNER, Christopher. et al. The EU General Data Protection Regulation (GDPR): A commentary. Oxford Press, 2020).

postura positiva na concretização da transparência, tanto do seu tratamento de dados, como do algoritmo utilizado.

O direito à explicação está no âmbito da transparência passiva, visto que o agente é provocado pelo titular de dados a fornecer uma resposta ao tratamento realizado por algoritmos decisionais, e por isso contribui com os demais instrumentos e obrigações previstas na LGPD, como é o caso do Relatório de Impacto da Proteção de Dados (RIPD),

No entanto, diversos são os detalhes que devem ser preenchidos para garantir uma resposta efetiva ao direito à explicação exercido.

A informação fornecida deve estar disponível ao titular, ao mesmo tempo em que tem que estar completa para que seja possível ao titular compreendê-la. Todavia, para além dessas duas características, a informação deve ser suficiente, em qualidade e quantidade, e permitir a compreensão do titular de dados, sendo ele capaz de retirar suas conclusões.

Logo, o direito à explicação exige tanto a explicabilidade do algoritmo, no sentido de dar explicações sobre o modelo computacional, como também exige a interpretabilidade, compreendida como a capacidade do algoritmo de fornecer respostas compreensíveis/interpretáveis ao ser humano.

A importância de se garantir uma resposta efetiva, e materialmente adequada, ao titular de dados, é de afastar a opacidade algorítmica desses sistemas computacionais, o que acarreta maior controle (*accountability*) e eficiência.

Mostra-se, com isso, que o ato de explicar os resultados e o funcionamento dos algoritmos com o cuidado e zelo aqui descritos, é, para além do princípio da transparência, uma condição de *boa prática* na gestão das políticas de privacidade, bem como no exercício da atividade do Encarregado de dados, sendo imprescindível constatar efetivamente se o interessado a compreendeu.

Referências bibliográficas

ALEMANHA, Bundesverfassungsgericht (BVerfG). **BvR 209/83.** Volkszählungsurteil. Absatz 146.

ARRIETA, Alejandro Barredo. DÍAZ-RODRÍGUEZ, Natalia. et. al. **Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI.** In: Information Fusion, vol. 58, 2020.

ARUN, Chinmayi. **AI and Global South: Designing for Other Worlds.** In: PASQUALE, Frank; et. al. The Oxford Handbook of Ethics of AI. Oxford Press, 2020.

BECKER, Daniel; FERRARI, Isabela. **O direito à explicação sobre decisões automatizadas: uma análise comparativa entre a União Europeia e o Brasil.** In: Revista de Direito e as Novas Tecnologias, vol. 1. São Paulo: Thomson Reuters/RT, Out-Dez/2018.

BIEGA, Asia J. et al. **Operationalizing the Legal Principle of Data Minimization for Personalization** In: SIGIR '20, July 25–30, 2020. Preprint. Disponível em: <https://arxiv.org/pdf/2005.13718.pdf >. Acesso em 05 de maio de 2022.

DE TERWANGNE, Cecile. **Principles relating to processing of personal data.** In: KUNER, Christopher. et al. The EU General Data Protection Regulation (GDPR): A commentary. Oxford Press, 2020.

BLUM, Renato Ópice. **LGPD Comentada.** 2ª Ed. São Paulo: RT, 2021.

BRASIL, Supremo Tribunal Federal (STF). **ADI 6389 MC-REF / DF**, Voto do Min. Gilmar Mendes.

DIAKOPOULOS, Nicholas. **Transparency.** In: PASQUALE, Frank; et. al. The Oxford Handbook of Ethics of AI. Oxford Press, 2020.

EBERS, Martin. **Regulating AI and Robotics: Ethical and legal challenges**. In: EBERS, Martin; NAVAS, Susana. Algorithms and Law, 2020.

EMIRADOS ÁRABES UNIDOS, **Smart Dubai: AI Ethics principles & Guidelines.** 2018.

ESPANHA, Agencia Española de Protección de Datos (AEPD). **Procedimiento n. E/00739/2021.** Disponível em: <https://www.aepd.es/es/documento/e-00739-2021.pdf>. Acesso em 20 de junho de 2022.

FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. **Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation.** In: International Data Privacy Law, Volume 7, Issue 2, May 2017.

FREITAS, Jurez; FREITAS, Thomas Beillini. **Direito e Inteligência Artificial: Em defesa do humano**. Belo Horizonte: Editora Fórum, 2020.

KAMATH, Uday; LIU, John. **Explainable Artificial Intelligence: Na introduction to interpretable Machine Learning.** Springer Verlag, 2021.

LU, Sylvia. **Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial intelligence.** In: Vanderbilt Journal of Entertainment & Technology Law, vol. 99, 2021.

MANKIW. N. Gregory. **Principles of Economics**. Cengage, 2021.

MAGRANI, Eduardo. SOUZA; Carlos Affonso; PERRONE, Christian. **O direito à explicação entre a experiência europeia e a sua positivação na LGPD.** In: SARLET, Ingo Wolfgang; et. al. Tratado de Proteção de Dados Pessoais. Editora Forense, 2021.

MARCINKEVICS; Ricard, VOGT, Julia E. **Interpretability and Explainability: A Machine Learning Zoo Mini-tour.** Preprint. Disponível em: <https://arxiv.org/abs/2012.01805> Acessado em: 21 de junho de 2022.

MEIJER, Albert. **Transparency.** In: BOVENS, Mark; GOODIN, Robert E. et. al. The Oxford Handbook of Public Accountability, 2014.

MENDES, Laura Schendel; MATTIUZZO, Marcela. **Algorithms and Discrimination: The case of credit scoring in Brazil.** In: ALBERS, Marion; SARLET, Ingo Wolfgang (org.). Personality and Data Protection Rights on the Internet: Brazilian and German Approaches. Springer Verlag, 2022.

MICHENER, Greg; BERSCH, Katherine. **Identifying transparency.** In: Information Polity 18 (2013).

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information.** Harvard University Press, 2015.

PECK, Patrícia. **Proteção de dados pessoais: Comentários à Lei n. 13.709/2018 (LGPD).** Saraiva, 2021.

PINTO, Edson Pontes. **Precedentes e algoritmos: uma abordagem de *law and economics*.** In: BECKER, Daniel. et. al. Litigation 4.0: O futuro da justiça e do processo civil vis-à-vis as novas tecnologias. Thomson Reuters, 2021.

PINTO, Edson Pontes; CÔRREA, Nicolas Kruge. et. al. **Worldwide AI Ethics: a review of 200 guidelines and recommendations for AI governance.** Arxiv. Preprint. Disponível em: <https://arxiv.org/abs/2206.11922>. Acessado em 27 de junho de 2022.

PORTUGAL, Comissão Nacional de Proteção de Dados (CNPD). **Deliberação 2021/622.** Disponível em: <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887>. Acessado em 20 de junho de 2022.

RIBEIRO, Marcia Carla Pereira; MARTINS, João Victor Ruiz. **Economia do compartilhamento, assimetria informacional e regulação econômica consumerista.**

In: Revista de Direito, Economia e Desenvolvimento Sustentável. V.2. N.2. Jul/Dez.2016.

RODOTÀ, Stefano**. Il mondo nella rete: Quali i diritti, quali i vincoli.** Roma: Laterza, 2014.

RODRIGUES, Karina Furtado. **Desvelando o conceito de transparência: seus limites, suas variedades e a criação de uma tipologia.** Cad. EBAPE.BR, v. 18, nº 2, Rio de Janeiro, Abr./Jun. 2020.

RUDIN, Cynthia. **Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead.** In: Nature Machine Intelligence, 1(5).

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. **Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de *big data*.** In: Direitos Fundamentais & Justiça. n. 41. jul./dez., 2019.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal Brasileira de 1988: Contributo para a construção de uma dogmática constitucionalmente adequada.** In: Direitos Fundamentais & Justiça. Belo Horizonte, ano 14, n. 42, jan./jun. 2020.

SELBST, Andrew D.; POWLES, Julia. **Meaningful information and the right to explanation.** In: International Data Privacy Law, Volume 7, Issue 4, November 2017.

SUÉCIA, Integritetsskyddsmyndigheten (IMY). **DI-2019-4062**. Disponível em: <https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf.>. Acessado em 22 de junho de 2022.

UE, União Europeia. A29WP. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**.

UE, União Europeia. **Guia Prático Comum do Parlamento Europeu, do Conselho e da Comissão para as pessoas que contribuem para a redação de textos legislativos da União Europeia**, 2013.

VRABEC, Helena. **Data Subject Rights under the GDPR**. Oxford Press, 2021.
WITTE, Robert S.; WITTE, John S. **Statistics**. 11th Ed. Wiley, 2017.

6. GOVERNANÇA COMO ARTÍFICE DA TUTELA DOS DADOS PESSOAIS

https://doi.org/10.36592/9786581110994-06

Evaldo Osorio Hackman[1]

Sumário

1. Introdução

A Ciência do Direito não deve se manter alheia ao processo evolutivo da humanidade. Ao contrário, tem de buscar formas de explicação e soluções para acomodar o avanço das relações em sociedade oriundas do contrato social que, com o passar dos tempos, é repactuado constantemente por todos nós.

Nas últimas décadas, especificamente a partir da segunda metade do século XX, o avanço tecnológico foi determinante para que alcançássemos uma série de conquistas que, talvez, em tempos remotos nem fossem almejadas pelo homem. A utilização massiva de computadores em larga escala, a automação de processos repetitivos pela robotização, a elaboração de diagnósticos clínicos com invulgar precisão, o desenvolvimento de políticas públicas mais assertivas, a organização eficiente do estado, tudo isto foi produto da indelével e inovadora revolução digital[2] que segue em constante e acelerado aprimoramento.

---

[1] Advogado. Mestrando da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). MBA em Gestão Empresarial pelo CEAD/Universidade Federal do Rio Grande do Sul (UFRGS). Especialista em Compliance (PUCRS). Graduado em Direito (UFRGS). E-mail: evaldo.osorio@edu.pucrs.br. Currículo Lattes: http://lattes.cnpq.br/1021977144196107.

[2] Para maiores dados e exemplos sobre a temática, recomenda-se: SCHWAB, Klaus. *The Fourth Industrial Revolution*. New York: Currency Books, 2017.

Em face da aludida transformação, não se pode deixar de mencionar a hiper conectividade presente nas mais diversas culturas e sociedades. Atualmente, ainda mais após o período de reclusão forçada, imposto pela epidemia do Coronavírus em todas as geografias, é cada vez mais comum que se utilizem os mais diversos *devices* tecnológicos[3] conectados à rede mundial de computadores para as mais sortidas ações, tais quais, compras de itens de necessidades básicas, agendamentos de consultas, reuniões de trabalho e operações financeiras a título de exemplificação tão-somente.

De outra banda, essa conexão alargada e quase permanente pode ser fonte geradora de externalidades negativas em igual medida, isto é, caso não sejam observados alguns importantes requisitos elementares de segurança da informação, expondo-se os usuários de seus recursos aos mais diversos riscos associados a essas atividades digitais. Não por acaso, tem-se noticiado quantidade assombrosa de vazamentos e violações de dados, sejam de natureza pessoal, sejam de natureza corporativa, nos mais diferentes setores de da economia mundial. Estes incidentes cibernéticos, apenas em 2021, resultaram em prejuízos financeiros vultosos conforme aponta conhecido relatório[4] que totaliza os custos de violação de dados por segmento de mercado.

Nesse sentido, assiste razão aos que preconizam estar-se vivendo o período chamado de sociedade da informação[5]. Nesta quadra, mais do que em qualquer outro momento da história da humanidade, os dados – pessoais ou corporativos – têm um valor significativo para a maioria dos agentes econômicos que, por sua vez, procuram acessá-los das mais alternativas formas existentes, nem sempre

---

[3] Recente reportagem aponta que já existem mais *smartphones* que habitantes em território brasileiro. Disponível em: <https://www.cnnbrasil.com.br/business/brasil-tem-mais-smartphones-que-habitantes-apontafgv/20atualmente%20mais,de%20acordo%20com%20o%20IBGE.> Acesso em: 15/06/2022.

[4] A pesquisa foi conduzida de forma independente pelo Instituto Ponemon e os resultados foram patrocinados, analisados, relatados e publicados pela IBM Security: tratam-se de 537 violações reais, ocorridas em 17 países e em 17 verticais de negócios diversas. Disponível em: < https://www.ibm.com/br-pt/security/data-breach.>. Acesso em 16/06/2022.

[5] "*In some quarters at least, there has been a move away from technology as the source of comments towards what one might consider the softer sides of information. This is reflected in a shift from computer communications technologies towards interest in social media, where commentary move from concern with what technology is doing to society towards what people can do with technologies that are now pervasive, accesible and adaptable*." WEBSTER, Frank. *Theories of the Information Society*. London: Routledge, 2014, p.17.

respeitando os direitos fundamentais dos indivíduos e o desenvolvimento econômico das organizações empresariais.

Para fins de elaboração do presente trabalho, por ora, apartam-se os dados pessoais dos demais. Estes podem ser considerados o objeto de desejo das grandes organizações que movem a nova economia[6], modelo que se baseia num denso e veloz processo de mineração de dados pessoais, tratamento seletivo de informações e geração de conhecimento com vistas à obtenção das preferências do maior número de consumidores possível, com o cristalino objetivo de aumento de vantagem econômica nessa relação – inequivocamente – assimétrica de poder.

A assimetria em destaque é um dos fatores que determina o gigantismo das *Big Techs*, empresas globais de tecnologia que, por vezes, detêm mais capacidade econômico-financeira que estados nacionais, e utilizam sua força de quase monopolistas no sentido de exercer dominância e atuarem no papel de reguladores *ad hoc*.

Dessa feita, é necessário que o Direito exerça seu mister protetivo em relação a resguardar o direito fundamental à proteção de dados pessoais dos indivíduos[7]. Antes que haja interpretação em sentido oposto, cumpre-se destacar que não se adere aquela falsa dicotomia entre o desenvolvimento econômico e a tutela dos direitos fundamentais. Ao revés, o que se busca é o estabelecimento de uma atuação da Ciência Jurídica pautada na justa medida entre o progresso da economia, o avanço da tecnologia e o respeito aos direitos acima referidos[8].

Outrossim, acredita-se que o Direito pode servir de catalisador do processo de desenvolvimento tecnológico, sustentando de maneira harmônica, segura e

---

[6] Para melhor entendimento do modelo econômico, leia-se: PENTLAND, Alex. LIPTON, Alexander. HARDJONO, Thomas. *Building the new economy – Data as Capital*. Cambridge: MIT Connection, Science & Engineering, 2021.

[7] Sobre o tema, impõe-se a leitura da consagrada obra: SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 13 ed. Revisada, atualizada e ampliada. Porto Alegre: Livraria do Advogado, 2021.

[8] Assim, leciona a melhor doutrina: "As inovações provocam respostas à questão de se e em que medida as regras legais tradicionais são adequadas para lidar com a situação problemática alterada e para a realização otimizada dos novos objetivos valorativos já ancorados na ordem jurídica e social ou mesmo importantes sob as condições alteradas. Os objetivos importantes incluem a proteção da liberdade individual, a manutenção dos princípios do Estado de Direito, o funcionamento da ordem democrática, mas também a promoção do desenvolvimento econômico e tecnológico e a viabilização das inovações necessárias para tal." HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital: transformação digital: desafios para o direito*. Rio de Janeiro: Forense, 2022, p.7.

responsável o surgimento das inovações. Precisamente neste ponto, verifica-se uma característica própria da expansão globalizada da tecnologia, pois, em que pese as diferenças geográficas, sociopolíticas e culturais, as falhas oriundas da atuação indevida das grandes corporações de tecnologia se repetem, e podem ser enfrentadas com soluções que se assemelham, em termos de conteúdo normativo, nos diversos sistemas jurídicos espalhados ao redor do globo.

Entretanto, soluções tradicionais protetivas de direitos fundamentais não estão aptas, no mais das vezes, a enfrentarem os problemas ocasionados pelo hodierno processamento contínuo e onipresente [9] dos dados pelos agentes econômicos da indústria tecnológica.

Dessa forma, assume-se que a mais correta medida aos desafios impostos pelo avanço tecnológico não pode prescindir de uma solução jurídica que incorpore em sua resposta aspectos conceituais e pragmáticos de governança. Esta é área do conhecimento concebida sob a ideia de um sistema de relações multidisciplinares, guardião de direitos, customizável e direcionado aos melhores resultados no interesse de todos os *stakeholders*.

Com efeito, o conceito e os fundamentos de governança são estudados e disseminados no seio de todas as gigantes da indústria da tecnologia da informação e comunicações. Por isto mesmo, reputa-se que a utilização desta área do conhecimento como parte da solução jurídica para a proteção de direitos fundamentais, em face do avanço indiscriminado e inescrupuloso dessas tecnologias, seria uma alternativa desejada e bem aceita pelas empresas deste pujante setor econômico, podendo facilitar a continuidade de seus negócios em estrita conformidade com os ordenamentos jurídicos locais e baseada em parâmetros éticos.

De fato, cumpre ao trabalho em tela perquirir como a governança pode colaborar efetivamente na tutela do direito fundamental à proteção de dados

[9] "A proteção de dados pessoais alcançou uma dimensão sem precedentes no âmbito da assim chamada sociedade tecnológica, notadamente, a partir da introdução do uso da tecnologia da informática e da ampla digitalização que já assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica, política, cultural contemporânea no mundo, fenômeno comumente designado *Ubiquituous Computing*." SARLET, Ingo Wolfgang. *Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados*. *In*: DONEDA, Danilo. et al. Tratado de Proteção de Dados Pessoais. 2ª ed. Rio de Janeiro: Forense, 2021, p.21 e ss.

pessoais em razão dos riscos associados ao avanço tecnológico, constituindo-se num legítimo e autêntico *standard* jurídico promotor de boas condutas, atendendo às legítimas expectativas de todas as partes envolvidas nessa relação conflituosa. Para isto, recorre-se ao método de interpretação exegético, com adoção da interpretação histórica, lógica e literal das regulações e autorregulações; adicionalmente, opta-se pelo tipo de pesquisa bibliográfica, legal e doutrinária, de modo a sustentar-se a escolha que se julga inarredável e mais alinhada à essência da fidúcia depositada pelos indivíduos na Ciência do Direito.

Finalmente, no intuito de colaborar com a elaboração de uma posição sobre o tema, bem como agregar argumentos verdadeiramente assertivos ao estabelecimento de uma resposta positiva aos desafios supra referidos, mas sem a pretensão de exaurir a necessária discussão que o tema suscita, concluir-se-á o presente artigo com as considerações finais, sustentando-se a linha-mestra deste modesto contributo acadêmico.

2. Proteção de dados pessoais: considerações gerais e conceito

O tema proteção de dados e privacidade corresponde, atualmente, a um dos objetos de maior interesse no campo do Direito Digital. Isto, pois, a cada dia que passa verifica-se a necessidade de tutela desses direitos fundamentais em meio às tentativas monetizar a sua utilização, não raramente, ao arrepio do consentimento[10] emanado pelo titular dos dados.

Todavia, equivoca-se quem pensa que se trata de assunto surgido há pouco e ditado pelo *zeitgeist*. Essa temática jurídica, como bem lembra a doutrina[11], tem sua construção pavimentada há mais de cinco décadas.

---

[10] Neste ponto, convém a lembrança de que o consentimento deverá ser válido (livre, comprovado e inequívoco), voltado à finalidade específica e de modo que ao titular dos dados não reste dúvidas quanto à forma de utilização de suas informações. Nessa seara, ver-se: BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* 3ª. ed. Rio de Janeiro: Forense, 2021, p. 113 e ss.

[11] "A Lei de Proteção de Dados do Land alemão de Hesse, de 1970, é identificada como o primeiro diploma normativo que trata especificamente dessa matéria, e debates que tiveram lugar na segunda metade da década de 1960 foram extremamente ricos e fundamentais para definir o perfil dessa disciplina que, de acordo com as expectativas, hoje está presente de forma concreta em mais de 140 países." DONEDA, Danilo. *Panorama histórico da proteção de dados pessoais*. *In*: DONEDA, Danilo. et al. Tratado de Proteção de Dados Pessoais. 2ª ed. Rio de Janeiro: Forense, 2021, p.3 e ss.

Adicionalmente, impõe-se destacar que em relação à edição das legislações protetivas de dados e privacidade, verifica-se um fenômeno de harmonização de conceitos, institutos e ferramentas disseminados nesses diplomas[12] e, certamente, objetivado pelo legislador positivo em cada país. De modo que, mesmo tendo em conta as diferentes realidades dos locais em que foram gestadas, há – de certa maneira – uma gramática e estruturas universais comuns que se mimetizam e se assemelham, formando um verdadeiro sistema extraterritorial e integrado de proteção de dados e privacidade

Com efeito, na época atual, a proeminência desse tema tem tomado os mais destacados espaços de discussões acadêmicas não apenas pela complexidade do assunto, mas também pela necessidade de adequação da vida contemporânea cada vez mais impactada pela transformação digital já conceituada neste artigo.

Assim, convencionou-se que a proteção de dados pessoais se refere ao conjunto de regras que tem por objetivo primordial impedir o tratamento inadequado desses dados e informações, repelindo qualquer conduta antiética, abusiva, discriminatória ou injusta que guarde relação com uma pessoa natural identificada ou identificável, i.e., o titular dos dados.

Dessa forma, as leis gerais e regulamentos de proteção de dados visam não apenas à proteção dos direitos fundamentais dos titulares de dados, mas – em via de mão dupla – garantir que organizações empresariais possam realizar o tratamento desses dados ou informações em conformidade com os principais marcos regulatórios e as Cartas Constitucionais, delineando uma política de tratamento baseada nos mais destacados princípios que norteiam esse tema como veremos a seguir.

2.1. Princípios informadores da proteção de dados pessoais e privacidade

Conforme apontado anteriormente, o nascedouro da preocupação com a proteção de dados guarda mais de cinco décadas em relação ao tempo presente.

[12] Sobre elementos conceituais harmônicos ou próximos às definições de proteção de dados e privacidade, em diferentes ordenamentos jurídicos, busque-se: BENNET, Colin. *Regulating Privacy, Data Protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992.

Contudo, a sistematização dos princípios comuns às leis gerais emergiu alguns anos depois. Dentre os marcos históricos delineadores do assunto, destacam-se a decisão do Tribunal Constitucional Alemão (decisão do censo) e os *guidelines* de privacidade da OCDE.

Ambos os acontecimentos, em razão de sua importância e influência exercidas sobre os mais importantes diplomas acerca da tutela de proteção de dados pessoais e privacidade, serão conteúdo das próximas passagens do trabalho.

2.1.1. Princípio da autodeterminação informativa

Quando se trata de proteção de dados pessoais, cabe trazer à baila a histórica decisão do Tribunal Constitucional Alemão, na década de 80, conhecida como "Decisão do Censo". Nessa oportunidade, o egrégio tribunal deu significado emblemático a expressão "autodeterminação informativa", promovendo as bases de uma autêntica teoria geral.

A expressão prolatada naquela sentença constitucional determina que é direito do indivíduo, pessoa natural assim considerada, decidir acerca da possibilidade ou não do compartilhamento de informações que digam respeito à sua pessoa exclusivamente.

Os argumentos utilizados pelos juízes constitucionais[13], à época, serviram de base para o estabelecimento de princípios que, até hoje, estão presentes nas legislações mais importantes sobre o assunto.

---

[13] Conforme apontado pela doutrina, seguem importantes trechos do julgado paradigmático: "(...) aquele que não pode vislumbrar, com segurança suficiente, quais informações pessoais a si relacionadas existem em áreas determinadas de seu meio social, e aquele que não pode estimar em boa medida qual o conhecimento que um possível interlocutor tenha da sua pessoa, pode ter a sua liberdade consideravelmente tolhida.
(...) aquele que não tem segurança se o seu modo comportamental desviante, está ou não, a todo o momento registrado, e como informação, sendo armazenado ao longo do tempo e utilizado ou disponibilizado a terceiros, tentará não incidir em tal modo comportamental. Aquele que parte do pressuposto de que, por exemplo, a participação em uma reunião ou em uma iniciativa do exercício de cidadania seja registrado por um órgão público, e que a partir dessas atividades possam lhe advir riscos, provavelmente, abdicará do exercício dos direitos fundamentais relativos a essas atividades." ARTESE. Gustavo. *Compliance Digital e Privacidade*. *In*: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINI, Otávio, *Manual de Compliance*. 2.ed. São Paulo: Editora Forense, 2020, p.462.

Como ver-se-á adiante, nessa mesma década, ao lado da decisão do Tribunal Constitucional Alemão, marco da promoção ao direito humano e fundamental tema desta seção, surge a publicação *Guidelines on the Protection and Transborders Flows of Personal Data*, da OCDE (Organização para Cooperação e Desenvolvimento Econômico), cuja importância se revelará orientadora para a edição dos atuais marcos regulatórios de proteção de dados e privacidade atuais e será esposada nas linhas adiante.

2.1.2. OCDE – *Guidelines on the Protection and Transborders Flows of Personal Data*

Outro marco na promoção do direito a proteção de dados e privacidade merecedor de registro neste escrito são as "Diretrizes para Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais"[14], de lavra da OCDE.

A exposição de motivos dessa diretriz trouxe invulgar contribuição ao fortalecimento do arcabouço protetivos dos dados pessoais e privacidade, alertando para a introdução da tecnologia de informação em várias áreas da vida econômica e social, bem como chamou à atenção para a importância do incremento no processamento automatizado de dados. Em sua revisão, no ano de 2013, destacou o desenvolvimento veloz e predominantemente das tecnologias e infraestruturas de informação e comunicação, propiciado pelo significativo aumento de acesso à Internet, potencializando a rápida evolução para uma sociedade global de informação como já identificado no início do artigo. Assim, a OCDE enfocou na

[14] Na página da OCDE, destaca-se a seguinte informação acerca desse *guideline*: *The Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data was adopted by the OECD Council on 23 September 1980 ("1980 Guidelines"). The 1980 Guidelines were adopted to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. They represent the first internationally agreed-upon set of privacy principles and have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, they were updated on 11 July 2013 due to changes in personal data usage, as well as new approaches to privacy protection. The Recommendation aims to promote and protect the fundamental values of privacy, individual liberties and the global free flow of information to foster the development of economic and social relations among Adherents*. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188#backgroundInformation>. Acesso em 18/06/2022.

melhor maneira de implementar estas diretrizes com vistas a assegurar o respeito à privacidade e à proteção dos dados pessoais.

Nessa esteira, o conteúdo do documento denota um consenso internacional sobre a orientação geral a respeito da coleta e do gerenciamento da informação pessoal. Os princípios nele determinados são caracterizados pela clareza, maleabilidade de aplicação e pela formulação genérica afim de possibilitar a adaptação às mudanças tecnológicas, abrangendo todos os tipos de processamento de dados pessoais e todas as categorias de dados pessoais ordinários ou sensíveis[15].

Em linha com os conceitos acima expostos, a OCDE sistematizou, na segunda parte[16] do documento, os *FIPP's – Fair Information Privacy Principles*, princípios que serviram de inspiração para as leis gerais e regulamentos de proteção de dados pessoais e privacidade em todos os ordenamentos jurídicos.

Destarte, pode-se destacar alguns dos mais significativos que se encontram inseridos nos principais marcos regulatórios, total ou parcialmente.

O princípio de limitação da coleta determina que a captura de dados pessoais seja limitada, atendo-se, apenas, aos dados necessários para aquele propósito. Ainda, que seja precedida do consentimento do titular de dados. De outro lado, o princípio da qualidade dos dados guarda estrita relação com a qualidade, a integralidade e a exatidão dos dados objeto de tratamento.

Avançando, o princípio da definição da finalidade (*corporate liability*) reforça que a destinação dos dados coletados, ou seja, a finalidade (propósito) da coleta deverá ser informado ao titular, imediata e inequivocamente, para que este tenha ciência acerca do que será realizado com os seus dados pessoais. Trata-se de uma verificação de compatibilidade entre a consentimento e o tratamento propriamente

---

[15] ORGANISATION FOR ECONOMIC CO-OPERATON AND DEVELOPMENT. OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD Publishing, 2002. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.>. Acesso em 18/06/2022.

[16] ORGANISATION FOR ECONOMIC CO-OPERATON AND DEVELOPMENT. OECD *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. OECD Publishing, 2002. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188#mainText>. Acesso em 18/06/2022.

dito. Em caso de alteração de propósito para uso dos dados pelo controlador, o titular deverá ser informado novamente acerca dessa mudança.

O princípio da limitação de utilização manda que os dados pessoais tenham como fronteira instransponível a finalidade informada ao titular no momento da coleta. Ou seja, não poderá haver destinação contrária, salvo em dois casos: com o novo consentimento do titular ou por força de lei.

Já o princípio do backup de segurança impõe a necessária implantação de mecanismo de segurança da informação que garanta a proteção dos dados coletados contra perda, acessos espúrios, destruição, modificação ou utilização indevida.

No que guarda relação com o princípio da transparência (*disclousure*), tem-se que para o esclarecimento de qualquer dúvida suscitada pelo titular dos dados, deverão existir mecanismos que permitam o acesso, a verificação da finalidade, a identificação do fluxo e a comprovação do ciclo de vida desses dados junto ao controlador que, igualmente, deverá ser identificado e individualizado.

Noutra seara, o princípio da participação do indivíduo (*fairness*) exemplifica a relação entre o titular dos dados pessoais e o controlador. Deve-se fornecer toda e qualquer informação acerca do tratamento de dados ao titular: confirmar se há dados que o pertencem na organização, como esses dados estão sendo tratados, a possibilidade de retificação ou esquecimento desses dados em caso de encerramento da relação entre a instituição e o titular. Tudo isto, evidentemente, de forma transparente, ágil e numa linguagem acessível a titular. De modo que a ele não reste qualquer dúvida no que diz respeito ao tratamento de dados.

Finalmente, o princípio da prestação de contas (*accountability*) traduz que o controlador deverá prestar contas sempre que acionado pelo titular sobre o tratamento realizado enquanto estiver de posse dos dados pessoais do mesmo.

A compreensão dos conceitos relacionados aos chamados *Fair Information Privacy Principles*, tendo em vista que os mesmos estão alinhados e suportam o regulatório acerca dessa matéria significativamente, podem servir de fundamento à Governança Digital e suas boas práticas como parte da solução jurídica como pretende-se mostrar no próximo item do presente estudo.

3. Governança digital para a tutela do direito fundamental à proteção de dados pessoais

3.1. A governança corporativa (gênero)

Antes de destacar-se um conceito de Governança Digital (espécie), é fundamental que se traduzam os elementos essenciais da Governança Corporativa (gênero). Assim, com o fito de situar o leitor diante da multiplicidade de definições sobre o tema, é prudente que se opte por um conceito base de Governança Corporativa para ter-se o mesmo como farol à tese que será esposada a seguir.

Preliminarmente, destaque-se que não existe um conceito estático e definitivo, tendo em vista que se trata de um tema fluido e em constante aprimoramento, que busca adaptar-se às mudanças culturais e socioeconômicas das nações nas quais se desenvolve.

Pois bem, existe uma variedade de definições acerca da expressão governança. No entanto, por mais diversas que possam ser, sempre há pontos em comuns, elementos fundamentais que nos permitem identificá-la sem maiores dificuldades, quais sejam, sistemas de relações, guardiã de direitos, estrutura de poder e sistema normativo[17].

Para o Instituto Brasileiro de Governança Corporativa[18], a Governança Corporativa traduz-se no sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria e demais partes interessadas. Além disso, reforça que as boas práticas de governança convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

---

[17] ROSSETI, José P. ANDRADE, Adriana. *Governança Corporativa: fundamentos, desenvolvimento e tendências*. 7. ed. – São Paulo: Atlas, 2016, p. 140.
[18] IBGC – Instituto Brasileiro de Governança Corporativa. *Código das melhores práticas de governança corporativa*. 5ª edição. São Paulo: IBGC, 2015.

Por outro lado, a OCDE[19] adota um viés que busca garantir o interesse de todos os envolvidos com as atividades desempenhadas pelos entes empresariais. Ou seja, além de contemplar o conceito de sistema de relações, esta organização de alcance global traz em sua definição sobre o tema aspectos que nos levam a determinar que a Governança Corporativa, igualmente, pode ser um sistema normativo e, principalmente, a guardiã de direitos dos demais *stakeholders* na continuidade dos negócios das organizações[20].

Em face do exposto, prefere-se adotar um conceito ampliado de governança, *stakeholder oriented*, nos moldes propostos pela OCDE, em face da crença na conjugação entre a maximização dos lucros e os interesses de todos os demais envolvidos no entorno da corporação.

3.2. A governança digital (espécie)

Inicialmente, destaca-se que a Governança Digital não está adstrita ao setor público. Em razão da disponibilidade de soluções cibernéticas e da necessidade de aproximar-se o estado do cidadão, há uma justa apropriação do termo pelas instituições governamentais[21] com mais frequência e, com isso, o leitor menos habituado ao tema pode pensar que a mesma se aplica a elas exclusivamente.

Evidentemente, não se admite a interpretação acima, pois, os dados pessoais São igualmente tratados pelos entes privados, na condição de controladores, demandando que se reforcem as políticas e medidas protetivas, com base na

[19] Nas palavras da organização referida: A Governança Corporativa é o sistema segundo o qual as corporações de negócios são dirigidas e controladas. A estrutura da Governança Corporativa especifica a distribuição dos direitos e responsabilidades entre os diferentes participantes da corporação, tais como o conselho de administração, os diretores executivos, os acionistas e outros interessados, além de definir regras e procedimentos para a tomada de decisão em relação a questões corporativas. E oferece também as bases através das quais os objetivos da empresa são estabelecidos, definindo os meios para se alcançarem tais objetivos e os instrumentos para se acompanhar o desempenho. OCDE – ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Corporate governance principles*. Disponível em: <https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf>. Acesso em 20/06/2022.

[20] Adota-se o conceito denominado *Stakeholder Capitalism*, cuja essência pode ser verificada, entre outras fontes, em: SCHWAB, Klaus; VANHAM, Peter. *Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet*. John Wiley & Sons: New Jersey, 2021.

[21] A título de exemplo, veja-se: TRIBUNAL DE CONTAS DA UNIÃO. *Relatório de Políticas e Programas de Governo*. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação (Sefti), 2018.

mesma espécie de governança como se demonstrará a seguir.

Resumidamente, define-se a Governança Digital como o sistema de relações que dirige, monitora e controla as organizações, concebendo políticas e medidas amparadas na utilização de tecnologias da informação e comunicação e boas práticas de governança, com vistas à obtenção dos melhores resultados para a corporação e todos os demais *stakeholders* de forma ética, segura e responsável.

Decompondo-se essa sentença, vê-se que – com o perdão da repetição – o estabelecimento de boas práticas da governança em destaque se aproveita, salvo melhor juízo, a todos os que estão imersos no que se chama de transformação digital.

Por um lado, a maior parte das empresas que tratam dados pessoais o fazem em razão da busca pela maximização dos lucros de seus acionistas. Como forma de delimitar a temática, às *Big Techs* (sociedades anônimas listadas em mercados de capitais) os conceitos de governança estão no dia a dia das organizações, servindo de baliza para a tomada de decisão de seus administradores e demais colaboradores.

De outra banda, entre os demais interessados, *stakeholders*, estão os titulares de dados pessoais que devem ter seus direitos fundamentais preservados quando do tratamento dessas informações com base nessas boas práticas.

Em razão da hiper conectividade, ganha mais relevância a implantação de políticas e medidas que possam mapear os riscos associados às tecnologias da informação e comunicação. No modelo de negócios originado em meio à transformação digital, e que sustenta a sociedade da informação, é necessário que se previnam condutas inadequadas em contraposição à tutela dos direitos fundamentais à proteção de dados pessoais e à privacidade.

Com razão, afirma-se que a proteção de dados tem um marcante sinal de autoconformação[22], isto é, quando apenas o titular de dados pode determinar o âmbito da sua privacidade, expressando sua vontade de modo livre, inequívoco e expresso. Entretanto, pergunta-se – ainda que intimamente saiba-se a reposta em face da realidade que se impõe à mera divagação – existe como afirmar ser o

[22] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor – Linhas gerais de um novo direito fundamental.* São Paulo: Saraiva, 2014, p. 60.

consentimento, a autodeterminação do titular de dados, exercido dentro de sua plenitude na sociedade da informação? Acredita-se que a resposta é negativa.

Com o massivo e acelerado processamento de dados em escala sem precedentes na história da humanidade, fala-se do fenômeno chamado de *Big Data*[23], é bem mais prudente que se perceba uma diluição consentimento por parte dos titulares. São tantas as informações, os meios digitais, os aparelhos, as formas de conexão que não se admite que o indivíduo possa deter condições suficientes para controlar ou definir suas preferências de privacidade, em relação às quais ele emite um consentimento viciado, contrariando o preceito da autodeterminação informativa frontalmente. Numa palavra, o titular perde o controle diante de tamanha complexidade digital.

É com base nisso que se comenta sobre a diluição do consentimento a partir da perspectiva do titular de dados pessoais, usando-se expressões que denotam perda de noção, sentido, resignação e ausência de condições de insurgir-se contra esses abusos da transformação digital[24].

Conclui-se que a alternativa mais indicada para mitigar os riscos associados à diluição do consentimento é implementação de políticas e medidas estruturais de Governança Digital em colaboração às determinações das leis gerais e regulamentos de proteção de dados pessoais e privacidade, pois, é mister que se imponha às *Big Tech* um arranjo normativo que faça as vezes de um *standard* jurídico determinante da utilização de dados pessoais em padrão ético superior e que, ao mesmo tempo, promova uma cultura protetiva dessas informações[25].

Assim, de um lado, resguardar-se-á de forma preventiva (a partir de uma conduta proativa do controlador) o titular de dados (antecipando-se ao consentimento), mitigando-se os riscos da indevida usabilidade de suas informações sensivelmente. Na outra ponta dessa relação, ter-se-á uma forma de

---

[23] *Big Data*: é o ato de gerar, combinar, processar e obter resultados a partir de uma grande coleção de dados com o objetivo de estabelecer tendências, padrões de consumo e condutas que possam gerar maior conversão de vendas e produzir resultados mais positivos (lucratividade) para as empresas.

[24] *Op. cit.*, p. 469.

[25] Na medida em que se verifica benefícios na adoção desses mecanismos de governança, prescreve a doutrina: "Uma das tarefas do Estado é criar leis ou modificá-las de forma a possibilitar e estimular a boa governança digital." HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital: desafios para o direito. Rio de Janeiro: Forense, 2022, p.158.

exigir-se a conformidade do controlador, responsabilizando a organização pelo tratamento inadequado de dados pessoais se o caso concreto assim requerer.

Tomando-se como opção as boas práticas mencionadas para superação da dificuldade vivenciada pelo titular de dados, qual seja, o consentimento diluído, deve-se traçar os principais componentes dessas políticas de governança, tema sobre o qual discorrer-se-á na parte final do presente artigo.

3.3. Políticas e boas práticas de governança digital

As políticas de governança devem levar em consideração para sua criação as condições socioeconômicas, a cultura organizacional, os riscos associados ao processamento dos dados nas atividades empresariais e as peculiaridades de cada corporação. Com isso, intenta-se demonstrar que não existe uma fórmula mágica para a concepção dessas medidas, ou seja, afasta-se a máxima *one size fits all* desde logo.

Para atingir-se a finalidade deste estudo, esclarece-se que o desenho da Governança Digital que se pretende endereçar leva em consideração a aplicação de suas normas por empresas de grande porte pertencentes ao setor de tecnologia da informação e comunicação. Estas organizações, em virtude de sua atuação globalizada, detêm maior proximidade com os conceitos que serão expostos, sobretudo, em razão de possuírem capital aberto, o que facilitará a sua incorporação nas rotinas organizacionais[26].

