

CENTRO UNIVERSITÁRIO AUTÔNOMO DO BRASIL
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITOS FUNDAMENTAIS E
DEMOCRACIA – MESTRADO E DOUTORADO

ROBSON PASCOAL PEREIRA

DIREITO FUNDAMENTAL AUTÔNOMO À PROTEÇÃO DE DADOS PESSOAIS E
A EFICÁCIA DO CONSENTIMENTO NA LGPD

CURITIBA
2023

ROBSON PASCOAL PEREIRA

**DIREITO FUNDAMENTAL AUTÔNOMO À PROTEÇÃO DE DADOS PESSOAIS E
A EFICÁCIA DO CONSENTIMENTO NA LGPD**

Dissertação apresentada ao Programa de Pós-Graduação stricto sensu em Direitos Fundamentais e Democracia, Centro Universitário Autônomo do Brasil, para obtenção do grau de Mestre em Direito.

Orientador: Prof. Dr. Paulo Ricardo Schier

CURITIBA

2023

Ficha catalográfica elaborada pelo Sistema Universitário de Bibliotecas (UniBrasil), com os dados fornecidos pelo(a) autor(a)

Pereira, Robson Pascoal

Direito fundamental autônomo à proteção de dados pessoais e a eficácia do consentimento na LGPD. /

Robson Pascoal Pereira. -- Curitiba, 2023.

133 f.

Orientador: Prof. Dr. Paulo Ricardo Schier

Dissertação (Mestrado) - UniBrasil, 2023.

1. Direitos Fundamentais. 2. Privacidade. 3. Lei Geral de Proteção de Dados. I. Schier, Paulo Ricardo, orient. II. Título.

TERMO DE APROVAÇÃO

ROBSON PASCOAL PEREIRA

DIREITO FUNDAMENTAL AUTÔNOMO À PROTEÇÃO DE DADOS PESSOAIS E A EFICÁCIA DO CONSENTIMENTO NA LGPD

Dissertação aprovada como requisito parcial para a obtenção do grau de Mestre em Direito pelo Programa de Pós-Graduação stricto sensu – Curso de Mestrado em Direitos Fundamentais e Democracia do Centro Universitário Autônomo do Brasil – UniBrasil, pela seguinte banca examinadora:

Orientador: Prof. Dr. Paulo Ricardo Schier

Centro Universitário Autônomo do Brasil - UniBrasil

Avaliadores: Profa. Dra. Cinthia Obladen de Almendra Freitas

Pontifícia Universidade Católica do Paraná – PUCPR

Prof. Dr. Bruno Meneses Lorenzetto

Centro Universitário Autônomo do Brasil - UniBrasil

Curitiba, 26 de abril de 2023.

AGRADECIMENTOS

A jornada do mestrado me trouxe gratas surpresas. As horas de estudo, as leituras (nem tanto os fichamentos) foram mais do que aprendizado. Foram, verdadeiramente, momentos prazerosos. As aulas, apesar de no início de forma remota, eram oportunidades de conversa com amigos. Amigos que ganhei durante o curso.

Agradeço o corpo docente da instituição. Todos os professores com quem pude aprender muito e compartilhar ideias. Tive a felicidade de ter convido com excelentes profissionais, cuja dinamicidade e a capacidade de condução das aulas me impressionaram. Cada um com suas particularidades, mas sempre com a mesma paixão pelo ensino.

A mesma sorte que me apresentou com o orientador Prof. Paulo Schier. Além da inquestionável competência, foi meu professor em duas disciplinas, conduzidas de forma diversa, mas igualmente extraordinárias. Aulas que me fizeram pensar nos direitos fundamentais por outras perspectivas e que solidificaram minha escolha da dissertação. Agradeço os materiais e os essenciais direcionamentos na pesquisa.

Agradeço a minha esposa Kellen, que me apoiou nestes dois anos. Além de minha revisora dos artigos, foi quem me ouviu explicar o que eu pretendia com cada texto. Apesar de não ser da área jurídica, tinha a paciência de repetidas vezes me ouvir criticar modelos para os quais eu não tinha resposta.

Enfim, agradeço os que, ainda que não nominados, participaram deste processo que, como diziam alguns professores, “vai ser duro, mas igualmente recompensador”.

“A proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isso a cada momento não é verbosidade, pois toda mudança que afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar.”

Stefano Rodotà

RESUMO

O presente trabalho tem como objetivo o estudo do direito fundamental à proteção de dados pessoais e a avaliação do consentimento, qualificado na Lei Geral de Proteção de Dados como uma manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados. Apesar da inexistência de hierarquia entre as hipóteses de tratamento de dados pessoais, o consentimento é considerado um dos pilares do respeito à privacidade e a autodeterminação informativa. A pesquisa busca avaliar se o consentimento, ao invés de servir de abrigo ao direito fundamental à proteção de dados pessoais, pelo contrário, não legitima o tratamento de dados pelo Estado e pelo mercado. Problema este que se amplifica em uma sociedade cada vez mais marcada pelo uso e compartilhamento de dados comportamentais, por meio de um modelo de vigilância que arquiteta uma nova forma de poder e controle social. Partindo da hipótese de que é demasiadamente complexa a possibilidade em se estabelecer os riscos e prever os impactos futuros da autorização para coleta, o trabalho analisa cada uma das adjetivações do consentimento, estabelecendo seus escopos, limites e vulnerabilidades. Por meio do método dedutivo e a partir de pesquisas bibliográficas, o trabalho aponta problemas do consentimento, como: seu aspecto vinculante, nos quais a renúncia significa a exclusão de acesso a determinados bens ou serviços; falta de esclarecimentos prévios a respeito do motivo da coleta; falsa suposição da eficácia de uma autogestão da privacidade; políticas de privacidade e termos de uso complexos. Em conclusão, o consentimento só pode ser considerado livre, informado e inequívoco se atender a certas condições, como possibilidade de escolha ou recusa sem restrições e informação prévia, clara e suficiente, a respeito do tratamento de seus dados pessoais. Para tal, implica na necessidade de buscar novas formas de comunicação e obtenção do consentimento, assim como enxergar a viabilidade em uma solução que considere legítimo que o Estado possa, em contextos em que os indivíduos são inexperientes, estreitar os limites, inclusive temporais, do consentimento em prol de um resultado mais benéfico ao titular. Papel que deve ser executado em harmonia com o livre exercício da vontade do titular, de modos que os mecanismos se complementem.

Palavras-chave: privacidade; proteção de dados; consentimento livre, consentimento informado; consentimento inequívoco.

ABSTRACT

This paper aims to study the fundamental right to the protection of personal data and the evaluation of consent, qualified in the General Law of Data Protection as a free, informed and unequivocal manifestation, by which the holder agrees with the treatment of his data. Despite the lack of hierarchy among the hypotheses of personal data processing, consent is considered one of the pillars of respect for privacy and informational self-determination. The research seeks to evaluate whether consent, instead of serving as a shelter for the fundamental right to the protection of personal data, does not legitimize data processing by the State and the market. This problem is amplified in a society increasingly marked by the use and sharing of behavioral data, through a surveillance model that architects a new form of power and social control. Starting from the hypothesis that it is too complex to establish the risks and predict the future impacts of consent for collection, the paper analyzes each of the adjectivations of consent, establishing its scopes, limits and vulnerabilities. By means of the deductive method and based on bibliographical research, the paper points out problems with consent, such as: its binding aspect, in which waiver means exclusion from access to certain goods or services; lack of prior clarification regarding the reason for collection; false assumption of the efficacy of privacy self-management; complex privacy policies and terms of use. In conclusion, consent can only be considered free, informed and unequivocal if it meets certain conditions, such as the possibility of choice or refusal without restrictions and prior, clear and sufficient information regarding the processing of one's personal data. To this end, it implies the need to seek new ways of communicating and obtaining consent, as well as to see the viability in a solution that considers it legitimate for the State to be able, in contexts in which individuals are inexperienced, to narrow the limits, including temporal, of consent in favor of a more beneficial result for the holder. This role should be performed in harmony with the free exercise of the holder's will, so that the mechanisms complement each other.

Keywords: privacy; data protection; free consent, informed consent; unequivocal consent.

SUMÁRIO

INTRODUÇÃO	9
1. SOCIEDADE DA INFORMAÇÃO	14
1.1 ECONOMIA DE VIGILÂNCIA - O CIDADÃO COMO ESPECTADOR DE SUAS INFORMAÇÕES	17
1.2 ERA DA HIPERINFORMAÇÃO – COMO O BIG DATA E A INTELIGÊNCIA ARTIFICIAL PODEM CONDICIONAR A CONDUTA HUMANA	22
1.3 INTERNET DAS COISAS E A FUSÃO HOMEM-MÁQUINA	35
2. DIREITO À PERSONALIDADE, DIREITO À PRIVACIDADE E DIREITO À PROTEÇÃO DE DADOS	44
2.1 RECONSTRUÇÃO DA PRIVACIDADE – DA AUTONOMIA DO INDIVÍDUO À MONETIZAÇÃO DE CONTEÚDO	48
2.2 DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS	62
3. TRATAMENTO DE DADOS NA LEI GERAL DE PROTEÇÃO DADOS	73
3.1 REGULAMENTO GERAL SOBRE PROTEÇÃO DE DADOS – RGPD	75
3.2 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD	78
3.3 DISTINÇÕES APLICÁVEIS ENTRE OS DADOS ANÔNIMOS E OS DADOS SENSÍVEIS	85
4. CONSENTIMENTO DO TITULAR DOS DADOS	92
4.1 CONSENTIMENTO LIVRE - MANIFESTAÇÃO DE VONTADE E LIVRE-ARBÍTRIO	96
4.2 CONSENTIMENTO INFORMADO E O PRINCÍPIO DA FINALIDADE	101
4.3 CONSENTIMENTO INEQUÍVOCO – SOBRECARGA DE INFORMAÇÕES E OBSCURIDADE DAS POLÍTICAS DE PRIVACIDADE	104
4.4 LIMITAÇÃO DO CONSENTIMENTO E TECNOLOGIA COMO APRIMORAMENTO DO RESPEITO À PRIVACIDADE	109
CONCLUSÃO	118
REFERÊNCIAS BIBLIOGRÁFICAS	122

INTRODUÇÃO

Com praticamente cinco bilhões de pessoas utilizando a internet no mundo, produzindo e compartilhando dados, dizer que a sociedade está migrando para uma sociedade da informação é no mínimo reducionista. Esta migração já foi feita e, neste cenário, a evolução tecnológica, ao mesmo tempo que entrega uma série de facilidades e automatizações de tarefas, traz consigo um conjunto de riscos associados à utilização dos dados produzidos por estes bilhões de pessoas.¹

Termos como inteligência artificial, *big data*, algoritmos, nanotecnologia e neurotecnologia passaram a integrar o dicionário não somente de profissionais de tecnologia, mas de outras áreas de conhecimento, como o direito. Esta incorporação reflete que a tecnologia deixou de estar relacionada apenas a execuções de tarefas repetitivas em menor tempo e maior quantidade. Este distanciamento da tecnologia com seu caráter meramente instrumentalista reverbera nas relações dos cidadãos, seja na relação vertical com o Estado ou na horizontal com outros particulares.

Valendo-se do método dedutivo e a partir de pesquisas bibliográficas, o estudo planeja analisar a complexidade da ordem jurídica interna e externa ao tratar proteção de dados, considerando sua interface com outras esferas, como sociais e econômicas, assim como com outros direitos fundamentais, como privacidade, intimidade e o direito ao livre desenvolvimento da personalidade. Pretende ainda examinar o papel do consentimento como legitimador do tratamento de dados pessoais.

Partindo da análise do principal instrumento normativo sobre proteção de dados no Brasil, a Lei 13.709 de 2018 — LGPD, o objetivo da pesquisa é verificar se o tratamento de dados pessoais realizado com o consentimento do titular garante efetivamente à proteção de seus dados pessoais e, em simultâneo, se tal manifestação pode ser considerada livre, informada e inequívoca, em uma sociedade onde os dados são ubíquos, transversais, transfronteiriços e a velocidade de coleta e transmissão são crescentes.

¹ Apesar da pesquisa concentrar seus esforços nos dados produzidos pelos 5 bilhões de pessoas da internet, não se pode olvidar que do outro lado que, praticamente 3 bilhões de pessoas ainda vivem off-line, sendo que destes, grande parte estão em países em desenvolvimento ou subdesenvolvidos. Tendo em vista o período atual, onde alguns serviços passaram a ser fornecidos exclusivamente pela internet, esse número é assustador e reflete que a desigualdade digital caminha ao lado da desigualdade social.

No primeiro capítulo, o estudo se concentra na nova forma de organização social transformada pela tecnologia. O cidadão está conectado o tempo todo. Seja para satisfazer necessidades de interações sociais ou profissionais, estas conexões são formatadas de forma que as experiências humanas produzem dados primários para modelos de negócios cuja arquitetura se baseia na predição do comportamento. Essa economia dirigida a dados, ao mesmo tempo que abre uma série de oportunidades para o aprimoramento das tecnologias, fere princípios de tratamentos de dados pessoais, ao associar a utilização de dados para finalidades distintas do esperado pelos seus titulares no momento da captura.

Lançando mão do conceito de *prosumer* de Ricardo Bioni, o estudo visa avaliar como as experiências dos usuários auxiliam no processo de produção e tendem a modelar novos produtos e serviços, uma vez que este mercado define novos resultados baseados em probabilidades matemáticas de consumo. Experiências estas que se equivalem a commodities, que para serem processadas necessitam de uma tecnologia mais robusta, capaz de trabalhar com grandes volumes de dados e em alta velocidade.

A utilização dos dados comportamentais é apresentada como o *trade-off* entre inovação (facilidade) e privacidade. Aliado ao *big data*, a inteligência artificial proporciona efeitos que implicam em uma mudança na subjetividade das relações entre as pessoas e a tecnologia, principalmente ao executar tarefas que eram consideradas prerrogativas humanas.

No segundo capítulo o estudo conceitua o direito à personalidade, trazendo a compreensão de uma abordagem mais elástica que este direito passou a possuir na sociedade atual. Contornando ao direito à intimidade e à vida privada, deixa de ser compreendido pelo aspecto patrimonial e insere o indivíduo como componente essencial deste direito. Em seguida, o capítulo aborda o direito à privacidade, desde sua concepção histórica, que tem como referência inicial o artigo jurídico escrito em 1890 por Samuel Warren e Louis Brandeis, até o entendimento corrente.

Entendimento que se distancia do estabelecimento de um núcleo duro do direito à privacidade, na medida que tal acepção diminui a multiplicidade de interesses à que se propõe este direito, a qual é a tutela da pessoa humana. Ainda que o direito à privacidade mantenha as raízes de proteção à intimidade, ganha novas proporções, acelerados principalmente pelo crescimento do uso da internet.