Como mencionado anteriormente, esse movimento é complementar e colaborativo em relação às disposições das leis gerais e regulamentos protetivos de dados pessoais. Repise-se, não se pretende (e nem seria o caso) substituir-se à regra posta. Ao contrário, o que se busca é agir antecipadamente para que o diploma não precise ser acionado para sancionar conduta que afronte as disposições contidas em seu texto.

---

[26] "(...) é de se esperar que a maioria, especialmente as empresas de TI dominantes no mercado, privilegiem os princípios éticos em detrimento de uma obrigação legal e procurem evitar ao máximo a legalização e a sanção, preservando, assim, a liberdade de salvaguarda seus próprios interesses." HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital: transformação digital: desafios para o direito*. Rio de Janeiro: Forense, 2022, p.163.

É cediço que mesmo que haja uma imprescindibilidade de procedimentos sancionatórios ínsitos ao direito positivado, o objetivo precípuo da medida é gerar a conformidade legal e a adequação comportamental, e não a punição (*ultima ratio*), sendo a prevenção peça-chave para o atingimento desse desiderato[27]. Gize-se, em tempo, que a prevenção é princípio expresso na Lei Geral de Proteção de Dados – LGPD.

Nessa toada, exsurge surge como pedra angular da Governança Digital o *Compliance*, cujo sistema de gestão adaptado e concebido diante da realidade da organização que controla os dados será fundamental para a mitigação dos riscos associados ao tratamento dos mesmos. Este sistema ou programa de integridade vem ganhando espaço em um cenário de complexa e necessária regulação, como no caso das atividades de tecnologia da informação e comunicação, onde as soluções legislativas tradicionais não conseguem acompanhar os desafios que são impostos à sociedade na mesma velocidade. Inclusive, a própria legislação[28] é incentivadora do estabelecimento desses programas de *Compliance* como forma de repartição das responsabilidades do Poder Público com as organizações privadas.

De fato, a LGDP, em seu artigo 50, enumera uma série de disposições sobre as boas práticas de Governança Digital, indicando a possibilidade de incorporação de destas medidas pelos agentes de tratamento de dados[29]. Dito isso, cumpre-se destacar os pilares desse mecanismo interno (programa da *Compliance* Digital) de

[27] "Sem desconsiderar a relevância de regras punitivas, é notório na literatura que o desenvolvimento de estratégias regulatórias em que governança e repressão caminham juntas são mais efetivas. Ver: FRIEDMAN, Lawrence M. *Impact*. Harvard University Press, 2016, p. 139-153; ROBERTS, Robert. *The rise of compliance-based ethics management: implications for organizational ethics*. Public Integrity, v. 11, n. 3, p. 261-278, 2009." CARVALHO, Vinicius Marques de. MATTIUZZO, Marcela. PONCE, Paula Pedigoni. *Boas práticas e governança na LGPD*. In: DONEDA, Danilo. et al. *Tratado de Proteção de Dados Pessoais*. 2ª ed. Rio de Janeiro: Forense, 2021, p.361.

[28] A Lei Anticorrupção (art. 7º, inc. VIII, da lei nº 12.846/2013) prevê que a existência de programas dessa espécie, comprovadamente disseminados na organização, poderá ser levada em consideração para mitigação das sanções legais.

[29] BRASIL, Lei Geral de Proteção de Dados Pessoais (lei nº 13.709/2018), art. 50, *caput*: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.>. Acesso em 20/06/2022.

forma individualizada.

4. Requisitos do programa de *Compliance* Digital

Existem alguns requisitos básicos [30] à constituição de um programa de *Compliance* Digital que devem ser levados em consideração pelos agentes de tratamento de dados quando da sua elaboração. Estes itens têm por escopo delimitar a atuação do programa, bem como fomentar a disseminação de uma cultura de dados pessoais no seio das organizações.

Um adequado programa deverá contar com o apoio da alta administração. Nesse sentido, é legítima a expectativa de que os controladores fomentem em suas organizações o cumprimento dessas medidas em todos os níveis das empresas e, ainda, destinem recursos humanos e financeiros suficientes para que o escopo do programa seja alcançado.

Outrossim, todo e qualquer dados pessoal tratado pela corporação ou pela sua cadeia de prestadores de serviços deverá ser alvo dessas boas práticas. Assim, deverão ser mensuradas a escala e o volume dos dados tratados, ainda, efetuar-se a prudente classificação dos mesmos como sensíveis[31] ou não.

---

[30] BRASIL, Lei Geral de Proteção de Dados Pessoais (lei nº 13.709/2018), art. 50, inciso I:
I – implementar programa de governança em privacidade que, no mínimo:
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

[31] Especialmente, no que diz respeito ao tratamento de dados sensíveis, recomenda-se: RUARO, Regina. SALES SARLET, Gabrielle Bezerra. *O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados*

Para que não se assemelhe a um corpo estranho dentro das normas atinentes às atividades empresariais, é fundamental que se comunique a todos os colaboradores e terceiros que o programa integra a Governança Corporativa institucional. Isto é, que se demonstre que o cumprimento das medidas dispostas no programa de *Compliance* Digital é mandatório a todos que tenham relação com a organização e, com isso, indique-se que haverá constante e necessária atuação de supervisão das condutas por eles praticadas.

Ao lado dessas medidas, é fundamental que se avaliem os riscos associados às atividades desenvolvidas pelo ente empresarial. Nessa linha, a elaboração de uma avaliação de impacto prévia a utilização de dados pessoais é extremamente importante.

Igualmente, após essa avaliação, deve-se criar um plano de gestão de crises para acionamento em caso de falha nas medidas de segurança da informação que visam suportar o adequado tratamento dos dados para o caso de incidentes cibernéticos, vazamento e violação de sistema, por exemplo.

Por fim, é necessário que esse programa seja constantemente monitorado e atualizado com base em boas práticas de segurança da informação e standards internacionalmente reconhecidos. Isto será essencial para manter-se a integridade do sistema de informações da corporação, protegendo os dados por ela tratados.

Na essência do programa de *Compliance* Digital está o atendimento às legitimas expectativas depositadas pelo titular dos dados tratados pela organização. À empresa controladora caberá firmar uma relação de confiança e credibilidade com aquele, possibilitando a sua participação nesse processo de forma transparente e segura.

Finalmente, tendo em vista o aspecto pragmático do estudo em tela, faz-se imperioso destacar os elementos fundamentais do programa de com amparo nas lições de Giovani Saavedra:

1.*Privacy by Design*: essa metodologia abarca o conceito de que cada produto ou serviço entregue ao usuário final da solução deverá considerar, desde a sua concepção, os aspectos fundamentais de proteção de dados e privacidade. Assim,

---

(LGPD) – Lei 13.709/2018. *In*: DONEDA, Danilo. et al. Tratado de Proteção de Dados Pessoais. 2ª ed. Rio de Janeiro: Forense, 2021, p.177 e ss.

deverão levar em consideração o c*ompliance* de digital durante todo o seu ciclo de vida, sempre conjugando esse fundamento com as boas práticas de segurança da informação.

2.Código de Ética de Conduta: é exigido pelos principais regulamentos de proteção de dados, RGPD e LGDP, que os referidos códigos possuam seções específicas que digam respeitos aos aspectos, conceitos e princípios atinentes à proteção de dados e privacidade.

3.*Data Protection Officer* (DPO): trata-se de uma exigência legal a eleição de um Encarregado de Dados (LGPD) ou DPO (RGPD) para que centralize as ações relativas ao tratamento de dados pela organização. Esta figura será a responsável, entre outras coisas, por atender as demandas dos titulares de dados, receber e responder as comunicações provenientes da Autoridade Nacional de Proteção de Dados (ANPD), implementar as medidas necessárias à proteção de dados e privacidade. Além disso, deverá ser o principal motivador e disseminador da cultura de dados dentro da organização.

4.Política de Proteção de Dados e Privacidade: a partir de uma adequada *Data Assessments*[32], criar, implantar e difundir mandamentos que traduzam os principais aspectos regulatórios do tema proteção de dados e privacidade, customizando as condutas em conformidade com as leis à realidade da empresa, ao seu porte e ao mercado no qual está inserida.

5.Políticas de Terceiros e *Due Dilligence*: ao lado da implantação da política descrita no item imediatamente superior, a revisão do relacionamento comercial com terceiros e a verificação de conformidade documental são alguns dos pontos principais e que requerem maior atenção das organizações. Em razão disso, trataremos em seção específica novamente esses assuntos.

6.Canal de Denúncias: deverá propiciar que qualquer colaborador ou interessado possa, identificando um ilícito ou irregularidade, denunciar o suposto infrator sem o receio de ser identificado ou exposto de modo constrangedor, preservando a

[32] A importância e a geração de valor de *Data Assessments* podem ser verificadas na medida de sua contribuição para equilibrar o apetite ao risco e a estratégia da empresa, mitigando danos aos titulares de dados e à reputação da organização em caso de incidentes, identificando os principais riscos associados ao tratamento de dados pessoais, racionalizando os investimentos financeiros realizados para este fim.

identidade do denunciante. A forma pela qual a denúncia será realizada pode ser variada: por e-mail, software, via telefone, canal externo, etc. Esses canais de denúncias não devem ser excludentes, mas complementares. Ainda, é importante que se crie uma forma de premiação ou incentivo a essas denúncias, estimulando a participação dos funcionários de boa-fé, garantindo a higidez do ambiente de trabalho.

7.Políticas de Consequências: as medidas corretivas a serem aplicadas em caso de desvios de conduta, não conformidade ou ilícitos deverão levar em consideração a extensão do dano, os códigos internos, obedecendo a transparência e a publicidade na divulgação desses atos. Evidentemente, sem causar constrangimento ilegal ao colaborador punido. Além disso, é fundamental que seja um procedimento de apuração e decisão onde se garanta ao investigado o acesso aos autos, o contraditório e a ampla defesa, bem como que se observe o princípio da proporcionalidade nas sanções advindas dessa apuração.

8.Auditoria: a execução das medidas e boas práticas de governança constantes do programa deve ser objeto de monitoramento e auditoria (interna ou externa) periódicos. Isto, com vistas ao aprimoramento do mesmo, bem como com o propósito de comprovar a sua eficácia a partir de indicadores de performance previamente estabelecidos. Não se trata de um sistema estático, ao contrário, trata-se de mecanismo de gestão de *compliance* de dados *ongoing*.

Por derradeiro, cabe salientar que a instituição do referido programa de *compliance* pelas *Big Techs* não deve ser encarado como um processo penoso ou que crie embaraços ao desenvolvimento de suas atividades. Muito pelo contrário, a ausência de investimento de tempo e recursos para a elaboração desse importante componente da Governança Digital pode, no final do dia, causar intenso prejuízo financeiro à corporação (risco tangível), mas também danos irreparáveis à sua reputação a depender do caso concreto.

Dessa maneira, pode se concluir que no *trade off* realizado entre os custos e os benefícios agregados pela implantação desse tipo de medida, o segundo revela-se muito superior ao primeiro, colaborando – inclusive – para a obtenção de vantagem competitiva frente aos concorrentes se bem trabalhada essa política pela empresa controladora dos dados.

5. Considerações finais

Por tudo o que foi exposto ao longo deste breve artigo, nutre-se a expectativa de ter-se colaborado com a compreensão de que o tratamento de dados pessoais de forma ética, segura e transparente não é uma opção ofertada ao controlador de dados, trata-se de uma imposição inafastável.

Na sociedade de informação, em razão da multiplicidade e complexidade das relações entre indivíduos e agentes econômicos, não há como deter-se o controle do consentimento na integralidade do tempo em que se está exposto pela hiper conectividade. Dessa forma, pugna-se pela adoção de medidas complementares[33] ao desiderato da regulação, de modo que se enfoque no cumprimento das disposições *a priori*, evitando-se prejuízos aos titulares de dados e, consequentemente, o acionamento dos procedimentos sancionatórios.

Os danos podem (e devem) ser preventivamente mitigados a partir do estudo e da comprovada implementação dos princípios destacados ao longo do texto. Com efeito, tratam-se de disposições que possuem seu fundamento em conhecidos valores de governança, demandando o tratamento de dados pessoais pelas empresas com assento na transparência, na equidade, na prestação de contas e na responsabilidade corporativa. Por isto mesmo, vê-se um ganho tremendo às relações de mercado com a implantação dos referidos programas de *Compliance* Digital, o que será um promotor de credibilidade nos mais diversos segmentos econômicos.

Os regulamentos protetivos de dados pessoais e privacidade não se constituem barreiras para a economia. De forma oposta, traduzem-se em pontes que ligam a atuação ética dos agentes econômicos ao respeito à esfera de direitos dos cidadãos.

---

[33] Uma vez mais, busca-se auxílio nos ensinamentos do renomado doutrinador germânico: "São, portanto, necessários novos conceitos, acordos e instituições de governança transnacional, que devem ser orientados para a cooperação entre os atores públicos e os interessados envolvidos, como associações e empresas da economia digital, mas também das organizações não governamentais (ONGs) e outros representantes de interesses da sociedade civil." HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital: desafios para o direito. Rio de Janeiro: Forense, 2022, p.164.

Destarte, respeitando-se as opiniões em contrário, ressalta-se que não há como sustentar a falácia dicotômica que contrapõe o desenvolvimento econômico e o necessário resguardo dos direitos fundamentais, neste caso, à proteção de dados pessoais e à privacidade.

Por fim, reforça-se que cabe a cada entidade empresarial ou setor organizado encontrar a política de Governança Digital mais alinhada ao desenvolvimento de seus negócios, e em observância aos regulamentos existentes em cada ordenamento jurídico, isto é, na justa medida do respeito aos direitos fundamentais como aqui preconizados, não se admitindo qualquer conduta antiética ou retrocesso potencializador de danos à esfera de direitos dos indivíduos.

Referências bibliográficas

ARTESE. Gustavo. ***Compliance Digital e Privacidade*.** In: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINI, Otávio, **Manual de Compliance.** 2.ed. São Paulo: Editora Forense, 2020.

BENNET, Colin. ***Regulating Privacy, Data Protection and public policy in Europe and the United States*.** Ithaca: Cornell University Press, 1992.

BIONI, Bruno Ricardo. ***Proteção de Dados Pessoais: a função e os limites do consentimento*.** 3ª. ed. Rio de Janeiro: Forense, 2021.

CARVALHO, Vinicius Marques de. MATTIUZZO, Marcela. PONCE, Paula Pedigoni. ***Boas práticas e governança na LGPD*.** In: DONEDA, Danilo et al. **Tratado de Proteção de Dados Pessoais.** 2ª ed. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. ***Panorama histórico da proteção de dados pessoais*.** In: DONEDA, Danilo et al. **Tratado de Proteção de Dados Pessoais.** 2ª ed. Rio de Janeiro: Forense, 2021.

HOFFMANN-RIEM, Wolfgang. ***Teoria geral do direito digital: transformação digital: desafios para o direito.*** Rio de Janeiro: Forense, 2022.
IBGC – Instituto Brasileiro de Governança Corporativa. ***Código das melhores práticas de governança corporativa.*** 5ª edição. São Paulo: IBGC, 2015.

MENDES, Laura Schertel. ***Privacidade, proteção de dados e defesa do consumidor – Linhas gerais de um novo direito fundamental*.** São Paulo: Saraiva, 2014.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATON AND DEVELOPMENT. OECD. ***Corporate governance principles*.** Disponível em:

<https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf>. Acesso em 20/06/2022.

_____. OECD. ***Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*** OECD Publishing, 2002. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em 18/06/2022.

_____. OECD. ***Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*****.** OECD Publishing, 2002. Disponivel em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188#mainText.> Acesso em 18/06/2022.

PENTLAND, Alex. LIPTON, Alexander. HARDJONO, Thomas. ***Building the new economy – Data as Capital*****.** Cambridge: MIT Connection, Science & Engineering, 2021.

ROSSETI, José P. ANDRADE, Adriana. ***Governança Corporativa: fundamentos, desenvolvimento e tendências*****.** 7. ed. – São Paulo: Atlas, 2016.

RUARO, Regina. SALES SARLET, Gabrielle Bezerra. ***O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018*****.** In: DONEDA, Danilo et al. Tratado de Proteção de Dados Pessoais. 2ª ed. Rio de Janeiro: Forense, 2021.

SARLET, Ingo Wolfgang. ***A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*****.** 13. ed. Revisada, atualizada e ampliada. Porto Alegre: Livraria do Advogado, 2021.

_____. ***Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados*****.** In: DONEDA, Danilo et al. **Tratado de Proteção de Dados Pessoais.** 2ª ed. Rio de Janeiro: Forense, 2021.

SCHWAB, Klaus. ***The Fourth Industrial Revolution*****.** New York: Currency Books, 2017.

SCHWAB, Klaus; VANHAM, Peter. ***Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet.*** John Wiley & Sons: New Jersey, 2021.
BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. ***Relatório de Políticas e Programas de Governo.*** Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação (Sefti), 2018.

WEBSTER, Frank. ***Theories of the Information Society*****.** London: Routledge, 2014.

7. DEMOCRACIA FALSEADA: COMO O USO ARBITRÁRIO DOS DADOS DE ELEITORES PODE FISSURAR A SOBERANIA POPULAR – UM DEBATE BRASIL E ESPANHA

https://doi.org/10.36592/9786581110994-07

Gabrielle Bezerra Sales Sarlet[1]

Filipe Madsen Etges[2]

Sumário

1. Introdução

No ano de 2019, os espanhóis enfrentaram uma dura disputa judicial acerca de como os partidos políticos poderiam manipular dados relativos às suas opiniões políticas, especialmente quando externadas na rede mundial de computadores. O caso chegou à Corte Constitucional Espanhola[3] apresentado pelo *Defensor del Pueblo* (análogo ao Ministério Público Brasileiro) onde se contestava a constitucionalidade de artigo incluído no *régimen electoral general* da Espanha, legislação que encontraria correspondência no Código Eleitoral do Brasil.

O dispositivo legal contestado foi acrescido pela *Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales* e

[1] Gabrielle é advogada, consultora, graduada e mestre em Direito pela Universidade Federal do Ceará (UFC), doutora em Direito pela Universidade de Augsburg (UNIA), pós-doutora em Direito pela Universidade de Hamburgo e pela PUCRS e especialista em neurociências e ciências do comportamento pela PUCRS. É professora dos cursos de graduação, mestrado e doutorado (PPGD) da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). E-mail: gabriellebezerrasales@gmail.com lattes.cnpq.br/9638814642817946.

[2] Professor na Universidade de Santa Cruz do Sul – UNISC e Consultor Legislativo na Assembleia Legislativa do Rio Grande do Sul. Possui graduação em Ciências jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul - UFRGS. Especialização em Direito do Estado pela Universidade Federal do Rio Grande do Sul - UFRGS. Mestre em Constitucionalismo Contemporâneo pela Universidade de Santa Cruz do Sul – UNISC e Doutorando em Fundamentos Constitucionais do Direito Público e do Direito Privado na Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Correio Eletrônico: filipe.etges@al.rs.gov.br. lattes.cnpq.br /4382749890742599.

[3] ESPANHA. TRIBUNAL CONSTITUCIONAL. Sentencia 76/2019, de 22 de mayo, BOE núm. 151, de 25 de junho de 2019. Disponível em <https://www.boe.es/boe/dias/2019/06/25/pdfs/BOE-A-2019-9548.pdf>. Acesso em 10 de outubro de 2020.

trazia que a coleta e utilização dos dados relativos às opiniões políticas dos eleitores, em atividades eleitorais realizadas pelos partidos políticos, respeitaria o interesse público se estivesse amparada em garantias adequadas[4]. Ou seja, os partidos políticos poderiam, em suas atividades eleitorais, recolher e manipular dados encontrados na *internet* que revelassem a opinião política dos eleitores.

O *Defensor del Pueblo* entendeu pela violação de diversos dispositivos da constituição de Espanha, posto que a alteração legislativa não apresentou limites para utilização (tratamento) de dados reveladores da orientação e opinião política dos cidadãos. Não estabeleceu critérios para determinação destes limites, veículo normativo responsável pela regulamentação ou autoridade pública que impusesse tais restrições. Também não referiu direitos dos titulares dos dados ou condição de exercício. Assim, dados sensíveis, especialmente protegidos, poderiam ser manipulados sem consentimento ou ciência, dos titulares, de sua utilização ou da finalidade do uso. Tampouco foram definidas condições de oposição ou cancelamento. A situação criava um estado de insegurança jurídica ao não demonstrar garantias adequadas para proteção dos dados pessoais, afetando o direito de liberdade ideológica e de participação política, sob uma genérica referência ao cumprimento do interesse público.

O Advogado do Estado, por seu turno, referiu que a alteração legal se baseou no regramento europeu que permite o recolhimento deste tipo de dados por razões de interesse público, sempre que oferecidas as garantias necessárias. Estas garantias são encontradas de forma expressa na leitura sistemática do próprio *Reglamento (UE) 2016/679, de 27 de abril de 2016, de protección de datos*, na *Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, bem como na *Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos*. Refere ainda que a finalidade da nova legislação é o melhor funcionamento do sistema democrático.

A decisão da Corte Constitucional foi no sentido de que os partidos políticos só podem compilar, para suas atividades, dados que revelem a posição política dos

[4] *"Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales. 1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas."*

cidadãos quando são oferecidas garantias adequadas. E, no caso da alteração promovida ao Código Eleitoral, essas garantias não foram apresentadas pelo legislador. Foram apontadas violações ao art. 18.4 em conexão com o art. 53.1 da Constituição de Espanha, todas vinculadas à insuficiência da lei e resultando na violação do mandato de preservação do conteúdo essencial do direito fundamental de proteção de dados pessoais, na medida em que a falta de segurança jurídica cria um perigo para todos aqueles a quem possa ser aplicada a recolha dos dados. Também a indeterminação da finalidade do tratamento e a falta de garantias adequadas ou dos requisitos mínimos exigidos pela lei, constituem interferência no direito fundamental.

Para fundamentar juridicamente a decisão tomada, a Corte espanhola sustentou que a legislação traz como regra geral a proibição do tratamento de dados que revelem opiniões políticas, do mesmo modo que proíbe o tratamento em relação aos dados pessoais que indiquem origem étnica ou racial, convicções religiosas ou filosóficas, filiação sindical, dados genéticos ou biométricos que permitam identificar o indivíduo que os possui, dados relativos à saúde, à vida sexual ou à orientação sexual das pessoas.

No entanto, existem exceções. Uma delas é quando o tratamento for necessário por motivos de interesse público essencial. Mesmo nesse caso, a permissão deve respeitar dois requisitos: a) identificar claramente os fins de interesse público essencial e a apreciação da proporcionalidade do tratamento ao fim perseguido, buscando o máximo respeito ao direito à proteção dos dados; b) o estabelecimento de medidas adequadas e específicas para proteger os interesses e direitos fundamentais do interessado, devendo o Estado que visa se habilitar ou permitir o tratamento destes dados, apresentar tais garantias, como a necessidade de consentimento expresso do interessado e a normatização por instrumento com *status* de lei. Assim, o Regulamento Geral sobre o tema não proíbe a utilização de dados pessoais relativos às opiniões políticas em atividades eleitorais, mas condiciona ao estabelecimento de garantias adequadas.

Considerando que os direitos fundamentais não possuem caráter absoluto, eles podem ser restringidos pela lei, desde que a restrição corresponda a uma finalidade de interesse geral, os requisitos e o alcance desta estejam suficientemente

descritos na norma e respeitem o princípio da proporcionalidade. No caso, a reserva legal teria dupla função: a) ser necessária uma lei para habilitar a ingerência ao direito fundamental e b) que essa lei reúna todas as características indispensáveis para garantir a segurança jurídica, apresentando as condições e pressupostos da intervenção.

Ou seja, a lei afronta à Constituição caso não apresente certeza e previsibilidade quanto aos seus limites ou modo de aplicação. Se a própria lei não cumpre sua função de proteger o direito fundamental que restringe, deixa que, em seu lugar, opere a simples vontade de quem a aplica. Em se tratando de dados sensíveis, uma regulamentação generalista de suas garantias não é suficiente, devendo assegurar transparência, supervisão, tutela judicial efetiva, evitar que dados sejam recolhidos de maneira desproporcional ao fim vislumbrado e que não sejam utilizados para finalidades distintas das legalmente previstas.

No caso, verificou-se que a legislação que impunha restrição ao direito fundamental não esclareceu o interesse público almejado que justificaria o uso dos dados [5]. Não limitou o tratamento possível e nem apresentou as restrições necessárias. Também não previu garantias adequadas e nem as bases legais para ao uso destes dados. Segundo a doutrina espanhola, as garantias não podem ser dadas *a posteriori*, devendo estar incorporadas a própria regulação do tratamento dos dados, seja de forma direta ou por remissão expressa à normativa com *status* legal adequado.

Por fim, a Corte refutou o argumento de que uma leitura sistemática dos diversos dispositivos legais existentes traria uma limitação adequada ao uso dos dados. Para os magistrados são normativas extensas e que não trazem dispositivos específicos em relação à proteção de dados relativos à opinião política das pessoas. Tampouco houve remissão expressa a esse conjunto de normas e algumas não possuem nem mesmo *status* de lei.

[5] A justificativa do projeto de lei trazia a seguinte motivação: "*Adecuar el Reglamento a las especificidades nacionales y establecer salvaguardas para impedir casos como el que vincula a Cambridge Analytica con el uso ilícito de datos de 50 millones de usuarios de facebook para mercadotecnia electoral*." ("Boletín Oficial de las Cortes Generales. Congreso de los Diputados", serie A, núm. 13-2, de 18 de abril de 2018, pág. 209).

A decisão da corte Suprema da Espanha, desse modo, serve de guia para a análise de um problema comum na maior parte das democracias do planeta: evitar que o recolhimento e tratamento de dados (especialmente as sensíveis) seja utilizado para violar a lisura do processo eleitoral e colocar em xeque a própria existência da democracia. Com efeito, a experiência política "customizada" em razão da coleta e do tratamento excessivo, desproporcional e abusivo de dados pessoais oportuniza grandes danos ao Estado democrático de direito, sobretudo em razão da manipulação da vontade e das campanhas de desinformação.

Para instrumentalizar o raciocínio, serão analisadas as possíveis influências deletérias, associadas à tecnologia, que podem influir na decisão do eleitor, sua inevitabilidade e a necessidade regulatória. Em segundo momento, se enfrentará a questão de como combater a manipulação dos dados pessoais dos eleitores e de maneira a Lei Geral de Proteção de Dados brasileira, em leitura sistemática com a legislação eleitoral, dá conta de apresentar garantias adequadas aos direitos fundamentais envolvidos. Trata-se de uma pesquisa bibliográfica e de caráter exploratório que se empreendeu por meio do emprego do método hipotético-dedutivo.

2. A regulação do inevitável: dados pessoais sensíveis serão utilizados nas eleições.

A era da informação propôs à humanidade que um amplo acesso informacional seria libertador. Períodos históricos anteriores apontaram *déficits* informacionais como entraves ao desenvolvimento humano e das democracias. Entretanto, o acesso ao conhecimento e à educação parecem não se confundir, criando terreno fértil para chistes e falsetes tecnológicos, inclusive visando influenciar resultados eleitorais. Não que a prática seja novidade no Brasil, pois desde panfletos jogados às beiras das urnas eleitorais ao direcionamento de conteúdo de acordo com o perfil político do destinatário, somos pródigos em aplicar a regra de que "os fins justificam os meios" na busca do poder político. Ocorre que agora a escala é outra! Mas para quem pretende refutar esta mazela como própria da cultura nacional, engana-se. Trata-se de fenômeno plurinacional e que permite,

inclusive, a influência de um Estado, organização ou pessoa sobre as eleições de outro Estado.

A alteração legislativa analisada pelo Tribunal Constitucional Espanhol decorre, como em muitos outros países, de uma reação ao escândalo de manipulação de dados com fins eleitorais verificado no plebiscito relacionado à separação do Reino Unido da União Europeia, o *Brexit*, e também nas eleições presidenciais americanas de 2016.

Pybus[6] sustenta que a ação da empresa *Cambridge Analytica*, apoiadora do candidato vencedor nas eleições presidenciais norte americanas de 2016, influenciou o resultado por meio da tecnologia desenvolvida pela empresa, que localizava eleitores indecisos e suscetíveis à influência de opinião, formatando as mensagens a partir do resultado da análise do perfil psicológico do receptor. Essa contaminação/deturpação da democracia, na qual há a intrusão de governos e corporações (e dos partidos políticos) na liberdade e privacidade de terceiros é identificada por Molinaro e Sarlet[7] como um fruto do fenômeno de novo modelo estatal, chamado de Estado de Vigilância. Em rigor, o incremento do emprego de tecnologias baseadas em dados acarretou uma superexposição, além da hiperaceleração da vida, de modo geral, em um contexto de confissão e de perda da privacidade.

Neste sentido, práticas como cyberattacks, *fake News* e utilização de inteligência artificial para entregar, massivamente, propaganda eleitoral específica de acordo com o comportamento do usuário têm sido reportadas desde as eleições de 2016, intervindo nocivamente nos processos eleitorais[8]. Outras práticas depreciativas são utilizadas no processo eleitoral, conforme aponta Wang[9], como a

---

[6] PYBUS, Jennifer. Trump, the first Facebook president: why politicians need our data too. *In*: Trump's Media War. Ed. Happer, Catherine, Hoskins, Andrew e Merrin, William. London: Palgrave Macmillan, pp. 8-13, 2019, p. 8-13.

[7] MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Sociedade em rede, internet e estado de Vigilância: algumas aproximações. *Revista da AJURIS* – v. 40 – n. 132 – Dezembro, 2013, p. 65.

[8] MANHEIM, Karl; KAPLAN, Lyric. Artificial Intelligence: risks to privacy and democracy. Forthcoming. *Yale Journal of Law and Technology*, 2019. Disponível em: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3273016_code332621.pdf?abstractid=3273016&mirid=1&type=2>. Acesso em 08 de dezembro de 2020, p. 22.

[9] WANG, Celeste Tien-hsin – Is intellectual property "disrupted" by the algorithm that feeds you informations in an era of fake news? *La Revue des Juristes de Sciences Po-Printemps*. nº. 15, pp. 230-251, 2018. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3222669>. Acesso em 10/12/2020, p. 248.

atuação de robôs e de perfis falsos para influenciar a opinião e o comportamento do usuário mediante o compartilhamento e suporte numérico a notícias falsas ou desinformativas, visando criar uma errônea percepção virtual de consenso popular.

É assim, portanto, que o direcionamento de mensagens com viés ideológico, qualquer que seja sua forma, permite a manipulação da opinião pessoal do eleitor por meio da construção de um acervo informativo desvirtuado da realidade, especialmente se for associado à ação de programas de reprodução automática, criando, por sua vez, uma falsa impressão de apoio massivo a uma ideia[10].

Esse fenômeno conhecido como *Eco Chambers*[11] é o grande responsável pelo maniqueísmo das posições políticas da população, da concretização da ilusória certeza de que a razão está ao seu lado como a sua "bolha" de opiniões concordantes assim comprova. Neste contexto não há espaço para a dialética, culminando em escolhas eleitorais cada vez mais próximas ao extremismo. Só quem perde nesse jogo é o cidadão, sobretudo pela formação de guetos, de bolhas e de ilhas que fragmentam e enfraquecem o poder social e o exercício pleno da cidadania.

Além do exposto, Chester e Montgomery[12] acrescentam a ocorrência de: a) dossiês digitais, com identificação de perfis individuais de eleitores, com o uso de *data mining;* b) divisão geográfica, com a localização dos eleitores a partir do monitoramento da comunicação de equipamentos móveis em redes de *wi-fi, bluetooth* e posicionamento por GPS (*global position system*); c) monitorização individualizada em razão de *identity graph*, na identificação do uso de recursos variados por um mesmo indivíduo; d) automatização do processo de identificação do eleitor e envio de mensagens individualizadas; e) personalização da propaganda por meio da TV a cabo, a partir de dados individualizados da audiência; e) direcionamento emocional de mensagens, com o uso de psicologia comportamental

[10] IENNACO, Luiz Antonio de Paula; COSTA, Eva Dias. Interferência do uso de dados eletrónicos em processos eleitorais. Revista Jurídica Portucalense, n.º 27, Porto: Universidade Portucalense, 2020, p. 3.

[11] PETERSON, Erik; GOEL Sharad; IVENGAR, Shanto. *Eco Chambers and Partisan Polarization: evidence from de 2016 presidentian campaign*, 2017. Diponível em: < https://pcl.stanford.edu/research/2017/peterson-echo-chambers.pdf> Acesso em 01 de dezembro de 2020.

[12] CHESTER, Jeff e MONTGOMERY, Kathryn C. *The Influence Industry*. Disponível em: <https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-usa.pdf>. Acesso em 10 de dezembro de 2020, 2018, p. 7-9.

e das neurociências para influenciar o eleitor. Enfim, deve-se relembrar que o processo que caracteriza a chamada internet 3.0 já perfaz um movimento que se volta para a individualização ou granulagem.

A medida legislativa aplicada na Espanha tentou regulamentar o inevitável uso dos dados pelos partidos políticos a partir da experiência pós *Cambridge Analytica*, cuja prática viu-se alastrar nas eleições subsequentes. Entretanto, a iniciativa deu-se de modo açodado, sem maiores cautelas quanto às garantias dos direitos fundamentais relacionados. Apesar da boa intenção, uma regulação insuficiente poderia gerar mais efeitos adversos do que sua ausência, pois criaria uma falsa impressão de permissividade.

Na mesma linha veio a crítica da doutrina espanhola ao comentar a sentença da Corte Suprema, de que a lei fora deficiente na hora de definir as exigências para o uso dos dados, lhe faltando densidade normativa, posto que não estabeleceu o interesse público que a inspirou e tampouco as garantias e limites do tratamento. Primordial lembrar que os políticos criadores da referida lei também são seus destinatários. Casos como esse, em que há conflito de interesse, exigem do Estado um reforço nas cautelas apresentadas[13].

Portanto, desde o pioneirismo "maquiavélico" operado pela empresa *Cambridge Analytica*, muitas outras eleições ao redor do mundo replicaram a experiência "exitosa" do uso das tecnologias para influenciar de forma deletéria as preferências eleitorais do cidadão. Nada indica que a prática vai simplesmente esmaecer por uma epifania republicana dos atores envolvidos na disputa do poder. Ao contrário, vai prevalecer o "fogo contra fogo" entre os partidos políticos, ampliando seu uso, e o surgimento de técnicas ainda mais sofisticadas de manipulação. Ocorre que essa democracia falseada, até aqui descrita, carece de um insumo essencial: os dados dos eleitores.

Mas, como enfrentar a questão? Abandonamos a tradição democrática representativa e partimos para um sorteio aleatório de nossos representantes como

[13] MATEO, Fabio Antonio Pascua. Un nuevo capítulo en la tutela del derecho a la protección de datos personales: los datos de contenido político. Comentario a la sentencia del Tribunal C1onstitucional 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019. *Revista de las Cortes Generales, nº 106,* primer semestre (2019): pp. 549-558, p. 558.

na ficção de Chesterton[14]? Por óbvio que não! Interessa apontar a democracia constitucional como um grande regime que amadureceu e se fundiu com as lutas do século XX[15].

3. O enfrentamento brasileiro da questão do uso de dados sensíveis de eleitores

Nos mesmos moldes da Espanha, o Brasil protege constitucionalmente os direitos fundamentais, cujo pluralismo conceitual permite abarcar a proteção de dados pessoais no seu bojo. E para dar conteúdo e proteção a este direito, para além da Emenda Constitucional n.º 115, igualmente editou uma Lei Geral de Proteção de Dados (doravante LGPD), muito concatenada com as principais normativas estrangeiras, em especial a da União Europeia.

Analisando o nosso ordenamento jurídico, seria possível questionar a legalidade de um partido político remeter uma propaganda eleitoral específica para pessoas negras, ou então para a comunidade LGBTQ+, identificados pelos seus perfis nas redes sociais ou por "curtidas" a determinados conteúdos? Ou até mesmo a remessa de publicidade para os seus próprios filiados? Em todos os casos, há uma identificação do indivíduo em razão de coleta e tratamento de dados sensíveis, constitucionalmente protegidos em face de um direito fundamental explicitado pela EC 155. Todos os exemplos, de qualquer sorte, remeteram à coleta e tratamento de dados inerentes à esfera mais intima da pessoa, ou seja, a raça, a orientação sexual ou a ideologia política. Em paralelo à solução de total inconstitucionalidade do tratamento deste tipo de dados sem a efetiva garantia, pronunciado pelo Tribunal

[14] Na ficção do autor inglês, escrita em 1904, os governantes de uma Londres do futuro são sorteados aleatoriamente entre os cidadãos ao invés de serem escolhidos pelo processo eletivo tradicional. G. K. Chesterton. *O Napoleão de Notting Hill*, 212 p., 2016.

[15] "*Estado democrático de Direito*, como referido no artigo 1º da Constituição brasileira, é um regime político fundado na soberania popular, com eleições livres e governo da maioria, bem como em poder limitado, Estado de direito e respeito aos direitos fundamentais de todos, aí incluído o mínimo existencial. Sem terem as suas necessidades vitais satisfeitas, as pessoas não têm condições de ser verdadeiramente livres e iguais. Há também um elemento emocional, humanístico, na democracia, que é o sentimento de pertencimento, de participação efetiva em um projeto coletivo de autogoverno, em que todos e cada um merecem igual consideração e respeito. " In: <https://www.conjur.com.br/2022-ago-03/roberto-barroso-populismo-autoritarismo-resistencia>. Acesso em: 08.08.2022.

Constitucional Espanhol, vamos verificar como o Brasil enfrenta (ou tenta enfrentar) a questão do uso de dados sensíveis.

Partiremos supondo que uma legislação com o mesmo conteúdo da espanhola fosse aprovada no país, autorizando os partidos políticos a recolher, na rede mundial de computadores, e tratar dados relativos às preferências políticas do eleitorado. Nesse caso, a simples remessa à LGPD, lida em sintonia com a legislação eleitoral, traria garantias adequadas à proteção dos dados dos eleitores? Em principio, deve-se atentar que, mesmo se tratando de dados tornados públicos pelo titular, não se pode falar em espécie de renuncia tácita à proteção constitucional.

Apesar de não o fazer expressamente, a legislação eleitoral remete à Lei Geral de Proteção de Dados Pessoais (LGPD) o tema do tratamento de dados pessoais, inclusive nos meios digitais. A questão da proteção de dados que revelem a ideologia política dos eleitores não foi objeto de preocupação específica das normas eleitorais. A Lei n.º 9.504/97, que estabelece as normas para as eleições no Brasil, recebeu alteração no ano de 2017 para regular a propaganda eleitoral na internet. Entre outros temas, seu art. 57-E vedou, a um rol de entidades pertencentes ou ligadas à Administração Pública, a utilização, a doação ou a cessão de cadastro eletrônico de seus clientes, em favor de candidatos, de partidos ou de coligações.

Aos particulares, importa lembrar, a disponibilização é livre, desde que gratuita e de origem nacional. No entanto, não foi adiante para determinar restrições ao uso dos dados obtidos. Ao contrário, liberou o uso de cadastros particulares privados. Restou à Lei Geral de Proteção de Dados (LGPD)[16] cuidar do tema, especialmente em se tratando dos dados sensíveis, como os reveladores de perfil eleitoral dos cidadãos.