Crescimento que provoca a necessidade de verificação de limites e restrições quando estes direitos se chocam com outros, como direitos de informação, transparência ou vedação ao anonimato. Neste ponto o estudo se vale dos textos de Ingo Sarlet ao trazer a exigência de testes de proporcionalidade, não apenas no sentido de proibição de uma intervenção, mas também, no sentido de proibição de uma proteção insuficiente.²

Um dos ramos destas proteções se refere justamente ao direito à proteção dos dados pessoais. Assim como o direito ao livre desenvolvimento da personalidade e o direito à privacidade, o direito à proteção de dados pessoais possui forte ligação com elementos básicos da democracia, já que o provoca a ordem jurídica a se reorganizar e assegurar proteção adequada, principalmente em um quadro de reequilíbrio de poderes no ambiente digital.

Razão pela qual, em seu tempo, a Constituição Federal brasileira incluiu no catálogo de direitos e garantias fundamentais, através da Emenda Constitucional n.º 115/2022, o direito fundamental à proteção dos dados pessoais, em um inciso distinto da já protegida intimidade e vida privada. Essa incorporação parte da compreensão que a tutela da intimidade e vida privada se exterioriza essencialmente de forma individual, estática e negativa. Já a proteção de dados abrange a necessidade de conferência de um poder positivo e dinâmico ao titular.

Ao assumir características próprias, além do respeito à privacidade, o direito à proteção de dados pessoais busca efetiva tutela de formas de controle, de discriminação e de outras liberdades como de expressão, de informação, de comunicação e de opinião. Assume ainda o reconhecimento do direito à autodeterminação informativa, garantindo ao titular dos dados a escolha da forma e do conteúdo no tratamento de seus dados.

O terceiro capítulo faz uma análise dos conceitos, princípios e fundamentos jurídicos da LGPD a partir de suas similitudes com outros instrumentos normativos, principalmente o Regulamento Geral de Proteção de Dados Europeu. Traçando uma linha histórica de modelos normativos autônomos de proteção de dados, verifica-se a passagem de enunciações pautadas na autonomia individual e ligação com princípios fundamentais, independentemente da existência real de uma violação.

² SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados, in: Danilo Doneda ... [et al.]. **Tratado de Proteção de Dados Pessoais**, Editora Forense Ltda. Rio de Janeiro - RJ, 2021. p. 53.

A necessidade de estabelecimento de igualdade de níveis de proteção de dados na União Europeia ensejou a promulgação da Diretiva 95/45/CE, tida como referência e fundamento para o modelo atualmente vigente, o RGPD. O regulamento europeu, além unificar legislações internas específicas, fortaleceu a necessidade de justificação do tratamento mediante consentimento ou outro fundamento jurídico. No Brasil, a insuficiência de legislações específicas sobre tratamento de dados pessoais perdurou até 2018, com a sanção da LGPD. Ainda que não vinculado ao direito europeu, a exigência de atendimento de parâmetros de proteção nas relações comerciais do Brasil com países da União Europeia foi um dos pontos que influenciou o país a avançar neste marco regulatório.

Essa semelhança dos dois modelos normativos é percebida tanto nas definições, como na construção dos princípios que a legislação brasileira optou por trazer de forma explícita, como princípios da finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas.

O capítulo aborda ainda as distinções aplicáveis a dados com rótulos específicos como os dados anônimos e sensíveis. Quanto ao primeiro, em que pese a definição legal enquadrar como anônimo o dado relativo ao titular que não possa ser identificado, levanta-se a questão se com o desenvolvimento tecnológico e novas técnicas de agregação de dados, a anonimização total não seria um mito, na medida que tais técnicas poderiam reidentificar o indivíduo.

Da mesma forma, os dados sensíveis, espécie de dados cujo tratamento é mais rigoroso por se observar um potencial de lesividade maior aos seus titulares. A interrogação neste ponto é a taxatividade, ou ainda a definição prévia de quais dados podem determinar características sensíveis a respeito de seus titulares. Torna-se cada vez mais complexo antecipar os efeitos da coleta de algumas informações.

O quarto e último capítulo intenta verificar se o consentimento, proposto como fundamento jurídico para o tratamento de dados na LGPD, é realmente uma manifestação livre, informada e inequívoca, garantindo ao seu titular efetivamente o direito de controlar seus dados.

A pesquisa examina ocasiões nas quais o não consentimento ao tratamento de dados impede o acesso a alguns serviços essenciais (cláusulas *take it or leave it*). Nestes casos, a assimetria de poder entre usuário e controlador esvazia a autonomia individual e impede uma manifestação livre da vontade. Ainda, o consentimento não

é uma carta-branca para compartilhamento de dados de forma irrestrita. Por isso exigem-se mecanismos que tornem claro as finalidades da coleta e a capacitação do usuário para manifestação de um consentimento informado.

Neste ponto, o dilema da autogestão do consentimento surge como uma barreira, ao revelar que é muito custoso para o usuário identificar os benefícios e riscos associados ao compartilhamento de seus dados, seja pela impossibilidade de compreender todo fluxo que seus dados podem percorrer ou por associações que podem surgir com fragmentos de dados.

Quanto à adjetivação de consentimento inequívoco, diante de políticas de privacidade e termos de tratamento de dados complexos, extensos e com linguagens de difícil compreensão de grande parte dos usuários, questiona-se a capacidade de um aceite representar a corporificação do dever de informação sobre os tratamentos de dados.

Por fim, verifica-se a possibilidade de estabelecimento de limites e restrições ao consentimento, sejam elas temporais ou substantivas, ao perceber que embora haja na LGPD um papel de protagonismo do titular quanto ao controle de seus dados, persiste uma vulnerabilidade na efetiva tutela de dados pessoais.

A pesquisa, assim, conclui que o consentimento, para que possa ser considerado livre, informado e inequívoco, requer que: seja resultado da possibilidade de escolha ou recusa sem circunstâncias que impeçam ou limitem a decisão; seja precedido de informações necessárias e suficientes para avaliação a respeito da forma e conteúdo do tratamento e, que não paire dúvidas sobre a declaração de vontade do titular, o que implica na necessidade de busca por novas formas de comunicação e obtenção do aceite.

Para tal, a pesquisa aponta para a construção do chamado consentimento contextual, que se estrutura sob a premissa de que o fluxo informacional deve ser apropriado conforme as suas respectivas esferas sociais. Propõe, em seguida, a revisão da perenidade do consentimento, sugerindo a criação de processos de determinação da duração ou da renovação do consentimento.

1. SOCIEDADE DA INFORMAÇÃO

Sociedade dos dados, sociedade da informação ou sociedade do conhecimento são termos que, apesar da diferença técnica, revelam um cenário que já não é tão novo, principalmente em se tratando de tecnologia. O ritmo incessante de tratamentos de dados oriundos da adoção de novas tecnologias, apesar de facilitar o cotidiano dos cidadãos, também implica em novos riscos. Onipresente nas esferas públicas e privadas, o impacto destas tecnologias já não é mais dissociado do ambiente jurídico, emergindo desta forma a necessidade da realização de uma leitura conjunta com direitos fundamentais, principalmente após o reconhecimento de um direito fundamental à proteção de dados.

Embora etimologicamente a palavra tecnologia, derive do grego e signifique o estudo de uma arte ou de um ofício³, não se limitando desta forma à computação, é utilizada de forma estreita com a matemática e com a informática, e assim será abordada ao longo da pesquisa. Ademais, não é incomum ao pensar em tecnologia, pensar na forma de acesso e, neste caso, a internet representa o principal meio como ferramenta de comunicação.

A tecnologia, lida como ferramenta, se apresenta em caráter meramente instrumentalista. Todavia, considerá-la apenas como meio para atingir um fim seria desprezar o que Danilo Doneda chama de “perfil dinâmico da tecnologia”⁴ e assim o presente estudo perderia o objeto. Afinal, os efeitos que o desenvolvimento tecnológico causa nas relações verticais (Estado-cidadão) e horizontais (cidadão-cidadão) não são estáticos.