A LGPD coloca entre os dados considerados sensíveis[17], v.g., a opinião política das pessoas e também acerca de sua filiação à organização partidária. Portanto, temos que a coleta, o tratamento e o emprego destes dados recebe proteção

[16] BRASIL, Lei Federal n. 13.709, de 14 de agosto, Lei Gral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 02.08.2022

[17] Art. 5º, (...) II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

especial, tendo a sua utilização restrita às hipóteses em que, em regra, o titular ou seu responsável legal consentir, de forma inequívoca e destacada, para finalidades especificadas. Sem esse consentimento o manejo dos dados também é possível, mas nas hipóteses elencadas exaustivamente no inciso II do art. 11 da LGPD[18].

De todo modo, nenhuma das hipóteses contempla o processamento dos dados para fins eleitorais, como no caso espanhol. Finkelstein[19] destaca a rigidez das normativas brasileiras e europeias em relação ao consentimento, pois exigem que seja expresso e possa ser comprovado, ao passo que em outros países, como os Estados Unidos, é comum que o cidadão apenas receba uma notificação a respeito da renovação da política de tratamento de dados, necessitando sinalizar seu desejo de que não sejam tratados.

Nessa altura interessa lembrar a estrutura básica do consentimento remete à anuência e à especificidade, afastando-se todas as possibilidades genéricas e sem a devida atenção, e.g., à finalidade, ao tempo, à quantidade dos dados e à qualidade do tratamento empregado.

Cabe atenção à "válvula de escape" estabelecida pelo §1º do próprio art. 11 da lei de proteção de dados brasileira, pois enseja a possibilidade de que legislação específica crie mais permissivos à utilização de dados sensíveis. Ou seja, uma alteração na legislação eleitoral, nos moldes da inconstitucional proposta feita na

---

[18] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
(...)
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[19] FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados. *Revista de Direito Brasileira*, Florianópolis, SC, v. 23, n. 9, p. 284-301, Mai./Ago., 2019, p. 298.

Espanha, em tese e do ponto de vista infraconstitucional, poderia ser concebida, desde que as proteções dispostas na LGPD recebessem indicação expressa. Isto porque, no papel, a LGPD parece apresentar garantias adequadas. Mas quais garantias são estas?

Inicialmente, vamos recapitular os principais quesitos que a Corte Constitucional da Espanha apontou como necessários para uma adequada permissão da utilização de dados sensíveis do eleitorado, pelos partidos políticos. Partindo-se de uma regra geral de proibição total de uso de dados sensíveis, a inclusão de uma lei (reserva legal) permitindo o tratamento não poderia ser generalista.

Portanto, deveria assegurar transparência, supervisão, tutela judicial efetiva, evitar que dados sejam recolhidos de maneira desvirtuada e desproporcional ao fim vislumbrado e que os dados não sejam utilizados para iniciativas distintas das legalmente previstas. Além disso, deveria conter os direitos dos titulares, a obrigatoriedade do consentimento do titular e a ciência da finalidade do tratamento. Em se tratando de permitir o uso no processo eleitoral, a lei deveria, ainda, identificar claramente os fins de interesse público essencial e a apreciação da proporcionalidade do tratamento ao fim perseguido, buscando o máximo respeito ao direito à proteção dos dados.

Com foco nos quesitos da Corte espanhola, caso uma legislação fosse criada para permitir o uso de dados dos eleitores em campanhas eleitorais, a LGPD ofereceria este nível de proteção? Nossa legislação traz como requisito para o tratamento dos dados a obrigatoriedade de consentimento expresso, com identificação da finalidade específica, sendo nulas autorizações genéricas. Estabelece uso restrito, com exceções exaustivas quanto ao uso de dados sensíveis. Considera dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Além disso, garante, em certa medida, a despeito do posicionamento do Supremo Tribunal Federal quanto à terminologia, uma espécie de direito ao esquecimento por meio da eliminação/desindexação dos dados após o tratamento e a possibilidade de revogação de seu uso. Esta prerrogativa de ser esquecido digitalmente é fundamental em um contexto de hiperinformação, no qual convicções

ideológicas e partidárias se alteram, garantindo a possibilidade de moldar e reconstruir a própria imagem social em vista das mudanças que ocorrem com o indivíduo com o transcurso do tempo, permitindo ser diferente de si mesmo em relação ao passado[20].

Seguindo na análise do liame de proteção dos dados sensíveis indicado pela LGPD, ainda pode ser destacado um capítulo inteiro sobre os direitos do titular dos dados, o seu uso pelo Poder Público e até mesmo a regulação da transferência internacional de dados. Foram contempladas, ainda, formas de responsabilização e boas práticas. O fato é que, para além dos usos para fins discriminatórios que obviamente são vedados no ordenamento pátrio, deve-se enfatizar a sua relevância para a composição da subjetividade e da identidade, dentro e fora da sociedade informacional, e, notadamente, a sua inalterabilidade quando se tem em mente os de natureza biométrica.

Nesse contexto, no papel, existe um robusto arcabouço de medidas de proteção que poderiam receber indicação de aplicabilidade de uma lei que permitisse o uso de dados, pelos partidos políticos, para fins eleitorais. O que faltaria esclarecer, tanto no Brasil, quanto na Espanha, é o interesse público almejado com a permissão ao uso dos dados pelos partidos políticos. Para além disso, uma regulação seria salutar, considerando que os dados continuarão sendo utilizados para fins de manipulação da opinião dos eleitores.

Cabe à educação, regulação adequada e a utilização do filtro do princípio da precaução para estipular ao Estado-Administração o dever de, prospectivamente, avaliar o nexo causal e interrompê-lo antes que os danos irrompam[21]. Ou seja, quando a finalidade do uso dos dados sensíveis não puder identificar claramente seus potenciais danos, seu uso não deve ser permitido. Em face disso, visando o amadurecimento do sistema de proteção de dados no cenário nacional é perceptível a articulação de diversas instituições e da sociedade civil para a garantia do Estado democrático de direito, mormente por meio de eleições livres.

---

[20] SARLET, Ingo Wolfgang; NETO, Artur Ferreira. O Direito ao Esquecimento na Sociedade da Informação, Porto Alegre: Livraria do Advogado, 2018, p. 73-74.

[21] FREITAS, Juarez, *Sustentabilidade: Direito ao Futuro*. Belo Horizonte: Fórum, 4ª edição, 415 p., 2019, p. 226.

3.1. ANPD e aplicação da lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral

A Autoridade Nacional de Proteção de Dados (ANPD) e o Tribunal Superior Eleitoral (TSE) publicaram, em 03 de janeiro de 2022, o Guia Orientativo para a Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por Agentes de Tratamento no contexto eleitoral. O Guia traz recomendações práticas sobre a aplicação da LGPD e é voltado para os agentes de tratamento de informações que participarão do processo eleitoral. Há igualmente algumas recomendações e boas práticas a serem seguidas pelos candidatos, partidos políticos, coligações e federações partidárias, visando garantir a proteção de dados, a privacidade das pessoas e a lisura do processo eleitoral.

De fato, mediante acordo de colaboração técnica, a ANPD juntamente com o TSE, sobretudo com base na LGPD e em confluência com a legislação eleitoral, tem engendrado esforços para sensibilizar os partidos políticos, as lideranças partidárias, os candidatos e os eleitores para a efetividade das premissas regentes do sistema de proteção de dados pessoais no Brasil.

A Cartilha, fruto desse empreendimento, reforça a importância da intersecção entre o panorama eleitoral e as regras de proteção de dados pessoais, em razão do novo cenário globalizado e hiperconectado, e, consequentemente, das transformações da sociedade contemporânea e da cultura digital. Nesse sentido, intenta-se alinhar os partidos políticos, os candidatos, as plataformas digitais, as coligações e as organizações partidárias, de modo geral, para que realizem as campanhas eleitorais, assegurando os direitos fundamentais e, para tanto, vinculando-as ao dever de *accountability*, também denominado de Princípio da Responsabilização e Prestação de Contas.

Por oportuno, o escrutínio deve ser a regra geral, especialmente em razão da gravidade e das implicações de eleições gerais como as previstas para 2022, em que devem ser combatidos os usos abusivos de dados pessoais, particularmente em campanhas pautadas na desinformação, na intolerância e nos discursos de ódio. De fato, os partidos políticos desempenham um papel inarredável na democracia representativa e não podem, e nem devem, ser impedidos dessa função. Contudo, é

imprescindível que a atuação e a comunicação entre os candidatos e seu eleitorado decorram de um modelo jurídico pautado na transparência, na confiabilidade e, particularmente, na autodeterminação informacional.

Ab initio, o guia reintroduz a relevância da proteção de dados pessoais no contexto eleitoral brasileiro e diferencia os dados sensíveis na medida em que os projeta como aqueles que exigem maior cautela quanto à coleta e ao tratamento. Alerta ainda que a LGPD os atribuiu um valor adicional no sentido protetivo na medida em que presumiu que a utilização indevida dessas informações forjadas a partir de tratamento de dados sensíveis tem o potencial de gerar restrições significativas ao exercício de direitos fundamentais, como atos de discriminação racial, étnica ou em razão de orientação sexual, considerando a pessoa titular de dados em posição mais vulnerável em relação a agentes de tratamento[22].

Ainda aduz que os dados tornados públicos pelo titulares, à guisa de exemplo, não deixam de merecer a tutela consoante com a LGPD e, daí, dispõe que todo e qualquer tratamento de dados pessoais deve atentar para os princípios da legislação, notadamente, a finalidade, a qualidade dos dados, a necessidade, a adequação e a transparência em todas as fases. Em outras palavras, o circuito que vai desde a coleta até o descarte deve ser alinhado aos dispositivos constitucionais e legais em vigor no país.

Destaque-se a posição dos agentes de tratamento nessa configuração eleitoral, em especial a do controlador que deve atender às especificações da LGPD e, deste modo, devendo ser publicamente apontado por partidos políticos e pelas coligações, responsabilizando-se inclusive pela contratação de terceiros, bem como de equipamentos e de softwares para o tratamento de dados dos eleitores. Nessa altura, importa salientar a existência de controladoria conjunta quando uma mesma operação de tratamento de dados pessoais envolva mais de um controlador com poder de decisão sobre elementos essenciais de tratamento.

De sorte que configura como controladoria conjunta quando: mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais; há interesse mútuo de dois ou mais controladores, com base em finalidades próprias,

[22] BRASIL, Tribunal Superior Eleitoral. Disponível em: <https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf>. Acesso em 09.08.2022.

sobre um mesmo tratamento; e dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e os elementos essenciais do tratamento. Na qualidade de controlador há o dever de apontar qual ou quais são as hipóteses legais para o tratamento de dados pessoais, advertindo-se que não há hierarquia entre as mesmas a despeito do que já se pensou acerca do consentimento.

No âmbito da LGPD, o consentimento não ocupa uma posição preponderante em relação às demais bases legais. Em relação a isso, evidencia-se o consentimento livre, informado, inequívoco e especifico como pressuposto para o disparo das mensagens instantâneas referentes às campanhas publicitárias em massa de acordo com o artigo 34 da Res.-TSE nº 23.610/2019. Para a perfectibilização do consentimento como manifestação genuína da vontade do titular dos dados há diversas implicações que vão desde a ação que demonstre o ato de consentir, passando pela exigência por uma informação clara e precisa no sentido quantitativo e qualitativo do volume e do tratamento a ser empreendido, mas, igualmente implica na possiblidade de retirar a anuência a qualquer tempo, bem como na clareza quanto à finalidade e à duração temporal do uso dos dados.

O guia faz referência incisiva à principiologia da LGPD, destacando o principio da finalidade de forma que devem ser considerados quatro requisitos: ser legítima, isto é, deve ser lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal que autorize o tratamento de dados pessoais; ser específica, isto é, a partir da finalidade, deve ser possível delimitar o escopo do tratamento e estabelecer quais as garantias necessárias para a proteção dos dados pessoais; ser explícita, isto é, deve ser expressa de maneira clara e precisa; e ser informada, isto é, deve ser disponibilizada em linguagem simples e de fácil acesso para a pessoa titular de dados[23]. E traça igualmente caminhos para se evitar os desvios de finalidade.

A orientação aponta para a necessidade dos atores do pleito eleitoral encetarem esforços para a implementação de Programa de Governança em Privacidade (PSG) de sorte que, em consonância com o artigo 50, paragrafo 2, inciso I da LGPD demonstrem a integridade e o comprometimento do agente de tratamento em adotar processos e políticas internas que assegurem o cumprimento, de forma

[23] BRASIL, Tribunal Superior Eleitoral. Disponível em: <https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf >. Acesso em 09.08.2022.

abrangente, de normas e boas práticas relativas à proteção de dados pessoais. Ou seja, atue em uma convergência com as regras de *compliance* digital.

A natureza do PSG se aproxima com a de um arrolamento na medida em que deve apontar, e.g., a quantidade e a qualidade dos dados a serem tratados, as bases legais, as respostas e as medidas de segurança para casos de vazamento de dados, a existência de decisões com base em tratamento automatizado, a ocorrência de compartilhamento de dados, especialmente quando se trate de transferência internacional de dados, o tempo de retenção e as formas de anonimização e de descarte de dados pessoais. Além disso, deve informar as formas e os canais para que os direitos dos titulares sejam plenamente exercidos e se há a utilização de *cookies* e de outros rastreadores.

Igualmente notável é necessidade de um acompanhamento em um processo sistemático de avaliação das medidas e das salvaguardas manejadas em função dos riscos e dos impactos de riscos à privacidade das pessoas. E, para tanto, emerge com bastante importância o emprego do instrumento conhecido como RIPD, ou seja, relatório de impacto à proteção de dados pessoais. De acordo com o art. 5º, XVII da LGPD, esse documento contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, proteções e mecanismos de mitigação de risco.

A ANPD recomenda ainda que seja realizado um gerenciamento de contratos de modo a observar todas as cadeias que podem comprometer a segurança e a confiança bem como a legalidade e a legitimidade do tratamento de dados pessoais, evitando situações de privilegio ou de abuso. Nessa linha recomenda um gerenciamento continuo das vulnerabilidades, físicas ou maquínicas que podem comprometer o emprego de dados pessoais nas campanhas politicas.

4. Considerações finais

A atividade político-partidária é inerente ao processo de alternância e de sucessão no poder e, dessa maneira, torna-se o pivô central da manutenção do regime democrático e para o exercício democrático. Em face da alteração do giro cultural erigido a partir da imersão em um mundo forjado pelas tecnologias de

informação e de comunicação – TICs, evidenciam-se trocas simbólicas inusitadas, modos de existência e de coexistência vanguardistas e, por outro lado, emergem as externalidades negativas que tem o condão de impactar negativamente o cenário mundial hiperconectado. Dentre os impactos mais significativos pode-se elencar os riscos de manipulação da vontade popular por meio da distorção e da usurpação dos pleitos eleitorais. Tal risco parece iminente na medida em que se projetam e reverberam ainda os efeitos de escândalos como o da *Cambridge Analytica*[24] e as eleições presidenciais norte americanas.

Ao revisar as considerações feitas ao longo do texto, em especial a partir da referência ao modelo espanhol, se pode apontar a suficiência, em tese, da legislação existente no Brasil como fator de contenção dos eventuais abusos no uso de dados pessoais, sobretudo dados pessoais sensíveis que revelam, dentre outros aspectos, a opinião política dos eleitores por parte dos partidos políticos. Na prática, a teoria ainda carece de comprovação em face do pouco tempo de vigência da Lei Geral de Proteção de Dados. Também falta o enfrentamento de um pleito majoritário, de âmbito nacional, que teste este plexo de proteção normativa. Há necessariamente de se louvar a iniciativa do TSE nessa parceria estabelecida com a ANPD por meio da qual veio à tona o guia orientativo, o qual se mencionou no final desse manuscrito.

Uma regulação específica que permitisse ainda mais transparência, segurança jurídica e sindicabilidade seria bem-vinda, uma vez que pressuposta a inevitável utilização dos dados por parte dos partidos políticos no intento de falsear a democracia em prol da ascensão ou manutenção do poder político. Sem dúvida alguma o Brasil, bem como a sua população, possui uma estrutura constitucional e legal que possibilita a contenção e, quiçá, a superação de agravos na próxima eleição geral. Oxalá, o pleno emprego dos dispositivos legais seja uma forma de expansão da conscientização do titular dos dados e dos agentes de tratamento, bem como da solidificação do sistema de proteção de dados e da cidadania no ambiente nacional.

[24] Trata-se de caso, que foi revelado em 2018, envolvendo o uso de dados de 87 milhões de usuários, segundo a rede social informou à época. A Cambridge Analytica usou essas informações a serviço da campanha de Donald Trump na eleição presidencial dos Estados Unidos em 2016.

Referências bibliográficas

CHESTER, Jeff e MONTGOMERY, Kathryn C. ***The Influence Industry***. Disponível em: <https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-usa.pdf>. Acesso em 10 de dezembro de 2020, 2018.

ESPANHA. TRIBUNAL CONSTITUCIONAL. Sentencia 76/2019, de 22 de mayo, BOE núm. 151, de 25 de junho de 2019. Disponível em: <https://www.boe.es/boe/dias/2019/06/25/pdfs/BOE-A-2019-9548.pdf>. Acesso em 10 de outubro de 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. **Privacidade e Lei Geral de Proteção de Dados.** *Revista de Direito Brasileira*, Florianópolis, SC, v. 23, n. 9, p. 284-301, Mai./Ago. 2019.

FREITAS, Juarez, **Sustentabilidade: Direito ao Futuro**. Belo Horizonte: Fórum, 4ª edição, 2019, 415 p.

IENNACO, Luiz Antonio de Paula; COSTA, Eva Dias. Interferência do uso de dados eletrónicos em processos eleitorais. Revista Jurídica Portucalense, n.º 27, Porto: Universidade Portucalense, 2020.

MANHEIM, Karl; KAPLAN, Lyric. **Artificial Intelligence: risks to privacy and democracy. Forthcoming**. *Yale Journal of Law and Technology*, 2019. Disponível em <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3273016_code332621.pdf?abstractid=3273016&mirid=1&type=2>. Acesso em 08 de dezembro de 2020.

MATEO, Fabio Antonio Pascua. **Un nuevo capítulo en la tutela del derecho a la protección de datos personales: los datos de contenido político. Comentario a la sentencia del Tribunal C1onstitucional** 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019. *Revista de las Cortes Generales, nº 106,* primer semestre (2019): pp. 549-558.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. **Sociedade em rede, internet e estado de Vigilância: algumas aproximações**. *Revista da AJURIS* – v. 40 – n. 132 – Dezembro, 2013.

PETERSON, Erik; GOEL Sharad; IVENGAR, Shanto. ***Eco Chambers and Partisan Polarization: evidence from de 2016 presidentian campaign***, 2017. Diponível em < https://pcl.stanford.edu/research/2017/peterson-echo-chambers.pdf>. Acesso em 01 de dezembro de 2020.

PYBUS, Jennifer. **Trump, the first Facebook president: why politicians need our data too.** *In*: Trump's Media War. Ed. Happer, Catherine, Hoskins, Andrew e Merrin, William. London: Palgrave Macmillan, pp. 8-13, 2019.

SARLET, Ingo Wolfgang; NETO, Artur Ferreira. **O Direito ao Esquecimento na Sociedade da Informação**, Porto Alegre: Livraria do Advogado, 2018.

WANG, Celeste Tien-hsin – **Is intellectual property "disrupted" by the algorithm that feeds you informations in an era of fake news?** *La Revue des Juristes de Sciences Po-Printemps*. nº. 15, pp. 230-251, 2018. Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3222669>. Acesso em 10/12/2020.

8. IMBRICAÇÕES ENTRE DIREITO E TECNOLOGIA: CPF NAS FARMÁCIAS E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

https://doi.org/10.36592/9786581110994-08

Helen Lentz Ribeiro Bernasiuk[1]

Sumário

1. Introdução

A crescente possibilidade de armazenamento de dados e informações, proporcionada pelos avanços tecnológicos, marca as primeiras décadas do século XXI como sociedade da informação ou, ainda, como sociedade digital. Os recursos tecnológicos atuais permitem a formação de colossais bancos de dados, conjuntos estruturados de dados pessoais, que podem ser intercruzados. Nessa esteira, entram também os dados pessoais de saúde, que são amplamente utilizados pela indústria farmacêutica para fins de marketing de medicamentos.

Diante disso, ressalta-se a existência de coleta, manutenção e armazenamento de dados pessoais de saúde para fins de envio de mensagens por farmácias e drogarias, com vistas à nova compra de medicamentos por clientes, sob a alegação de descontos que interessam a pacientes. Todavia, é necessário questionar: as práticas de coleta, armazenamento e uso de dados pessoais de saúde

[1] Doutoranda em Direito pela PUCRS. Mestre em Direito pela PUCRS. Especialista em Direito Civil pela UFRGS. Especialista em Direito Público pela Uniderp. Diritto Costituzionale Comparato e Cultura Giuridica Europea pela Sapienza, Università di Roma. Bolsista Capes/Proex PPGD/PUCRS. Advogada. E-mail: helenbernasiuk@gmail.com. Lattes: http://lattes.cnpq.br/4798723812833494.

para envios de mensagens a clientes de farmácias, drogarias e programas de descontos de laboratórios respeita os princípios da Lei Geral de Proteção de Dados – LGPD?

Cumpre assinalar que, exceto nos casos de coleta de dados pessoais de saúde para fins de controle sanitário, devidamente previstos em Lei, estabelecimentos que comercializam fármacos coletam e armazenam informações de seus clientes. Estes, muitas vezes, fornecem número de telefone e CPF para obtenção de descontos nas medicações que utilizam, seja de forma pontual, seja de maneira contínua. Contudo, a manipulação de tais informações se dá em descompasso com práticas determinadas pela LGPD, uma vez que a relação de medicamentos usados por uma pessoa, atrelada ao seu número de telefone e CPF, pode ser considerada dados pessoais de saúde e, consequentemente, sensíveis, permitindo que o cliente seja identificado ou identificável, o que fere uma série de direitos constitucionais da pessoa humana.

Nesse panorama, investiga-se a legalidade de ações de marketing realizadas por uma rede de farmácias brasileira no que tange ao envio de mensagens a celulares de clientes com a finalidade de ofertar descontos em medicamentos, ou seja, de interesse desses clientes.

Assim, o objetivo é analisar de que modo dados pessoais fornecidos por clientes de farmácias configuram-se em dados pessoais de saúde, ou dados pessoais sensíveis. Ainda, na qualidade de objetivos específicos, busca-se compreender de que forma dados pessoais de saúde são protegidos pela legislação brasileira e, consequentemente, os limites impostos a comerciantes de medicamentos no que tange à coleta, armazenamento e utilização desses dados.

Trata-se de uma investigação que se faz necessária diante da possibilidade de, na era digital, na qual vazamento desses dados sensíveis de saúde não são casos raros, o indivíduo sofrer discriminações em diversas searas, afetando a dignidade da pessoa humana e a própria proteção de dados inserida no texto constitucional. No recorte deste artigo, é importante assinalar que o faturamento do varejo farmacêutico foi de R$ 152,1 bilhões em 2021[2], o que indica que se está diante de um

[2] MERCADO E CONSUMO. Varejo farmacêutico termina 2021 com crescimento de 10,8%. Mercado & Consumo, São Paulo, 2022. Disponível em:

mercado que, para além das questões de saúde individual e coletiva, movimenta fatias significativas da economia brasileira. Nesse sentido, retoma-se que que um dos fundamentos da LGPD é o desenvolvimento econômico, bem como a livre iniciativa e livre concorrência[3]. Ou seja, o objetivo não é o de inviabilizar o comércio, tampouco a indústria, mas sim fornecer segurança jurídica em consonância com o respeito à privacidade e o direito dos indivíduos quanto aos seus dados pessoais.

De antemão, nota-se que um das problemáticas concernentes ao tema é que o cliente concede seu número do Cadastro de Pessoa Física – CPF para fins de desconto, mas sequer tem conhecimento sobre com quem os seus dados serão compartilhados ou como eles serão armazenados e utilizados. Em muitos casos, as pessoas também não têm conhecimento de que o fornecimento de tais informações, como o CPF atrelado ao uso de determinados medicamentos, pode se tornar um dado sensível, permitindo que terceiros vislumbrem o seu histórico médico a partir das medicações utilizadas ou adquiridas. Portanto, tem-se que as práticas de coleta, armazenamento, uso e compartilhamento de dados devem seguir os princípios da LGPD, fundamentada na observância do princípio da dignidade humana, basilar do Estado Democrático de Direito.

Nesta investigação, emprega-se o método exploratório, de cunho qualitativo. Parte-se de um caso concreto, no qual uma pessoa, após comprar um medicamento em uma rede de farmácias brasileira, passou a receber mensagens de SMS com lembretes e oferta de desconto para nova aquisição. Tal situação, real e que chegou ao conhecimento da pesquisadora, é tomada como objeto de investigação, e enseja as reflexões aqui tecidas, à luz dos preceitos da LGPD, Constituição Federal e teoria do paradoxo da privacidade. Discute-se o caso com um olhar para o arcabouço legislativo brasileiro, bem como para decisões já tomadas por membros do judiciário do País. Assim, são empregados os procedimentos bibliográfico e jurisprudencial e a interpretação se dá via método sociológico.

Na primeira subdivisão do desenvolvimento deste artigo, conceitua-se dados pessoais e a vulnerabilidade dos menos na era digital. Na sequência, aborda-se o

<https://mercadoeconsumo.com.br/09/02/2022/noticias/varejo-farmaceutico-termina-2021-com-crescimento-de-108/. Acesso em: 19 abr. 2022.

[3] Expressamente, o art. 2º da LGPD que trata acerca dos fundamentos da proteção de dados pessoais dispõe como fundamentos, em seus incisos, V e VI, os explicitados acima.

tema dos dados pessoais sensíveis em sua interface com os direitos fundamentais. Já a seção que se dedica à análise do caso concreto trata, além dos limites do marketing para a indústria farmacêutica, dos cenários obscuros que se antevê, para pessoas físicas e jurídicas, em situações de vazamentos de dados de clientes de farmácias, consoante determinações da LGPD.

2. Dados pessoais e a vulnerabilidade dos direitos fundamentais na era digital

A definição mais simples acerca de dados pessoais é dada pelo Tribunal Europeu de Direitos Humanos – TEDH, que os entende como todo tipo de informação que se relaciona a um indivíduo, seja ele identificado ou identificável[4]. Por seu turno, o Regulamento Europeu de Proteção de Dados acrescenta que eles se referem a uma pessoa singular, ou seja, titular dos dados pessoais, que poderia ser identificável de forma direta ou não. Nesse caso, o órgão se refere a um código identificador, tal como um nome, um número de identificação, dados de localização, identificadores eletrônicos. Ademais, trata-se, aqui, de um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular[5]. Vale observar que este também é o entendimento da Lei Geral de Proteção de Dados – LGPD, que conceitua, em seu art. 5º, inciso I, dado pessoal como informação relacionada a pessoa natural identificada ou identificável[6].

Os dados pessoais sensíveis são aqueles que podem gerar discriminação a um indivíduo caso outrem tenha acesso a eles. Nesse sentido, a LGPD, em seu art. 5º, inciso II, traz um rol de quais dados considera sensíveis, quando vinculados a uma pessoa natural: dados genéticos ou biométricos, de opinião política, de convicção religiosa, dados de saúde, dentre outros[7].

---

[4] RUARO, Regina Linden. Responsabilidade civil do Estado por dano moral em caso de má utilização de dados pessoais. Direitos Fundamentais &Justiça, Porto Alegre, v. 1, n. 1, p. 231-245, out. 2007. p. 245.

[5] UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF&from=EN>. Acesso em: 21 abr. 2022.

[6] BRASIL. Palácio do Planalto. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22 abr. 2022.

[7] Art. 5º, II, da LGPD - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou

Os dados de saúde entram no rol de dados sensíveis, pois, uma vez conhecidos por terceiros, os cidadãos tornam-se vulneráveis, passíveis de discriminações. À guisa de exemplo, em contratos de trabalho, caso o empregador tenha conhecimento das questões de saúde do candidato, poderá selecionar o indivíduo que considera livre de problemas de saúde física ou mental, com vistas à produtividade do seu quadro de colaboradores. Consequentemente, tal quadro tem o potencial de gerar grupos de excluídos do mercado de trabalho. Uma outra situação diz respeito aos contratos de seguro de saúde[8], já que as seguradoras poderiam segregar uma categoria de pessoas não elegíveis ou gerar um aumento excessivo da apólice.

Percebe-se que o meio ambiente digital agrava sobremaneira tais riscos, uma vez que não se pode descartar as hipóteses de falhas de sistema, vazamentos acidentais ou mesmo disseminação e venda ilegal de dados de saúde. Ressalta-se que a evolução tecnológica transformou as sociedades contemporâneas, que passaram a ser denominadas de sociedade da informação[9]. Trata-se de uma organização social que, alicerçada nos meios digitais informacionais, assiste à interdependência entre as tecnologias de coleta, armazenamento e compartilhamento de dados e as estruturas políticas e econômicas do coletivo[10].

O fenômeno da massiva e acelerada digitalização alcançou tamanha envergadura que, agora, fala-se em *Era Digital* ou mesmo *Sociedade Digital*. Trata-se de uma etapa além do que, há alguns anos, designava-se de Sociedade da Informação e/ou do Conhecimento. Em outras palavras, a despeito de discussões sobre nomenclaturas, o fato é que, nesta segunda década do século XXI, vivencia-se um momento inédito na história, o que envolve uma reconfiguração na forma como

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

[8] No que tange aos dados de saúde, cumpre assinalar que a LGPD, em seu artigo 11, §5º veda expressamente, às operadoras e planos privados de assistência à saúde, o tratamento de dados de saúde para a prática e seleção de riscos na contratação de qualquer modalidade, assim como na exclusão e contratação de beneficiários.

[9] CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. *In*:_____. CASTELLS, Manuel; CARDOSO, Gustavo (Org.). A sociedade em rede: do conhecimento à acção política. São Paulo: Paz e Terra, 2000. v. 1. p. 17-31.

[10] VIEIRA, Tatiana Malta. Proteção de dados pessoais na sociedade de informação. Revista de Direito de Informática e Telecomunicações: RDIT, Belo Horizonte, v. 2, n. 2, p. 213-235; jan./jun. 2007. p. 213.

as sociedades coletam, armazenam e utilizam dados pessoais de cidadãos[11].

O fácil acesso a esses dados, bem como a velocidade da transmissão e recursos para cruzamentos, potencializa chances de direitos fundamentais do indivíduo serem afetados, uma vez que novas tecnologias possibilitam maior conhecimento e controle de informações sobre a vida pessoal, privada e social de cidadãos[12]. Nesse sentido, a proteção de dados pessoais, bem como o seu reconhecimento de um direito fundamental correspondente, atinge um novo status e atualiza os sentidos de proteção da pessoa humana, bem como a liberdade e a dignidade inerentes a esse contexto[13].

O exposto até aqui sai do campo hipotético quando se olha para situações já ocorridas recentemente e que afetaram direitos fundamentais de indivíduos. Uma clínica de cirurgia plástica da Lituânia, em 2017, teve seu sistema invadido por criminosos que atuam nos meios digitais. Nesse caso, eles sequestraram dados pessoais de pacientes e exigiram resgate em bitcoin, moeda digital de difícil rastreio pelas autoridades. Como não houve pagamento, os invasores publicaram mais de 25 mil fotos, incluindo de pessoas nuas, e diversos dados pessoais, como número de seguridade social, passaporte, dentre outros dados sensíveis[14].

Situação semelhante ocorreu na Finlândia, desta vez com uma clínica de psiquiatria. Os pacientes do estabelecimento foram chantageados pelos criminosos que tiveram acesso a dados registrados em sessões de terapia. O governo finlandês chegou a intervir no caso, mas ao menos 300 registros foram vazados, inclusive de menores de idade. Outro agravante nesse episódio é que os terapeutas anotavam as sessões em um caderno e os pacientes não tinham conhecimento de que os registros seriam armazenados em um servidor, o que gerou preocupação entre frequentadores da clínica que, mesmo anos depois de suas consultas, precisaram

[11] Conforme bem assinalado pelo Professor Dr. Ingo Sarlet em prefácio da obra: BERNASIUK, Helen Lentz Ribeiro. Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos. Rio de Janeiro: Lumen Juris, 2021.

[12] MIRANDA, Jorge; MEDEIROS, Rui. Constituição Portuguesa Anotada. 1. ed. Coimbra: Coimbra Editora, 2006. p. 379-380.

[13] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. Direitos Fundamentais & Justiça, v. 13, n. 41, p. 183-212, jul./dez. 2019.

[14] HERN, Alex. Hackers publish private fotos from cosmetic surgery clinic. Guardian, 31 mai. 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments>. Acesso em: 17 abr. 2022.

reviver os sofrimentos causados pelas suas doenças mentais[15].

Evidentemente, tais questões dizem respeito aos cidadãos brasileiros e o País também tem histórico de vazamentos similares aos citados. Em 2018, devido a uma falha no aplicativo e-saúde, disponibilizado pelo Ministério da Saúde, informações médicas e de medicamentos utilizados por cidadãos brasileiros foram expostos[16]. Dois anos depois, em 2020, outra vulnerabilidade no aplicativo e-SUS expôs dados de cerca de 243 milhões de brasileiros na internet, incluindo o de pessoas falecidas. No caso, uma fragilidade no sistema deu visibilidade a CPF, nome completo, telefone e endereço de usuários do Sistema Único de Saúde e de planos privados[17]. Já durante a pandemia de Sars-Cov-2, foram expostos dados pessoais, inclusive de autoridades, que se submeteram a testes de Covid-19. Além de endereços, o vazamento apresentou números de documentos e informações sobre doenças preexistentes[18].

A fim de evidenciar o valor de mercado de dados pessoais, cita-se o caso Serasa, também no Brasil. Em 2020, a justiça brasileira determinou que a instituição cessasse a comercialização de dados pessoais. Neste caso, a empresa ofertava serviços das chamadas "Lista Online" e "Prospecção de Clientes", pelo valor de R$ 0,98 cada – existe um universo de 150.000.000,00 CPFs. No processo, a empresa ré sustentou que a ação foi proposta de forma precipitada, com base em informações superficiais buscadas no site institucional, sem qualquer aprofundamento acerca de suas atividades. Alegou também que os produtos já existiam há anos e que, até então, não foram questionados ou alvo de reclamações por parte dos consumidores. Ainda, sustentou que as práticas tampouco produzem danos, bem como estão

---

[15] KLEINMAN, Zoe. Therapy patients blackmailed for cash after clinic data breach. BBC News, 26 out. 2020. Disponível em: < https://www.bbc.com/news/technology-54692120>. Acesso em: 17 abr. 2022.
[16] CONGRESSO EM FOCO. Usuários acusam falhas em app do Ministério da Saúde há meses. Congresso em Foco, 11 dez. 2021. Disponível em: <https://congressoemfoco.uol.com.br/area/governo/conectesus-usuarios-acusam-falhas-em-app-do-ministerio-da-saude-ha-meses/>. Acesso em: 04 mai. 2022.
[17] PORTAL G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet. Portal G1, 02 dez. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em 04 maio 2022.
[18] PEIXOTO, Sinara. 16 milhões de pacientes de Covid-19 têm dados expostos; Saúde investiga. CNN Brasil, 26 nov. 2020. Disponível em: <https://www.cnnbrasil.com.br/saude/16-milhoes-de-pacientes-de-covid-19-tem-dados-expostos-saude-investiga/>. Acesso em: 22 abr. 2022.

alinhadas com as predisposições da LGPD. Outro argumento utilizado em sua defesa diz respeito à interpretação de que a própria lei prevê situações em que o consentimento específico do titular dos dados é dispensável. Assim, informou que a comercialização de dados é inerente às suas atividades e que não há divulgação de dados sensíveis dos titulares, abuso ou violação à intimidade e privacidade dos consumidores, uma vez que reúne informações públicas de natureza cadastral, fornecidas em situações cotidianas.

Nesse caso, a decisão judicial ressaltou que o tratamento e o compartilhamento dos referidos dados, na forma como é feito pela ré, exigiria o consentimento claro e expresso do indivíduo retratado, condição para viabilizar o fluxo informacional realizado, com caráter manifestamente econômico. No caso dos autos, o entendimento foi o de que inexiste o consentimento, indispensável, em relação à universalidade de pessoas catalogadas. Além disso, a decisão se pautou no argumento de que somente a permissão explícita do titular dos dados pode ser compreendida como autorização à empresa para a comercialização de dados pessoais e que isso se refere a um direito do indivíduo no que tange ao repasse de seus dados a terceiros. Ademais, o magistrado reforçou que, mesmo para os dados públicos, exige-se o propósito legítimo e específico, a preservação dos direitos dos titulares e a observância das diretrizes básicas da LGPD[19].

Como visto nesta seção, vazamentos e comercialização de dados pessoais fazem parte do cotidiano de cidadãos em diversos setores. Ainda, cumpre ressaltar, mais uma vez, que a exposição de dados pessoais, especialmente os sensíveis, tem potencial devastador na vida de pessoas, uma vez que vítimas de vazamentos, criminosos ou acidentais, estão suscetíveis a uma série de discriminações. Os casos mais emblemáticos levam a considerar prejuízos no que tange a planos de saúde e contratos de trabalho, dentre outros. Todavia, situações como as citadas até aqui podem atingir diversos direitos fundamentais, inclusive de ordem imprevisível neste momento. Mais do que isso, é imprescindível reforçar que a própria proteção dos dados pessoais é, *per si*, um direito fundamental, sendo este o tema da próxima seção.

[19] DISTRITO FEDERAL, Tribunal de Justiça. Número do processo: 0733785-39.2020.8.07.0001. 17ª Vara Cível de Brasília. Disponível em: <www.tjdf.jus.br>. Acesso em 19 abr. 2022.

3. Direitos fundamentais: lei geral de proteção de dados pessoais e demais legislações

A conceituação de *Direitos Fundamentais* passa por uma dificuldade que se relaciona com as inúmeras expressões usadas para designá-los. Entre elas, cita-se os termos direitos naturais, humanos, do homem, individuais e direitos públicos subjetivos, bem como liberdades fundamnetais e públicas[20]. Nesse sentido, adota-se o argumento de que há diferenças entre as expressões direitos humanos e fundamentais. Compreende-se, assim, que os direitos humanos são os constantes em documentos internacionais, que almejam a validade universal para todos os povos, e possuem um caráter internacional. Dessa forma, o pensamento ao qual este artigo se filia percebe os direitos fundamentais como direitos positivados no âmbito do direito constitucional de determinado Estado[21].

Acrescenta-se ao exposto a ideia de que o alicerce desses direitos é a preservação dos pressupostos de uma vida em liberdade, assim como da dignidade humana. Por essa razão, trata-se de direitos que o conjunto de leis de uma determinada nação qualifica como fundamentais e, por extensão, devem ser nomeados e expressos no texto constitucional[22]. Em outras palavras, direitos fundamentais são reconhecidos e protegidos pelo direito constitucional interno de cada Estado.

Dito isso, sustenta-se que o direito à proteção de dados pessoais é um direito fundamental, uma vez que ele está expresso no texto constitucional, por meio da promulgação da Emenda Constitucional n. 115/2022. O dispositivo foi inserido no inciso LXXIX no artigo 5º da Constituição Federal Brasileira e, além de reconhecer a proteção de dados pessoais como um direito fundamental, assevera que tais

[20] SILVA, José Afonso da Silva. Curso de Direito Constitucional Positivo. 36. ed. rev. e atual. São Paulo: Malheiros, 2013. p. 177.
[21] SARLET, Ingo Wolfgang. A eficácia dos Direitos Fundamentais. 12. ed. Porto Alegre: Livraria do Advogado, 2015. p. 29.
[22] BONAVIDES, Paulo. Curso de Direito Constitucional. 25. ed. São Paulo: Malheiros, 2010. p. 565-561.

prerrogativas também dizem respeito aos meios digitais [23] . Decorre daí o entendimento de que, a partir da sua inclusão no texto constitucional, o conceito de proteção de dados pessoais é aplicável a inúmeras situações problemáticas, já previstas ou não, ligadas à coleta, processamento, armazenamento e transmissão de dados.

Adentrando no conceito de dados de saúde, cerne desta análise, procede-se primeiro à compreensão do que são dados sensíveis. Estes estão elencados na LGPD, em seu art. 5º, II, e abarcam dados pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico. Ainda, a LGPD acrescenta que tais dados se tornam sensíveis quando vinculados a uma pessoa natural[24]. Nesse sentido, dados pessoais de saúde, consoante a legislação citada, fazem parte do rol de dados pessoais sensíveis.

Todavia, a LGPD não explicita o que pode ser considerado um dado pessoal de saúde. Trata-se uma lacuna não encontrada, por exemplo, no Regulamento Geral de Proteção de Dados – RGPD europeu, o qual inspira a legislação brasileira. De toda sorte, considera-se, à luz do exposto pela regulamentação europeia, em seu art. 4º, que dados relativos à saúde dizem respeito à saúde física e mental de qualquer indivíduo identificado ou identificável. Ainda com base no RGPD, compreende-se que a prestação de serviços de saúde e/ou outras informações reveladoras do estado de saúde de uma pessoa integram o conjunto de dados pessoais de saúde e, portanto, dados pessoais sensíveis[25].

A coleta desses dados é expressamente proibida pela norma da União Europeia, sendo permitida apenas nos casos em que tal coleta sirva à medicina

[23] BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 3 maio 2022.>. Acesso em: 15 abr. 2022.

[24] Art. 5º, II, da LGPD - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

[25] Em seu art. 4º, definições 15 do RGPD.

preventiva ou ocupacional, assistência médica e gestão de serviços de saúde. Já a Lei Brasileira, em seu art. 11º, prevê que o tratamento de dados pessoais sensíveis poderá ocorrer nos casos em que o titular consentir, sempre atrelado a uma finalidade específica. A ausência de consentimento, no entanto, não impede a coleta e tratamento de dados pessoais nos casos em que tal procedimento vise a uma obrigação legal ou regulatória, para execução de políticas públicas previstas em lei ou regulamentos, ao exercício de direitos, proteção da vida, do indivíduo ou de terceiros[26].

Em síntese, as questões relacionadas aos dados pessoais sensíveis, entre eles os dados de saúde, são um problema a ser debatido pelos operadores de direito. Isso porque tais dados compõem perfis e identidades digitais, têm valor econômico e político, porquanto podem ser usados, inclusive por sistemas que se baseiam em algoritmos, para fins de vigilância e controle social que transcendem os limites naturalmente impostos pelo Estado Democrático de Direito [27]. Os riscos de implementação de condutas discriminatórias são óbvios diante do exposto e, consequentemente, potencial afronta aos princípios da dignidade da pessoa humana. Assim, procede-se, na próxima seção, à análise de um caso concreto que envolve o uso de dados pessoais de saúde com objetivos comerciais.

4. Caso concreto: análise de uso de dados pessoais de saúde para fins de marketing

Nesta seção analisa-se o uso de dados pessoais de saúde para fins de marketing, bem como das limitações desses. Ainda, aborda-se a necessidade de adequação à LGPD, no que tange à coleta, armazenamento e compartilhamento de dados pessoais para fins de marketing. Assim, toma-se como objeto de análise uma situação específica, mas que é facilmente reconhecível por qualquer cidadão brasileiro que faça uso de medicações compradas em farmácias no País.

---

[26] BRASIL. Palácio do Planalto. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/2015-2018/2018/lei/l13709.htm>. Acesso em: 22 abr. 2022.

[27] SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. Civilistica.com, v.8, n.1, p.1-27, 29 abr. 2019.

No caso em questão, uma pessoa comprou o fármaco que utiliza em uma loja de uma rede de farmácias brasileira e, na ocasião, o vendedor que a atendeu solicitou informações pessoais para efetivar a venda. Frisa-se que o medicamento comprado, embora de uso contínuo e recomendado em consulta médica, não faz parte da lista de substâncias controladas, as quais devem ser informadas aos órgãos regulatórios por parte das farmácias. Ademais, o remédio usado pela pessoa pode ser adquirido sem receituário. Próximo à data em que os comprimidos chegariam ao fim, a pessoa recebeu uma mensagem no seu celular, via SMS, na qual a empresa alertava que já era hora de comprar uma nova unidade. Na sequência, outras mensagens foram recebidas, ofertando descontos e/ou advertindo que a pessoa cadastrada não havia efetuado compras dessa medicação recentemente.

Trata-se de uma prática que se assemelha a outras ações características da área de marketing. Não raro, estabelecimentos adotam, como estratégia de fidelização de clientes, a inclusão de informações referentes às preferências e comportamento de consumo do indivíduo. Assim, criam ofertas customizadas, com base, por exemplo, na frequência e volume de compra. Todavia, importa, nesta análise, olhar para tais estratégias no contexto específico de medicações, que são reveladoras do histórico e condições de saúde de clientes de farmácias. Dessa forma, passa-se a tematizar a coleta, armazenamento, compartilhamento de dados pessoais de saúde para fins de marketing e a adequação de tais ações à LGPD.

4.1. Das limitações do marketing na indústria farmacêutica

Chama-se atenção para os montantes movimentados pela indústria farmacêutica, que caracterizam o setor, de um lado, como expressivo na economia brasileira e, de outro, como uma área que merece atenção no que tange aos dados pessoais de saúde. Para se ter uma ideia, o faturamento do varejo farmacêutico foi de R$ 152,1 bilhões em 2021, considerando as lojas das redes associadas à Federação Brasileira das Redes Associativistas e Independentes de Farmácias – Febrafar. Esses estabelecimentos cresceram 15,9% em relação a 2020. Isso significa

um incremento na ordem de aproximadamente 50% acima do mercado[28].

Diante disso, é de se esperar que o setor adote estratégias com vistas à venda de medicamentos, inclusive porque há, naturalmente, concorrência e interesses financeiros envolvidos no assunto. Por conseguinte, uma vez que envolve a saúde da população, trata-se de assunto passível de regulamentação jurídica. No estado de Santa Catarina, por exemplo, o tema foi matéria da Lei nº 16.751, de 2015[29], com o objetivo de evitar o marketing de medicamentos. Assim, a referida unidade da federação brasileira vedou a propaganda de fármacos, seja os de venda sob prescrição médica, seja os de venda livre e similares. Essa lei abrange os meios de comunicação sonoros, audiovisuais e escritos.

Todavia, ajuizada ação direta de inconstitucionalidade, face à Lei nº 16.751, de 2015, o Supremo Tribunal Federal entendeu que a matéria era de competência legislativa privativa da União e julgou procedente a demanda para declarar inconstitucional a legislação do estado de Santa Catarina. Desse modo, o posicionamento foi o de que, ao legislar sobre vedação de propaganda de medicamentos, o estado de Santa Catarina acabou por usurpar a competência para legislar acerca da propaganda comercial, que é matéria privativa da União, a teor do disposto no art. 22, inciso XXIX, da Constituição, especialmente no que tange ao tema de medicamentos, consoante entabula o disposto no art. 220, § 4º, da CF/88. Além disso, acabou contrariando o regramento federal sobre o tema, que permite que medicamentos anódinos e de venda livre sejam anunciados nos órgãos de comunicação social, desde que apresentem advertências acerca do abuso de tais drogas, bem como a necessidade de buscar auxílio médico (Lei Federal nº 9.294/1996, art.12)[30]. Contudo, não chegou a ser analisada, pelo STF, a possibilidade ou não do marketing de medicamentos. Assim, a Ação Direta de

---

[28] MERCADO E CONSUMO. Varejo farmacêutico termina 2021 com crescimento de 10,8%. Mercado de Consumo. São Paulo, 2022. Disponível em: <https://mercadoeconsumo.com.br/2022/02/09/varejo-farmaceutico-termina-2021-com-crescimento-de-108>. Acesso em: 19 abr. 2022.

[29] SANTA CATARINA. ASSEMBLEIA LEGISLATIVA DO ESTADO DE SANTA CATARINA. Lei nº 16.751, de 2015. Proíbe a propaganda de medicamentos e similares nos meios de comunicação do Estado de Santa Catarina. Disponível em: <http://leis.alesc.sc.gov.br/html/2015/16751_2015_lei.html>. Acesso em: 03 maio 2022.

[30] BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 5432. Tribunal Pleno. Relator: Ministro Dias Toffoli. Julgado em 19 set. 2018. Disponível em: <https://www.stf.jus.br>. Acesso em: 03 maio 2022.

Inconstitucionalidade foi julgada procedente e declarada a inconstitucionalidade da Legislação do Estado de Santa Catarina.

Já no contexto específico das ações de marketing que visam diretamente a um indivíduo, como no caso de envio de mensagens personalizadas aos clientes, ressalta-se que a LGPD dispõe sobre o tratamento dos dados pessoais, inclusive nos meios digitais, por pessoa natural, bem como pessoa jurídica de direito público ou privado. Desse modo, as farmácias e demais atores da indústria farmacêutica, bem como empresas de marketing, pessoas jurídicas de direito privado, submetem-se às determinações dessa legislação. Ainda, frisa-se que a LGPD tem por objetivo principal a proteção de direitos fundamentais, tais como de liberdade e de privacidade e, ainda, o livre desenvolvimento da personalidade da pessoa natural[31]. Isso não significa um obstáculo às ações de marketing, mas as empresas devem obedecer aos ditames da norma, adequando-se aos preceitos por ela determinados.

Assim, práticas como compra e venda de listas de contatos, que já não eram consideradas moralmente aceitas, passaram a ser ilegais com a vigência da LGPD, que estabelece regramentos específicos acerca da gestão de dados pessoais sensíveis. Ademais, ações como envio de SMS aos telefones dos clientes, mesmo que seja para ofertar descontos ou lembrá-los de que a medicação está acabando, precisam respeitar as bases da LGPD, uma vez que se está, aqui, falando de uma série de operações que dizem respeito diretamente à coleta, armazenamento, compartilhamento e uso de dados pessoais de saúde. Dessa forma, resta evidente que, ao pedir o número do celular do cliente para cadastro, os estabelecimentos que comercializam medicações, ou seja, dados atrelados à saúde do indivíduo, devem informar de que modo os dados pessoais serão tratados. Ademais, com o advento da nova legislação, é basilar que possuam autorização dos clientes para utilização dos dados e que lhes seja dado autonomia para decidir como os dados serão controlados.

[31] O art. 1º da LGPD explicita do que se trata a lei e a quem é destinada, bem com qual é o seu objetivo fundamental.

4.2. Da coleta, armazenamento e compartilhamento de dados pessoais de saúde para fins de marketing

No tocante ao fornecimento voluntário de dados pessoais, como CPF, para cadastro em programas de desconto, poder-se-ia argumentar que se trata de uma escolha do indivíduo, que o faz em troca de uma vantagem financeira. Ou seja, a pessoa que, espontaneamente, concede número de celular, CPF, endereço e outros dados, atrelados à medicação que utiliza, estaria abrindo mão da sua privacidade, tendo, como contrapartida, o benefício de receber descontos.

Essa situação pode ser analisada sob o viés do paradoxo da privacidade, um o fenômeno no qual as pessoas dizem valorizar muito a privacidade, mas, em seu comportamento, renunciam a seus dados pessoais em troca de muito pouco, como um abatimento, por vezes irrisório, na compra de medicamentos, ou deixam de adotar medidas para proteger sua privacidade[32]. Todavia, está-se diante de um contexto cultural no qual é necessário considerar que muitos indivíduos sequer imaginam ou mensuram os riscos que correrão em caso de mau uso ou vazamento de seus dados pessoais de saúde. Ademais, pondera-se sobre as conjunturas socioeconômicas dos sujeitos que, mesmo compreendendo os potenciais riscos oriundos de usos irresponsáveis ou criminosos de seus dados pessoais sensíveis, consideram o fornecimento dessas informações uma contrapartida aceitável diante dos benefícios dos descontos.

Nesse cenário, o Estado de São Paulo já se ocupou da matéria, visando evitar que as farmácias exijam o CPF de clientes de forma indiscriminada. Assim, editou a Lei 17301/20, a qual prevê a proibição de as farmácias exigirem o CPF do consumidor no ato da compra, sem que seja informado, de forma clara e adequada, sobre a abertura de tal cadastro, que condiciona a concessão de determinadas promoções. Ainda, determinou que os estabelecimentos deveriam afixar avisos em suas dependências, informando que a exigência do CPF no ato da compra, como

[32] SOLOVE, Daniel J. The Myth of the Privacy Paradox. GWU Legal Studies Research Paper, v. 89, n. 10, p. 1-51, 2020. Disponível em: <http://dx.doi.org/10.2139/ssrn.3536265>. Acesso em: 19 abr. 2022.

condicionante a promoções, é proibida[33].

Diversas indagações surgem quanto à temática, a primeira seria um aspecto formal, no sentido de se verificar a competência ou não do Estado de São Paulo para regular acerca da temática. Isso porque pode-se considerar uma competência da União, a teor do disposto no art. 22, I, da CF, já que trata de dados pessoais e, também, de direito comercial, ao determinar regras de exercício da atividade empresarial. Ainda, pode-se entender por uma competência concorrente (nos moldes do art. 24, inciso V, VIII e XII, ambos da CF), já que se trata da relação das farmácias e consumidores e com a proteção da saúde[34].

De toda sorte, tem-se que a Lei de São Paulo acaba por regular a atividade empresarial de certas pessoas jurídicas (farmácias e drogarias), o que, de certa forma, já se mostra regulado pela LGPD. Uma questão importante é que, ao fornecer o CPF na farmácia, que é um dado pessoal, ele se torna um dado pessoal sensível. Isso porque, a partir dele, é possível verificar as medicações utilizadas pelo consumidor e, por conseguinte, quem tiver acesso ao sistema poderá conhecer os dados de saúde dos sujeitos que constam no cadastro. Frise-se, mais uma vez, que os dados de saúde receberam um tratamento diferenciado pela LGPD, justamente porque são considerados dados sensíveis e, caso haja vazamento ou má utilização, os indivíduos podem sofrer discriminações em diversas searas.

Outro ponto que merece atenção refere-se ao conceito de privacidade contextualizada, ou privacidade em contexto. Nesse sentido, estabelecendo-se paralelos com o tema ora em análise, em um contexto de saúde, pacientes esperam que seus médicos mantenham informações médicas confidenciais, mas devem

---

[33] SÃO PAULO. ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO. Lei nº 13.701, de 01 de dezembro de 2020. Proíbe farmácias e drogarias de exigir o CPF do consumidor, no ato da compra, sem informar de forma adequada e clara sobre a concessão de descontos, no Estado, e dá outras providências. Disponível em: <https://www.al.sp.gov.br/repositorio/legislacao/lei/2020/lei-17301-01.12.2020.html>. Acesso em: 22 abr. 2022.

[34] Ao analisar algumas decisões envolvendo farmácias no âmbito do STF, percebe-se que a questão não é unânime e dependerá de apreciação pela Corte. A título de exemplo, os municípios teriam competência para legislar acerca do funcionamento das farmácias. (BRASIL, Supremo Tribunal Federal. Agravo Interno 629125 AgR, Relator(a): DIAS TOFFOLI, Primeira Turma, Julgado em 30 agosto 2011. Disponível em:< https://portal.stf.jus.br/>. Acesso em: 21 abr. 2022. Os Estados possuem competência para regular acerca da comercialização de artigos de conveniência por drogarias (BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 4955, Relator (a): DIAS TOFFOLI, Tribunal Pleno, Julgado em 24 set. 2014. Disponível em: <https://portal.stf.jus.br/>. Acesso em: 21 abr. 2022.

aceitar que sejam compartilhadas com especialistas, caso necessário. Entretanto, essas expectativas estariam sendo violadas na hipótese de, por exemplo, os médicos venderem as informações dos pacientes para empresas de marketing ou enviá-las para empregadores[35].

Assim, compreende-se que, nos casos das farmácias, na hipótese de compartilhamento de dados pessoais de clientes com planos de saúde, por exemplo, tratar-se-ia de informações descontextualizadas, uma vez que o fornecimento dos dados ocorreu apenas para a concessão do desconto.

4.3. Cenários obscuros: risco aos direitos fundamentais

No âmbito dos dados de saúde, no contexto do fornecimento do CPF para obtenção de descontos, há diversos cenários obscuros a serem ponderados pela sociedade em geral e pelos operadores do Direito, em específico. Entre eles, cogita-se a hipótese de casos nos quais a pessoa recebe um SMS de que seu medicamento está terminando ou com promoções e é induzida a aproveitar o desconto, seguir na mesma dosagem medicamentosa, adiando a consulta médica. Ainda, no caso de o médico prescrever outra medicação, o indivíduo poderia se confundir ou até mesmo modificar o caminho terapêutico por conta das vantagens promocionais.

Já na seara exclusiva da proteção dos dados pessoais, um sistema de SMS acerca da medicação, em conjunto com outros dados de saúde, pode traçar um perfil do indivíduo. Ademais, é preciso questionar: quais pessoas têm acesso aos cadastros realizados nos balcões de farmácias? Com quem são compartilhados os dados fornecidos pelos clientes? Mirando nessas questões, o Ministério Público do Distrito Federal iniciou, em 2018, uma investigação para apurar se redes de farmácias do País estão repassando ou vendendo dados sigilosos de clientes, após exigir o CPF deles em troca de desconto. A suspeita é de que a lista de compra de cada consumidor esteja sendo divulgada para empresas de planos de saúde e de análise de crédito, em uma espécie de mercado paralelo. Para o promotor Frederico Meinberg, coordenador da Comissão de Dados Pessoais do MP, a intenção é "abrir

[35] NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Palo Alto: Stanford University Press, 2010. p. 33.

uma caixa preta" e descobrir o uso que farmácias fazem dos dados sensíveis dos clientes.[36]. Entende-se que a mera hipótese de que dados pessoais de saúde sejam usados para fins escusos, por parte de farmácias, colaboradores ou terceiros com acesso aos bancos de dados, já se configura em um cenário que exige atenção por parte de legisladores.

Vale salientar que não se questiona, aqui, o fornecimento de dados para determinados medicamentos controlados, porquanto é um requisito da Agência Nacional de Vigilância Sanitária[37] e outros órgãos, com vistas à saúde pública. Todavia, questiona-se a solicitação indiscriminada dos dados pessoais nos estabelecimentos que comercializam medicamentos, bem como a sua guarda e posterior utilização.

Outrossim, frisa-se que, dentre os fundamentos da disciplina de proteção de dados, está o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, bem como a dignidade e o exercício da cidadania pelas pessoas naturais[38]. A fim de assegurar a titularidade dos dados pessoais, toda pessoa natural tem direito a obter, do controlador, a qualquer momento, e mediante requisição, a confirmação da existência do tratamento, o acesso aos seus dados, a correção dos dados incorretos, a anonimização e bloqueio de dados desnecessários, dentre outros. O titular possui, inclusive, o direito de peticionar contra o controlador dos seus dados perante a autoridade nacional[39].

Ainda, ressalta-se que o titular dos dados pessoais tem direito ao acesso facilitado às informações relativas ao tratamento de seus dados, como a finalidade específica, a forma de duração do tratamento, informações acerca do uso compartilhado, dentre outros[40]. Todavia, no caso apresentado neste estudo, a rede de farmácias em questão apenas cita, em seu site, que os cadastros dos clientes

[36] REVISTA VEJA. MP investiga se farmácias repassam dados de clientes a planos de saúde. Revista Veja, São Paulo, 10 abr. 2018. Disponível em: <https://veja.abril.com.br/economia/mp-investiga-se-farmacias-repassam-dados-de-clientes-a-planos-de-saude/>. Acesso em: 04 maio2022.
[37] AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA – ANVISA. Substâncias Sujeitas a Controle Especial. Disponível em: <http://antigo.anvisa.gov.br/en/controlados>. Acesso em: 10 mai. 2022.
[38] O art. 2º da LGPD disciplina os fundamentos da proteção de dados pessoais.
[39] O capítulo III da LGPD trata especificamente acerca dos direitos do titular dos dados pessoais.
[40] O art. 9º da LGPD exemplifica quais as informações que o titular de dados pessoais tem direito de acesso.

podem ser compartilhados com parceiros, sem, no entanto, especificar quem são esses terceiros e qual, exatamente, o conjunto de dados é repassado. Também não informa como os cadastros de clientes e, por extensão, os dados pessoais sensíveis desses sujeitos são armazenados e acessados por colaboradores da empresa.

Face ao exposto, ressalta-se que o princípio da responsabilidade, constante na LGPD, determina que as empresas privadas e a administração pública são responsáveis pela coleta, armazenamento e proteção dos dados. Ainda, há previsão de notificação, em caráter obrigatório, para a Autoridade Nacional de Proteção de Dados, a qual deve se dar no máximo em 72 (setenta e duas) horas, em caso de violação ou vazamento[41].

A LGPD trouxe, ainda, critérios de responsabilização por eventuais danos ocorridos pelo tratamento dos dados pessoais. Os danos podem ser patrimoniais, individuais ou coletivos. Importante frisar que o operador responde solidariamente quando descumprir as obrigações da LGPD, ou não tiver seguido as instruções lícitas do operador. Outrossim, os controladores que estiverem diretamente envolvidos também respondem solidariamente[42].

Além disso, entende-se por tratamento irregular dos dados pessoais circunstâncias em que a legislação não é observada, bem como a inexistência de dispositivos que garantam segurança da informação de forma condizente. Ainda, as hipóteses de violação no âmbito das relações de consumo permanecem aplicáveis, a teor do que disciplina o art. 45 da LGPD. Desse modo, tendo em vista que a referida lei foi criada também para dar segurança jurídica às instituições públicas e privadas no que tange à proteção de dados pessoais, procede-se a uma breve análise dos riscos que farmácias e drogarias, bem como seus colaboradores, correm ao adotar a prática de coleta e uso de dados pessoais de saúde para fins de marketing.

---

[41] POLIDO, Fabrício B. Pasquot *et al*. GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. [*S.l.*]: Instituto de Referência em Internet e Sociedade, 2018. Disponível em: <https://irisbh.com.br/wp-content/uploads/2018/06/GDPRpercuss%c3%b5es-no-direito-brasileiro-Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf.>.Acesso em: 09 mai. 2022.

[42] O art. 42 e seguintes da LGPD tratam, especificamente, da responsabilidade e do ressarcimento de danos, inclusive com a possibilidade de o juiz, no processo civil, inverter o ônus da prova a favor do titular dos dados, quando houver hipossuficiência para fins de produção de prova ou essa for excessivamente onerosa (art.43, §3º da LGPD).

4.4. Cenários obscuros: riscos às farmácias

A LGPD especifica, a partir do art. 37, quem são os agentes de tratamento de dados pessoais, basicamente três figuras. A primeira delas é o controlador, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. A segunda figura em destaque é o operador, também pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador[43]. No caso em análise, o controlador é aquele a quem compete as decisões referentes ao tratamento de dados pessoais, que pode ser pessoa jurídica ou natural, tanto de direito público como privado, ou seja, pode ser a pessoa jurídica da respectiva farmácia e, também, a pessoa física que determina como os dados serão tratados; o operador é aquele que realiza o tratamento dos dados pessoais, como por exemplo, o atendente do balcão, o atendente de caixa, o farmacêutico etc[44]. Cumpre assinalar que a legislação traz, ainda, a figura do encarregado[45], que é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD, ou seja, um colaborador da empresa que executa tal tarefa.

No caso de descumprimento da LGPD, há também a previsão de sanções administrativas, que podem ser uma advertência, para adoção de medidas corretivas, como multa de 2% do faturamento da pessoa jurídica de direito privado até o valor de R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Inclusive, podem ser sancionados com suspensão das atividades pelo período de seis meses, prorrogáveis, e até mesmo a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados[46].

---

[43] A LGPD traz os conceitos dos agentes de tratamento de dados pessoais, no art.5 º, inciso VI, VII, VIII e IX.
[44] No art. 5º, inciso VI e VII, a LGPD traz o conceito de controlador e operador.
[45] Também denominado "DPO" – Data Protection Officer. Conforme consta no art. 5º inciso VIII, da LGPD, o encarregado atua como canal de comunicação entre os titulares dos dados e ANPD.
[46] BRASIL. Palácio do Planalto. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03o2015-2018/2018/lei/l13709.htm>. Acesso em: 08 abril 2022.

Nesse sentido, questiona-se se os balconistas, atendentes, desenvolvedores e gestores de marketing estão cientes dos riscos que correm caso não cumpram as determinações da LGPD quanto ao tratamento dos pessoais de saúde de clientes desses estabelecimentos. Isso porque, conforme a nova legislação, no caso de vazamento acidental ou criminoso de dados pessoais sensíveis, esses colaboradores poderiam ser responsabilizados.

Ressalta-se que empresários, sociedades em geral e todos aqueles que realizam o tratamento de dados pessoais, através da coleta, armazenamento, bem como compartilhamento, estão sujeitos às sanções constantes na LGPD. Decorre daí a necessidade de os operadores de direito estarem atentos aos parâmetros da legislação, a fim de prestar assessoria jurídica adequada, sob pena, inclusive, de a empresa ter a proibição de suas atividades, em caso grave de descumprimento das normas protetivas. Trata-se, portanto, de tema que exige a atenção dos gestores, sejam eles da área de direito ou não, pois as atuais práticas no que tange ao cadastro de clientes e envio de mensagens para fins de venda de medicações podem, num futuro próximo, gerar prejuízos de ordem econômica e consequências jurídicas, especialmente se o tratamento inadequado dos dados de saúde de clientes gerar dano aos direitos fundamentais dessas pessoas.

Ainda, importa esclarecer que a Autoridade Nacional de Proteção de Dados[47] é o agente fiscalizador da LGPD. A essa agência, criada recentemente, caberá elaborar parâmetros necessários acerca do assunto abordado, inclusive, prevendo e aplicando sanções, bem como editar normas sobre a temática, dentre outras providências. Por fim, observa-se que no próprio site da ANPD há um canal de denúncias e sugestões. Ademais, cabe à ANPD a elaboração de regulamentos, estudos, bem como orientações específicas no que concerne à interpretação e à aplicabilidade prática da LGPD. Portanto, no que tange à prática da solicitação de CPF nas farmácias para fins de participação em sistemas de descontos e ações promocionais, urge um posicionamento firme da entidade, com vistas à garantia de direitos fundamentais consagrados no ordenamento brasileiro e à segurança jurídica

[47] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. Site da ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em: 07 mai. 2022.

para que redes de farmácias e drogarias atuem em plena compatibilidade entre os direitos dos seus clientes e as suas metas financeiras, via estratégias de marketing.

5. Considerações finais

A fim de sintetizar o exposto nesta investigação, retoma-se que o tema da utilização e ao vazamento dos dados pessoais, especialmente os de cunho sensível, como os de saúde, é um problema que tem ocupado a atenção de juristas. O assunto, inclusive, recebeu um tratamento diferenciado pela Lei Geral de Proteção de Dados e, recentemente, a proteção de dados pessoais foi inserida no texto constitucional, com a promulgação da Emenda Constitucional n.º 115/2022, que incluiu, no artigo 5º da Constituição Federal, o inciso LXXIX, dispositivo que reafirma o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais.

Trata-se de uma ação de salutar relevância, pois, do contrário, o ordenamento jurídico brasileiro estaria deixando vácuos regulatórios, zonas livres da proteção de dados pessoais, em descompasso com o contexto cultural destas primeiras décadas do século XXI, a era digital. Todavia, reforça-se que a ausência de uma regulação específica não poderia servir de obstáculo a esse direito fundamental, dada a sua aplicabilidade imediata, seja expresso, seja implicitamente positivado. A partir da Constituição Federal, é possível reconhecer, em diversas situações, a proteção de dados pessoais, independente de uma regulação específica para esse domínio. Este é um dos fatores de maior destaque da importância da inclusão da proteção de dados no texto constitucional.

Cumpre assinalar que a questão da coleta e compartilhamento de dados pessoais ganhou notoriedade na sociedade, em parte pela hiperconectividade que caracteriza o contexto contemporâneo. O caso envolvendo a empresa Cambridge Analytica, cujo acesso aos dados de usuários do Facebook gerou discussões sobre a utilização de dados pessoais para influenciar em decisões eleitorais, foi emblemático e acendeu o alerta de cidadãos de diversos países[48]. Nesse panorama,

[48] SANTOS, M. C. C. L. dos; LOMBARDI, L. P. V. A ética e bioética nas relações de proteção de dados genéticos pessoais sensíveis face aos direitos humanos. Revista Brasileira de Bioética, [*S. l.*], v. 14, n. edsup, p. 135-150, 2019. Disponível em: <https://periodicos.unb.br/index.php/rbb/article/view/26294>. Acesso em: 5 maio. 2022.

surgiu o Regulamento Geral de Proteção de Dados, aplicável aos países da União Europeia, em 2018, que foi utilizado como base da LGPD[49]. Nesse sentido, a proteção de dados mostra-se de salutar importância, sendo, inclusive, base da economia digital, porquanto assinala que os indivíduos têm o direito de controle e acesso dos seus dados[50]. Além disso, há a proibição de intercâmbio de dados entre empresas sem que haja o consentimento dos titulares.

No que tange ao foco deste estudo, qual seja, a solicitação de CPF de clientes de farmácias para fins de ações promocionais em troca de descontos em medicações, não se caracteriza como um paradoxo da privacidade. Ressalta-se que a problemática se dá justamente porque esse dado pessoal torna-se sensível, ao transparecer, via conhecimento das medicações utilizadas por um indivíduo, o seu histórico de saúde. Eventuais falhas na guarda desse conjunto de informações têm potencial danoso à vida dos cidadãos, que correm o risco de discriminações em suas atividades laborais, no que tange a custos de planos de saúde, bem como exposição de informações que impliquem em constrangimentos de toda espécie. Como visto, tais circunstâncias já saíram do campo hipotético e, no caso dos dados de saúde coletados por farmácias, o terreno pode ser ainda mais espinhoso, uma vez que existem suspeitas de que tais dados possam ser repassados a terceiros, de forma intencional ou acidental.

Embora a solução pareça simples do ponto de vista das medidas que cada sujeito pode adotar para proteger seus dados pessoais de saúde, questiona-se: quais são as ferramentas ao alcance dos titulares de dados pessoais, quando, em grande medida, os indivíduos sequer conhecem as possíveis consequências de fornecer o número de CPF para receber descontos em farmácias? Além do mais, como visto no caso tomado por objeto para estas reflexões, não há uma cultura consolidada quanto ao tema da autodeterminação informativa. De um lado, os

---

[49] INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. Disponível em: <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%c3%b5es-no-direito-brasileiro-Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf>. Acesso em: 10 maio. 2022.

[50] PELOSO PIURCOSKY, Fabrício *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. Suma neg., Bogotá, v. 10, n. 23, p. 89-99, dez. Disponível em: <http://www.scielo.org.co/scielo.php?script000300089&lng=en&nrm=iso>. Acesso em: 05 mai. 2022.

clientes não são devidamente informados sobre seus direitos quanto à coleta, armazenamento e utilização de seus dados de saúde. De outro, possivelmente, atendentes desses estabelecimentos comerciais restringem-se a cumprir tarefas que lhes foram determinadas, ou seja, abastecer um poderoso banco de dados e oferecer, ao cliente, a contrapartida de um desconto que pode ser sedutor, dependendo das circunstâncias socioeconômicas de quem precisar comprar medicações de uso contínuo ou mesmo destinadas a tratamentos de enfermidades que são alvo de preconceitos sociais.

Cumpre assinalar que, em razão das inúmeras possibilidades de discussões envolvendo o tema objeto deste estudo, não se pretendeu esgotar o assunto. Todavia, reforça-se urgência de se questionar a legalidade e a necessidade de coleta de CPF pelas farmácias. Como ficou evidente, trata-se de dados que se tornam sensíveis e transcendem uma simples operação comercial e suas consequentes ações de marketing. Sendo assim, resta ainda afirmar que se está diante de uma necessidade de conscientização dos indivíduos acerca do fornecimento dos seus dados de saúde, a fim de que tenham condições de exercer o seu direito de autodeterminação informativa no ato da compra de medicamentos. Aos estabelecimentos que adotam práticas como a exposta neste texto, alerta-se que as sanções podem ser pesadas no caso de vazamentos de dados de saúde de clientes, sobretudo se eventuais exposições afrontarem direitos individuais salvaguardados no ordenamento jurídico brasileiro, ainda que não sejam fruto de má fé.

Referências bibliográficas

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA – ANVISA. **Substâncias Sujeitas a Controle Especial**. Disponível em: <http://antigo.anvisa.gov.br/en/controlados>. Acesso em: 10 mai. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Site da ANPD**, 2022. Disponível em:< https://www.gov.br/anpd/pt-br>. Acesso em: 07 mai. 2022.

BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 25. ed. São Paulo: Malheiros, 2010. p. 565-561.

BRASIL, Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 5432**. Tribunal Pleno. Relator: Ministro Dias Toffoli. Julgado em 19 set. 2018. Disponível em: <https://portal.stf.jus.br>. Acesso em: 03 maio 2022.

BRASIL, Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4955**, Relator (a): DIAS TOFFOLI, Tribunal Pleno, Julgado em 24 set. 2014. Disponível em: <https://portal.stf.jus.br>. Acesso em: 21 abr. 2022.

BRASIL, Supremo Tribunal Federal. **Agravo Interno 629125 AgR**, Relator(a): DIAS TOFFOLI, Primeira Turma, Julgado em 30 agosto 2011. Disponível em: <https://portal.stf.jus.br>. Acesso em: 21 abr. 2022.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 3 maio 2022>. Acesso em: 15 abr. 2022.

BRASIL. Palácio do Planalto. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 08 abril 2022.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. *In*:_____. CASTELLS, Manuel; CARDOSO, Gustavo (Org.). **A sociedade em rede**: do conhecimento à acção política. São Paulo: Paz e Terra, 2000. v. 1. p. 17-31.

CONGRESSO EM FOCO. Usuários acusam falhas em app do Ministério da Saúde há meses. **Congresso em Foco**, 11 dez. 2021. Disponível em: <https://congressoemfoco.uol.com.br/area/governo/conectesus-usuarios-acusam-falhas-em-app-do-ministerio-da-saude-ha-meses/>. Acesso em: 04 mai. 2022.

DISTRITO FEDERAL, Tribunal de Justiça. Número do processo: 0733785-39.2020.8.07.0001. 17ª Vara Cível de Brasília. Disponível em:<www.tjdf.jus.br>. Acesso em 19 abr. 2022.

HERN, Alex. Hackers publish private fotos from cosmetic surgery clinic. **Guardian**, 31 mai. 2017. Disponível em: < https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments>. Acesso em: 17 abr. 2022.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. **GDPR e suas repercussões no direito brasileiro**: primeiras impressões de análise comparativa. Disponível em: <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-

repercuss%c3%b5es-no-direito-brasileiro-Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf>. Acesso em: 10 maio. 2022.

KLEINMAN, Zoe. Therapy patients blackmailed for cash after clinic data breach. **BBC News**, 26 out. 2020. Disponível em: <https://www.bbc.com/news/technology-54692120>. Acesso em: 17 abr. 2022.

MERCADO E CONSUMO. Varejo farmacêutico termina 2021 com crescimento de 10,8%. **Mercado & Consumo**, São Paulo, 2022. Disponível em: <https://mercadoeconsumo.com.br/09/02/2022/noticias/varejo-farmaceutico-termina-2021-com-crescimento-de-108/>. Acesso em: 19 abr. 2022.

MIRANDA, Jorge; MEDEIROS, Rui. **Constituição Portuguesa Anotada**. 1. ed. Coimbra: Coimbra Editora, 2006.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 183-212, jul./dez. 2019.

NISSENBAUM, Helen. **Privacy in Context**: Technology, Policy, and the Integrity of Social Life. Palo Alto: Stanford University Press, 2010.

PEIXOTO, Sinara. 16 milhões de pacientes de Covid-19 têm dados expostos; Saúde investiga**. CNN Brasil**, 26 nov. 2020. Disponível em: <https://www.cnnbrasil.com.br/saude/16-milhoes-de-pacientes-de-covid-19-tem-dados-expostos-saude-investiga/>. Acesso em: 22 abr. 2022.

PELOSO PIURCOSKY, Fabrício *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma neg**., Bogotá, v. 10, n. 23, p. 89-99, dez. Disponível em: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2215-910X2019000300089&lng=en&nrm=iso>. Acesso em: 05 mai. 2022.

POLIDO, Fabrício B. Pasquot *et al*. **GDPR e suas repercussões no direito brasileiro**: primeiras impressões de análise comparativa. [*S.l.*]: Instituto de Referência em Internet e Sociedade, 2018. Disponível em: <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%c3%b5es-no-direito-brasileiro-Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf>. Acesso em: 09 mai. 2022.

PORTAL G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet. **Portal G1**, 02 dez. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em 04 maio 2022.

REVISTA VEJA. MP investiga se farmácias repassam dados de clientes a planos de saúde. **Revista Veja**, São Paulo, 10 abr. 2018. Disponível em: <https://veja.abril.com.br/economia/mp-investiga-se-farmacias-repassam-dados-de-clientes-a-planos-de-saude/> . Acesso em: 04 maio2022.

RUARO, Regina Linden. Responsabilidade civil do Estado por dano moral em caso de má utilização de dados pessoais. **Direitos Fundamentais &Justiça**, Porto Alegre, v. 1, n. 1, p. 231-245, out. 2007.

SANTA CATARINA. ASSEMBLEIA LEGISLATIVA DO ESTADO DE SANTA CATARINA. **Lei nº 16.751, de 2015**. Proíbe a propaganda de medicamentos e similares nos meios de comunicação do Estado de Santa Catarina. Disponível em: <http://leis.alesc.sc.gov.br/html/2015/16751_2015_lei.html>. Acesso em: 03 maio 2022.

SANTOS, M. C. C. L. dos; LOMBARDI, L. P. V. A ética e bioética nas relações de proteção de dados genéticos pessoais sensíveis face aos direitos humanos. **Revista Brasileira de Bioética**, [*S. l.*], v. 14, n. edsup, p. 135-150, 2019. Disponível em: <https://periodicos.unb.br/index.php/rbb/article/view/26294>Acesso em: 5 maio. 2022.

SÃO PAULO. ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO. **Lei nº 13.701, de 01 de dezembro de 2020**. Proíbe farmácias e drogarias de exigir o CPF do consumidor, no ato da compra, sem informar de forma adequada e clara sobre a concessão de descontos, no Estado, e dá outras providências. Disponível em: <https://www.al.sp.gov.br/repositorio/legislacao/lei/2020/lei-17301-01.12.2020.html.> Acesso em: 22 abr. 2022.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica.com**, v.8, n.1, p.1-27, 29 abr. 2019.

SARLET, Ingo Wolfgang. **A eficácia dos Direitos Fundamentais**. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

SILVA, José Afonso da Silva. **Curso de Direito Constitucional Positivo**. 36. ed. rev. e atual. São Paulo: Malheiros, 2013.

SOLOVE, Daniel J. The Myth of the Privacy Paradox. **GWU Legal Studies Research Paper**, v. 89, n. 10, p. 1-51, 2020. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265> . Acesso em: 19 abr. 2022.

UNIÃO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Disponível em: <https://eur-lex.europa.eu/legal-

content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN>. Acesso em: 21 abr. 2022.

VIEIRA, Tatiana Malta. Proteção de dados pessoais na sociedade de informação. **Revista de Direito de Informática e Telecomunicações: RDIT**, Belo Horizonte, v. 2, n. 2, p. 213-235; jan./jun. 2007.