O estudo da *International Telecommunication Union* – ITU estima que atualmente 4,9 bilhões de pessoas no mundo estejam utilizando a internet. Este número significa que 63% da população mundial está conectada e representa um aumento de 17% em relação ao mesmo dado de 2019 (apenas 3 anos atrás), muito embora este número bruto não represente a qualidade e velocidade do acesso.⁵ São

³ Universidade Federal de Santa Catarina - UFSC, **Glossário Midia-Educação**, 2022. Disponível em: <https://moodle.ufsc.br/mod/glossary/print.php?id=575670&mode=date>. Acesso em: 17 dez. 2022.

⁴ DONEDA, Danilo, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**, 3 ed. São Paulo: Thomson Reuters Brasil, 2021. p. 56-57.

⁵ INTERNATIONAL TELECOMMUNICATION UNION - ITU. **Measuring digital development: Facts and figures 2021**. Place des Nations CH-1211 Geneva Switzerland, 2021 Disponível em: <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>. Acesso em: 25 mar. 2022. p. 1-2.

praticamente mais 800 milhões de pessoas produzindo, classificando, transmitindo e armazenando dados diariamente, em um volume jamais mensurado.

Obviamente este número revela outra face. A de que praticamente 3 bilhões de pessoas ainda vivem off-line, sendo que destes, grande parte estão em países em desenvolvimento ou subdesenvolvidos. Este número é refletido na mesma pesquisa quando se mede a cobertura de sinal de banda larga. Ao passo que a cobertura 4G na Europa é de 99%, na África é de apenas 49%.⁶

No Brasil, a Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD contínua – revela que, em 2019, 78,3% da população com 10 anos ou mais utilizam a internet. Este número, se comparado com 2016, representa um crescimento de 13,6%, quando 64,7% utilizavam a internet. Assim como o indicador da ITU, o número no Brasil reflete a conexão entre uso de internet e desigualdade econômica. Como exemplo, na região Sudeste o percentual de uso da internet é de 83,8%, contra 68,6% na região Nordeste. Se comparada a utilização na rede de ensino, a disparidade é ainda maior. Enquanto 98,4% dos estudantes da rede privada têm acesso à internet, este número reduz para 83,7% na rede pública de ensino.⁷

A similitude entre desigualdade digital e social fica ainda mais evidente se comparado o percentual de domicílios com acesso à internet por renda familiar. Segundo o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br, das famílias que possuem renda maior que cinco salários-mínimos – SM, 99% têm internet em casa. Em contrapartida, este número cai consideravelmente para 68% quando a renda familiar é de até 1 SM.⁸

Fato é que, ainda que conceda uma nova interface de comunicação, a penetrabilidade da internet (que se tornou parte de toda atividade humana) não garante, por si só, direitos de liberdade e igualdade.⁹ Por mais que o ciberespaço

⁶ *Ibid.*, p. 11.

⁷ BRASIL. IBGE - Instituto Brasileiro de Geografia e Estatística. **Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua**. Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2019. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf. Acesso em: 25 mar. 2022. p. 7-8.

⁸ COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros** - TIC Domicílios 2020 (Edição COVID-19 - Metodologia adaptada). Disponível em: <https://www.cetic.br/pt/tics/domicilios/2020/domicilios/A4/>. Acesso em: 25 mar. 2022.

⁹ NUNES, Luiz Felipe, **Os desafios da democracia participativa: o desenvolvimento da sociedade da informação e a necessária inclusão de grupos sociais desfavorecidos ou marginalizados**.

possibilite a criação de conhecimentos de diversos gêneros, estes números demonstram que a exclusão digital deriva de desigualdades socioeconômicas como desemprego, baixa educação e baixa renda.¹⁰

Apesar de emergente a discussão sobre estas exclusões, cumpre destaque que estes 63% da população conectada refletem uma sociedade organizadas de uma nova forma, onde a informação é o elemento nuclear para o desenvolvimento da economia. Essas informações são processadas e transmitidas em uma velocidade e quantidade jamais vista. Inexistem obstáculos físicos territoriais, em especial nas redes sociais.¹¹

Neste sentido, Bioni reforça que “A ciência jurídica como um fato social deve adequar, ou, pelo menos, repensar as suas categorias para encarar os novos desafios regulatórios emergentes deste novo quadro”¹². A proteção de dados como direito fundamental se insere neste novo quadro que transcende as fronteiras territoriais dos estados.

Os desafios relacionados à proteção de dados impactam todos os espaços, robustecendo sua transversalidade e ubiquidade. As inovações tecnológicas, que ocupam estes espaços e se abastecem destes dados, são elementos que passam despercebido no cotidiano de grande parte desta sociedade da informação. Causam cada vez menos espanto e são naturalmente absorvidas no dia a dia. Localizações em tempo real, hábitos de consumo, preferências pessoais e toda informação direta ou derivada tornam-se mercadorias.¹³

Estes movimentos naturais de incorporação destas tecnologias na rotina dos cidadãos os impedem de enxergar todos os riscos associados à utilização indevida de dados pessoais. Se não se tem ciência nem mesmo de quais dados são coletados, muito menos de como são processados, para quem são transferidos ou

Anais da VII Jornada de Direitos Fundamentais, v. 1, 2020. p. 1-12. Disponível em: <https://unifor.br/web/pos-graduacao/jornada-de-direitos-fundamentais/actual>. Acesso em: 03 jun. 2022.

¹⁰ CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil**. Sequência: Estudos Jurídicos e Políticos, v. 41, n. 84, 2020. p. 224–229. Disponível em: <https://doi.org/10.5007/2177-7055.2020v43n84p209>. Acesso em: 25 mar. 2022.

¹¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**; Editora Forense, 3. ed.; São Paulo, 2021. p. 4-5.

¹² *Ibid.*, p. 5.

¹³ BITTENCOURT, Rui Carlos Sloboda; BERBERI, Marco Antônio Lima, Do compartilhamento da economia à fragmentação da privacidade do trabalhador 4.0, *in*: CALOMENO, Cassiana Gomes; BERBERI, Marco Antônio Lima (Orgs.), **Direitos Fundamentais e Tecnologia**, Curitiba: Editora Íthala, 2020, p. 12-18.

comercializados e quais efeitos em suas vidas. De meros espectadores podem ser condicionados ou conduzidos por quem detêm estas informações.

1.1 ECONOMIA DE VIGILÂNCIA - O CIDADÃO COMO ESPECTADOR DE SUAS INFORMAÇÕES

“*There’s an app for that*”¹⁴. Há um aplicativo para isso. O slogan registrado pela empresa Apple em 2010 reflete o hábito do ser humano em ter seus desejos atendidos de forma imediata e na palma da mão. O cidadão está conectado o tempo todo. Seja uma informação, uma curiosidade, ou uma atualizada nas visualizações da rede social, esperar não é uma opção. Para cada demanda existe um aplicativo que promete satisfazer as necessidades destes indivíduos de forma “gratuita”, bastando aceitar os termos e condições de uso.

A arquitetura de negócio dos grandes *players* de mercado, mais especificamente de redes sociais tal como *Facebook*, se sustenta nesta necessidade de estar conectado e principalmente de ser reconhecido. Por trás desta forma de impaciência que toma conta de todo mundo, há uma nova maneira de se relacionar. Sendo criaturas sociais, o indivíduo reclama aprovação dos que estão em volta.¹⁵

Cada curtida é uma carícia maternal no ego do usuário.¹⁶ Esse comportamento que se manifesta na relação do indivíduo com as novas tecnologias diz respeito, portanto, “ao desejo intrínseco de ser incluído, de fazer parte, e que está atrelado ao funcionamento do sistema dopaminérgico, pois se trata de uma sequência contínua de estímulos para a liberação da dopamina”.¹⁷ Essa dose que atua no sistema nervoso central do ser humano é liberada quando alguém curte sua foto ou sua publicação e abre espaço para uma psicologia de condicionamento e para um capitalismo de vigilância.