9. O PRINCÍPIO DA PUBLICIDADE DAS DECISÕES JUDICIAIS E A DIVULGAÇÃO DE DADOS PESSOAIS: O POTENCIAL EFEITO DISCRIMINATÓRIO

https://doi.org/10.36592/9786581110994-09

Regina Linden Ruaro[1]

Fernanda Linden Ruaro Peringer[2]

Sumário

1. Introdução

O progresso na área das tecnologias e o advento da internet propiciam que a informação e a comunicação (TIC) possam, instantaneamente, processar textos,

[1] Advogada e Consultora Jurídica nas áreas do Direito Administrativo, Direito Digital e Proteção de Dados Pessoais. Professora Titular da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. Procuradora Federal/AGU aposentada. Doutora em Direito pela Universidad Complutense de Madrid (1993) com titulo revalidado pela UFRGS e Pós-Doutora pela Universidad San Pablo - CEU de Madri/Espanha (2006/2008), Estágio Pós-doutoral na Universidade San Pablo - Ceu de Madri (2016). Compõe o Grupo Internacional de Pesquisa "Protección de Datos, Transparencia y Acceso a la Información". Coordenadora no Brasil pela PUCRS/PPGD/PUCRS no Projeto "Identidad Digital, Derechos Fundamentales y Neuroderechos" - Espanha. Professora convidada do Máster en Protección de Datos, Transparencia y Acceso a la Información da Universidad San Pablo de Madrid-CEU/ Espanha. Decana Associada da Escola de Direito (2018/2021). Membro do Comitê Gestor do Biobanco da PUCRS. Membro Honorário do Instituto Internacional de Estudos de Direito do Estado - IEDE. Lidera o Grupo de Pesquisa cadastrado no CNPq: Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação no Estado Democrático de Direito na linha de Direito, Ciência, Tecnologia e Inovação. Coordenadora do Grupo do PPGD/ESCOLA DE DIREITO/PUCRS no Projeto HANGAR (criação *startup* jurídica).
E-mail: ruaro@pucrs.br; link Lattes: http://lattes.cnpq.br/8023231740817826.

[2] Advogada e Professora de Direito. Mestre em Direito pela PUCRS (2022). Sócia do Escritório Regina Ruaro Advogados Associados. Pesquisadora na área de Direito, Ciência, Tecnologia & Inovação na PUCRS. Integrante do grupo de pesquisa Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação no Estado Democrático de Direito na linha de Direito, Ciência, Tecnologia e Inovação na PUCRS. Integrante do Grupo de Pesquisa Empresa e Desenvolvimento Econômico e Social na PUCRS. Especialista em Direito Público pela PUCRS (2012). Graduada pela Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul (2007). Possui ênfase nas áreas de Contratos Empresariais e Cíveis, *Compliance*, Proteção de Dados Pessoais e Direito Administrativo. Membro da Comissão de Mediação da OAB/RS (2017/2018). Integrante do Grupo do PPGD/Escola de Direito/PUCRS no Projeto Hangar (criação *startup* jurídica). Integrante do Grupo Aires (*AI Robotics Ethis Society*). E-mail: fernanda@ruaro.adv.br; link Lattes: https://lattes.cnpq.br/0024967764963913.

imagens, sons e dados num espaço global. As tecnologias mudaram o modo de produção e incluíram várias nações e seus indivíduos em um mesmo espaço virtual global. Assim, o acesso à informação ganha novos contornos expandindo alcance e propiciando educação e conhecimento.

Par e passo com essa realidade, que em muito atua para expandir o progresso na sociedade da informação ao qual tudo se expõe e tudo se sabe, vislumbra-se uma nova *comodity* – o dado pessoal. Além disso, essa realidade impacta também o exercício da jurisdição brasileira, bem como os novos contornos que assumem as publicidades dos atos processuais. Assim, se antes o princípio da publicidade objetivava franquear acesso a autos que se encontravam fisicamente no poder dos servidores da justiça, nos dias de hoje, conferem potencial acesso até mesmo àqueles que, por determinado interesse e alheio às partes nos processos, se dirijam aos espaços físicos do Poder Judiciário a fim de tomar conhecimento de suas decisões. Como se denota, o avanço tecnológico presente na rede mundial de computadores se apresenta como ferramenta que confere mais agilidade e cumprimento do princípio da publicidade, um dos previstos no artigo 37, *caput*, da Constituição Federal de 1988 – sem, no entanto, deixar ampliar a área de superfície em que podem ocorrer possíveis vulnerabilidades aos interesses das partes.

A imposição para que o Poder Judiciário torne públicas as decisões que não estão cobertas pelo segredo de justiça ou outra restrição que legitime o sigilo[3] atende, também, ao direito fundamental de acesso à informação que, dada a sua dimensão, se tenciona com o direito fundamental à proteção de dados pessoais. Ou seja, temos aqui uma equação a ser resolvida: direito ao acesso à informação e seus limites em face do direito à proteção de dados fundamentais.

Além dos pontos anteriores, outra reflexão que se apresenta necessária é a perpetuação das informações constantes nos processos judiciais, sejam elas relativas às decisões do Poder Judiciário ou, ainda, aos dados pessoais dos litigantes mesmo depois de baixados ou arquivados os processos judiciais. Desse modo, a fim de melhor expor o tema, é necessário encontrar os limites do princípio da publicidade

[3] O princípio da publicidade das decisões judiciais insculpido no artigo 93, inciso IX, da CF, determina que o sigilo seja aplicado apenas a casos que não ofendam o interesse público à informação. Ademais, o mesmo dispositivo legal versa sobre o direito à intimidade, sem, no entanto, adentrar na seara do que é a intimidade, bem como quais informações são de interesse público.

que proporciona o amplo acesso à informação, fora daqueles já estudados no direito processual [4]. Intentando alinhavar algumas reflexões, por óbvio, sem qualquer pretensão de esgotar o tema, o presente ensaio articula o que segue: o princípio da publicidade das decisões judiciais, na era digital, coloca em xeque o direito à proteção de dados pessoais?

Para atingir os objetivos a que se propõe, acolheu-se o método de abordagem dialético por meio de revisão bibliográfica acerca do tema. Além de discorrer sobre os referidos dispositivos legais, este ensaio está fundado em estudos que versam sobre a proteção de dados pessoais em uma contemporânea "razão hiperconectada"[5]. Desse modo, a divisão das seções obedece à linha de raciocínio característica do método dialético.

De plano, abordar-se-á acerca do princípio da publicidade e sua dimensão na divulgação das decisões judiciais, na era digital, como corolário do direito de acesso à informação. Logo após, o foco recai sobre a proteção de dados pessoais estabelecendo-se as tensões ora descritas. Por fim, serão apresentadas notas conclusivas e caminhos possíveis para compatibilizar a publicização dos atos judiciais e proteção de dados pessoais.

O presente artigo está ancorado na linha de pesquisa Direito, Ciência, Tecnologia & Inovação e no Projeto de Pesquisa, Proteção de Dados Pessoais e Acesso à Informação no Estado Democrático de Direito, do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

2. Princípio da publicidade das decisões judiciais

O princípio da publicidade é basilar nas democracias. Bobbio já percebia que a publicidade se revela como uma 'categoria iluminista' representando um dos

[4] TUCCI, Rogério Lauria. Direitos e Garantias Individuais no Processo Penal Brasileiro. 3. ed. São Paulo: Saraiva: 2009, pp. 178-179.

[5] Sobre o tema, conforme a Coletânea organizada por Ovidiu Vermesan e Joël Bacquet, Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution. River Publishers, 2017. Disponível em: <https://europeaniotpilots.eu/wpcontent/uploads/2020/06/Cognitive_Hyperconnected_Digital_Transformation_IERC_2017_Cluster_eBook_Web.pdf>. Acesso em: 12. abr. 2022.

aspectos da batalha de quem se considera chamado a derrotar o 'reino das trevas'. Utilizava-se, por isso, da metáfora da luz, do clareamento, para contrastar o 'poder visível do invisível'. Portanto, dar visibilidade é viabilizar o acesso e o controle dos atos públicos, tanto pela sociedade, quanto pelos órgãos de controle de cada democracia[6].

Na atualidade, referido princípio se mostra mais importante ainda. Isto porque todos os envolvidos na administração, sejam eles autoridades públicas ou de supervisão e tribunais, gradualmente, se encontraram e se encontram perante o desafio de "dar vida" a textos normativos em um ambiente clássico essencialmente de "papel"; contudo, na realidade de hoje (onde estamos diante de um contexto cada vez mais eletrônico) tudo está em permanente transformação. Os computadores invadiram todos os andares da administração, bem como dos Poderes Legislativo e Judiciário. Redes conectam máquinas e homens sistematicamente permitindo diálogo e intercâmbios muito além dos departamentos inicialmente compartimentados e muitas vezes estéreis. Os servidores eletrônicos estão abertos a qualquer hora do dia, prontos para fornecer as informações solicitadas e receber formulários e petições preenchidos – de modo eficiente e rápido.

No entanto, os benefícios dos avanços tecnológicos não deixam de levantar questões e suscitar dificuldades. Além disso, a identificação da pessoa com informações em um contexto de processo eletrônico é óbvia devido à passagem do processo físico para o processo eletrônico em rede.

Com o advento das TIC (Tecnologias da Informação e Comunicação), que possibilita a oportunidade de tornar públicas as decisões judiciais, em maior nível possível, a transparência foi incrementada e se deu força ao aspecto democrático por estabelecer um canal via rede mundial de comunicação direta entre o Poder Público e os cidadãos. Esse meio de comunicação resultou num aprofundamento democrático e em uma maior publicidade, transparência e eficiência na atividade pública, porquanto, mais controlada através dos mecanismos constitucionais postos à disposição da sociedade. O pluralismo informativo, o livre acesso e a circulação de informações atuam como regra geral a propiciar o controle.

[6] BOBBIO, Norberto. O futuro da democracia. 7. ed. São Paulo: Paz e Terra, 2000, p. 103.

Nesse passo, a publicidade dos atos processuais (ações praticadas no decorrer de um processo judicial), expressa no artigo 5º, inciso LX[7], da CF, possui uma relação de fluxo e refluxo com a democracia, uma vez que, ao mesmo tempo em que é decorrente do princípio democrático constitui-se, também, em um elemento fundamental de sua consolidação ao afastar o sigilo como regra.

Cumpre destacar que a Emenda Constitucional nº 45, datada de 2004, já no contexto da era digital, reafirma o exposto no artigo 93, inciso IX, da CF, *in verbis*:

> 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[8].

De fato, a necessidade do controle do processo judicial pelas partes e pela sociedade impõe o cumprimento do princípio da publicidade das decisões pelo Poder Judiciário. Desse modo, protege as partes de arbítrios de agentes do Estado, o magistrado ao permitir que a sociedade tenha uma exata noção de sua atuação, bem como a coletividade na medida em que permite o controle dos atos processuais e sua consonância com os objetivos constitucionais[9]. Isto porque as decisões judiciais devem ser públicas na medida em que o acesso à informação se trata de um direito fundamental que visa permitir o controle da opinião pública sobre os serviços da justiça, máxime ante o poder de que foi investido o juiz[10]. Ademais, "existe para vedar

[7] BRASIL. Planalto. Artigo 5º, inciso LX, da Constituição Federal de 1988: "A lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem".
[8] BRASIL. Planalto. Redação dada pela Emenda Constitucional nº 45, de 2004. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc45.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%2045%2C%20DE%2030%20DE%20DEZEMBRO%20DE%202004&text=Altera%20dispositivos%20dos%20arts.,A%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias>. Acesso em: 04. mai. 2022.
[9] COPETI, André. J.J. GOMES CANOTILHO (et al). Comentários à Constituição. São Paulo: Saraiva/ Alamedina, 2013, pp. 451-452.
[10] JUNIOR, Fredie Didier. Teoria Geral do Processo e processo de conhecimento. 7. ed. Bahia: Juspodivm, 2007, p. 59.

o obstáculo ao conhecimento, pois todos têm o direito de acesso aos atos do processo, exatamente como meio de se dar transparência à atividade jurisdicional"[11].

O direito fundamental de acesso à informação dos atos do Poder Judiciário é mais do que o interesse privado defendido pelas partes, pois encontra-se presente um interesse público maior que consiste na "garantia da paz e harmonia social, procurada através da manutenção da ordem jurídica", uma vez que, todos os cidadãos e não apenas os litigantes da demanda, têm direito de ter ciência e acompanhar os trâmites processuais[12].

3. O princípio da publicidade e o direito de acesso à informação (Art. 5, XXXIII, da CF)

Uma das principais características do Estado Democrático de Direito diz respeito à presença do dever de informar que recai sobre o Estado, bem como o direito de ser informado conferido à população. O artigo 5°[13], inciso XXXIII, da Constituição Brasileira refere que todos os cidadãos têm direito de receber dos órgãos públicos informações de interesse particular, coletivo ou geral, que serão prestadas, conforme o prazo previsto em lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança do Estado e da sociedade.

Nesse sentido, Patricia Peck Pinheiro destaca que o Estado Democrático de Direito se desmembra em três categorias "de acordo com o sujeito de direito": "a) direito de informar, que é um direito ativo; b) o direito de ser informado, que é um direito passivo; c) o direito de não receber informação, que é um direito ativo e passivo."[14]

Nessa perspectiva, e em cumprimento à norma constitucional foi promulgada

[11] WAMBIER, Luiz Rodrigues. Curso Avançado de Processo Civil. Vol I, 5 ed., São Paulo: Revista dos Tribunais, 2013, p. 80.
[12] THEODORO JÚNIOR, Humberto. Curso de Direito Processual Civil: Teoria geral do direito processual civil e processo de conhecimento. v. I. 50 ed. Rio de Janeiro: Forense, 2009, p. 52.
[13] BRASIL. Planalto. Artigo 5º, inciso XXXIII, da Constituição da República Federativa do Brasil de 1988. Diário Oficial da República Federativa do Brasil. Brasília, DF, 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 07. abr. 2022.
[14] PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Saraiva Jur, 7ª ed. 4ª tiragem, 2021, p. 83.

a Lei n.º 12.527/2011[15] – Lei de Acesso à Informação. Referida normativa estabelece que órgãos e entidades públicas divulguem informações de interesse coletivo, salvo aquelas cuja confidencialidade esteja prevista no texto legal, a saber: "aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado."[16]

Cabe reforçar, aqui, que o dispositivo constitucional mencionado excepciona o dever geral de informar, na hipótese de "informações imprescindíveis à segurança da sociedade e do Estado"[17]. O sigilo mencionado seria necessário ao bom desempenho da Administração Pública e não, simplesmente, à omissão de informações para o administrador. Nesses termos, as informações detidas pelo Estado vinculam-se ao direito de os indivíduos terem acesso a elas, seja por interesse particular, seja por interesse coletivo.

No que concerne às informações pessoais, a Lei de Acesso à Informação, em seu artigo 31[18], refere que o tratamento dessas informações deve ser realizado com

---

[15] BRASIL. Planalto. Lei n. 12.527 de 18 de novembro de 2011. Regula o acesso à informação previsto no inciso XXXIII do art. 5º, bem como no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.> Acesso em: 04. mai. 2022.

[16] BRASIL. Planalto. Consoante se verifica do art. 4º, inciso III, da Lei de Acesso à informação. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.>. Acesso em: 08. abr. 2022.

[17] Importante referir que Ingo Wolfgang Sarlet destaca que antes da decisão do Google do TJUE, o direito ao esquecimento já havia sido reconhecido na jurisprudência nacional, pelo Superior Tribunal de Justiça, no caso emblemático denominado "chacina da candelária", o qual atraiu os meios de comunicação e jurídicos na época. SARLET, Ingo Wolfgang; Ferreira Neto, Arthur M. O direito ao "esquecimento" na Sociedade de Informação. Livraria do Advogado Editora, 2019, p. 161.

[18] BRASIL. Planalto. Lei nº 12.527, de 18 de novembro de 2011. 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

respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais prevendo, ainda, que aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

A era digital com as diversas inovações tecnológicas suscitou a existência de múltiplos riscos que provocam novas formas de violação aos direitos de personalidade. A partir da necessidade de uma proteção da privacidade e do acesso e circulação de informações informatizadas, consolidou-se um desafiador contexto com o reconhecimento jurídico do denominado "direito ao esquecimento".[19]

Referido direito diz respeito à possibilidade de uma pessoa não permitir que um fato, "verdadeiro ou não, relacionado ao indivíduo, seja exposto perpetuamente, causando-lhe dor ou sofrimento, bem como a renovação da repercussão social já vivenciada"[20]. É tratado ainda como "um dos aspectos do direito da personalidade, derivando da proteção da intimidade e à privacidade". [21] Para tanto, uma das problemáticas da sociedade digital é, justamente, a perda da possibilidade de "esquecimento", porquanto, os dados ficam armazenados para sempre, nada obstante sua importância, o mesmo não será objeto de nossas reflexões.

Todavia, a virtualização dos processos pode trazer uma série de consequências aos sujeitos direta ou indiretamente envolvidos como, também, a divulgação de suas informações pessoais. E isso porque, como já aqui mencionado, a regra do processo judicial é a publicidade de seus atos, razão pela qual a informação processual se coloca como um dever do Estado. No entanto, no âmbito do direito brasileiro, igualmente, está a proteção de dados pessoais como um direito

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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.>. Acesso em: 08. abr. 2022.

[19] Por todos, cf., SARLET, Ingo Wolfgang; Ferreira Neto, Arthur M. O direito ao "esquecimento" na Sociedade de Informação. Porto Alegre: Livraria do Advogado, 2019, pp. 33-34.

[20] SILVEIRA, Beatriz de Oliveira da et al. O direito ao esquecimento para a sociedade digital. A Leitura: Caderno da Escola Superior da Magistratura do Estado do Pará, Belém, v.7, n. 12, pp. 50-60, maio 2014, p. 52.

[21] KHOURI, Paulo Roberto Roque Antonio. O direito ao esquecimento na sociedade de informação e o enunciado 531 da VI Jornada de Direito Civil. Revista de Direito do Consumidor, São Paulo, v. 22, n. 89, pp. 463-465, set./out. 2013, p. 463.

fundamental, tema que será abordado a seguir.

4. A lei geral de proteção de dados (LGPD) e a virtualização de processos

No contexto do direito brasileiro, a Lei Geral de Proteção de Dados Pessoais (13.709/2018)[22] está alicerçada em princípios básicos no que tange ao direito à privacidade e não violação da mesma, da liberdade de expressão e dos Direitos Humanos.[23]

Do mesmo modo que o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), a legislação brasileira – LGPD - baseia-se também no princípio do consentimento. Deste modo, o titular dos dados pessoais deverá saber a finalidade para a qual seus dados serão utilizados, bem como estar de acordo com a utilização de referidos dados. Ademais, ao titular é dado o direito de solicitar atualizações para fins de correção ou exclusão de dados tratados de forma contrária às determinações legais, dependendo, ainda, a portabilidade de dados de aprovação do titular. A LGPD também segue o Regulamento Geral de Proteção de Dados (RGPD) no tocante à definição de responsáveis, pelas empresas, para o tratamento de dados pessoais. Estes são encarregados de formular políticas de adequação à Lei e de responder sobre eventuais solicitações de caráter pessoal ou governamental. Além do aspecto técnico, as responsabilidades se estendem a ações educativas entre colaboradores da organização, bem como supervisão de riscos.[24] Insta salientar que a inclusão da proteção de dados no texto constitucional reforça a implementação da LGPD no país.[25]

---

[22] BRASIL. Planalto. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.> Acesso em: 08. abr. 2022.

[23] BERNASIUK, Helen Lentz Ribeiro. Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos. Rio de Janeiro: Lumen Juris, 2021.

[24] PIURCOSKY, Fabrício Peloso. *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. Suma neg., Bogotá, v. 10, n. 23, p. 89-99, dez. Disponível em:<http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2215910X2019000300089&lng=en&nrm=iso.>. Acesso em: 05. mai. 2021.

[25] BRASIL, Planalto. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 08. abr. 2022.

A Resolução n.º 143, de 30 de novembro de 2011, em seu artigo 4º, dispõe duas formas de busca que se constituem no uso de dados pessoais, por exemplo: o nome das partes (inciso II) e o número do CPF (inciso III)[26]. Neste sentido, a Lei Geral de Proteção de Dados Pessoais – LGPD em seu art. 5º, inciso I, define dado pessoal como aquela informação relacionada a uma pessoa natural seja ela identificada ou identificável.[27]

O tema tratado pelas disposições da LGPD foi objeto de julgamento pelo Supremo Tribunal Federal antes mesmo de sua tardia vigência. Isso porque, em sede de controle de constitucionalidade, a Corte Constitucional declarou a fundamentalidade autônoma do direito à proteção de dados pessoais no Brasil, ao tratar das medidas governamentais relativas ao enfrentamento e ao combate à pandemia da COVID-19 no nosso país.[28]

Posteriormente ao paradigmático julgamento houve no ano de 2022, a promulgação da Emenda Constitucional n.º 115/2022, que inseriu no artigo 5º, do texto constitucional o inciso LXXIX, assegurando, nos termos da lei, o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais.

Alinhando-se à maior parte das legislações sobre a matéria, o conceito de dado pessoal é compreendido na LGPD de maneira ampliada (teoria expansionista). Sempre será possível, no entanto, proceder a anonimização dos dados, o que, se realizado com êxito, afasta a incidência da legislação. De toda sorte, o que caracteriza um dado como pessoal é a relação a partir de uma análise contextual, bem como o uso e a qualidade da tecnologia empregada. Importante frisar que toda

[26] BRASIL. Art. 4.º As consultas públicas dos sistemas de tramitação e acompanhamento processual dos Tribunais e Conselhos, disponíveis na rede mundial de computadores, devem permitir a localização e identificação dos dados básicos de processo judicial segundo os seguintes critérios: (Redação dada pela Resolução nº 143, de 30.11.2011) I – número atual ou anteriores, inclusive em outro juízo ou instâncias; II – nomes das partes; III – número de cadastro das partes no cadastro de contribuintes do Ministério da Fazenda;..." CONSELHO NACIONAL DE JUSTIÇA. Resolução n. 121/2010 e n. 143/2011. Disponível em: <https://atos.cnj.jus.br/files/resolucao_143_30112011_10102012202834.pdf>. Acesso em: 07.abr. 2022.

[27] BRASIL, Planalto. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, art. 5º: Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável.

[28] BRASIL, Supremo Tribunal Federal. Medida cautelar na Ação Direta de Inconstitucionalidade n. 6.387. Relator: Ministra Rosa Weber. Julgado em: 24 abr. 2020. Disponível em: <www.stf.jus.br>. Acesso em: 08. abr. 2022.

anonimização, ou seja, essa parametrização pode ser revertida se aliada ao passar do tempo e ao inexorável avanço da técnica.

Pode-se destacar a supressão, a generalização, a randomização e a pseudoanonimização como técnicas importantes para desvincular o dado e a pessoa correspondente àquele dado. Todo o processo de anonimização acaba tornando-se precário decorrente do desenvolvimento de novas técnicas, especialmente, porque temos a criação de algoritmos para a desanonimização de bases de dados pessoais, inclusive de dados sensíveis.

Tendo em vista as várias possibilidades de reidentificação de dados anonimizados, todo e qualquer dado, ainda que anonimizado é um dado pessoal, com a possiblidade de ocorrência de diversas formas de descriminalização. A pseudoanonimização constitui um meio-termo entre o dado pessoal e o dado anonimizado. De salientar que, a depender do contexto, o dado pessoal pode se tornar um dado sensível, porquanto, torna a identificabilidade de elementos essenciais da personalidade cada vez mais plausível.

Importante destacar que os princípios norteadores previstos no artigo 6º[29], da LGPD são a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas, permeados pelo princípio da boa-fé e pelos princípios constitucionais previstos na Constituição Federal de 1988.

Da leitura de referida norma é possível verificar os desdobramentos da proteção de dados que, dentre outros direitos, podemos elencar: o livre acesso aos dados, à qualidade desses dados, à segurança, à prevenção e, merece destaque a não discriminação.

5. A divulgação de dados pessoais na rede mundial de computadores e o risco da discriminação

Conforme o anteriormente exposto dispõe o artigo 93, inciso IX da CF, que

[29] BRASIL. Planalto. Artigo 6º, da Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/2018/2018/lei/l13709.htm>. Acesso em: 08. abr. 2022.

todos os atos processuais provenientes do Poder Judiciário serão públicos, sejam eles administrativos ou judiciais. O texto constitucional consagra a publicidade de seus atos processuais, ao estabelecer que a lei possa apenas restringi-la quando da defesa à intimidade ou do interesse processual (art. 5º, LX, da CF).

A fim de dar concretude ao disposto na Constituição Federal de 1988, o Conselho Nacional de Justiça expediu a Resolução n.º 121/2010, posteriormente alterada pela Resolução n.º 143/2011, que disciplina ser direito de qualquer cidadão o acesso a dados básicos em processo judicial na internet, incluindo o nome das partes, o teor e as sentenças. A referida Resolução também prevê que esses dados sejam acessíveis, via internet, a qualquer cidadão, dispensando a demonstração de interesse na causa. Tudo dentro do que se espera sobre o agir dos agentes públicos e consectário do Estado Democrático de Direito não fosse o fato de que de outro lado LGPD resguarda direitos dos indivíduos acerca dos seus dados pessoais, alicerçando-se sobre o princípio da dignidade da pessoa humana[30]. Nesse sentido, urge confrontar as referidas bases legais com o objetivo de compreender as tensões inerentes às mesmas no contexto da era da comunicação.

Convém enfatizar que a publicização de dados pessoais no que tange a processos judiciais importa em riscos discriminatórios em diversas esferas da vida pessoal. Dentre eles, apenas a guisa de exemplo, considerando-se situações de contratação, já que, valendo-se do acesso público e facilitado por buscadores na internet ao nome de candidatos a uma vaga, o recrutador poderia verificar quais sujeitos já demandaram contra antigos empregadores na esfera da Justiça do Trabalho[31]. Sabe-se, ainda, que pessoas perdem oportunidades de trabalho apenas por terem uma ação judicial em seu nome (mesmo que não seja na esfera trabalhista como, por exemplo, uma execução fiscal, uma ação de cobrança de dívidas etc.).

A LGPD surge como um importante mecanismo para barrar a discriminação digital, conforme afirma Daniel Piñeiro Rodrigues:

---

[30] O princípio da dignidade da pessoa humana encontra-se previsto no artigo 1º, inciso III, da Constituição Federal de 1988. Referido princípio se refere à garantia das necessidades vitais de cada indivíduo. Tal princípio é um dos fundamentos do Estado Democrático de Direito.

[31] Não são poucas as reclamações contra divulgação de reclamatórias trabalhistas que têm causado problemas para admissão em empregos. Como exemplo cita-se: <https://www.reclameaqui.com.br/escavador/meus-dados-e-processos trabalhistas_X3ZFSmHcz3vV8Q4N/.>. Acesso em: 07. jun. 2022.

> Afinada a essa nova ótica, a LGPD buscou encartar verdadeira disposição antidiscriminatória, prevendo, em seus dispositivos, que os dados pessoais relativos ao exercício regular de direitos não podem ser usados em prejuízo de seu titular[32].

Assim, não se nega que a regra é a publicização dos atos judiciais, por expressa determinação constitucional. O Conselho Nacional de Justiça (CNJ) em atendimento ao previsto na Constituição Federal de 1988, conforme já referido, expediu a Resolução n.º 121/2010, posteriormente, alterada pela Resolução n.º 143/2011, que regula, dentre outras matérias, consultas públicas de acompanhamento processual na rede mundial de computadores. A normativa está assentada em alguns fundamentos e, dentre eles, os três primeiros estão diretamente ligados ao tema objeto de estudo, veja-se:

> (i) "O princípio da publicidade como garantia da prestação de contas da atividade jurisdicional"; (ii) "necessidade de divulgação dos atos processuais a fim de conferir transparência e garantir o direito de acesso à informação..." e (iii) "exercício da publicidade restrita ou especial dos atos processuais, segundo a qual a divulgação pode e deve ser restringida sempre que a defesa da intimidade ou interesse público o exigir".[33]

Nesse sentido, a referida Resolução e sua posterior alteração permite que qualquer cidadão tenha acesso a dados básicos que constem no processo judicial como, por exemplo, o nome das partes litigantes, o teor das decisões e suas respectivas sentenças, sem haver a necessidade de demonstrar o seu interesse na causa. No que concerne ainda aos advogados é autorizado o acesso à integralidade dos documentos e aos atos processuais digitais, mesmo que não possuam

---

[32] RODRIGUEZ, Daniel Piñeiro. O Direito Fundamental à Proteção de Dados Pessoais: Vigilância, Privacidade e Regulação. Rio de Janeiro: Editora Lumen Juris, 2021, p. 25.

[33] CONSIDERANDO que o Estado Democrático de Direito sob o qual é alicerçada a República Federativa do Brasil adotou o princípio da publicidade como garantia da prestação de contas da atividade jurisdicional; CONSIDERANDO a necessidade de divulgação dos atos processuais a fim de conferir transparência e garantir o direito de acesso à informação, conforme dispõe o art. 5º, XXXIII e XXXIV, b, da Constituição Federal; CONSIDERANDO que o art. 93, XI, da Constituição Federal garante o exercício da publicidade restrita ou especial dos atos processuais, segundo a qual a divulgação pode e deve ser restringida sempre que a defesa da intimidade ou o interesse público o exigir.

autorização específica para tal fim e, desde que não seja caso de sigilo ou segredo de justiça.[34]

Por tais razões, a publicidade dos atos processuais é considerada geral ou plena quando o acesso aos autos do processo, bem como os atos praticados no curso deste como audiências, sessões e julgamentos, forem acessíveis ao público em geral. Por sua vez, ocorre a publicidade restrita, específica ou especial quando o acesso for restrito aos sujeitos da relação processual[35].

Desse modo, com o escopo de dar transparência à atividade jurisdicional, os atos processuais devem, em regra, ser públicos. Em razão da utilização da tecnologia e dos meios eletrônicos o princípio da publicidade possui grande relevância pela amplitude e rapidez com que se disseminam as informações através do meio digital, asseguradas às partes a adoção de medidas conformes com a LGPD em proteção contra a discriminação digital.

6. Considerações finais

A problemática do tema abordado surge porque, de um lado, tem-se a publicidade como princípio fundamental da Administração Pública e, de outro, a necessidade de proteção de dados pessoais, ainda que seja na perspectiva de dados judiciais. Todavia, há a necessidade de se distinguir a publicidade como forma de acesso ao inteiro teor do processo pelos interessados (dimensão subjetiva, em que se demonstra quais os sujeitos principais e secundários do processo), da publicidade como um dever orientador da administração pública (dimensão objetiva, dever de informação do serviço jurisdicional). Inclusive, há que se diferenciar o que é interesse público do que interesse do público (curiosidade). A tecnologia também acaba alterando a nossa maneira de viver, na medida em que estamos em um "presente constante".

---

[34] BRASIL. Conselho Nacional de Justiça. Resolução n.º 121/2010 e n.º 143/2011. Disponível em: <https://atos.cnj.jus.br/files/resolucao_143_30112011101020122028 34.pdf>. Acesso em: 07. abr. 2022.

[35] TOURINHO FILHO, Fernando da Costa. Processo Penal, v. 1. 29 ed. rev. e atual. São Paulo: Saraiva, 2007, p. 44.

Os dados constantes em informações processuais são necessários e atendem aos princípios constitucionais, bem como as determinações do Conselho Nacional de Justiça. Todavia, a proteção de dados pessoais é também um direito constitucional onde se questiona: qual a necessidade de o número do CPF, que é um dado pessoal, estar disponível nos julgados? Para além disso, quantas formas de discriminação o indivíduo pode sofrer apenas por constarem ações judiciais em seu nome pela simples consulta no "*google*" que, muitas vezes, decorrem de decisões já transitadas em julgado enfrentando, inclusive, dificuldades para ingressar no mercado de trabalho?

Muito embora o Supremo Tribunal Federal tenha fixado o entendimento de que é incompatível com a Constituição Federal a ideia de um "direito ao esquecimento", do voto de alguns Ministros extrai-se a possibilidade de se utilizar uma "exceção de publicitação", porquanto é decorrência lógica do princípio da dignidade da pessoa humana.

Assim, vislumbra-se que uma das possibilidades de proteção de dados pessoais seria a anonimização do desse. A anonimização e pseudoanonimização (atribuição de um código ao indivíduo) se mostram como formas de garantir a preservação da identidade do sujeito, desde que observadas normas de segurança e, frise-se, não se garantindo uma segurança plena. Desse modo, espera-se que os entes públicos e privados ajam com transparência informando aos titulares dos dados acerca do armazenamento e descarte dos mesmos, bem como instruindo as pessoas que têm acesso a referidos dados sobre as formas de proteção e responsabilização em casos de eventuais abusos e negligências.

Referências bibliográficas

BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021.

BOBBIO, Norberto. **O futuro da democracia**. 7ª ed. São Paulo: Paz e Terra, 2000;
BRASIL. Planalto. **Artigo 5º, inciso XXXIII, da Constituição da República Federativa do Brasil de 1988.** Diário Oficial da República Federativa do Brasil. Brasília, DF, 05 de outubro de 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 07.abr. 2022.

BRASIL. Planalto. **Redação dada pela Emenda Constitucional nº 45, de 2004**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc45.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%2045%2C%20DE%2030%20DE%20DEZEMBRO%20DE%202004&text=Altera%20dispositivos%20dos%20arts.,A%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias>. Acesso em: 04.mai.2022.

BRASIL. Planalto. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm .Acesso em 8 abr.2022>. Acesso em: 08. abr. 2022.

BRASIL. Planalto. Consoante se verifica do art. 4º, inciso III, da Lei de Acesso à informação. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.>Acesso em: 08. abr. 2022.

BRASIL, Superior Tribunal de Justiça. **Recurso Especial n. 1.334.097/RJ**. Relator: Min. Luis Felipe Salomão, 28-05-2013. Disponível em: <http://www.stj.jus.br>. Acesso em: 08. abr. 2022.

BRASIL, Supremo Tribunal Federal. **Recurso Extraordinário nº 1.010.606/RJ**. Relator: Min. Dias Toffoli. Julgado em: 11 fev. 2021. Disponível em: <www.stf.jus.br>. Acesso em: 08. abr. 2022.

BRASIL, Supremo Tribunal Federal. **Medida cautelar na Ação Direta de Inconstitucionalidade n.º 6.387.** Relator: Ministra Rosa Weber. Julgado em: 24 abr. 2020. Disponível em: <www.stf.jus.br>Acesso em: 08. abr. 2022.

BRASIL. Planalto. Artigo 6º, da Lei n.º 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD).** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.>. Acesso em: 08. abr. 2022.

BRASIL. **Conselho Nacional de Justiça**. Resolução n. 121/2010 e n. 143/2011. Disponível em: <https://atos.cnj.jus.br/files/resolucao_143_30112011_10102012202834.pdf.>. Acesso em: 07. abr. 2022.

BRASIL. Conselho Nacional de Justiça. **Enunciado trata do direito ao esquecimento na sociedade da informação**. Disponível em: <https://www.cjf.jus.br/cjf/noticias/2013/abril/enunciado-trata-do-direito-ao esquecimento-na-sociedade-da-informacao> Acesso em: 07.abr.2022.

CARVALHO, Matheus. **Manual de Direito Administrativo**. 7. ed. rev., ampl. e atual.- Salvador: JusPODIVM, 2020.

COPETI, André. J.J. GOMES CANOTILHO (et al). **Comentários à Constituição**. São Paulo: Saraiva/ Alamedina, 2013.

JUNIOR, Fredie Didier. **Teoria geral do processo e processo de conhecimento.** 7 ed. Bahia: Juspodivm, 2007.

KHOURI, Paulo Roberto Roque Antonio. O direito ao esquecimento na sociedade de informação e o enunciado 531 da VI Jornada de Direito Civil. **Revista de Direito do Consumidor.** São Paulo, v. 22, n. 89, pp. 463-465, set./out. 2013.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 1 ed. São Paulo: Saraiva, 2007.

MONTENEGRO FILHO, Misael. Curso de direito processual civil v. 1: **Teoria geral do processo e processo de conhecimento.** 5 ed. São Paulo: Atlas, 2009.

PIURCOSKY, Fabrício Peloso. *et al*. A Lei Geral de Proteção de Dados Pessoais em Empresas Brasileiras: **uma análise de múltiplos casos**. Suma neg., Bogotá, v. 10, n. 23, pp.89-99, dez. Disponível em: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2215910X2019000300089&lng=en&nrm=iso. >. Acesso em: 05. mai. 2021.

PINHEIRO, Patricia Peck. **Direito Digital**. São Paulo: Saraiva Jur, 7ª, ed. 4ª tiragem, 2021;
RODRIGUEZ, Daniel Piñeiro. O Direito Fundamental à Proteção de Dados Pessoais: **Vigilância, Privacidade e Regulação**. Rio de Janeiro: Editora Lumen Juris, 2021.

SARLET, Ingo Wolfgang; Ferreira Neto, Arthur M. **O direito ao "esquecimento" na Sociedade de Informação**; Porto Alegre: Livraria do Advogado, 2019.

SILVEIRA, Beatriz de Oliveira da et. al. **O direito ao esquecimento para a sociedade digital.** A Leitura: Caderno da Escola Superior da Magistratura do Estado do Pará, Belém, v.7, n. 12, pp. 50-60, maio, 2014.

TOURINHO FILHO, Fernando da Costa. **Processo Penal**, v. 1. 29 ed. rev. e atual. São Paulo: Saraiva: 2007.

TUCCI, Rogério Lauria. **Direitos e Garantias Individuais no Processo Penal Brasileiro**. 3. ed. São Paulo: Saraiva: 2009.

THEODORO JÚNIOR, Humberto. Curso de Direito Processual Civil: **Teoria geral do direito processual civil e processo de conhecimento.** v. I. 50 ed. Rio de Janeiro: Forense, 2009.

WAMBIER, Luiz Rodrigues. **Curso Avançado de Processo Civil**. Vol. I, 5 ed., São Paulo: Revista dos Tribunais, 2013.

10. A NECESSIDADE DE PROTEÇÃO DOS DADOS PESSOAIS NO USO DE TECNOLOGIAS PARA PROMOÇÃO DO DIREITO À SEGURANÇA PÚBLICA

https://doi.org/10.36592/9786581110994-10

Tapir Rocha Neto[1]

Camila Trindade Galvão[2]

Sumário

1. Introdução

O avanço tecnológico ocorre em tamanha velocidade que diversas ferramentas já estão sendo utilizadas por entes estatais para fins de segurança pública sem que haja uma regulamentação específica para orientar o seu emprego. Diante deste cenário, no Brasil, cada unidade federativa está desenvolvendo seus sistemas e estabelecendo suas contratações com outras instituições públicas e privadas, no intuito de prestar um serviço de segurança mais eficaz e eficiente para a população.

Todavia, a ânsia de estar à frente dos crimes e o deslumbramento com relação aos infinitos poderes possibilitados pela tecnologia podem estar incentivando a supressão de direitos humanos cujo histórico de desrespeito já demonstrou acarretar retrocesso social.

---

[1] Doutorando em Ciências Criminais na Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Mestre em Ciências Criminais pela PUCRS. Especialista em Ciências Penais pela PUCRS. Professor convidado de cursos de Extensão e de Pós-Graduação da Universidade de Caxias do Sul (UCS) com ênfase em Direito Penal Econômico. Parecerista da Revista Brasileira de Ciências Criminais (RBCCRIM). Advogado criminalista sócio do escritório Andrei Zenkner Schmidt Advogados Associados.
E-mail: tapirneto@gmail.com. Lattes: http://lattes.cnpq.br/3070048405534188

[2] Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Bolsista CAPES. Pesquisadora no Tecnopuc Law. Advogada e sócia do escritório Galvão Advogados Associados.
E-mail: camila@galvaoadvogados.net. Lattes: http://lattes.cnpq.br/5642729982602808

A questão se torna ainda mais problemática na medida em que a Lei n. 13.709, de 2018, conhecida como Lei Geral da Proteção de Dados (LGPD), promulgada para impor limites ao tratamento de dados pessoais, excluiu de sua abrangência o tratamento de dados realizado no âmbito da segurança pública, defesa nacional, atividades de investigação e repressão de infrações penais, abrindo uma lacuna legislativa que pode ser perigosa.