¹⁴ Apple Inc. **Apple Trademark List**. Disponível em: <https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html>. Acesso em: 31 mar. 2022.

¹⁵ EMPOLI, Giuliano Da. **Os engenheiros do caos**; tradução: Arnaldo Bloch. 1. ed.; 3. reimp. - São Paulo; Vestígio, 2020. Título original: Les ingénieurs du chaos. p. 74-77.

¹⁶ *Ibid.*

¹⁷ SARLET, Gabrielle Bezerra Sales, **A Inteligência Artificial no Contexto Atual: uma Análise à Luz das Neurociências Voltada para uma Proposta de Emolduramento Ético e Jurídico**. Revista de Direito Público, v. 18, 2022. Disponível em: <https://doi.org/10.11117/rdp.v18i100.5214>. Acesso em: 30 mar. 2022. p. 275-276.

Zuboff define capitalismo de vigilância como um processo que “reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais”.¹⁸ Por mais que parte destes dados capturados e processados possam servir para incrementar a experiência do usuário na utilização das plataformas digitais, a autora destaca que o excedente é declarado como superávit comportamental do proprietário. Este superávit, que não é enxergado pelo titular destes dados, alimenta modelos matemáticos e estatísticos.

Para a autora, o capitalismo de vigilância pode ser considerado uma nova espécie de poder econômico, que ocupa espaço a cada curta. Cliques que deixam rastros, são analisados e monetizados por alguma companhia.¹⁹ O armazenamento destas experiências humanas compreende mais do que dados de identificação e localização, exemplos corriqueiros ao se tratar de proteção de dados. Constituem-se de dados de natureza comportamental, como voz, personalidade, opiniões e emoções. “Com tal reorientação transformando conhecimento em poder, não basta mais automatizar o fluxo de informação sobre nós; a meta agora é nos automatizar”.²⁰

Os principais alvos de críticas de Zuboff, por óbvio, mas não somente, são as grandes empresas de tecnologia como *Facebook* ou *Google*. Por trás do senso de inevitabilidade que os serviços destas empresas estimulam, da retórica de empoderamento e emancipação do usuário, esconde-se a verdadeira natureza do mercado que exige esta matéria-prima, o mercado futuro comportamental, que é maior do que a monetização da publicidade *online*.

O controle e vigilância sobre as expressões buscadas no Google, por exemplo, permitem traçar um perfil. Consumidores entregam voluntariamente a observações panópticas que controlam e satisfazem suas necessidades [...] neste sentido, o *Facebook* nunca foi mero programa de interação social. Sempre teve como função coletar o maior número de dados dos consumidores para que as ofertas sejam direcionadas.²¹

Rodotà frisa que a vigilância passa de um caráter excepcional para uma ação do cotidiano das pessoas. “*La multitud ya no es solitaria y anónima*” (A multidão não é mais solitária e anônima). A busca incessante por dados engendra uma produção

¹⁸ ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução: George Schlesinger. 1. ed. - Rio de Janeiro: Intrínseca, 2020. Título original: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. p. 18.

¹⁹ *Ibid.*, p. 72.

²⁰ *Ibid.*, p. 19.

²¹ SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. 1. ed. São Paulo: Tirant lo Blanch, 2021. p. 146.

contínua de perfis e grupos de usuários.²² Para Rodotà esta vigilância arquiteta uma nova forma de poder e controle social.

A política de dados do *Facebook* estabelece quais os dados são coletados²³, como estas informações são utilizadas²⁴ e compartilhadas²⁵. Apesar de constar na política de compartilhamento que o *Facebook* “não vende dados de usuários e jamais o fará”, a reportagem do *The New York Times*, baseada em documentos internos do *Facebook* e entrevistas com cerca de 50 ex-funcionários, revelou que ao invés de vender os dados a estratégia do Facebook foi outra, compartilhar os dados dos usuários com cerca de 150 empresas parceiras.²⁶

Documentos internos obtidos pelo *The Times* mostraram que estas empresas, das quais a maioria do ramo da tecnologia, como *Microsoft* e *Amazon*, receberam dados de centenas de milhões de usuários, mesmo que estes clientes tivessem desativado todo o compartilhamento. Estes acordos permitiram ao *Facebook* atrair novos usuários, incentivá-los a usar a rede social com mais frequência e aumentar a receita de publicidade.

²² RODOTÀ, Stefano, Democracia y protección de datos, **Cuadernos de Derecho Público**, v. 19–20, 2003. p. 23.

²³ A política de privacidade da empresa estabelece as informações coletadas: “...coletamos o conteúdo, comunicações e outras informações que você fornece quando usa nossos produtos [...] isso pode incluir também o que você vê por meio dos recursos que fornecemos, como nossa câmera, de modo que possamos realizar ações como sugerir máscaras e filtros de que você pode gostar, ou dar dicas sobre o uso de formatos da câmera. [...] Coletamos informações sobre como você usa nossos Produtos, como o tipo de conteúdo que você visualiza ou com o qual se envolve; os recursos que você usa; as ações que você realiza; as pessoas ou contas com que você interage; e o tempo, frequência e duração das suas atividades. Por exemplo, registramos quando você está usando e a última vez que usou nossos Produtos, quais publicações, vídeos e outro conteúdo você visualizou nos nossos Produtos”. Meta. **Central de Privacidade**, 2022. Disponível em: <https://www.facebook.com/about/privacy>. Acesso em: 30 mar. 2022.

²⁴ A política de privacidade estabelece como suas informações são compartilhadas nos Produtos da Meta ou com Parceiros Integrados: “Usamos as informações que temos para oferecer nossos Produtos, inclusive para personalizar recursos e conteúdo (como os anúncios, o Feed de Notícias do Facebook, o Feed do Instagram e o Instagram Stories) e apresentar sugestões a você (como grupos ou eventos pelos quais você pode se interessar ou tópicos que talvez você queira seguir) dentro e fora dos nossos Produtos”. *Ibid.*

²⁵ A política de privacidade estabelece os compartilhamentos de informações com parceiros, fornecedores, provedores de serviços e terceiros: “Fornecemos estatísticas agregadas e *insights* que ajudam pessoas e empresas a entender como os usuários estão se engajando com as publicações, os classificados, as Páginas do Facebook, os vídeos e outros conteúdos delas dentro e fora dos Produtos da Meta. [...] Fornecemos aos anunciantes relatórios sobre os tipos de pessoas que visualizaram os anúncios deles e sobre o desempenho de tais anúncios, mas não compartilhamos informações que identifiquem você pessoalmente (informações como seu nome ou endereço de e-mail que possa ser usado por si só para contatar ou identificar você), a menos que você nos dê permissão para tanto”. *Ibid.*

²⁶ The New York Times. **Facebook’s Data Sharing and Privacy Rules: 5 Takeaways From Our Investigation**, 2018. Disponível em: <https://www.nytimes.com/2018/12/18/us/politics/facebook-data-sharing-deals.html>. Acesso em: 30 mar. 2022.

Este modelo de negócio, em que os agentes de tratamentos têm muitas informações de seus clientes, ao mesmo tempo que destes agentes pouco se sabe, é o que Frank Pasquale define de *one way mirror*. “Nós não vivemos em um reino pacífico de jardins murados privados; o contemporâneo mundo se assemelha mais a um espelho unidirecional”.²⁷ Este espelho unidirecional permite examinar os outros, evitando o escrutínio a si mesmo. Destacando as empresas dos setores de crédito e de mecanismos de buscas, Pasquale considera que estes atores têm conhecimento sem precedentes dos detalhes da vida dos cidadãos. Por mais que este imenso volume de dados possa influenciar decisões importantes na vida das pessoas, estas mesmas pessoas pouco ou nada sabem dos detalhes de pontuações, classificações e cálculos efetuados sobre seus dados.²⁸

Dados estes que são registrados a cada movimento que o usuário faz na internet. Preferências de consumo e hábitos são observados por sistemas sem a percepção dos cidadãos. Até mesmos desejos internos e anseios mais subconscientes podem ser coletados nos *clicks* e usados contra o próprio sujeito.²⁹ Essa confiança e dependência das informações na internet, a busca pelo conhecimento em aplicativos ao invés dos tradicionais métodos de consulta e análise como livros, ou relações interpessoais, é o que Byung-Chul Han chama de dataísmo. A aspiração ao saber total, “alcançado não pela narração ideológica, mas pela operação algorítmica”.³⁰ Para os dataístas, as ações advêm da observação de comportamentos e a troca eficiente de informações garante mais desempenho.³¹

Os dataístas colocam sua fé na informação como única fonte verdadeira de valor. Depositam sua confiança no processamento e resposta dos algoritmos. No que diz respeito ao conhecimento se apoiam nos metadados. A informação está imediatamente acessível. É mais rápido e conveniente recorrer ao software. Como citado no *slogan* da Apple, há um aplicativo para isso. Razão pela qual, o dataísmo

²⁷ “Firms seek out intimate details of potential customers’ and employees’ lives, but give regulators as little information as they possibly can about their own statistics and procedures. Internet companies collect more and more data on their users but fight regulations that would let those same users exercise some control over the resulting digital dossiers”. PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Cambridge, Massachusetts London, England: Harvard University Press, 2015. p. 3-4.

²⁸ *Ibid.*, p. 6-10.

²⁹ SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. *Op. cit.*, p. 156-157.

³⁰ HAN, Byung-Chul, **Infocracia: digitalização e a crise da democracia**, Petrópolis, RJ: Editora Vozes, 2022.

³¹ *Ibid.*, p. 75-77.

depende de uma liberdade de informação que privilegia a livre circulação dos dados em detrimento do direito das pessoas de manterem os dados para si.

Assim como a autoridade divina foi legitimada por mitologias religiosas, e a autoridade humana foi justificada pela narrativa liberal, a futura revolução tecnológica poderia estabelecer a autoridade dos algoritmos de Big Data, ao mesmo tempo que solapa a simples ideia de liberdade individual.³²

Ainda, segundo a concepção dataísta, os computadores pertencentes a uma grande rede que ninguém conhece ao certo. Incontáveis volumes de dados são recepcionados pelos humanos, seja através dos e-mails, nas redes sociais, nos *feeds* de notícias ou em qualquer outro dispositivo que inundam as pessoas de informações e exigem uma conexão constante.

As experiências humanas também têm valores diferentes. Se não forem compartilhadas não tem significado. O novo lema é: “Se você experimentar algo, grave. Se gravar algo, faça *upload*. Se fizer *upload* de algo, compartilhe”.³³ Estes comportamentos ratificam os modelos dos *players* de tecnologia, os quais são altamente eficientes e orientados a dados.

Essa economia dirigida a dados (*data-driven economy*) ao mesmo tempo que abre uma série de oportunidades para o aprimoramento das tecnologias, muitas das quais se convertem em benefícios para os cidadãos, como inovações da área de saúde e mobilidade (apenas para citar alguns exemplos), por se enquadrarem como ativos de negócios, envolvem riscos, principalmente à privacidade, liberdade e à autonomia do indivíduo.

Por exemplo, inovações baseadas em dados projetados para gerenciamento do tráfego podem auxiliar na redução do trânsito caótico em grandes metrópoles, na medida que, monitorando os veículos em tempo real, conseguem reordenar sinais, liberar vias mais congestionadas e apontar rotas alternativas. Por outro lado, a mesma informação oferece a possibilidade de um estado de vigilância dos cidadãos. Cada carro passa a ser reconhecido com um objeto identificável. Informações cruzadas do

³² HARARI, Yuval Noah. **21 lições para o século 21**. Tradução de Paulo Geiger. 1ª ed. São Paulo: Companhia das Letras, 2018. Título original: 21 Lessons for the 21st Century. p. 72.

³³ HARARI, Yuval Noah. **Homo Deus: Uma breve história do amanhã**. Tradução de Paulo Geiger. 1ª ed. São Paulo: Companhia das Letras, 2016. Título original: Homo Deus: A Brief History of Tomorrow. p. 338.

GPS do veículo com o celular do motorista têm o potencial de saber onde cada cidadão está em tempo real.³⁴

A empolgação e o marketing em torno da ideia de que uma economia dirigida a dados é o melhor jeito de endereçar problemas sociais complexos, como crime, pobreza e educação, não leva em consideração que as consequências deste processo são as de tornar a sociedade cada vez mais tecnocrática e ainda de favorecer o *control creep*, por meio do qual dados reunidos para um propósito podem receber outros novos propósitos, o que, embora, possa ser positivo do ponto de vista da eficiência do sistema, é extremamente preocupante do ponto de vista das liberdades civis.³⁵

O *control creep* está associado a utilização de dados para finalidades distintas do esperado pelos seus titulares no momento da captura. Para esta economia dirigida a dados, este procedimento faz parte do negócio, visto que constantemente os dados coletados são recombinaados para ser possível alcançar novos “*insights*”. Um sistema baseado em reconhecimento facial, teoricamente desenhado para autenticar usuários na entrada de estádios, pode ser rapidamente implantado em diferentes situações, como arquivos policiais. Um sistema baseado no GPS de veículos, utilizado para monitorar tráfego em rodovias, pode ser usado por seguradoras para medir o grau de risco do cliente.³⁶

1.2 ERA DA HIPERINFORMAÇÃO – COMO O BIG DATA E A INTELIGÊNCIA ARTIFICIAL PODEM CONDICIONAR A CONDUTA HUMANA

Apesar de serem recorrentemente tratados como sinônimos, dado, informação e conhecimento se distinguem semanticamente. Os dados são o estado mais primitivo, ou a matéria-prima da informação. São números, símbolos ou sinais que não

³⁴ OLK, Christopher; GRAFENSTEIN, Max von; WERNICK, Alina. **Data Governance: Enhancing Innovation and Protecting Against Its Risks**. Intereconomics. v. 54, n.4, 2019. p. 228–232. Disponível em: <https://www.intereconomics.eu/contents/year/2019/number/4/article/data-governance-enhancing-innovation-and-protecting-against-its-risks.html>. Acesso em: 01 abr. 2022.

³⁵ FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019. p. 36.

³⁶ HONG, Sun-há. **Control Creep: When the Data Always Travels, So Do the Harms**. Center for International Governance Innovation, 2021. Disponível em: <https://www.cigionline.org/articles/control-creep-when-data-always-travels-so-do-harms/>. Acesso em: 01 abr. 2022.

são estruturados, portanto, carecem de uma organização para que deles possa ser extraída uma informação.³⁷

Desta forma, a informação é o resultado do processamento desta matéria-prima (dados), que se transforma em algo inteligível. Um nome, um número, um valor, de forma atômica não tem significado. Todavia, arrançados em conjunto possuem carga valorativa (se o nome representa um produto em uma loja de departamentos, se o número representa a quantidade de vendas deste produto em um período e se o valor representa o período de vendas), o conjunto destes três dados geram uma informação.