Deste modo, a presente pesquisa tem o objetivo de desvendar as seguintes hipóteses: se a utilização de tecnologia para fins de segurança pública possui outras limitações previstas no ordenamento jurídico atual para coibir a invasão das garantias individuais e/ou se há necessidade de algum aperfeiçoamento no regramento interno brasileiro. O mapeamento de ferramentas utilizadas pelos governos do Brasil e de outros países, em conjunto com a revisão bibliográfica de doutrinas e de julgado paradigma do Supremo Tribunal Federal, parece relevante para diagnosticar (e assim evitar) eventuais excessos e violações à proteção de dados pessoais, à privacidade e à intimidade decorrentes do uso indiscriminado de tecnologias por agentes de segurança pública.

Assim, o primeiro item do presente estudo examina exemplos que demonstram o quanto a tecnologia bem empregada pode agregar na segurança da sociedade. No segundo item, listam-se alguns impactos já mapeados em casos práticos, avaliando-se as distorções que o uso ilimitado da tecnologia pode provocar. No último tópico, problematiza-se a complexidade jurídica das situações avaliadas e, a partir de uma revisão bibliográfica, busca-se identificar os limites constitucionais que vedam o excesso por parte do Estado, encontrando o equilíbrio entre proteger os cidadãos sem, contudo, desenvolver uma permanente vigilância, isto é, uma devassa que viole a proteção aos dados pessoais, a privacidade e a intimidade, o que, em última análise, venha a tolher a própria noção de existência do ser humano.

2. O emprego de tecnologias como aliadas na promoção do direito à segurança pública

A combinação de tecnologias atualmente disponíveis, tais como inteligência artificial potencializada pelo *machine leargning*, *big data* e a internet das coisas,

cidades inteligentes, multibiometria, computação cognitiva, serviços em nuvem, entre outros, permitem infinitas possibilidades de controle e vigilância, as quais não tardaram a chamar a atenção de agentes de segurança pública.

É certo que todos os cidadãos desejam sentir-se seguros em suas cidades. Bauman explica que o surgimento da sensação de medo que impera nos centros urbanos contemporâneos perpassou pela substituição do axioma da solidariedade pelo atual individualismo da competição[3]. As pessoas veem, nos outros, indivíduos capazes de subtrair os bens que seriam necessários à fruição plena de sua vida, do seu sucesso pessoal, e passam então a projetar a existência da figura de um delinquente que, por causar temor, deve ser combatido[4].

A sensação de insegurança atingiu as pessoas e alcançou a própria pauta de medidas estatais. Com o objetivo de amenizar o medo que assola a sociedade contemporânea, milhares de tentativas de soluções estão sendo desenvolvidas e implementadas para tornar mais eficiente o trabalho da polícia e otimizar a gestão dos recursos públicos.

Entretanto, é preciso cuidado na avaliação das tecnologias que vêm sendo utilizadas pelo poder público persecutório para solucionar a questão da segurança pública, sobretudo em virtude dos "efeitos colaterais" que seu uso pode acarretar. Os novos sistemas têm permitido desde a integração de bancos de dados[5] de órgãos governamentais até apoio tático para operações policiais.

A tecnologia que mais impressiona, tanto em razão de sua eficiência quanto em razão de seu grau de invasão, é o reconhecimento facial. A conexão dos bancos

---

[3] BAUMAN, Zygmunt. Confiança e medo na cidade. Tradução de Eliana Aguiar. Rio de Janeiro: Jorge Zahar Ed., 2009, p. 17.

[4] A aguda e crônica experiência da insegurança é um efeito colateral da convicção de que, com as capacidades adequadas e os esforços necessários, é possível obter uma segurança completa. Quando percebemos que não iremos alcançá-la, só conseguimos explicar o fracasso imaginando que ele se deve a um ato mau e premeditado, o que implica a existência de algum delinquente. Poderíamos dizer que a insegurança moderna, em suas várias manifestações, é caracterizada pelo medo dos crimes e dos criminosos. Suspeitamos dos outros e de suas intenções, nos recusamos a confiar (ou não conseguimos fazê-lo) na constância e na regularidade da solidariedade humana. *In:* BAUMAN, Zygmunt. Confiança e medo na cidade. Tradução de Eliana Aguiar. Rio de Janeiro: Jorge Zahar Ed., 2009, p. 15.

[5] Apesar de parecer algo simples, a cultura dos órgãos públicos era de utilizar os sistemas cujo melhor valor era vencedor da licitação. Isto, por vezes, ocasionava a descontinuidade dos sistemas e a dificuldade de consulta nos bancos de dados legado, como demonstra o exemplo noticiado em: <http://www.abtlp.org.br/index.php/tecnologias-da-prf-seopi-e-senasp-sao-integradas-para-operacionalizar-o-maior-sistema-de-monitoramento-viario-do-pais/ .>. Acesso em: 23/06/2022.

de dados de diversas organizações privadas e governamentais, tais como órgãos emissores de registro civil (RG) e carteira de habilitação para dirigir (CNH), permite que as máquinas "treinem"[6] para reconhecer características dos rostos humanos, tais como distância entre os olhos, formato do queixo, entre outras peculiaridades. Aliando isto à multibiometria[7], permite-se uma maior precisão na identificação de indivíduos em perícias criminais de maneira instantânea.

Dotados destas informações, câmeras de vigilância, drones e até mesmo *smart* óculos se tornam capazes de vasculhar todos os bancos de dados até identificar similitude de um suspeito com sua correspondente identidade. E tudo isso pode ser feito em tempo real, durante uma investigação ou perseguição, pois leva poucos segundos para indicar um resultado.

Só na cidade de Salvador (BA), em menos de dois anos, 264 foragidos da polícia foram localizados pelas câmeras de vigilância com reconhecimento facial[8]. No Ceará, um latrocínio foi desvendado em apenas uma manhã com o apoio desta tecnologia[9] – que se não existisse, demandaria o envio de ofícios a diversos órgãos e muitos dias até a conclusão das diligências (que poderiam resultar infrutíferas ou

---

[6] HOFFMANN-RIEM, ao abordar sobre aprendizado de máquina (*machine learning*), explica que: "Cada vez mais, os sistemas de aprendizagem algorítmica são capazes de se adaptar a novas situações problemáticas de forma independente e de continuar a escrever seus próprios programas. Os algoritmos de aprendizagem são assim programados não só para resolver problemas específicos, mas também para aprender como os problemas são resolvidos. Eles devem então ser capazes de se desenvolver independentemente da programação humana. Falamos de Deep Learning quando o sistema aprende a compreender inter-relações, estruturas e arquiteturas sem intervenção humana adicional, de tal forma que pode melhorar seu desempenho de forma independente. A capacidade de aprendizagem do sistema condiciona assim seu processo de forma independente. As etapas individuais como tais permanecem deterministicamente controladas, mas existem em grande número e muitas vezes estão dinamicamente ligadas umas às outras, de modo que é difícil ou, em muitos casos, quase impossível reconstruir a determinação. Tais programas, que dependem da capacidade de aprender, são utilizados, por exemplo, no processamento de imagem e fala, robótica e prognóstico." (HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital. Transformação Digital – Desafios para o Direito. Rio de Janeiro: GEN-FORENSE, 2021, p. 36).

[7] Mapeamento de diversos dados do indivíduo, que podem combinar características faciais, impressões digitais, análise da íris, varredura de retina, voz, geometria da mão e termogramas faciais e até dados genéticos. (ARAÚJO JÚNIOR, Jozias Rolim de. Reconhecimento multibiométrico baseado em imagens de face parcialmente ocluídas. Dissertação [Mestrado em Ciências] – Programa de Pós-Graduação em Informação, Escola de Artes, Ciências e Humanidades. Universidade de São Paulo: 2018).

[8] SECOM, Bahia apresenta resultado do Reconhecimento Facial na China. Publicado em 19/05/2019. Disponível em: <https://www.ssp.ba.gov.br/2022/06/12517/Homicida-e-traficante-sao-flagrados-pelo-Reconhecimento-Facial.html>. Acesso em: 23/06/2022.

[9] SSPDS, Secretaria da Segurança Pública e Defesa Social do Governo do Estado do Ceará. Big Data da Segurança Pública, Spia e videomonitoramento da SSPDS são utilizados na elucidação de crime em Fortaleza. Publicado em: 11/12/2019. Disponível em:

permitir a fuga do autor do crime). No Carnaval da Bahia, um suspeito foi reconhecido mesmo fantasiado de mulher e em meio a uma multidão[10], tamanha a precisão das ferramentas.

Quando um *site* solicita provar que "não sou um robô", indicando "identifique as imagens com carros"[11] ou ainda quando "ajude-nos a melhorar o google fotos"[12], na verdade, além de provar que não é um robô operando, também se está demonstrando para a máquina como humanos podem reconhecer estas figuras, ainda que nunca tenham visto aquela imagem específica. A partir destas classificações, a máquina "aprende" quais características em comum existem entre os carros indicados por humanos e cria sua própria "imagem" correspondente a um objeto[13] (que também pode ser um caractere ou um rosto).

Desta forma, além de reconhecer rostos, a inteligência artificial pode reconhecer placas de carro com grande velocidade, o que também auxilia na resolução de crimes. No Ceará, com a utilização do sistema Spia, o tempo médio de recuperação de um veículo furtado reduziu para 5-10 minutos[14], pois, tão logo a

---

<https://www.ceara.gov.br/2019/12/13/big-data-da-seguranca-publica-spia-e-videomonitoramento-da-sspds-sao-utilizados-na-elucidacao-de-crime-em-fortaleza/.> Acesso em 23/06/2022.

[10]ALVES, Alan Tiago. Flagrado por câmera vestido de mulher no carnaval na BA matou homem após vítima passar perto dele de moto em alta velocidade. G1. Publicado em: 07/03/2019. Disponível em: <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>. Acesso em: 23/06/2022.

[11]DZIEZA, Josh. Why Captchas Have Gotten So Difficult: Demonstrating you're not a robot is getting harder and harder. The Verge. Publicado em 01/02/2019. Disponível em: <https://www.theverge.com/2019/2/1/18205610/google-captcha-ai-robot-human-difficult-artificial-intelligence>. Acesso em 23/06/2022.

[12]VINCENT, James. Google wants you to help train its AI by labeling images in Google Photos: A new optional feature in Google Photos on Android. The Verge. Publicado em: 11/11/2020. Disponível em: <https://www.theverge.com/2020/11/11/21559930/google-train-ai-photos-image-labelling-app-android-update>. Acesso em: 23/06/2022.

[13]Sobre o ponto, Pedro Domingos: "Todo algoritmo tem uma entrada e uma saída: os dados entram no computador, o algoritmo faz o que precisa com eles, e um resultado é produzido. O *machine learning* faz o contrário: entram os dados e o resultado desejado, e é produzido o algoritmo que transforma um no outro. Os algoritmos de aprendizado – também conhecidos como aprendizes – são aqueles que criam outros algoritmos. Com o machine learning, os computadores escrevem seus próprios programas, logo não precisamos mais fazê-lo. – No exemplo descrito nesta pesquisa, o dado seria "carro" e o resultado esperado são as diversas imagens apontadas como carros. Assim, o algoritmo, por método de tentativa e erro, cria seu caminho até que consiga chegar ao resultado "carro" em imagens semelhantes aos resultados esperados." (DOMINGOS, Pedro. O Algoritmo Mestre: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. 1ª edição. São Paulo: Novatec, 2017, p. 20).

[14] REDAÇÃO. Média de tempo para recuperar veículo no Ceará é de 5 a 10 minutos. Diário do Nordeste. Publicado em: 14/07/2019. Disponível em:

ocorrência é comunicada à polícia por meio de aplicativo, as câmeras de videomonitoramento dotadas de inteligência artificial identificam onde o veículo está transitando e rapidamente a equipe policial mais próxima pode se conduzir até o local, permitindo a recuperação do bem e a submissão do responsável a processo penal perante o Poder Judiciário. O superintendente de Pesquisa e Estratégia de Segurança Pública (Supesp), Aloísio Lira, explica que os carros roubados normalmente eram utilizados para realizar outros delitos, de modo que a tecnologia também permite a interceptação do veículo antes que um novo crime ocorra, evitando a prática de outros delitos.

Além disso, ainda há possibilidade de videomonitoramento com tecnologia infravermelha e sensores térmicos [15], que identificam invasões mesmo que os envolvidos não estejam no campo de visão das câmeras e que também sabem diferenciar quando se tratar de gatos e animais que circulam pelas propriedades, evitando que o alarme soe desnecessariamente.

Outra funcionalidade interessante é a que faz monitoramento de veículos e gerencia o comportamento de motoristas[16], com alertas em casos de sonolência, de motoristas que dirigem e falam ao celular ou fumam, além de outras transgressões das regras de trânsito, com o objetivo de reduzir a quantidade e a gravidade dos acidentes.

As inovações acima descritas foram viabilizadas pela combinação [17] de inteligência artificial com a enorme gama de dados (*big datas*) atualmente disponíveis para consulta e treinamento das máquinas – cuja acessibilidade se popularizou a partir (i) do armazenamento em nuvem (que não requer dispositivo físico e consequentemente é mais barato), (ii) da *internet* das coisas (e dos corpos)

<https://diariodonordeste.verdesmares.com.br/seguranca/media-de-tempo-para-recuperar-veiculo-no-ceara-e-de-5-a-10-minutos-1.2123188>. Acesso em: 23/06/2022.

[15] Revista Segurança Eletrônica. Tecnologia infravermelha pode oferecer proteção de perímetro acessível. Disponível em: <https://revistasegurancaeletronica.com.br/tecnologia-infravermelha-pode-oferecer-protecao-de-perimetro-acessivel/.>. Acesso em: 23/06/2022.

[16] Revista Segurança Eletrônica. Dahua Technology lança soluções em vídeo monitoramento para avaliar comportamento do motorista. Disponível em: <https://revistasegurancaeletronica.com.br/solucoes/>. Acesso em: 23/06/2022.

[17] GHOSH, Iman Ghosh. 4 key areas where AI and IoT are being combined. Global Technology Governance Summit. World Economic Forum. Publicado em: 15/03/2021. Disponível em: <https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/>. Acesso em: 23/06/2022.

que permite acessar e compartilhar a informação em qualquer dispositivo, e (iii) da tecnologia 5G, que dará mais velocidade no compartilhamento de um maior número de dados e em maior abrangência.

A enorme disponibilidade de dados leva inclusive à possibilidade de evoluir das análises estatísticas para o policiamento preditivo [18], baseado em dados quantitativos e qualitativos para tentar prever crimes e definir as melhores estratégias de gestão pública, com um nível de detalhamento muito maior e mais preciso do que se podia até então. Isso tudo tem proporcionado uma realocação dos recursos humanos e táticos em regiões mais perigosas, ensejando maior eficiência na prestação do serviço de segurança pública, na medida em que se torna possível resolver crimes quase em tempo real e antecipar as ações policiais para até mesmo impedir a consumação dos delitos.

Apesar dos incontestáveis benefícios que as tecnologias propiciam para o bem-estar coletivo, sobretudo com relação à proteção dada pelo Estado aos cidadãos contra os perigos e os danos causados por outros indivíduos, mister avaliar com cautela o domínio de tantos dados e informações, sob pena de o mau uso direcionar a sociedade para um estado de vigilância e assim viabilizar um controle totalitário por parte dos que participam do governo, cerceando e violando liberdades individuais.

3. Análise de impactos a partir de casos práticos

A tecnologia agrega eficiência, agilidade e eficácia nas ações de segurança pública, conforme verificou-se nos exemplos acima listados. Mas com o bônus surge um ônus que não pode ser desprezado, sobretudo quando se aborda intervenção estatal na esfera individual, por isso se torna fundamental avaliar os riscos inerentes ao mau uso que pode ser feito das combinações tecnológicas atualmente disponíveis.

[18] MEIJER, Albert. WESSELS, Martijn. Predictive Policing: Review of Benefits and Drawbacks, International Journal of Public Administration, Volume 42, Ed. 12, P. 1031-1039, Fev. 2019. DOI: https://doi.org/10.1080/01900692.2019.1575664. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664>. Acesso em: 23/06/2022.

Importante destacar que aqui não se vê a tecnologia como um "mal" necessário ou uma maldição que precisa ser evitada: o que se abordará neste trabalho é o abuso que o humano pode fazer a partir do poder que a tecnologia concede – poder este que deve ser usado para fins sociais pertinentes, em consonância com os direitos e garantias fundamentais.

3.1. Risco de abuso de autoridade

O Center on Privacy & Technology at Georgetown Law[19] realizou, no ano de 2016, um estudo a respeito do uso policial de reconhecimento facial por combinações tecnológicas sem regulamentação. A investigação apontou, dentre outras informações, que, de 52 (cinquenta e duas) agências americanas, apenas uma proibia expressamente seus oficiais de utilizar a tecnologia para rastrear indivíduos em decorrência de sua atividade política, religiosa ou outra liberdade de expressão protegida.

No mesmo ano, o *site* The Associated Press[20] denunciou que policiais dos Estados Unidos da América utilizavam bancos de dados oficiais para obter informações a respeito de parceiros românticos, negócios, vizinhos, jornalistas, entre outros, por motivos alheios ao trabalho.

Tais eventos são claros exemplos de abusos que devem ser devidamente sopesados. Isso porque, de um lado, demonstram que a instrumentalização da função pública em um proveito privado ilegítimo não é algo alheio à realidade. E, de outro, porque revelam que a concentração de tantos dados sobre a vida das pessoas pode ser utilizada para fins estranhos à segurança pública, caso não haja regulação e fiscalização dos acessos aos dados disponíveis.

3.2. Risco de ataques cibernéticos

---

[19] GARVIE, Claire. et. al. *The Perpetual Line-Up: Unregulated Police Face Recognition In America. Center on Privacy & Technology at Georgetown Law*. Out, 2016. Disponível em: <https://www.perpetuallineup.org/>. Acesso em: 23/06/2022.

[20] SADIE GURMAN, Sadie. AP: *Across US, police officers abuse confidential databases. The Associated Press*. Publicado em 28/09/2016. Disponível em: <https://apnews.com/article/699236946e3140659fff8a2362e16f43>. Acesso em 23/06/2022.

Outro risco muito presente é de ataques *hackers* aos bancos de dados. Desde o advento da Lei Geral da Proteção de Dados (Lei nº 13.709/2018[21]), diversos órgãos estatais brasileiros foram objeto de ciberataques[22], dentre eles o Superior Tribunal de Justiça, o Governo do Distrito Federal, o Ministério da Saúde e, posteriormente, o Tribunal de Justiça do Rio Grande do Sul, cujo ataque foi de maior extensão, ensejando limitações sistêmicas por mais de 30 dias[23].

Em junho de 2019, o Washinton Post veiculou a notícia[24] de que um banco de dados da agência de Alfândega e Proteção de Fronteiras dos Estados Unidos foi violado, ocasião em que vídeos e fotos de quase 100 mil pessoas, bem como placas de veículos, foram acessados e capturados para identificar indivíduos que entram e saem dos Estados Unidos (dentre as quais, muitos estrangeiros). O ataque ocorreu, pois, uma empresa subcontratada transferiu as imagens para sua própria rede, que veio a ser invadida. Tal situação evidenciou a vulnerabilidade da proteção dos dados armazenados pelo ente público.

Não bastasse a gravidade dos ataques ocorridos, a problemática envolvendo dados pessoais e multibiométricos de uma população exige uma resolução mais complexa, tendo em vista que hoje os dados biométricos são utilizados para desbloquear telefones pessoais, efetuar pagamentos e transações bancárias, exercer a e-cidadania por meio de serviços disponibilizados na plataforma "gov.br", entre outros. Diferente do que pode ocorrer com um cartão de crédito ou um *whatsapp* clonados, os quais são de fácil substituição, uma vez clonados dados biométricos,

---

[21] BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral da Proteção de Dados (LGPD). Diário Oficial da União. Brasília, 14/08/2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23/06/2022.

[22]PERON, Isadora Peron. RIBEIRO, Marcelo. Di Cunto, Raphael Di Cunto. Além do STJ, outros órgãos sofrem tentativas de ataques de hackers. Valor Econômico. Brasília: Nov, 2020. Disponível em: <https://valor.globo.com/politica/noticia/2020/11/05/alm-do-stj-outros-rgos-sofrem-tentativas-de-ataques-de-hackers.ghtml>. Acesso em: 23/06/2022.

[23] Suspensos em razão da pandemia, prazos de processos físicos são retomados no TJ. Correio do Povo, 2021. Disponível em: <https://www.correiodopovo.com.br/not%C3%ADcias/geral/suspensos-em-raz%C3%A3o-da-pandemia-prazos-de-processos-f%C3%ADsicos-s%C3%A3o-retomados-no-tj-1.635155>. Acesso em: 23/06/2022.

[24] HARWELL, Drew. FOWLER, Geoffrey A. U.S. *Customs and Border Protection says photos of travelers were taken in a data breach. The Washington* Post. Publicado em 10/06/2019. Disponível em: <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/>. Acesso em: 23/06/2022.

perde-se a identidade necessária para exercer a cidadania digital e, obviamente, não há como providenciar uma nova.

3.3. Risco de espionagem

Assim como no exemplo relatado acima, denota-se que boa parte das tecnologias utilizadas na segurança pública é oriunda de parcerias realizadas com empresas privadas, que acabam por ter acesso a toda base de dados da população que o governo possui. Apesar de existirem cláusulas contratuais de confidencialidade, a verdade é que não se tem pleno controle do que é feito com estes dados. A título de exemplo, cita-se a tecnologia empregada pela polícia de Salvador (BA), que utiliza o *software* de reconhecimento facial desenvolvido pela empresa Huawei[25], a qual responde por denúncias de fraude bancária, roubo de segredos industriais e espionagem para o governo chinês, já tendo sido banida por diversos países[26].

Tais denúncias, ainda inconclusivas, denotam a necessidade de se ter domínio da tecnologia e dos fluxos de trabalho das empresas parcerias, para que ao menos seja possível auditar e fiscalizar possíveis compartilhamentos indevidos de informações.

3.4. RISCOS DE IMPRECISÃO DOS ALGORITMOS

Empresas como Google e Facebook possuem excelentes ferramentas de reconhecimento facial, porém são inúmeras as vezes que indicam uma pessoa totalmente diferente da que está na foto ou no vídeo. Os algoritmos utilizados atualmente podem ser muito bons, mas não são infalíveis.

---

[25] SECOM, Bahia apresenta resultado do Reconhecimento Facial na China. Publicado em 19/05/2019. Disponível em: <https://www.cn1.com.br/noticias/1/62502,bahia-apresenta-resultado-do-reconhecimento-facial-na-china.html>. Acesso em: 23/06/2022.

[26] REDAÇÃO. *Huawei: qué países prohibieron la tecnología del gigante chino, el segundo mayor productor de celulares del mundo*. BBC News. Publicado em 28/11/2018. Disponível em: <https://www.bbc.com/mundo/noticias-46379805>. Acesso em: 23/06/2022.

Ainda que a tecnologia hoje tenha alto grau de acurácia, no Rio de Janeiro, uma mulher foi levada para a delegacia após ser identificada como foragida por uma das câmeras instaladas nas ruas. Ao chegar no distrito policial, as autoridades perceberam que se tratava de um engano – até mesmo porque a suposta foragida já estava presa. Ou seja, além da imprecisão do reconhecimento facial, o banco de dados estava desatualizado [27] . Em outro caso, um cidadão de 25 anos com necessidades especiais teve armas apontadas para sua cabeça até que os policiais percebessem que se tratava de um engano da tecnologia[28].

Veja-se que a tecnologia pode induzir a erros que, a depender do contexto de abordagem, podem levar a situações irremediáveis. Neste caso, é importante treinar o humano, usuário da tecnologia, para saber criticar a informação que lhe for fornecida, necessitando, para tanto, que as forças policiais tenham capacitação acerca das possíveis falhas e limitações das ferramentas, bem como façam uma validação das informações apontadas pela máquina, para somente após definir o tipo de abordagem que será feita ao sujeito.

3.5. Risco de perseguição

Em Hong Kong, na China, onde a vigilância estatal é ostensiva, manifestantes utilizam máscaras para cobrirem seus rostos nas ruas. O governo chinês inclusive proibiu manifestações públicas com uso de máscaras, justamente para não perder a possibilidade de identificação dos manifestantes e ter controle total sobre as ações passadas, atuais e futuras das pessoas. A intenção dos cidadãos mascarados, para muito além de se proteger das bombas de gás lacrimogênio, é especialmente evitar sua identificação, pois possuem o receio de sofrerem perseguição política pelo uso

[27]LAVADO, Thiago. Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debate sobre limites da tecnologia. G1. Publicado em 21/02/2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml>. Acesso em: 23/06/2022.

[28] PALMA, Amanda. PACHECO, Clarissa. Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA. Correio 24 horas. Publicado em: 05/01/2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/entenda-como-funciona-o-reconhecimento-facial-que-ajudou-a-prender-mais-de-100-na-ba>/. Acesso em: 23/06/2022.

indevido de seus dados pessoais[29].

3.6. RISCO DE DISCRIMINAÇÃO

O policiamento preditivo leva em consideração dados de crimes passados para tentar prever quais locais ou perfis de pessoas que possuem tendência para criminalidade. A prática pode ser altamente discriminatória[30]. Isso porque os algoritmos se utilizam de características comuns entre os dados analisados (fatos do passado) para indicar suas previsões. Assim, se, por exemplo, houver altos índices de crimes cometidos por homens negros, o algoritmo pode tender a acreditar que um homem negro tem mais chances de cometer crimes que mulheres ou que homens brancos, quase como um determinismo. Todavia, sabe-se que não é a cor da pele da pessoa que a condicionará ao cometimento de crimes, mas, devido à opacidade sobre o aprendizado dos algoritmos, situações como esta podem ocorrer, ainda que o critério cor da pele não seja uma característica programada para ser levada em consideração – como no famoso caso State v. Loomis[31], no qual a Suprema Corte dos EUA discutiu o enviesamento do *software* COMPAS[32].

Além disso, a tendência é que esta situação acarrete uma redundância: policiamento ostensivo em determinadas áreas e grupos de suspeitos poderá levar a uma maior constatação de crimes nestes focos, que farão com que os bancos de dados sejam alimentados com estes novos delitos, reforçando a crença sobre o risco ser maior nestes locais/grupos e, consequentemente, ensejando mais vigilância

[29] PRESSE, France. Manifestantes desafiam a lei usando máscaras em Hong Kong. G1. Publicado em: 06/10/2019. Disponível em: <https://g1.globo.com/mundo/noticia/2019/10/06/manifestantes-desafiam-a-lei-usando-mascaras-em-hong-kong.ghtml>. Acesso em: 23/06/2022.
[30] BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). Inteligência artificial e Direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2. ed., 2020, p. 700-710.
[31] STATE v. Loomis: *Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing. 130 Harvard Law Review*, 1530. Mar, 2017. Disponível em: <https://harvardlawreview.org/2017/03/state-v-loomis/>. Acesso em 23/06/2022.
[32] Sigla para Correctional Offender Management Profiling for Alternative Sanctions. Para mais informações, examinar: FERRARI, Isabela. Justiça Digital. 1ª edição. São Paulo: Thomsom Reuters Brasil, 2020, p. 86.

sobre eles[33].

3.7. Risco de inversão da lógica de presunção de inocência

Na medida em que os dados de civis passam a ser compartilhados com bancos de dados policiais, todos se tornam suspeitos. Para a análise de qualquer reconhecimento facial, o algoritmo presume que todos constantes no banco de dados são culpados, comparando os dados de civis que nunca praticaram nenhuma infração com o do suspeito procurado, desconsiderando somente se não houver alta probabilidade de correspondência entre as características analisadas (o que, como já visto, não é seguro, mas foi suficiente para constranger inocentes sem qualquer indício de envolvimento com crime, como já relatado anteriormente). A situação ainda se agrava, pois, na maioria das vezes, os envolvidos nem ficam sabendo que sua foto coletada para o RG foi utilizada em uma investigação policial sem qualquer vestígio de seu envolvimento no delito investigado.

No Brasil, em diversas cidades ocorreu um monitoramento intenso em festejos como Carnaval[34], envolvendo pessoas de todas as idades, inclusive crianças, altamente vigiadas, sem qualquer motivo para estarem sendo objeto de uma investigação policial em massa. Deste modo, verifica-se que, apesar de ser um grande passo para resguardar a segurança pública, a tecnologia provoca efeitos que demandam o cotejo entre direitos fundamentais em suas diferentes dimensões.

Todo esse contexto exige amplo debate coletivo para se estabelecer uma devida regulamentação, já que, conforme veremos a seguir, mesmo com o advento

---

[33] KUNICHOFF, Yana. SIER, Patrick. *The Contradictions of Chicago Police's Secretive List. Chicago magazine*. Publicado em: 21/08/2017. Disponível em: <https://www.chicagomag.com/city-life/august-2017/chicago-police-strategic-subject-list/>. Acesso em 23/06/2022.

[34] CRUZ, Elaine Patricia. Polícia usa sistema de reconhecimento facial no carnaval de São Paulo. Agência Brasil. São Paulo. 21/02/2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-02/policia-usa-sistema-de-reconhecimento-facial-no-carnaval-de-sao-paulo> e AVENDAÑO, Ana Clara; MENESES, Celimar de. Reconhecimento facial será utilizado pela primeira vez no carnaval. Correio Braziliense. 21/02/2020. Disponível em:<https://www.correiobraziliense.com.br/app/noticia/cidades/2020/02/21/interna_cidadesdf,829615/reconhecimento-facial-sera-utilizado-pela-primeira-vez-no-carnaval.shtml>. Acesso em: 23/06/2022.

da Emenda Constitucional nº 115, de 2022[35], que alçou à condição de direito fundamental a "proteção dos dados pessoais, inclusive nos meios digitais", o ordenamento jurídico brasileiro ainda não está amparado para coibir casos de extrapolação no uso da tecnologia pelos órgãos de segurança pública.

4. Limitações jurídicas à luz dos direitos fundamentais

Não há, hoje, no ordenamento brasileiro, normatização específica sobre o uso destas tecnologias pelos entes públicos no âmbito da segurança pública. Inclusive, a Lei Geral da Proteção de Dados excluiu este setor do seu foco de regulação (art. 4ª, III, a da Lei 13.709/2018), abrindo um leque de vulnerabilidades cuja neutralização deve ser demandada pela comunidade jurídica e pela sociedade em geral[36]. Até mesmo a Autoridade Nacional de Proteção de Dados (ANPD) ao emitir seu "Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público" em janeiro de 2022, ressalvou não se aplicar à segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais[37].

---

[35] BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União. Brasília, em 10/02/2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1>. Acesso em: 23/06/2022.

[36] PEREIRA, Fabio Luiz Barboza. SILVA, Cecília Alberton Coutinho. A Regulação Do Reconhecimento Facial E Seus Impactos Para Os Setores Público E Privado No Brasil: Uma Análise Comparativa Internacional. *In:* FRANCOSKI, Denise de Souza Luiz. TASSO, Fernando Antonio. A Lei Geral De Proteção De Dados Pessoais: Aspectos práticos e teóricos relevantes no setor público e no setor privado. 1. Ed. São Paulo: Thomson Reuters Brasil, 2021.

[37] O art. 4º, III, excepciona parcialmente a aplicação da LGPD aos tratamentos de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Os §§1º a 4º do mesmo artigo estabelecem que, nessas hipóteses, que serão regidas por legislação específica, devem ser observados o devido processo legal e os princípios gerais de proteção e os direitos do titular previstos na LGPD. Além disso, é atribuída à ANPD a competência para emitir opiniões técnicas e recomendações, bem como para solicitar a elaboração de relatório de impacto à proteção de dados pessoais. É vedado o tratamento de dados pessoais nessas hipóteses por pessoa jurídica de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à ANPD. A lei estabelece, ainda, que em nenhum caso a totalidade de tais dados poderá ser tratada por pessoa jurídica de direito privado, salvo por aquela que possua capital integralmente constituído pelo Poder Público. ANPD, Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público. Jan. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf >. Acesso em: 23/06/2022.

Em 05 de novembro de 2020, uma comissão de juristas chegou a apresentar ao Presidente da Câmara dos Deputados o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal[38], a fim de cumprir o disposto no §1º, do art. 4º da LGPD. O texto do anteprojeto teve forte influência da Diretiva 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, conforme reconhecido na exposição de motivos, e já foi objeto de duras críticas por parte do Ministério Público Federal, especialmente porque teria imposto restrições desproporcionais ao intercâmbio de dados entre autoridades persecutórias e porque inviabilizaria a utilização dessas informações para a identificação de riscos, criando obstáculos para a prevenção da ocorrência de crimes e também para a detecção de ilícitos já praticados, mas que estavam circunscritos às chamadas 'cifras ocultas'[39]. No entanto, até a submissão do presente artigo, não há notícia sobre a tramitação desse anteprojeto de lei no Congresso Nacional.

Há, ainda, o Projeto de Lei n. 1515/2022[40], apresentado em 07/06/2022 pelo Deputado Federal Coronel Armando (PL/SC), que propõe a "Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais". O texto está aguardando tramitação nas comissões pertinentes dentro da Câmara dos Deputados e ainda não há previsão para a votação em plenário.

A complexidade do tema certamente contribui para a lacuna legislativa atualmente existente no Brasil, porque se, de um lado, a tecnologia pode proteger bem jurídicos penalmente relevantes (como a vida, a integridade física e o patrimônio), de outro, pode deixar a sociedade desprotegida do controle e da

---

[38] MOTTA, Rayssa. MACEDO, Fausto. Comissão entrega 'LGPD Penal' a Maia e sugere CNJ como regulador de dados na Segurança. Estadão. Publicado em: 05/11/2020. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/comissao-entrega-lgpd-penal-a-maia-e-sugere-cnj-como-regulador-de-dados-na-seguranca/>. Acesso em: 23/06/2022.

[39] BARRETO, Coutinho Pablo. MARQUES, Paulo Rubens Carvalho. Procuradoria Geral da República. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Ministério Público Federal. Disponível em: <http://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf.> Acesso em: 23/06/2022.

[40] BRASIL. Projeto de Lei 1515, de 07 de junho de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Câmara de Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300>. Acesso em: 23/06/2022.

vigilância estatal, ameaçando direitos fundamentais como a proteção de dados pessoais, a privacidade, a intimidade e as liberdades de pensamento, de expressão, de culto etc.

Sobre o ponto, Regina Ruaro reflete que aceitar a utilização desmedida da tecnologia para fins de segurança pública implicaria a coisificação da vida privada e a renúncia deste direito essencial à natureza humana, ressaltando a intrínseca relação entre liberdade e privacidade, considerando ser preocupante considerar o direito à privacidade como um empecilho à segurança pública. Explica a estreita relação entre regimes totalitários e a perda de direitos à privacidade e à liberdade, referindo que isto enseja um maior controle e não maior segurança. A autora destaca que o direto à privacidade é essencial para que o ser humano desenvolva sua identidade e sua personalidade[41].

Molinaro e Sarlet também debatem semelhante ponto de vista, lecionando que o Estado enfrenta os desafios da sociedade em rede, necessitando intervir para se assegurar, utilizando-se de mecanismos de vigilância. Referem que medida afeta direitos humanos e fundamentais muito caros aos indivíduos, configurando uma ameaça à democracia, à liberdade de expressão e à privacidade. Destacam que não pode o Estado, sob o pretexto de a privacidade, a dignidade e a liberdade, violar ainda mais gravemente seus cidadãos. Os autores ainda questionam: "Quem está vigilando os vigilantes?"[42].

Wolfgang Hoffmann-Riem alerta que há risco de proteção e manipulação jurídica na seleção e controle digital para atos governamentais, caso eles não

[41] É no mínimo preocupante entender o direito à privacidade, em especial a autodeterminação informativa, como um empecilho à segurança pública. Essa tendência de se priorizar a ordem em detrimento de garantias inerentes a todo ser humano é merecedora de uma revisão histórica.
Seja com base em obras literárias como "1984" de George Orwell e "Vigiar e Punir" de Michael Foucault, seja com base em eventos históricos como os regimes militares da América latina ou os regimes totalitários nazifascistas, pode-se verificar uma estreita relação entre as perdas dos direitos à privacidade e da liberdade. Nesse sentido, é possível afirmar que informação não gera segurança, mas sim controle.
O respeito ao direito à privacidade é essencial para que o ser humano possa construir sua identidade e sua personalidade. Abrir mão desse "espaço" particular certamente afetaria aspectos como a autodeterminação pessoal e o próprio entendimento de liberdade em si. In: RUARO, Regina Linden. Privacidade e autodeterminação informativa obstáculos ao estado de vigilância? Arquivo Jurídico – ISSN 2317-918X – Teresina-PI – v. 2 – n. 1 – p. 41-60. Jan./Jun. de 2015, p. 17.
[42] MOLINARO, Carlos Alberto. SARLET, Ingo Wolfgang. Sociedade em rede, internet e estado de Vigilância: algumas aproximações. Revista da AJURIS – v. 40 – n. 132 – Dezembro, 2013, p. 87.

estejam sujeitos a controles constitucionais adequados. Atenta para o fato de que os procedimentos utilizados e os resultados não são transparentes e que não há rastreabilidade dos procedimentos para terceiros, impedindo que haja um controle externo. Reforça, portanto, que a transparência é uma condição para garantir a prestação de contas e que para isso é necessário haver requisitos legais. Aduz que, mesmo com a existência de legislações aptas a proteção de dados pessoais, não há possibilidade de ter uma noção mais ampla de como eles estão sendo utilizados – como na utilização de *big data*, que não é possível saber, por exemplo, quais dados são utilizados e compartilhados pelas empresas, com quais outros dados eles se relacionam e no que resultam etc. O autor também ressalta que tais situações se agravam no âmbito da segurança pública, pois muitas vezes depende-se do sigilo para que a investigação seja eficaz[43].

A necessidade de sigilo não deveria servir como justificativa para implementação de um Estado de plena vigilância. Bauman e Lyon já articularam que "Entre as racionalizações para o engajamento na vigilância, um motivo-chave é a busca de segurança. (...) Como tal, a vigilância parece ter um forte motivo de proteção: vigiar para cuidar"[44].

A tecnologia leva ao paradoxo dos direitos e garantias fundamentais: propicia a proteção da vida na dimensão biológica/física, porém mitiga a proteção dos dados pessoais, da vida íntima e privada, atingindo direitos de personalidade e adentrando à dimensão existencial; aumenta o exercício da liberdade de ir e vir atenuando o medo de ser vítima de um crime ou de um acidente de carro por desatenção do motorista, mas pode tolher a liberdade de acesso a direitos por meio do perfilamento de indivíduos, podendo também constranger a liberdade de expressão, de culto e de pensamento por receio da exposição e do julgamento público; proporciona maior segurança contra terceiros em troca de colocar em risco a segurança dos dados pessoais e até da própria identidade.

---

[43] HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital. Transformação Digital – Desafios para o Direito. Rio de Janeiro: GEN-FORENSE, 2021.

[44] BAUMAN, Zygmunt; LYON, David. Vigilância Líquida: Diálogos com David Lyon. Rio de Janeiro: Zahar, 2014, p. 70.

Como então encontrar o equilíbrio? Ingo Sarlet relembra que, desde as primeiras constituições, os direitos fundamentais estão presentes como direitos de defesa do indivíduo frente ao Estado, demarcando até que ponto o ente público pode intervir e a partir de quando ele deve recuar e respeitar a autonomia pessoal[45]. Nesta senda, traçaram-se os direitos à vida, à liberdade, à propriedade e à igualdade como limitações estatais, complementados pelo respeito às liberdades de expressão, de manifestação, de reunião e associação etc.

Superados estes contornos entre Estado e indivíduo, a revolução industrial e a consequente exploração da mão de obra em troca de subsistência (que deixou pouco espaço para se fruir dos direitos protegidos) demonstraram que não bastava o Estado não intervir na esfera privada, ele precisava promover subsídios para que os direitos fundamentais fossem viáveis de serem exercidos por todos – favorecendo uma autonomia individual real. É quando surgem os primeiros direitos sociais, tais como assistência social, saúde, educação e segurança, entre outros, no intuito de suprir as necessidades essenciais de sobrevivência para que o cidadão pudesse viver com dignidade.

Posteriormente, as demandas coletivas também não puderam ser excluídas da proteção constitucional, reconhecendo-se noções de grupo (família, povo, nação), que, por compor a identidade e amparar o exercício de direitos individuais, se tornam vinculados e essenciais. Discute-se ainda a existência de novas dimensões, notadamente com relação ao resultado da globalização dos direitos fundamentais, daí derivando o direito à democracia, ao pluralismo e até mesmo o direito à paz – não reduzida à ausência de guerra e violência, mas também como condição para efetividade dos direitos em geral.

A evolução histórica dos direitos, que podem ser avaliados nas suas mais diversas dimensões identificadas ao longo do tempo, permite entender que as atividades de segurança pública, enquanto responsabilidade do Estado, devem encontrar fronteiras entre circunstâncias aparentemente opostas, tais como: (i) a promoção do exercício da dignidade pelos cidadãos – que exige, entre muitos

[45] SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. e atual. – Porto Alegre: Livraria do Advogado, 2018, p. 45.

aspectos, controle e segurança dos membros de uma sociedade e (ii) a não invasão na esfera privada do indivíduo.

Assim, a implementação de novas tecnologias nas relações entre o Estado e cidadãos deve partir do princípio central da Constituição Federal de 1988: a dignidade da pessoa humana. Este princípio serve como um limitador da atuação estatal, tanto no sentido de impedir que o poder público possa violar a dignidade pessoal, quanto no sentido de exigir que promova condições para o exercício desta[46]. Destaca-se também ser incumbência do Estado proteger o indivíduo não só de sua própria invasão, mas também contra agressões de terceiros. Sendo assim, no âmbito da segurança pública, o Estado tem como obrigação proteger os cidadãos em suas relações e agressões entre si mesmos, sem, contudo, prejudicar a dignidade de um ou de outro.

Apesar dos claros contornos constitucionais, Danilo Doneda alerta que apesar de nosso ordenamento jurídico conferir valor máximo a proteção da pessoa humana e da dignidade como um direito fundamental, deixou entrever uma proteção que acaba por atuar de forma fracionada, em tópicos determinados (habeas data, precisões do código de defesa do consumidor), o que acaba por ser mais efetivo em seus respectivos campos, mas não tutela integramente a personalidade através da proteção dos dados pessoais[47].

Antes mesmo da promulgação da Emenda Constitucional nº 115, de 2022[48], que reconheceu ser um direito fundamental a proteção dos dados pessoais, inclusive

---

[46] SARLET, Ingo Wolfgang. Dignidade (da pessoa) humana e direitos fundamentais na Constituição Federal de 1988. 10. ed. rev. atual. e ampl. 3. tir. – Porto Alegre: Livraria do Advogado, 2019, p. 89.

[47] O ordenamento jurídico brasileiro contempla a proteção da pessoa humana como seu valor máximo e a privacidade como um direito fundamental. Uma análise do instrumental disponível para possibilitar a concreta atuação de tais direitos, porém, deixa entrever uma proteção que, embora devesse corresponder a uma proteção integrada e dirigida pela tábua axiológica constitucional, atua de forma fracionada, em focos de atuação determinados – sejam estes a ação de habeas data, as previsões do Código de Defesa do Consumidor ou outras – que tendem a orientar-se mais pela lógica de seus específicos campos do que por uma estratégia baseada na tutela integral da personalidade através da proteção dos dados pessoais. In: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 91.

[48] BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União. Brasília, em 10/02/2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1.>. Acesso em: 23/06/2022.

nos meios digitais, o Supremo Tribunal Federal (STF) obstou cautelarmente, na Ação Direta de Inconstitucionalidade (ADI) 6387, o tratamento de dados considerado excessivo pelo poder público, mesmo quando fundado em relevante interesse social, por reconhecer que essa tutela já era uma garantia fundamental implícita em na ordem constitucional brasileira.

No caso analisado, o STF declarou a inconstitucionalidade da medida provisória que determinava às empresas de telecomunicações o compartilhamento do nome, telefone e endereço de seus clientes com o Instituto Brasileiro de Geografia e Estatística (IBGE) para fins de produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

Apesar de a medida provisória objeto da Ação Direta de Inconstitucionalidade (ADI) 6387 não dizer respeito especificamente à segurança pública e ter tido sua vigência encerrada em agosto de 2020, prejudicando o julgamento de mérito em definitivo, é possível extrair da motivação da decisão do STF algumas balizas para a atuação estatal que podem ser aproveitadas para a seara ora estudada, tais como:

> (i) o tratamento e a manipulação de dados pessoais devem observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos;
>
> (ii) é necessário assegurar mecanismos técnicos e administrativos de proteção e segurança dos dados pessoais tratados, aptos a proteger acessos não autorizados, vazamentos acidentais ou utilização indevida, inclusive com previsão de auditoria externa;
>
> (iii) interesses coletivos, tais como o cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não puderam ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos

e atropelo de garantias fundamentais consagradas na Constituição[49];

(iv) é imperiosa a definição de critérios para responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais;

(v) precisa haver transparência na definição da finalidade e do uso dos dados compartilhados.

Vale mencionar que o estabelecimento de alguns critérios para utilização da tecnologia não tem a intenção de obstar os avanços que ela promove na prestação dos serviços públicos, mas, sim, de efetivar maior transparência e proteção individual às liberdades e privacidades dos cidadãos. A analogia feita pela Ministra Rosa Weber na decisão da mencionada ADI é elucidativa ao lembrar que a imposição de implementação de freios, airbags e espelhos retrovisores não significou um obstáculo ao avanço da indústria automobilística, assim como a adequação constitucional envolvendo direitos fundamentais e da personalidade não pode significar embaraço à atividade estatal.

O Distrito Federal, em iniciativa pioneira, promulgou a Lei 6.712/2020 que dispõe sobre o uso de tecnologia de reconhecimento facial (TRF) na segurança pública. Apesar de restrita à TRF e de não prever mecanismos de controle dos acessos e dos usuários, bem como suas respectivas responsabilidades, a legislação traça consideráveis restrições à polícia, tais como: vedação de vigilância contínua; uso somente em espaços públicos onde contenham placas visíveis fixadas informando sua utilização; necessidade de revisão por agente público antes de qualquer ação decorrente da sinalização da tecnologia; respeito às diretrizes da LGPD; prazo para guarda dos dados; entre outras. Mais um exemplo a revelar que a utilização de tecnologias para fins de segurança pública deve encontrar limites nos direitos e garantias fundamentais explícitos e implícitos na Constituição Federal de 1988, com eficácia imediata, mesmo que hoje ainda não exista um regramento específico sobre o tema.

[49] Importante mencionar que o direito à saúde, assim como a segurança, também está positivado no *caput* do art. 5º da CF e, na análise do STF, ainda que havendo evidente e urgente interesse social, prevaleceu a proteção aos direitos e garantias fundamentais.

5. Considerações finais

O presente estudo se propôs a entender se o ordenamento jurídico pátrio é suficiente para garantir que o emprego de tecnologias na segurança pública, tão benéficos à atividade estatal, não resulte em um estado totalitário, marcado pelo controle excessivo e vigilância constante.

Para tanto, foi feita uma extensa busca em publicações da imprensa para mapear o que já está em uso no Brasil, entendendo seus benefícios, bem como os danos que já foram causados a partir das experiências vivenciadas, devidamente listados em tópico específico.

Ao final, examinou-se o ordenamento pátrio, procurando na Constituição Federal, sobretudo a partir da promulgação da Emenda Constitucional nº 115, de 2022, os limites para a utilização desmedida da tecnologia por parte do poder estatal, tendo em vista que a Lei Geral da Proteção de Dados excluiu a segurança pública de sua competência e que as propostas de Lei de Proteção de Dados para segurança pública e persecução penal ainda não foram submetidas à votação parlamentar. A falta de uma legislação infraconstitucional específica sobre o tema poderia, aparentemente, supor que a privacidade, a intimidade e os dados pessoais dos cidadãos restariam desabrigados quando os casos envolvessem ações do poder persecutório brasileiro.

Entretanto, pôde-se concluir em sentido oposto: analisada doutrina especializada no tema, constatou-se que os direitos e garantias fundamentais como a privacidade, a intimidade e o agora explícito direito à proteção de dados pessoais possuem eficácia imediata, ainda que a regulação específica não esteja em vigor, conforme reconhecido pelo STF em situação diversa (ADI 6387), mas cujos fundamentos são suficientes para conhecer a preponderância dos direitos individuais frente a atuação estatal, ainda que esta ocorra em prol de evidente e urgente interesse coletivo. Importante destacar que, no julgado, o STF evidenciou sua interpretação constitucional e traçou requisitos mínimos a serem respeitados para que haja um seguro tratamento de dados pessoais.

Todavia, ainda , foi possível constatar que muitas das tecnologias já utilizadas no país não estão levando em consideração medidas tendentes a respeitar os direitos

individuais, pois, como visto, nem sempre ocorre (i) transparência sobre a finalidade que os dados pessoais poderão ser utilizados no momento em que é feita a coleta, (ii) fiscalização dos usuários que acessam os bancos de dados, (iii) um correto treinamento dos policiais e dos agentes persecutórios em geral para que tenham senso crítico e filtrem as sinalizações advindas da tecnologia, (iv) previsões de auditoria interna e externa sobre acesso, uso e tratamento dos dados pessoais, entre outros procedimentos que se tornam essenciais para preservação de garantias fundamentais.

Levando isto em consideração, denota-se, portanto, que para evitar os danos que uma atuação estatal desmedida pode acarretar, se faz imperiosa e urgente a edição de legislação específica para o tema, que, ao menos, institua critérios objetivos e condições necessárias para o uso e o tratamento de dados pessoais no âmbito da investigação e do processo penal, bem como estabeleça fluxos que reafirmem a privacidade, a intimidade e a proteção dos dados pessoais dos cidadãos em detrimento de qualquer justificativa utilitarista e/ou eficientista de promoção abstrata da segurança pública e que também apresente sanções específicas, inclusive de natureza penal, para os agentes que atuarem com desvio de função violando direitos constitucionalmente assegurados fora da destinação limitada e especial prevista na lei.

Referências bibliográficas

ABLT – Associação Brasileira de Logística e Transporte de Produtos Perigosos. **Informativos ABTLP.** Disponível em: <http://www.abtlp.org.br/index.php/tecnologias-da-prf-seopi-e-senasp-sao-integradas-para-operacionalizar-o-maior-sistema-de-monitoramento-viario-do-pais/ >. Acesso em 23/06/2022.

ALVES, Alan Tiago. Flagrado por câmera vestido de mulher no carnaval na BA matou homem após vítima passar perto dele de moto em alta velocidade. **G1**. Publicado em: 07/03/2019. Disponível em: <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>. Acesso em: 23/06/2022.

ANPD, **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**. Jan. 2022. Disponível em:<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 23/06/2022.

ARAÚJO JÚNIOR, Jozias Rolim de. **Reconhecimento multibiométrico baseado em imagens de face parcialmente ocluídas.** Dissertação (Mestrado em Ciências) – Programa de Pós-Graduação em Informação, Escola de Artes, Ciências e Humanidades. Universidade de São Paulo, 2018.

AVENDAÑO, Ana Clara; MENESES, Celimar de. Reconhecimento facial será utilizado pela primeira vez no carnaval. **Correio Braziliense**. 21/02/2020. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/cidades/2020/02/21/interna_cidadesdf,829615/reconhecimento-facial-sera-utilizado-pela-primeira-vez-no-carnaval.shtml.> Acesso em: 23/06/2022.

BARRETO, Coutinho Pablo. MARQUES, Paulo Rubens Carvalho. Procuradoria Geral da República. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. **Ministério Público Federal**. Disponível em: <http://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf>. Acesso em: 23/06/2022.

BAUMAN, Zygmunt. **Confiança e medo na cidade**. Tradução de Eliana Aguiar. Rio de Janeiro: Jorge Zahar Ed., 2009.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**: Diálogos com David Lyon. Rio de Janeiro: Zahar, 2014.

BRAGA, Carolina. **Discriminação nas decisões por algoritmos**: **polícia preditiva**. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). Inteligência artificial e Direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2. ed., 2020.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União. Brasília, em 10/02/2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1>. Acesso em: 23/06/2022.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral da Proteção de Dados (LGPD). Diário Oficial da União. Brasília, 14/08/2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23/06/2022.

BRASIL. Projeto de Lei 1515, de 07 de junho de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de

segurança pública, e de investigação e repressão de infrações penais. **Câmara de Deputados**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300>. Acesso em: 23/06/2022.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade (ADI) 6387. Relator: Min. Rosa Weber. 12/11/2020. Disponível em <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 23/06/2022.

CRUZ, Elaine Patricia. Polícia usa sistema de reconhecimento facial no carnaval de São Paulo. **Agência Brasil.** São Paulo. 21/02/2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-02/policia-usa-sistema-de-reconhecimento-facial-no-carnaval-de-sao-paulo>. Acesso em: 23/06/2022.

DOMINGOS, Pedro. **O Algoritmo Mestre:** como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. 1ª edição. São Paulo: Novatec, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DZIEZA, Josh. Why Captchas Have Gotten So Difficult: Demonstrating you're not a robot is getting harder and harder. **The Verge**. Publicado em 01/02/2019. Disponível em: <https://www.theverge.com/2019/2/1/18205610/google-captcha-ai-robot-human-difficult-artificial-intelligence>. Acesso em 23/06/2022.

FERRARI, Isabela. **Justiça Digital**. 1ª edição. São Paulo: Thomsom Reuters Brasil, 2020.

GARVIE, Claire. *et. al.* The Perpetual Line-Up: Unregulated Police Face Recognition In America. **Center on Privacy & Technology at Georgetown Law**. Out, 2016. Disponível em:<https://www.perpetuallineup.org/>. Acesso em: 23/06/2022.

GHOSH, Iman Ghosh. 4 key areas where AI and IoT are being combined. Global Technology Governance Summit. **World Economic Forum**. Publicado em: 15/03/2021. Disponível em: <https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/>. Acesso em: 23/06/2022.

HARWELL, Drew. FOWLER, Geoffrey A. U.S. Customs and Border Protection says photos of travelers were taken in a data breach. **The Washington Post**. Publicado em 10/06/2019. Disponível em: <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/>. Acesso em 23/06/2022.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**. Transformação Digital – Desafios para o Direito. Rio de Janeiro: GEN-FORENSE, 2021.

KUNICHOFF, Yana. SIER, Patrick. The Contradictions of Chicago Police's Secretive List. **Chicago magazine**. Publicado em: 21/08/2017. Disponível em: <https://www.chicagomag.com/city-life/august-2017/chicago-police-strategic-subject-list/>. Acesso em: 23/06/2022.

LAVADO, Thiago. Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debate sobre limites da tecnologia. **G1**. Publicado em 21/02/2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml>.Acesso em 23/06/2022.

MARAUX, Alberto. Reconhecimento Facial flagra foragido usando máscara. **Secretaria de Segurança Pública da Bahia**. Publicado em: 01/09/2020. Disponível em: <http://www.ssp.ba.gov.br/2020/09/8319/Reconhecimento-Facial-flagra-foragido-usando-mascara.html>. Acesso em 23/06/2022.

MEIJER, Albert. WESSELS, Martijn. Predictive Policing: Review of Benefits and Drawbacks, **International Journal of Public Administration**, Volume 42, Ed. 12, P. 1031-1039, Fev. 2019. DOI: https://doi.org/10.1080/01900692.2019.1575664.

MOLINARO, Carlos Alberto. SARLET, Ingo Wolfgang. Sociedade em rede, internet e estado de Vigilância: algumas aproximações. **Revista da AJURIS** – v. 40 – n. 132 – Dezembro/2013.

MOTTA, Rayssa. MACEDO, Fausto. Comissão entrega 'LGPD Penal' a Maia e sugere CNJ como regulador de dados na Segurança. **Estadão.** Publicado em: 05/11/2020. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/comissao-entrega-lgpd-penal-a-maia-e-sugere-cnj-como-regulador-de-dados-na-seguranca/.>. Acesso em: 23/06/2022.

PALMA, Amanda. PACHECO, Clarissa. Entenda como funciona o reconhecimento facial que ajudou a prender mais de 100 na BA. **Correio 24 horas.** Publicado em: 05/01/2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/entenda-como-funciona-o-reconhecimento-facial-que-ajudou-a-prender-mais-de-100-na-ba/>. Acesso em: 23/06/2022.

PEREIRA, Fabio Luiz Barboza. SILVA, Cecília Alberton Coutinho. A Regulação Do Reconhecimento Facial E Seus Impactos Para Os Setores Público E Privado No Brasil: Uma Análise Comparativa Internacional. *In:* FRANCOSKI, Denise de Souza Luiz. TASSO, Fernando Antonio. **A Lei Geral De Proteção De Dados Pessoais:** Aspectos práticos e teóricos relevantes no setor público e no setor privado. 1. Ed. São Paulo: Thomson Reuters Brasil, 2021.

PERON, Isadora Peron. RIBEIRO, Marcelo. Di Cunto, Raphael Di Cunto. Além do STJ, outros órgãos sofrem tentativas de ataques de hackers. **Valor Econômico**. Brasília: Nov, 2020. Disponível em: <https://valor.globo.com/politica/noticia/2020/11/05/alm-do-stj-outros-rgos-sofrem-tentativas-de-ataques-de-hackers.ghtml>. Acesso em: 23/06/2022.

PRESSE, France. Manifestantes desafiam a lei usando máscaras em Hong Kong. **G1**. Publicado em: 06/10/2019. Disponível em: <https://g1.globo.com/mundo/noticia/2019/10/06/manifestantes-desafiam-a-lei-usando-mascaras-em-hong-kong.ghtml.>. Acesso em: 23/06/2022.

Procuradoria Geral da República. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. **Ministério Público Federal**. Disponível em: <http://www.mpf.mp.br/pgr/documentos/Sppea_PGR00456556.20205.pdf>. Acesso em: 23/06/2022.

REDAÇÃO. Huawei: qué países prohibieron la tecnología del gigante chino, el segundo mayor productor de celulares del mundo. **BBC News**. Publicado em 28/11/2018. Disponível em: <https://www.bbc.com/mundo/noticias-46379805>. Acesso em 23/06/2022.

REDAÇÃO. Média de tempo para recuperar veículo no Ceará é de 5 a 10 minutos. **Diário do Nordeste**. Publicado em: 14/07/2019. Disponível em: <https://diariodonordeste.verdesmares.com.br/seguranca/media-de-tempo-para-recuperar-veiculo-no-ceara-e-de-5-a-10-minutos-1.2123188>. Acesso em 23/06/2022.

Revista Segurança Eletrônica. Tecnologia infravermelha pode oferecer proteção de perímetro acessível. Disponível em: <https://revistasegurancaeletronica.com.br/tecnologia-infravermelha-pode-oferecer-protecao-de-perimetro-acessivel/>. Acesso em: 23/06/2022.

Revista Segurança Eletrônica. Dahua Technology lança soluções em vídeo monitoramento para avaliar comportamento do motorista. Disponível em: <https://revistasegurancaeletronica.com.br/dahua-technology-lanca-solucoes-em-video-monitoramento-para-avaliar-comportamento-do-motorista/>. Acesso em: 23/06/2022.

RUARO, Regina Linden. Privacidade e autodeterminação informativa obstáculos ao estado de vigilância? **Arquivo Jurídico** – ISSN 2317-918X – Teresina-PI – v. 2 – n. 1 – p. 41-60. Jan-Jun/2015.
SADIE GURMAN, Sadie. AP: Across US, police officers abuse confidential databases. The **Associated Press**. Publicado em 28/09/2016. Disponível em: <https://apnews.com/article/699236946e3140659fff8a2362e16f43>. Acesso em: 23/06/2022.

SARLET, Ingo Wolfgang. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF? **Consultor Jurídico**. 4 de setembro de 2020. Disponível em: < https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf?fbclid=IwAR3g2EpB0bP_2w_Uhnp4gHt7QBMZFwqnGsCx0c9W6ra27UGmnbduxulQ4r0#_ftn2>. Acesso em 23/06/2022.

SARLET, Ingo Wolfgang. **Dignidade (da pessoa) humana e direitos fundamentais na Constituição Federal de 1988.** 10. ed. rev. atual. e ampl. 3. tir. – Porto Alegre: Livraria do Advogado, 2019.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. e atual. – Porto Alegre: Livraria do Advogado, 2018.

SECOM, Bahia apresenta resultado do Reconhecimento Facial na China. Publicado em 19/05/2019. Disponível em: <http://www.ssp.ba.gov.br/2019/05/5695/Bahia-apresenta-resultado-do-Reconhecimento-Facial-na-China.html>. Acesso em: 23/06/2022.

SSPDS, Secretaria da Segurança Pública e Defesa Social do Governo do Estado do Ceará. Big Data da Segurança Pública, Spia e videomonitoramento da SSPDS são utilizados na elucidação de crime em Fortaleza. Publicado em: 11/12/2019. Disponível em: <https://www.ceara.gov.br/2019/12/13/big-data-da-seguranca-publica-spia-e-videomonitoramento-da-sspds-sao-utilizados-na-elucidacao-de-crime-em-fortaleza/>. Acesso em 23/06/2022.

STATE v. Loomis: Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing. 130 **Harvard Law Review**, 1530. Mar, 2017. Disponível em: <https://harvardlawreview.org/2017/03/state-v-loomis/>. Acesso em 23/06/2022.

Suspensos em razão da pandemia, prazos de processos físicos são retomados no TJ. **Correio do Povo**, 2021. Disponível em: <https://www.correiodopovo.com.br/not%C3%ADcias/geral/suspensos-em-raz%C3%A3o-da-pandemia-prazos-de-processos-f%C3%ADsicos-s%C3%A3o-retomados-no-tj-1.635155>. Acesso em: 23/06/2022.

VINCENT, James. Google wants you to help train its AI by labeling images in Google Photos: A new optional feature in Google Photos on Android. **The Verge**. Publicado em: 11/11/2020. Disponível em: <https://www.theverge.com/2020/11/11/21559930/google-train-ai-photos-image-labelling-app-android-update>. Acesso em: 23/06/2022.

11. A ANONIMIZAÇÃO DE DADOS PESSOAIS COMO HIPÓTESE LEGAL DE TRATAMENTO E DIREITO DOS TITULARES – AJUSTES EM CONTRUÇÃO NO SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

https://doi.org/10.36592/9786581110994-11

Lucas Reckziegel Weschenfelder[1]

> *An old idea – If our paper has stood the test of time, it is because the core technical insight goes back at least 60 years: a small number of data points about an individual, none of which are uniquely identifying, are collectively equivalent to an identifier. […] We and other researchers have since demonstrated robust de-anonymization techniques in many other domains: social networks, genetic data, location data, credit card data, browsing histories, writing style, source code, and compiled binaries. This line of research has firmly established that high-dimensional data is inherently vulnerable to de-anonymization. This is also supported by theoretical evidence. When we consider the fact that 33 bits of entropy are sufficient to identify an individual uniquely among the world's population, these research findings should be no surprise.*
> *ARMIND NARAYAN; VITALY SHMATIKOV 2019, p. 1.*

Sumário

1. Introdução

Intenta-se expor a dogmática da doutrina da "base legal" para o tratamento de dados pessoais, vinculada ao tema dos dados anonimizados enquanto "base para

[1] Doutorando em Direito na Pontifícia Universidade Católica do Rio Grande do Sul. Advogado. E-mail: lucasweschen@yahoo.com.br. Currículo Lattes iD: http://lattes.cnpq.br/3929645670502613.

o tratamento", e, enquanto "direito dos titulares", e as divergências em construção, quanto ao instituto da "identificabilidade".

Há, comumente, o entendimento de que um tratamento de dados pessoais necessita de uma base legal para ser lícito (*lawful processing*). Diverge-se sobre a possibilidade de um tratamento de dados pessoais possuir mais de um fundamento legal. No geral, tanto no Brasil, com a Lei nº 13.709, de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) [2] como em âmbito europeu, assevera-se sobre a viabilidade de ser empregado mais de um fundamento legal para um "mesmo" tratamento de dados.

Ainda, na LGPD, coloca-se, como "hipóteses legais" para o tratamento de dados pessoais, aquelas previstas no art. 7º. Contudo, não se pode ignorar a previsão de outras bases legais de tratamento, podendo-se dizer, "indiretas", como o tratamento de dados pessoais realizado com fundamento no art. 4º, em que ocorre, a princípio, com a exclusão da incidência normativa da LGPD – em determinadas dimensões. Em suma, um processamento de dados pessoais perfectibilizado com fundamento no art. 4º, é um tratamento, supostamente paradoxal, realizado com fundamento legal previsto na LGPD, estritamente nas condições antepostas no art. 4º, em seus incisos e parágrafos, pregando-se a exclusão da incidência do referido diploma geral, e, para determinadas hipóteses, prescrevendo-se sobre a pertinência de ulterior produção legislativa específica (e ultrapassando-se a limitação encontrada no art. 7º).[3]

Designadamente sobre o tema a ser desenvolvido, alude-se à outra hipótese legal, prevista na LGPD, para viabilizar, com respaldo jurídico, um tratamento de dados pessoais, no caso, transmutados em dados anonimizados. Preserva-se, no art. 12, *caput*, da LGPD, a previsão de que os dados anonimizados não serão considerados pessoais para os fins da lei. Ou seja, se o fundamento legal de um tratamento de dados pessoais for "dados anonimizados", exsurge outra hipótese

[2] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709>. Acesso em: 15 nov. 2020.

[3] Art. 4º. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

legal.

Notando-se essa doutrina, da "base legal de tratamento", observa-se, também, o seu "caráter dúplice": possui uma funcionalidade para os agentes responsáveis pelo tratamento, como, também, uma funcionalidade como direito dos titulares. A base legal "anonimização", a propósito, possui um regime jurídico especial, distinto das demais, a qual merece muita atenção – exemplificativamente, por estar prevista como direito dos titulares, no art. 18, inciso IV, da LGPD[4].

O que importa desenvolver, nesse texto, em duas etapas, é a ideia sobre o teor normativo de dado pessoal e de dado anonimizado, e a estruturação jurídica dos respectivos tratamentos, concatenada a partir da doutrina da "base legal" e seus aparentes "déficits", vinculados ao instituto da "identificabilidade"/filtro de razoabilidade, e da anonimização enquanto direito dos titulares.

De modo a ordenar o trabalho, utiliza-se dos aportes/metodologia epistêmicos da hermenêutica, partindo de premissas (histórico-linguísticas-textuais) que se consubstanciam no problema. O método de procedimento utilizado é o monográfico, e a técnica de pesquisa, a bibliográfica.

O presente trabalho foi realizado com apoio da PUCRS através do Programa de Excelência Acadêmica – PROEX – CAPES.

2. O complexo teor normativo da concepção de dados pessoais anonimizados e dados pessoais não anonimizados

A dimensão que acoberta a escrita desse texto é a linguagem dogmática. Não se trata de uma tentativa de elucidações dogmatistas - a dogmática transformada em dogmatismo. Se pretende lidar com a dogmática de uma forma construtiva, expansionista da capacidade de "aderência" da realidade socionormativa à sua gramática "especializada". "É dizer: a condição dogmática estabelecendo uma fabulação da expansão racional do direito que só é admitida como tendência que

[4] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

marca uma primeira representação institucional do outro, o primeiro limite de meu poder frente ao outro", e ainda, "Trata-se, então, de uma confiança posta nas palavras da lei, como um algo semântico que está fora de toda transmutação interpretativa [...] (a interpretação como a arte de romper com a fantasia da plenitude semântica da lei jurídica)[5].

Falar de dogmática é falar de conceitualização, de (re)estruturação de sentidos direcionados à diminuição da complexidade da vida. A tentativa de redução da complexidade da vida, por meio de "conceitos", termina por criar outras complexidades, internas às linguagens especializadas comunicativamente intersubjetivas e integradas às outras, tornando a linguagem "operacional" e, com isso, a própria "realidade linguística", observável de uma certa maneira. Possuir a pretensão de se situar em um desenvolvimento linguístico dogmático, significa possuir a pretensão de "observar" a realidade ou, melhor, de apontar um "é" nesse contexto fenomenológico de ser-aí-ente, inexpugnavelmente finito e infinito.[6][7]

Conscientizando-se sobre isso, possui-se a humildade e, simultaneamente, a imodéstia de tecer alguns apontamentos relativos à dogmática jurídica e ao texto normativo da Lei Geral de Proteção de Dados Pessoais do Brasil, com algumas minúcias oriundas do que já se tem na Europa sobre a matéria. A dogmática é importante, pois é imprescindível, na quadra histórica-hermenêutica do Direito moderno, uma vez que é com ela, e a partir dela, que as direções e parâmetros (e antecipações de sentidos-normativos) para a decidibilidade do Direito são formuladas. Colocando-se essas observações como condicionais, passa-se ao desenvolvimento do trabalho.

---

[5] WARAT, Luis Alberto. Introdução geral ao direito III: O Direito não estudado pela teoria jurídica moderna. Porto Alegre: Fabris, 1997, p. 145.

[6] LUHMANN, Niklas. Sociologia do Direito II. Rio de Janeiro: Tempo Brasileiro, 1985.
____. La ciencia de la sociedad. Anthropos: México, 1996.

[7] HABERMAS, Jürgen. Direito e democracia: entre facticidade e validade, volume 1. Rio de Janeiro: Tempo Brasileiro, 1997.

2.1. Todos os dados são dados pessoais?

Iniciando-se essa seção como resposta ao subtítulo, é possível remeter a uma antecipação negativa. Entretanto, não se mostra simplória uma tentativa de resposta arrazoada sobre o assunto – e nem será realizada nesse espaço. Isso será exibido, atentando-se para uma particularidade que, por sua vez, se insere no questionamento aludido, e se soma à seguinte situação, presa ao objetivo do artigo: um dado pessoal anonimizado deixa de ser pessoal? Quais são os limites observáveis das respostas possíveis para esse questionamento? Para iniciar uma resposta a essas perguntas, é preciso requintar a doutrina do "filtro da razoabilidade", /identificabilidade, por sinal, adotada na LGPD.

Uma primeira observação, tida como plausível, e, frisa-se, independentemente do que dizem o "texto normativo" e as "decisões judiciais ou administrativas" sobre a matéria, é a qual, fundamentada em observações "técnicas", sinaliza sobre a viabilidade de se "desanonimizar" dados pessoais "transformados em anonimizados ou pseudoanonimizados".[8] Essa amostra significa outro ponto importante que, muitas vezes, passa sem atenção: um dado pessoal anonimizado já foi, em alguma circunstância, um dado pessoal. Isso representa, portanto, que, em algum momento, a normatividade da LGPD, ou, no caso Europeu, o Regulamento Geral e as leis nacionais dos países que compõe a União Europeia, regularam um tratamento de dados de uma maneira 'x', e, a partir do processo de anonimização, passaram a regular esse mesmo tratamento de dados de forma 'y'.

Essa circunstância normativa reflete que, a Lei brasileira, e o arcabouço legal da União Europeia, assumem como convergentes a existência de uma noção de dado pessoal e de dado pessoal anonimizado, mesmo tendo plena ciência das "habilidades técnicas" de possibilidade de efetiva reversão. Isso significa, além, que, a aparente contradição, na realidade, é enfrentada, a partir da dita doutrina do "filtro de

[8] De modo exemplificativo, cita-se um dos trabalhos pioneiros. ARVIND, Narayanan; SHMATIKOV, Vitaly. Robust De-anonymization of large sparse datasets. *In:* IEEE Symposium on Security and Privacy, Oakland, 2008. p. 111-125. Disponível em: https://ieeexplore.ieee.org/abstract/document/4531148#:~:text=Robust%20De-anonymization%20of%20Large%20Sparse%20Datasets%20Abstract:%20We,individual%20preferences,%20recommendations,%20transaction%20records%20and%20so%20on.> Acesso em: 15 out. 2020.

razoabilidade", a qual alavanca, para o centro da discussão, o instituto da "identificabilidade", assemelhando-se, a propósito, com ele.

O "filtro de razoabilidade" incute a ideia de que, nem toda "identificação" será considerada como legal, para ter-se uma "reversão", e suas consequências, geradoras de responsabilização (identificabilidade). Então, de maneira contrária, nem todo dado pessoal será considerado pessoal, se passar por um procedimento de anonimização/pseudoanonimização (ainda que seja possível a sua reversão). O presente texto, antecipando-se algumas considerações, insere-se na discussão sobre os "critérios" a serem construídos nos institutos "filtro de razoabilidade" e "identificabilidade".

Não obstante, deve-se salientar e organizar alguns elementos sobre essas diretrizes, também relacionados à praticabilidade da abrangência normativa do que seria um processo de desanonimização, tornando o dado anonimizado "(re)identificável", ou seja, em dado pessoal, com suas implicações e inseguranças.

Primeiramente, expõe-se o texto normativo da LGPD, citando-se, após, a atual construção da divergência sobre o tema na União Europeia, para, assim, ser possível tecer alguns apontamentos sobre o assunto, em atmosfera tupiniquim.

Consta, no art. 5º, inciso I, da LGPD, o conceito legal do que seria dado pessoal: informação relacionada a pessoa natural identificada e identificável. No inciso III, do art. 5º, do mesmo diploma, tem-se o conceito legal de dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. No art. 12, *caput*, há: os dados anonimizados não serão considerados dados pessoais para os fins desta Lei [...] Ou seja, uma exclusão normativa em razão da "anonimização", continua o texto normativo, [...] Salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. No art. 12, § 3º, da LGPD, há a diretiva, da qual "a autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização [...]. [9] Ainda, o processo de anonimização exsurge

[9] A Autoridade Nacional de Proteção de Dados Pessoais (ANPD), no guia orientativo, Tratamento de Dados Pessoais pelo Poder Público (2022, p. 14, 22, 23, 25), enfatiza a pseudonimização ou anonimização como estrutura normativa essencial, a ser organizada "sempre que possível", podendo

enquanto direito dos titulares, anteposto no art. 18, IV, da LGPD. Para não alongar mais a complexa situação normativa, tem-se no art. 13, *caput*, que os estudos em saúde pública [...] sempre que possível [...] serão realizados com [...] a anonimização e pseudoanonimização dos dados [...], constando, também, a anonimização como exceção para conservação de dados nas hipóteses de exclusão, art. 16, *caput*, inciso II, [...] autorizada a conservação para as seguintes finalidades: II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

No Brasil, com a LGPD, se está, a princípio, adotando a doutrina europeia "*If data are not personal data, the GDPR does not apply to anyone or anywhere*"[10], e, por claro, essa disposição vincula-se estritamente com outras máximas, da "base legal para um tratamento de dados pessoais", com o instituto da "identificação" e a anonimização enquanto direito dos titulares. Em âmbito europeu, particularmente na União Europeia, como explicitado, conforma-se a essa doutrina, embora, atualmente, haja divergência sobre um aspecto fulcral, o qual, a propósito, é desenvolvido nesse trabalho: o alcance normativo de um "conceito" de dados pessoais e a relação dessa noção com o instituto da "identificabilidade" (filtro de razoabilidade) de dados pessoais anonimizados.

Cita-se a divergência europeia para realçar esse assunto nas próximas seções. Em suma, com o Regulamento Geral Europeu, não ocorreu nenhuma modificação poderosa sobre a matéria, previamente normatizada pelo art. 29, do *Working Party*, cingido ao art. 30.3 da Diretiva anterior, 95/46/EC. Esse entendimento é o qual ainda está "vigente" na esfera da agência *Data Protection Board* (EDPB), mediante a *Opinion 05/2014*, e remonta a uma interpretação "ampla" do que seria dado pessoal. A "polêmica" discórdia está em uma questão constitucional de fundo (*rule of law*) existente entre a *Opinion* de uma agência, o texto normativo da União e dos países que a compõe, e o Breyer *case*, julgado na *European Court of Justice*, em outubro de 2016.[11]

---

ser pontualmente relativizada, somente quando existir condições empíricas concretas de que haverá o comprometimento do exercício do controle social, nas "operações" realizadas pelo Poder Público.

[10] GROOS, D.; VAN VEEN, E.B. Anonymised data and the rule of law. EDPL 4/2020 – European Data Protection Law Review. n. 4, p. 1, 2020, p. 1.

[11] Ver o trabalho de GROOS e van VEEN (2020), referenciado neste artigo.

Para sumarizar a contenda, ostenta-se o seu núcleo, relacionado ao assunto objeto. Da referida *Opinion* extrai-se as seguintes diretivas, no tocante ao processo de anonimização de dados e seu formato legal: não deve ser possível i) identificar um indivíduo, ii) conectar registros à um indivíduo, e iii) ser possível inferir informação sobre um indivíduo. No item 2.2, *Legal Analyses*, antepõe-se que o processo de anonimização deve ser absoluto, no sentido de que os dados pessoais tratados sejam irreversíveis, comparando-se a técnica de anonimização, com a propria "exclusão permanente" dos dados objeto, na finalidade de impedir uma possível identificação.[12][13][14]

A *Opinion* reverbera a abordagem absoluta sobre o assunto (*absolute approach*), enquanto que, no Breyer *case*[15], com o parecer da *The Advocate General* (AG), se estabeleceu a adoção da abordagem relativa (*relative approach*)[16], onde a anonimização, e a sua reversão, é visualizada consoante o contexto de agentes, tecnologia disponível, meios legítimos ou ilícitos, as características dos dados pessoais (sensíveis ou não) e os direitos atrelados à eles (a LGPD abraça essa locução, "filtro de razoabilidade" embora não determine, "exaustivamente", a

[12] WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA. Opinion 5/2014: Anonymisation Techniques. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Acesso em: 15 out. 2020, p. 6: *Anonymisation can be a result of processing personal data with the aim of irreversibly preventing identification of the data subject"* (OPINION 05/2014, p. 6), complementando, com "*The underlying rationale is that the outcome of anonymisation as a technique applied to personal data should be, in the current state of technology, as permanent as erasure, i.e. making it impossible to process personal data".*

[13] WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA. Opinion 5/2014: Anonymisation Techniques. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.> Acesso em: 15 out. 2020, p. 6.

[14] Nessa mesma seção da *Opinon 05/2014*, faz-se referência a norma ISO 29100:2011, a qual dita ser o processo de anonimização um *"process by which personally identifiable information (PII) is irreversibly altered in such a way that PII principal can no longer be identified directly or indirectly, either by the PII controler alone or in collaboration with other party".*

[15] UNIÃO EUROPEIA. Tribunal de Justiça (Segunda Seção). Breyer case: C-582/14. 2016. Reenvio prejudicial — Tratamento de dados pessoais — Diretiva 95/46/CE — Artigo 2.º, alínea a) — Artigo 7.º, alínea f) — Conceito de 'dados pessoais' — Endereços de protocolo Internet — Conservação por um prestador de serviços de meios de comunicação em linha — Regulamentação nacional que não permite ter em conta o interesse legítimo prosseguido pelo responsável pelo tratamento. Recorrente: Patrick Breyer. Recorrido: Bundesrepublik Deutschland. Relatora: A. Rosas, 19 de outubro de 2016. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=PT>. Acesso em: 10 out. 2020.