O conhecimento, no que lhe concerne, é a capacidade de processar a informação e gerar um entendimento que permita mudança do comportamento ou modo de agir. Na análise de dados é o resultado, gerando aprendizagem. No exemplo citado anteriormente, seria a capacidade de direcionar a publicidade dos produtos baseado nas aceitações e vendas dos produtos medidos. “Tal constatação obviamente não afasta a importância dos dados isolados ou “crus”, mas mostra que, sem o devido tratamento, dificilmente se poderá deles extrair o seu adequado potencial”.³⁸ Razão pela qual a qualidade e profundidade dos dados armazenados são cruciais para a eficiência destes modelos de negócios baseados em informação.

Este armazenamento atrela-se “à ideia de um sistema da informação, cuja dinâmica explícita, sequencialmente, um processo que se inicia com a coleta e estruturação de dados, perpassa a extração da informação que, por fim, agrega conhecimento”.³⁹ Percebe-se, portanto, que quanto mais dados são coletados, potencialmente mais conhecimento pode ser gerado.

Bioni ratifica esta tríade ao afirmar que o que alavanca a eficiência na atividade empresarial é o processamento-organização transformado em conhecimento aplicado. A reação do mercado consumidor, a mensuração do potencial de compra e o público-alvo são conhecimentos que indicam quais bens devem ser projetados.⁴⁰

O consumidor neste cenário passa a atuar como um assistente de vendas sem custo. Estes consumidores trocam experiências de consumo, compartilham opiniões, ou reclamações sobre determinados bens, ou funcionalidades (no caso do mercado

³⁷ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento.** *Op. cit.*, p. 31-32.

³⁸ FRAZÃO, Ana. **Fundamentos da proteção...**, *Op. cit.*, p. 26.

³⁹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais....** *Op. cit.*, p. 33.

⁴⁰ *Ibid.*, p. 11.

de software). Esta divulgação gera novos dados, que ciclicamente transformados auxiliam no processo de produção. “O produto ou serviço tende a ser modelado conforme os pontos negativos e positivos assinalados por este elo final da cadeia de produção.” É o que se denomina *prosumer*, o consumidor que não apenas consome, mas também produz o bem de consumo, participando desde a confecção até o descarte do produto.⁴¹

Fuchs sublinha que estes dados dos consumidores ativos na internet equivalem-se a *commodities* (estado bruto), produzidos em alta escala e cuja mensuração é totalmente algorítmica e preditiva, ou seja, adota um princípio que define novos resultados baseados em probabilidades matemáticas. Se um consumidor avalia positivamente um produto A, há grande perspectiva de gostar do produto B. Frisa ainda que as próprias políticas de privacidade legitimam este sistema, com frases do tipo: seus dados são utilizados para oferecer produtos personalizados; oferecer anúncios relevantes; garantir demonstrações direcionadas ou promover conteúdo customizados.⁴²

Nesta dinâmica, para processar uma montanha de fatos que, em volume que excedem a capacidade dos sistemas tradicionais, é necessária uma arquitetura mais robusta, de propósito específico, e o Big Data, segundo Bioni, representa o êxtase deste processo.⁴³ Mais robustos que os bancos de dados convencionais, suportam a transformação destes grandes volumes de dados, o que permite direcionar mensagens publicitárias personalizadas (conhecimento).

A tecnologia do Big Data funciona como um grande banco de dados, capaz de não somente armazenar, mas classificar grande volume de dados variáveis de natureza complexa.⁴⁴ Inicialmente a abordagem do Big Data era apoiada em três dimensões, ou os 3 (três) V's do Big Data: volume, variedade e velocidade.

O volume está relacionado a quantidade de dados processados. Nesta dimensão não importa a estruturação e o valor dos dados é desconhecido. Este

⁴¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais....** *Op. cit.*, p. 12-13.

⁴² FUCHS, Christian, **Mídias Sociais e a Esfera Pública**, Revista Contracampo, v. 34, n. 3, 2015. p. 42-44.

⁴³ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais....** *Op. cit.*, p. 33-34.

⁴⁴ ORACLE Brasil. **O que é Big Data?** Disponível em: <https://www.oracle.com/br/big-data/what-is-big-data/>. Acesso em: 03 abr. 2022.

volume pode chegar a milhares de *petabytes*⁴⁵. A variedade diz respeito as fontes, formatos e tipos de dados que podem ser estruturados ou não. Podem incluir áudios, vídeos e exigem um processamento adicional para obter significados. Já a velocidade é a taxa de recepção, gravação e transmissão. Sistemas que operam com Big Data exigem respostas em tempo real. Para possuírem valor o tempo de processamento é fundamental.⁴⁶

Mais recentemente, alguns autores adicionaram uma quarta dimensão, a veracidade⁴⁷. Outros acrescentaram ainda uma quinta, o valor⁴⁸. Enquanto a veracidade refere-se à qualidade dos dados e objetiva determinar sua relevância, correção e consistência, o valor está relacionado aos benefícios que podem ser derivados da análise do Big Data.⁴⁹ Estes dois pilares recentes, todavia, só detalham aspectos implícitos do modelo original ou de 3 (três) V's. Afinal, de nada serviria um banco de dados veloz, variável e com grande quantidade de dados se dele não se pudesse extrair informação atualizada ou verídica.

Um dos exemplos clássicos quando se fala em capacidade de previsão dos modelos de Big Data é o da empresa americana *Target*. Segundo a revista de negócios *Forbes*, em artigo publicado em 2012, a empresa descobriu que uma adolescente estava grávida antes de seu pai. Segundo a reportagem, a utilização de Big Data, alimentado pelo histórico de padrões de consumo da loja de varejos, permitiu inferir que a consumidora adolescente estava grávida com base na compra de cremes, suplementos de cálcio, magnésio e zinco.⁵⁰

De acordo ainda com a reportagem, o pai da adolescente descobriu a gravidez quando a Target passou a enviar na residência da família cupons para fraldas, chocalhos, carrinhos de bebê. Esta análise de dados em massa não requer um

⁴⁵ Um petabyte (PB) é um múltiplo da unidade bytes e representa a décima quinta potência (10^{15}) ou 1.125.899.906.842.624 bytes. Disponível em: <https://pt.wikipedia.org/wiki/Petabyte>. Acesso em: 03 abr. 2022.

⁴⁶ ORACLE Brasil. **O que é Big Data?** *Op. cit.*

⁴⁷ RIBEIRO, Claudio José Silva. **Big Data: os novos desafios para o profissional da informação**. Informação & Tecnologia (ITEC): João Pessoa/Marília, v.1. p. 96-105, jan./jun., 2014. Disponível em: https://www.brapci.inf.br/_repositorio/2015/12/pdf_616d318e35_0000015108.pdf. Acesso em: 03 abr. 2022. p. 99.

⁴⁸ YOUNAS, M. **Research challenges of big data**. SOCA v. 13, p. 105–107, 2019. Disponível em: <https://doi.org/10.1007/s11761-019-00265-x>. Acesso em: 03 abr. 2022.

⁴⁹ *Ibid.*

⁵⁰ HILL, Kashmir. **How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did**. Forbes, 2012. Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=3b55784b6668>. Acesso em: 08 abr. 2022.

sistema inteligente, com grande capacidade cognitiva, mas um sistema que possa processar rapidamente um volume de dados enorme e comparar acontecimento.