[16] A Corte não se manifesta expressamente sobre qual a abordagem a ser adotada, embora faça referência direta ao parecer da AG, concordando com a sua posição, "*the combination of two known parties matters*".

situação. Esse ponto será levemente desenvolvido na próxima seção, sobre a necessidade de enriquecimento normativo dos critérios "de filtro de razoabilidade" e "identificabilidade").

Não se comentará detidamente sobre a decisão da Corte, mas, sim, apresenta-se necessário colar, em resumo, o parecer da AG quanto ao tema, referenciado, a propósito, na decisão Breyer, como indício semântico gerador de criatividade normativa, a ser pensado para o Brasil. Os dispositivos discutidos no caso Breyer são previstos na antiga Diretiva 95/46, art. 2º, "*a*" e, art. 7º, "*f*"[17]. O parecer da AG, estritamente sobre o assunto, comunga a locução de que, "meios que possam ser razoavelmente utilizados pelo controlador ou por qualquer outra pessoa", merece ser encarada com uma divisão da questão em duas aberturas normativas: i) "por qualquer pessoa" não deve se entender tal como por qualquer terceiro concebível. Essa interpretação estrita não descartaria a certeza de que um terceiro seria capaz de revelar a identidade de uma pessoa; e ii) "meio capaz/razoavelmente a ser empregado" não significa qualquer meio, mas formas razoáveis e não proibidas.[18][19]

A AG alia-se à abordagem relativa (*relative approach*), doutrina esta que não pergunta se é possível identificar/realizar a reversão de um dado anonimizado, mas, sim, se, na realidade, é possível (re)identificar um dado pessoal, por um controlador/agente, em um certo contexto, com a ajuda legítima de um terceiro conhecido, mediante meios legítimos. A AG, explicitamente, não possuiu a intenção de expandir o conceito-normativo de identificação para além das situações que possam, ou que geram "incerteza jurídica", para evitar a circunstância na qual um

[17] Art. 2º, "*a*": <Dados Pessoais>, qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social; art. 7º, "*f*": Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se: o tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº do artigo 1º.

[18] Conclusões do Advogado-Geral, op. cit.

[19] Original: *means likely reasonably to be used by the controller or by any other person*", alicerça-se em duas etapas: i) "*by any person should not be seen as any conceivable third party. That overly strict interpretation would never rule out with absolute certainty that a third party would be capable of revealing a person's identity;* e ii) "*means likely reasonably to be used" does not mean any means, but reasonable and not prohibited means*".

dado nunca deixe de ser considerado um dado pessoal.

Pode-se retirar algumas conclusões sobre essa questão. A primeira: um dado pessoal anonimizado, com a tecnologia existente, no mais das vezes, poderá ser objeto de reversão. Essa observação é causadora de ruídos na sistemática legal sobre a proteção de dados pessoais. Assim, sabendo-se dessa "realidade", torna-se necessário decidir, mediante um artificialismo jurídico-normativo, em busca de arquiteturas jurídicas articuladas com o atual estado da arte de tratamento de dados (filtro de razoabilidade/identificabilidade).

No julgamento do caso Breyer, e no parecer da *The Advocate General*, o ponto "estratégico" foi o desenvolvimento de uma concepção de "reversão" "legal" ou "ilegal" (atrelando-se ao instituto da identificabilidade), e, sobre o que seria, para o Regulamento Geral, um "dado/informação identificável", e seus consectários obrigacionais e de responsabilização, associados à perspectiva do agente responsável pelo tratamento e do titular dos dados, levando em conta a alta insegurança existente na abordagem absoluta (*absolute approach*), que leva à ideia de que qualquer reversão possível, por meios ilícitos ou legítimos, e por qualquer pessoa, debilita um processo de anonimização de dados (e seus também consectários obrigacionais e de responsabilização).

A segunda "conclusão": ambas as abordagens (relativa ou absoluta) possuem resultados não antecipáveis, embora seja observável a imprescindibilidade de se construir algumas diretivas (como está sendo feito na União Europeia, mesmo havendo a aludida divergência entre a posição da Corte de Justiça, e a perspectiva da agência administrativa). Uma primeira percepção: a abordagem relativa (*relative approach*) se importa com os mecanismos de segurança e de *due dilligence* na cadeia de agentes responsáveis pelo tratamento e suas "transferências", e proporciona maior "segurança" aos controladores, quando de processamento de dados "anonimizados" – limitando, portanto, a possibilidade de responsabilização e, em uma leitura perfunctória, os direitos dos titulares. Nesse horizonte (dos agentes/controladores), a abordagem absoluta (*absolute approach*) é deficitária, uma vez que, notando-se a possibilidade de reversão de dados anonimizados ser um consenso, se qualquer reversão, realizada por qualquer pessoa, ou por qualquer meio, ser tida como fundamento para ampliar a noção normativa de dados pessoais,

nenhum tratamento de dados anonimizados poderá ter a "segurança" normativa que, em tese, o atual Regulamento Geral visa proporcionar (e as leis nacionais).

Terceira conclusão: "é necessário ignorar a realidade". Havendo consenso sobre a possibilidade de reversibilidade de dados anonimizados, tem-se, simultaneamente, a ampliação da percepção normativa vinculada aos dados pessoais.[20] Cuida-se, por conseguinte, de minudências normativas capazes de causarem ruídos em um sistema jurídico que visa acoplar expectativas "cognitivo-normativas", pautando-se pela dinâmica (uma das) do *rule of law*, no âmbito de um razoável grau de certeza jurídica-normativa (*reasonable degree of certainty*).

A conectividade de dados, representada por sistemas de *Big Data,* transforma a possibilidade de reversão em faticidade. Disso se observa a necessidade da dita "artificialidade jurídico-normativa", para se viabilizar/fomentar/potencializar tratamentos de dados pessoais pautados em dados anonimizados, com respeito aos direitos dos titulares ou, simplesmente, optar pela debilitação de empreendimentos que utilizam dados anonimizados – se qualquer "identificação" for considerada requisito para a responsabilização, sem dúvidas haverá um "*Chilling Effect*" na maturação e desenvolvimento de projetos e, por via reflexa, de criação e coordenação de mecanismos de segurança e adequação na cadeia de tratamento de dados anonimizados.

3. A abordagem (*absolute ou relative)* brasileira, a doutrina da base legal, e a anonimização como direito dos titulares

No Brasil será preciso desenvolver uma estrutura normativa sobre a questão, sabendo-se do caráter transnacional da prática de tratamento de dados pessoais e, também, pensando-se em coerência com as expectativas cognitivo-normativas (espelhada na doutrina do *rule of law*), garantia a direitos, e fomento a projetos tecnológicos nacionais ou internacionalizados.

[20] Não cabe tecer as múltiplas consequências disso, mas, veja-se que, a "anonimização" enquanto direito dos titulares é diretamente afetada, e, também, a "segurança" das expectativas das partes envolvidas, forjada a partir da doutrina da "base legal para o tratamento".

3.1. Parâmetros em construção

"A antítese"[21] existente entre dado pessoal e dado anonimizado, reporta a uma grande complexidade. Um dado pessoal é a pessoa, e, "juridicamente", as suas particularidades enquanto pessoa são protegidas por um arcabouço constitucional garantidor de direitos (paradigma do Estado Constitucional Contemporâneo). Um dado pessoal possui uma configuração altamente relacionada com a dignidade da pessoa humana e seu livre desenvolvimento ou realização, como denomina Ascensão[22]. Um dado pessoal anonimizado representa a existência, em alguma circunstância, de um tratamento prévio, de um dado pessoal, com seu posterior processamento, que o transmutou em "dado anonimizado". Esse dado deixa de possuir, nos termos legais atuais (na União Europeia e no Brasil), um grau de proteção "forte". Entretanto, não se pode ignorar que, ainda, esses dados não deixam de ser "pessoais" – o que a Lei prevê é, apenas, que, um dado, considerado legalmente e/ou tecnicamente "anonimizado", não será "dado pessoal" e, por consequência, "não será encarado com o mesmo tratamento" que o dado considerado "pessoal" por esta mesma lei (é um artifício legal, pois).

Não se ignora que, a dificuldade de identificação/filtro de razoabilidade, sem dúvidas, faz parte de uma estruturação legal e técnica sobre a noção de dado "anonimizado", que explora as distinções existentes entre uma "fácil identificação" e uma "difícil identificação" (filtro de razoabilidade – esse, por acaso, é um dos elementos mais complexos sobre a matéria. Não obstante, uma pessoa, não identificável "facilmente", classificada em certo grupo, mediante processamento de dados anonimizados e vinculado à *Big Data*, poderá sofrer danos em razão de uma "classificação absolutizante" ou, ainda, de uma "classificação equivocada ou preconceituosa" (problemas epistêmicos de fundo, graves, sobre a matematização do mundo). O espaço protetivo, nessas hipóteses, vincula-se aos riscos inerentes a prática de tratamento de dados, não, necessariamente, relacionando-se à

[21] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 111.
[22] ASCENSÃO, J. O. A dignidade da pessoa e o fundamento dos direitos humanos. Revista da Faculdade de Direito da Universidade de São Paulo, v. 103, p. 277-299, jan./dez .2008, p. 16.

preocupação de "quais dados estão sendo tratados", e os riscos e garantias específicos a eles.

A LGPD, por acaso, se importa com esse contexto. No dispositivo cujo conteúdo prevê a exclusão legal, *caput*, do art. 12 "os dados anonimizados não serão dados pessoais para os fins desta Lei [...], há, no § 2º, o seguinte texto normativo: "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada". Ou seja, um dado pessoal considerado anonimizado ainda poderá ser considerado um dado pessoal para os "os fins da Lei", nessas situações específicas (mas não apenas nelas, relembra-se).

A parte final desse parágrafo, "se identificada", visa conectar-se, pois, com a possibilidade de "identificação" de um dado anonimizado, estando esse instituto, da "identificabilidade", como já exposto na seção anterior, possuidor de muitas variáveis que necessitam ser sopesadas (a divergência na União Europeia é exemplo disso), no centro normativo da controvérsia. No mesmo art. 12, *caput*, diz-se, que, "os dados anonimizados não serão considerados dados pessoais [...] salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou, quando, com esforços razoáveis, puder ser revertido. No § 1º, busca-se trazer indícios semânticos para a construção de uma normatividade: A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios, aspecto subjetivo. E, ainda, no § 3º, do art. 12, convida-se a Autoridade Nacional de Proteção de Dados (ANPD), ouvido o Conselho Nacional de Proteção de Dados Pessoais (CNPD), "a dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança".

Em uma primeira leitura, parece que, o texto normativo da LGPD encerra o "objeto": no *caput*, do art. 12, há o excerto "utilização exclusiva de meios próprios", e no parágrafo § 1º, do art. 12, também, com a mesma locução, "utilização exclusiva de meios próprios". Existe, portanto, uma suposta "desvinculação" entre os agentes de tratamento, em eventual "cadeia de tratamento de dados anonimizados" e eventuais "terceiros".

Em um mundo ideal, ou fantástico, essa, com efeito, seria a solução mais adequada, no sentido de incumbir, a cada agente responsável, com "proporcionalidade" à suas possibilidades e atribuições, o nível de "responsabilidade". Muito embora louvável, salienta-se o desajuste desse comando legal (se entendido da maneira colocada supra), com a realidade existente, no que toca ao paradigma poroso (o estado da arte da alta conectividade) do tratamento de dados, e da ubiquidade informacional da contemporaneidade. A normatividade criticada não é adequada à perspectiva dos agentes de tratamento e suas parcerias comerciais, por exemplo, e, ainda, é redutora em demasia do próprio núcleo protetor dos direitos dos titulares, e este déficit se apresenta mais acentuado quando se tem em vista a anonimização de dados pessoais sensíveis.

Alude-se a essa "hermenêutica" justamente para mostrar, com poucas linhas, a sua "equivocidade", e, ainda, para notar, no próprio *caput* do art. 12, a previsão, em texto normativo, de outra possibilidade hermenêutica, mais atenta ao "atual paradigma" de tratamento de dados pessoais: "os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, *ou quando, com esforços razoáveis, puder ser revertido* (grifo nosso). A parte final do art. 12 corrobora para uma abertura semelhante à existente na União Europeia, trazendo, a propósito, os mesmos graus de complexidade e de possíveis divergências, cujas soluções, em busca de convergências, serão impreteríveis também no Brasil.

O que será tido como "esforços razoáveis"? De "quem"? De "qualquer terceiro", hackers e operadores? De "qualquer parceiro comercial ou de pesquisa"? Mediante "qualquer meio", ou seja, por mecanismos "legítimos" e "ilícitos? No § 1º, do artigo 12, parágrafo que visa dar amostras textuais-normativas para a solução desses problemas, não há um "regramento explícito" sobre a matéria: "a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios". O § 1º, do art. 12, parte final, utiliza-se da locução "*e a utilização exclusiva de meios próprios*" e pode,

para alguns, externalizar uma normatividade "fechada", simplesmente "subjetiva" e "enclausuradora", já criticada anteriormente.

Essa "análise" perfunctória, sobre o texto normativo da LGPD, realça uma problemática semelhante à existente atualmente na União Europeia. Como a "identificabilidade" de um dado pessoal anonimizado será vista no Brasil? A abordagem será a absoluta ou a relativa (*absolute ou relative approach*)? Estamos limitados a elas? Impossível, por claro, estabelecer as respostas antes das perguntas, mas o aviso de se ter como imprescindível a construção de uma normatividade adequada, a partir dessas orientações, especialmente quando de dados pessoais "sensíveis", está constituído.

No que toca à abordagem absoluta (*absolute approach)*, acredita-se que deverá ser descartada, observando-se as atuais possibilidades de reversão de dados pessoais anonimizados. Adotando-se a abordagem absoluta, avança-se na ampliação da concepção normativa de dado pessoal – todo dado pessoal deverá ser considerado pessoal, independentemente de um "procedimento" de anonimização. Essa percepção, sem dúvidas, causará espécie de "*Chilling Effect*" em empreendimentos (não apenas econômicos e privados, mas estatais e vinculados às políticas públicas) que detêm, como formato produtivo, o uso de inteligência artificial e dados anonimizados. A propósito, o dito não se pauta por uma fundamentação "consequencialista", "de ponderação", ou "*balance*" ou, ainda, de defesa sem críticas ao uso de "inteligência artificial e dados anonimizados".

A questão está relacionada ao fato de ser impossível ter-se certeza, na perspectiva dos agentes responsáveis pelo tratamento e titulares (pois a anonimização, não se esqueça, é também um direito), sobre as possibilidades de novas tecnologias de desanonimização – isso está fora da esfera de "controle" das partes, e gera uma incerteza jurídica contínua, que, a princípio, a abordagem absoluta ignora (da locução no texto normativo, a saber, "tecnologias disponíveis", não se pode concluir que advirá uma normatividade robusta sobre a questão, até porque, atualmente, a reversão de dados anonimizados é "solo comum"). Para aclarar o dito: não é importante, apenas, saber sobre a exequibilidade de reversão de dados "y", anonimizados. Há de se considerar, em quais contextos os dados "y", anonimizados, poderão ser "desanonimizados", e qual formato de desanonimização será

considerado como "responsabilizável" (se por qualquer terceiro, ou parte conexa, ou, se, por qualquer meio, "legítimo" ou ilícito"). Ocorre, com efeito, um enriquecimento normativo com a abordagem relativa, no tocante ao "filtro de razoabilidade" e "identificabilidade", o qual não se "pode" construir com a abordagem absoluta.

A abordagem relativa (*relative approach*), de modo a complementar o já exposto, é capaz, pois, de, ao mesmo tempo, ter como pressuposto a contingência da reversão de dados anonimizados (ela não ignora essa realidade), e repercutir em uma distribuição de responsabilidades entre os agentes responsáveis pelo tratamento e, ainda, permitir e fomentar a construção de mecanismos de governança atinentes e preocupados com os direitos de titulares e seus respectivos dados e espécies. Não se trata, simplesmente, de "reduzir o arcabouço normativo" da noção de "dados pessoais".

O enfoque a ser constituído, quanto à "identificabilidade" de dados anonimizados, é determinante para a regulação da proteção de dados pessoais como direito dos titulares, e, reflexamente, para se estabelecer parâmetros ao desenvolvimento socioeconômico que determinada comunidade declarará como constitucionalmente legítima, por intermédio do desenvolvimento tecnológico realizável com os "dados pessoais".

3.2. Impactos perceptíveis sobre a doutrina da "base legal do tratamento anonimização" vs. Anonimização enquanto direito dos titulares

O ângulo normativo até o momento apresentado expõe a máxima de que um "texto", no caso, um "texto normativo", nunca está sozinho. A sua leitura depende de outros textos e de uma concepção de "nós", de uma intersubjetividade. Não se mostra possível trazer uma abordagem mais robusta ou abrangente sobre a questão, e, por isso, o texto será desenvolvido, na parte final, com enfoque aos impactos da doutrina da "identificabilidade" (e suas percepções distintas) na doutrina da "base legal do tratamento anonimização" vs. anonimização enquanto direito dos titulares.

No que diz respeito à concepção/doutrina da "base legal do tratamento", pode-se afirmar que, há, no mínimo, uma dupla formatação jurídico-normativa. Julga-se, assim, "a base legal do tratamento", como uma extensão dos direitos dos titulares,

vista enquanto manifestação "objetiva" e "subjetiva" dos direitos fundamentais (na concepção doutrinária contemporânea). A partir do horizonte do titular, a base legal do tratamento, busca garantir meios idôneos para que o titular de dados pessoais saiba de, e possa acionar, verdadeiramente, os seus direitos. A saber, se um tratamento de dados está sendo realizado por meio da base legal "consentimento", subsiste uma gama de direitos e garantias voltadas ao titular dos dados, apenas para citar, os requisitos "livre, informada e inequívoca" e a "revogação do consentimento a qualquer momento" – e o mesmo se dá, especificamente ao tema do artigo, quanto à "anonimização". O processo de anonimização, visualizado como direito dos titulares, é de suma importância, principalmente para aqueles tratamentos voltados a dados sensíveis e, ainda, aos riscos inerentes de qualquer "tratamento de dados pessoais".

Da mesma paragem, a perspectiva dos agentes responsáveis pelo tratamento é guiada pela "base legal do tratamento". Verificando-se todas as particularidades exigíveis para um tratamento 'y' ser lícito, o agente responsável buscará respaldo jurídico-normativo com fundamento na "base legal para o tratamento" eleita. Trata-se, portanto, de uma expectativa cognitivo-normativa recepcionada pela doutrina do *rule of law*, em uma das suas particularidades elementares, assim denominada de razoável grau de certeza jurídica-normativa (*reasonable degree of certainty*).

Com isso, questiona-se: qual a "melhor" abordagem, sobre a "identificabilidade", apta a construir uma normatividade congruente aos horizontes comentados, dos titulares de dados pessoais, e de agentes responsáveis?

Antepõe-se, de pronto, que, a "multiplicidade" de base legal para "um mesmo" tratamento é absolutamente necessária e, ainda, harmônica ao caráter protetivo de qualquer arcabouço legal contemporâneo, no qual se visa regular "dados pessoais". Tal ideia é apoiada, aliás, na perspectiva normativa "ampla" sobre a base legal intitulada de "legítimo interesse", que corresponde, em suma, à seguinte condição normativa: todo tratamento de dados pessoais deve possuir um "legítimo interesse" – essa noção é adequada constitucionalmente, pois eleva o grau protetivo dos direitos dos titulares. Por exemplo, não basta o consentimento (com o preenchimento de todos os requisitos) para um tratamento de dados 'y', com a base legal "consentimento", ser considerado lícito. Os agentes responsáveis necessitam se

adequar à normatividade constitucional e infraconstitucional protetiva "objetiva", e essa "adequação" se realiza por uma substancial condução do tratamento a ser confeccionado, condicionado a um "legítimo interesse".

Entretanto, a base legal "anonimização" é de muito complexa, e demanda, em sua "desenvoltura interna", a construção de elementos atinentes a cada formato especifico de "anonimização" e "espécie de dado", e tal complexidade, enquanto direito dos titulares, expande-se, em razão de possuir um regime jurídico diferenciado – o instituto da "base legal" enquanto direito é consenso, contudo, a base legal "anonimização" é a única especificamente valorizada no art. 18, da LGPD, particularmente, no inciso IV (Capítulo III – Dos Direitos do Titular), e isso quer dizer muitas coisas - temos que ouvir o que os textos nos dizem, e o que o mundo imprime em "nós", e "Ter mundo quer dizer comportar-se para com o mundo. Mas comportar-se para com o mundo exige, por sua vez, que nos mantenhamos tão livres, face ao que nos vem ao encontro a partir do mundo, que consigamos pô-lo ante nós tal como ele é" como notifica Gadamer[23].

Diante disso, e pretendendo "escutar a mensagem que o texto emite", é possível "deduzir" que, a normatividade a ser buscada é aquela que requer uma construção envolta à "anonimização", enquanto base legal de tratamento, a partir de uma aproximação preocupada com a "anonimização" enquanto direito dos titulares, e não, simplesmente, enquanto expectativa-segurança jurídica dos agentes responsáveis pelo tratamento.

É justamente nessa perspectiva que o debate exposto anteriormente se insere (e impacta). A estruturação de uma normatividade, relativa ao instituto da "identificabilidade" de dados anonimizados, remonta-se ao contexto imprescindível de se decidir qual abordagem regula tais situações de maneira ótima, a partir, repetindo-se, da anonimização enquanto direito dos titulares, preponderantemente, e, por claro, enquanto expectativa de "segurança jurídica" dos agentes responsáveis pelo tratamento. Os elementos a serem constituídos, portanto, devem exsurgir com esse pressuposto.

[23] GADAMER, Hans-Georg. Verdade e método. Petrópolís: Vozes, 1999, p. 643.

Para avançar na discussão, é preciso tecer mais apontamentos específicos sobre as abordagens, absoluta e relativa, a respeito da "identificabilidade" (*absolute and relative approach*) e o quadro da "base legal anonimização" como direito dos titulares. A abordagem absoluta questiona: é possível a reversão de um dado anonimizado? Se a resposta for, apenas, "sim", sem qualquer outra perspectiva a ser ponderada, o dado pessoal transmutado em "anônimo" terá o mesmo tratamento que qualquer outro dado pessoal (o procedimento de anonimização será "inútil", e a concepção normativa de dado pessoal será "extensa"). No sentido contrário, tem-se que, a anonimização enquanto direito, é esvaziada normativamente, porque "inútil". Essa observação precisa ser melhor desenvolvida em um trabalho específico, não obstante seja possível incrementar, sucintamente, o que se está a defender.

A abordagem absoluta (*absolute approach*) carrega, em sua opção, a realidade da "reversão" de dados anonimizados, sem ponderar as partes inseridas nas práticas ubíquas de tratamento – ampliando-se a noção de dados pessoais e, ao mesmo tempo, transmitindo, aos agentes responsáveis, que, inobstante todos os cuidados concatenados internamente, ou com contatos externos (parceiros, por exemplo), se um terceiro qualquer, mediante ato legítimo ou ilícito, conseguir "desanonimizar" os dados tratados e os empregar para fins 'x', haverá possibilidade de responsabilização (tanto por agências, judiciário etc., quanto individualmente, em ações buscando reparações, de cada titular). Essa perspectiva gera uma contínua e absoluta atmosfera de incertezas, e, releva-se, a todas as partes envolvidas.

Veja-se, a realidade de ser viável a reversão de dados anonimizados não é ignorada pela abordagem relativa (*relativa approach*), tampouco se intenta, mediante essa percepção, "escapar" da normatividade da LGPD (e de outros textos normativos que preservam a proteção de dados pessoais). Muito pelo contrário, espera-se, com essa abordagem, constituir, a partir do horizonte do titular de dados, novas estruturas normativas e de governança capazes de fomentar um arcabouço institucional que assuma a complexidade dessa situação e, ao conjunto, promova a todos os agentes responsáveis possíveis, a arquitetura de projetos contundentes para o seu enfrentamento – acredita-se que, "ampliar" a noção normativa de dados pessoais, que é o que faz a abordagem absoluta, sem considerar as inúmeras variáveis perceptíveis, e a serem constituídas com o tempo, não seja a melhor opção.

Não se esqueça, a propósito, do art. 12, § 2º, da LGPD, já citado anteriormente, que acresce normatividade relevante à anonimização enquanto direito dos titulares (tema do perfilamento mediante dados anonimizados e decisões automatizadas, e eventuais prejuízos a interesses e direitos de titulares). Com a abordagem relativa, intenta-se fortalecer esse direito, exatamente por se aproximar a uma conjunção de "mais de uma base legal para o tratamento de dados pessoais ser lícito", funcionalizada/conexa à base legal mais relevante de um sistema de proteção de dados pessoais, qual seja, "do interesse legítimo", de um controlador e seus parceiros (há uma discussão no que toca a parceiros e subcontratados), ou terceiros, sabendo-se que, esse fragmento normativo, demanda desenvolvimento próprio, mas sendo cabível elencar que, o "interesse legítimo", não se molda a partir do que o controlador, individualmente, crê ser legítimo à sua atividade, mas, sim, a partir dos direitos dos titulares (em dimensões subjetiva e objetiva) e suas respectivas e razoáveis expectativas, relacionadas à atividade do agente de tratamento, normatizada a partir dos riscos inerentes a qualquer tratamento de dados a ser conduzido por intermédio dos deveres de diligência (arts 10, 37, art. 6º, I, 7º, IX e § 7º, da LGPD).[24]

Ainda, por intermédio da abordagem relativa, que é adotada, parcialmente, no texto normativo do art. 12, *caput,* e § 1º, da LGPD, torna-se possível incrementar os postulados insuficientes, embora observáveis, a partir do texto. Referencia-se o texto, novamente: utilizando "exclusivamente meios próprios", ou quando, "com esforços razoáveis, puder ser revertido"; a determinação do que seja razoável deve levar em consideração "fatores objetivos", tais como "custo e tempo", [...] "de acordo com as tecnologias disponíveis", e a "utilização exclusiva de meios próprios". A previsão, no *caput* "ou, quando, com esforços razoáveis, puder ser revertido", somada a "custo e tempo, de acordo com as tecnologias disponíveis, [...] e a utilização exclusiva de meios próprios", no § 1º, não pode levar a uma "compreensão/hermenêutica enclausurada" no tocante à problemática, alhures criticada, de passagem (o ignorar

[24] Mesmo que se discorde da doutrina da "ponderação", acolhida em muito no território brasileiro e europeu, cita-se a "ponderação" alocada pelo GT 29, no parecer 06/2014, sobre o conceito de interesses legítimos, em sede da União Europeia: i) avaliação do interesse legítimo do responsável pelo tratamento; ii) impacto nas pessoas em causa; iii) equilíbrio provisório; e iv) as garantias complementares aplicadas pelo responsável pelo tratamento para evitar qualquer impacto indevido nas pessoas em causa. Cada item contém outras características a serem "ponderadas".

das práticas de tratamento de dados pessoais anonimizados, intercambiáveis, e a ubiquidade informática).

No caso, se constituída uma normatividade, no grau de "identificabilidade", envolta a "qualquer terceiro", e "qualquer meio", oportunamente usados para o processo de desanonimzação, em verdade, com a LGPD, pode-se concluir, pela adoção da abordagem absoluta, com alguns indícios (tempo, custos, tecnologia disponível, meios próprios) da abordagem relativa, todavia, transformados em inutilidade: eis o ponto que impregna, com corrosão, toda a "sistemática" reguladora da lei, em relação aos dados pessoais anonimizados. Ademais, se haver uma compreensão fechada, sobre o postulado, "utilização exclusiva de meios próprios", também se estará postando uma normatividade insuficiente, individualizada, a qual, mediante a abordagem relativa (*relative approach*), também se descarta.

O "filtro de razoabilidade"/identificabilidade necessita ser desenvolvido com suas especificidades, e os elementos apresentados nesse texto servem somente para inicializar uma discussão, porque, e peca-se pela repetição: antes de visar o tema na finalidade de se ter "segurança jurídica para o tratamento", deve-se alocar o tema da anonimização enquanto direito dos titulares (ou seja, para todos os tipos de tratamento de dados, pessoais e/ou pessoais anonimizados), notando-se que, as estruturas jurídico-normativas e técnicas de sistemas merecem, antes, se pautar por medidas robustamente preventivas, mas cientes de suas falibilidades.[25]

Em outras palavras, a anonimização de há muito não cumpre o papel que representava no passado [26], e a aliança com outros mecanismos de

[25] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust de-anonymization of large sparse datasets: a decade later. Maio. 2019, p. 1.: The flood of de-anonymization demonstrations in the last decade makes for a strong argument that database privacy should rest on provable guarantees rather than the absence of known attacks [...] the truism that attacks get better applies not only to de-identification, but also to other data protection mechanisms such as searchable database encrypton and privacy-preserving machine learning. Schemes without provable guarantees in these areas were broken, too, by drawing on the auxiliary information from public databases.

[26] NARAYANAN; SHMATIKOV, op. cit., p. 1-3: if we want sophisticated privacy technologies to be adopted, we need to work on the sociotechnical infrastructures that minimize the gap between privacy guarantees and perception of privacy. Those infrastructures are sorely lacking today. We live in a world of massive aggregations of personal data. This leads to many privacy risks, of which de-anonymization is just one. […] Furthermore, over the last decade, we have come to realize the privacy implications of the ability to infer sensitive facts about people from seemingly innocuous data, such as pregnancy from shopping records or psychometric traits from Facebook likes. We have also come to better recognize that these aggregations of data may result in harms to society and democracy, rather than just to individuals, as illustrated by Cambridge Analytica's activities. In contexts such as

privacidade/proteção de dados são imperativos, notadamente em razão da miríade de relações complexas que, contemporaneamente, acorrem na sociedade, por intermédio de processamento de dados em grande escala, e os efeitos sociotécnicos, também distintos e imprevisíveis, que essas práticas geram - a abordagem relativa reivindica essa postura.

A confabulação de planos/políticas de desenvolvimento tecnológico é, sem dúvidas, componente fundamental para se ter uma sólida aproximação sobre o tema, entretanto, a hermenêutica/normatividade jurídica, oriunda dos textos normativos, faz-se protagonista nesse cenário, o qual, no Brasil (e também em outros lugares do mundo), ainda carece de maior desenvolvimento – com novas "hermenêuticas" ou, ainda, mediante novos passos regulatórios. Esse ponto de vista é corroborado, a saber, por HOFFMANN-RIEM[27], que alerta sobre a interseccionalidade das relações sociotécnicas e, sobre a necessária construção de normatividades também preocupadas em serem multifacetárias.

Acredita-se que, com a abordagem relativa sobre o instituto da identificabilidade/filtro de razoabilidade, ocorre uma potencialização de criatividade linguística-normativa sobre os critérios jurídicos disponíveis para aferição concreta das situações de "desanonimização", e de seus riscos, havendo direta correlação do assunto discutido, com a figura do relatório de impacto, e as possíveis consequências sancionatórias de um ilícito de dados, tais como as condições de *algorithmic destruction*[28], para os titulares e agentes de tratamento.

Como elencado nesse texto, sem qualquer pretensão de exaustão, assumir essa posição de abertura poderá ser um excelente ponto de partida para se criar um enfrentamento lúcido à essa conjuntura.

behavioral advertising, scholars argue that the power to influence behavior is deeply problematic even if the data is never linked to a real-world identity.

[27] HOFFMAN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital – desafios para o direito. Rio de Janeiro: Forense, 2021, p. 47-48.

[28] LI, Tiffany. Algorithmic destruction. SMU Law Review, forthcoming. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4066845>. Acesso em: 05 jun. 2022.

4. Conclusão

De maneira transitoriamente conclusiva, a partir das digressões apresentadas nesse texto, é possível defender uma postura de preocupação com a anonimização de dados pessoais enquanto direito dos titulares. As abordagens, absoluta e relativa, (*absolute and relative approach*), vinculadas ao tema da identificabilidade/filtro de razoabilidade, fazem parte de um projeto normativo que sinaliza um cuidado com a questão.

Descarta-se a abordagem absoluta, por esta paragem ignorar os "trâmites" ubíquos dos tratamentos de dados pessoais e não pessoais, e das práticas realizadas com dados anonimizados mediante *Big Data*. A simples elasticidade da noção normativa de dado pessoal, resultado da abordagem absoluta, não apresenta respostas adequadas para o enfrentamento da problemática.

A abordagem relativa, por outro lado, aspira a produzir mecanismos relevantes para ampliar o escopo protetivo sobre os dados pessoais anonimizados, assumindo a viabilidade de reversão com lucidez, fazendo-se, com isso, um fomento para a construção de um razoável grau de certeza jurídico-normativo (*reasonable degree of certainty*), tanto para os agentes responsáveis, quanto para os titulares de dados (pessoais e não pessoais), focando-se na "base legal para o tratamento de dados anonimizados", a partir de uma aproximação sobre o assunto, preponderantemente, como direito dos titulares, e, não, apenas, como "segurança jurídica para os agentes de tratamento". Não se trata, apenas, de "diminuição" da normatividade relativa a dados pessoais, muito pelo contrário.

Especificamente, o enriquecimento linguístico-normativo, atinente ao instituto da "identificabilidade/filtro de razoabilidade", exibe-se imprescindível. A divergência na União Europeia, exposta de passagem, forma um indício semântico de abertura criativa para novas observações, considerando, igualmente, a insuficiência "expressa" no texto normativo da LGPD. Eis o questionamento: qualquer procedimento de desanonimização será considerado responsabilizável? Nessa pergunta se insere: realizado por qualquer pessoa, portanto? Independente do meio empregado, sendo lícito ou ilícito? Tem-se que, essas questões abrem espaço para novas indagações, não abordadas no texto.

A abordagem relativa, sobre a anonimização enquanto base legal e direito dos titulares, somada à base legal imprescindível-estruturante para qualquer quadro normativo de proteção de dados pessoais, tal qual, "legítimo interesse", observada ampliativamente, enquanto eixo dos próprios direitos fundamentais dos titulares, forja (ou potencializa) novos arranjos normativos capazes de orientar qualquer tratamento de dados pessoais anonimizados, ou não anonimizados, com níveis maiores de esclarecimento sobre a circunstância estudada ("a cadeia de tratamentos", a reversibilidade de dados anonimizados, os riscos para os agentes e para os titulares).

Reporta-se ao estudo de Cordeiro[29], sobre a multiplicidade a ser considerada quando de tratamento de dados pessoais fundamentado em interesses legítimos, e antepondo, como pedra angular para o assunto, o defendido neste artigo, quanto ao "grau de identificabilidade dos dados". São três os eixos: Dados i) tipo ou a natureza dos dados pessoais tratados; ii) o grau de identificabilidade do titular dos dados; iii) a quantidade de dados objeto de tratamento; iv) a origem dos dados; e v) a qualidade dos dados; Partes i) o titular dos dados – natureza e característica; ii) número de titulares afetados pelo tratamento; iii) o número de entidades envolvidas no tratamento; iv) a natureza da relação existente entre o titular e o responsável; v) as expectativas dos titulares dos dados em relação às finalidades do tratamento; e vi) a eventual participação de responsáveis ou de subcontratantes não estabelecidos na União/no Brasil no processo de tratamento; Tratamento i) modo como o tratamento se realiza; ii) o tipo de tratamento realizado; iii) a duração do tratamento; iv) a freqüência do tratamento; v) os propósitos subjacentes ao tratamento; vi) o impacto do tratamento na esfera jurídica do titular. Colocadas essas observações, também há direta correlação do tema, com desenvolvimentos afeitos ao instituto do relatório de impacto, e as possíveis consequências sancionatórias de um ilícito de dados, tais como as condições de *algorithmic destruction*, para os titulares e agentes de tratamento.

[29] CORDEIRO, A.B.M. O tratamento de dados pessoais fundado em interesses legítimos. Revista de direito e tecnologia, n. 1, p. 1-31, 2019. Disponível em: <https://blook.pt/publications/publication/29c85b840a65/> . Acesso em: 06 mar. 2021, p. 28-29.

O Direito, enquanto instituto socionormativo, ao lado de políticas direcionadas ao desenvolvimento tecnológico, será determinante nessa caminhada. Ambas as esferas são constituídas por intermédio de uma hermenêutica intersubjetiva, defrontada com a faticidade. A abertura defendida nesse texto compromete-se com essa postura.

Referências bibliográficas

ASCENSÃO, J. O. A dignidade da pessoa e o fundamento dos direitos humanos. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 103, p. 277-299, jan./dez.2008.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo tratamento de dados pessoais pelo poder público**. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em: 02 jun. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 15 nov. 2020.

CORDEIRO, A.B.M. O tratamento de dados pessoais fundado em interesses legítimos. **Revista de direito e tecnologia**, n. 1, p. 1-31, 2019. Disponível em: <https://blook.pt/publications/publication/29c85b840a65/>. Acesso em: 06 mar. 2021.
GADAMER, Hans-Georg. Verdade e método. Petrópolís: Vozes, 1999.

GROOS, D.; VAN VEEN, E.B. Anonymised data and the rule of law. EDPL 4/2020 – **European Data Protection Law Review**. n. 4, p. 1, 2020.

HOFFMAN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital – desafios para o direito**. Rio de Janeiro: Forense, 2021.

HABERMAS, Jürgen. **Direito e democracia: entre facticidade e validade**, volume 1. Rio de Janeiro: Tempo Brasileiro, 1997.

LI, Tiffany. Algorithmic destruction. **SMU Law Review**, *forthcoming*. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4066845>. Acesso em: 05 jun. 2022.

LUHMANN, Niklas. **Sociologia do Direito II**. Rio de Janeiro: Tempo Brasileiro, 1985.

____. La ciencia de la sociedad. Anthropos: México, 1996.
NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of large sparse datasets. *In:* **IEEE Symposium on Security and Privacy**, Oakland, 2008. p. 111-125. Disponível em: <https://ieeexplore.ieee.org/abstract/document/4531148#:~:text=Robust%20De-anonymization%20of%20Large%20Sparse%20Datasets%20Abstract:%20We,individual%20preferences,%20recommendations,%20transaction%20records%20and%20so%20on>. Acesso em: 15 out. 2020.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust de-anonymization of large sparse datasets: a decade later**. Manuscrito. maio, 2019. Disponível em: <https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf>. Acesso em: 10 out. 2020.

UNIÃO EUROPEIA. Tribunal de Justiça (Segunda Seção). **Breyer case: C-582/14. 2016**. Reenvio prejudicial — Tratamento de dados pessoais — Diretiva 95/46/CE — Artigo 2.º, alínea a) — Artigo 7.º, alínea f) — Conceito de 'dados pessoais' — Endereços de protocolo Internet — Conservação por um prestador de serviços de meios de comunicação em linha — Regulamentação nacional que não permite ter em conta o interesse legítimo prosseguido pelo responsável pelo tratamento. Recorrente: Patrick Breyer. Recorrido: Bundesrepublik Deutschland. Relatora: A. Rosas, 19 de outubro de 2016. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=PT>. Acesso em: 10 out. 2020.

UNIÃO EUROPEIA. Tribunal de Justiça (Segunda Seção). Breyer case: C-582/14. 2016. **Conclusões do Advogado-Geral**. Manuel Campos Sánchez-Bordona. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid178241&doclang=PT>. Acesso em: 20 out. 2020.

WARAT, Luis Alberto. **Introdução geral ao direito III: O Direito não estudado pela teoria jurídica moderna**. Porto Alegre: Fabris, 1997.

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA. **Opinion 5/2014: Anonymisation Techniques**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Acesso em: 15 out. 2020, p. 6.