Razão pela qual autores, dentre os quais Bioni, ratificam que o Big Data, por mais que possa prever eventos, o faz com base em padrões de repetição e, desta forma, não é considerado um sistema inteligente. Distingue-se de um modelo de inteligência artificial, pois o Big Data trata-se de uma metodologia de inferir pela recorrência. Entretanto, esta capacidade de identificação de padrões é uma das chaves para abordagens publicitárias atuais. Base de dados podem ser utilizadas para uma série de finalidades e diferentes cenários podem ser construídos com as fotografias de consumos dos cidadãos.⁵¹

A grande capacidade de coletar e processar dados comportamentais permite conhecer as pessoas tão a fundo que torna o sistema capaz de conhecê-las mais do que elas mesmas. O consumidor, pessoa física, não lembra o site que entrou há três anos, mas seu algoritmo lembra. [...] De posse destes dados identifica-se a ação que sirva de causa a uma reação provocada, mas não reconhecida como tal, enquanto consumidores incapazes de processar dos dados de modo a calcular prováveis comportamentos simplesmente confiam, mergulhados em uma inundação de dados desordenados.⁵²

No campo da medicina estes sistemas já conseguem interpretar sinais corporais e dar um prognóstico do tratamento. A expectativa natural é de que, em breve, possam monitorar a saúde dos cidadãos 24 horas. Conseguirão detectar doenças em seus estágios mais iniciais, antes mesmo da percepção da pessoa de que há algo de errado. “Poderão nos recomendar tratamentos adequados, dietas sob medida para nossa compleição física, nosso DNA e nossa personalidade, que são únicos”.⁵³

Esta “incapacidade do cérebro humano em sua conformação atual de alcançar padrões de armazenamento ou de velocidades comparáveis aos que são tipicamente atribuídos aos computadores de última geração”⁵⁴ gera um estado de confiança nos modelos estatísticos e a percepção que não é mais possível ficar sem estes serviços. A utilização dos dados comportamentais, nestes cenários, é avaliada como um mal necessário para o alcance do progresso tecnológico. “Partindo da premissa de que haveria um verdadeiro *trade-off* entre inovação e privacidade, de forma que a violação

⁵¹ *Ibid.*, p. 36-38.

⁵² SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. *Op. cit.*, p. 168-169.

⁵³ HARARI, Yuval Noah. **21 lições para o século 21**. *Op. cit.*, p. 75.

⁵⁴ SARLET, Gabrielle Bezerra Sales, **A Inteligência Artificial no Contexto Atual...** *Op. cit.*, p. 282.

desta última seria o preço a pagar”⁵⁵, como se em nome da inovação se pudesse sacrificar direitos fundamentais elementares.

Os benefícios proporcionados por esta economia digital, além de dificultar o processo regulatório da utilização destas informações, poderiam afetar inclusive outras liberdades individuais. Estas fronteiras e limites são levantados pelo autor em relação à utilização futura de sensores biométricos e tratamentos automatizados. “Se a pessoa se recusar a receber um tratamento recomendado pelo algoritmo, talvez seu seguro-saúde seja cancelado, ou seu chefe o demita — por que deveriam pagar por sua teimosia”?⁵⁶

Por enquanto a corrida por estes dados é liderada pelos gigantes da tecnologia, como *Google*, *Amazon* ou *Facebook*. Adotando um modelo de captura da atenção dos consumidores, entregando serviços e entretenimento, reúnem e acumulam imensa quantidade de dados sobre seus usuários. Estes dados valem mais do que qualquer receita de publicidade. Para estas empresas a figura de cliente e produto se confundem.⁵⁷

Zuboff é ainda mais crítica em relação ao mercado comportamental futuro. Para a autora não há uma reciprocidade construtiva produtor-consumidor e muito menos vale a famosa frase “se for de graça, então o produto é você”. Estas plataformas seduzem usuários para operações de extração e nossas experiências são empacotadas. No capitalismo de vigilância somos as fontes de superávit e matéria-prima para as empresas que negociam nos mercados de comportamentos futuros.⁵⁸

A publicidade direcionada é apenas um dos estágios de valor deste acúmulo de dados. A médio prazo a própria indústria de publicidade será a vítima. O modelo de transferência de autoridade de humanos para algoritmos sugere que a assertividade em escolher o que comprar será maior dos algoritmos, que saberá sobre as necessidades, hábitos e opiniões dos cidadãos. Esta transferência de autoridade permitiria se cogitar até mesmo a pergunta: “Oi Google, com base em tudo que você sabe sobre carros e com base em tudo o que você sabe sobre mim, qual o melhor carro para mim?”⁵⁹ Quanto mais adequado for o carro escolhido pelo algoritmo

⁵⁵ FRAZÃO, Ana, Objetivos e alcance da Lei Geral de Proteção de Dados, *in*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 110.

⁵⁶ HARARI, Yuval Noah. **21 lições para o século 21**. *Op. cit.*, p. 75.

⁵⁷ *Ibid.*, p. 107.

⁵⁸ ZUBOFF, *Op. cit.*, p. 21-22.

⁵⁹ HARARI, Yuval Noah. **21 lições para o século 21**. *Op. cit.*, p. 108.

a nossas necessidades, mais reforçada estará a relação de confiança na decisão automatizada.

Para que estas respostas sejam mais precisas e adaptáveis, sistemas de processamento de grandes volumes de dados são combinados com sistemas de inteligência artificial - IA. Embora também sejam algoritmos⁶⁰, sistemas de IA buscam simular a inteligência humana. A partir de características como autonomia, habilidade social, cooperação, proatividade e reatividade, sistemas de IA possibilitam que “os programas de computador sejam criativos e desenvolvam, eles próprios, a habilidade de desempenhar ações e chegar a resultados que os seus criadores não eram capazes de alcançar ou de prever”.⁶¹

Neste sentido, diferentemente de algoritmos convencionais que transformam as mesmas entradas nas mesmas saídas, aplicações orientadas por IA tem a capacidade de acumular experiências e delas extrair resultado. Esse aprendizado, conhecido pelo seu termo em inglês *machine learning* é um tipo de IA e permite responder a mesma situação de formas distintas, a depender do desempenho da resposta anterior. Esta característica do *machine learning* faz com que o programa melhore gradualmente, assim como se espera da experiência humana.⁶²

Por esta razão, geralmente sistemas de inteligência artificial são combinados com Big Data, na medida que um volume maior de dados permite mais repostas e consequentemente maior aprendizado. Com a crescente disponibilidade de recursos computacionais, foi possível que sistemas deixassem de ser baseados em regras pré-fixadas e fossem alimentados por quantidade de dados suficientes para poderem fundamentar novas decisões.⁶³

⁶⁰ “Algoritmos são definidos pela matemática como um conjunto de instruções passo a passo a serem executadas de maneira mecânica para atingir algum resultado desejado. Dentro da ciência da computação, os algoritmos são entendidos como procedimentos codificados para transformar uma entrada de dados em uma saída desejada. Embora algoritmos não estejam limitados a processos matemáticos, em última análise, sua codificação na linguagem computacional é, ao cabo, uma redução à matemática”. FRAZÃO, Ana; GOETTENAUER, Carlos, O jogo da imitação jurídica: o direito à revisão de decisões algorítmicas como um mecanismo para a necessária conciliação entre linguagem natural e infraestrutura matemática ana fração, *in*: TEPEDINO, Gustavo; GUIA DA SILVA, Rodrigo (Orgs.), **O Direito Civil na era da inteligência artificial**, São Paulo: Revista dos Tribunais, 2019, p. 45–63.

⁶¹ TEPEDINO, Gustavo; GUIA SILVA, Rodrigo da. **Desafios da inteligência artificial em matéria de responsabilidade civil**. Revista Brasileira de Direito Civil – RBDCivil. Belo Horizonte, v. 21, jul./set. 2019. p. 63.

⁶² TEPEDINO, Gustavo; GUIA SILVA, Rodrigo da. **Desafios da inteligência artificial....** *Op. cit.*, p. 63-64.

⁶³ DONEDA, Danilo Cesar Maganhoto *et al*, **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal**. Pensar - Revista de Ciências Jurídicas, v. 23, n. 04, 2018. p. 3.

A redução do custo computacional proporciona que estes sistemas estejam presentes em inúmeras aplicações do cotidiano como Smart TVs, aplicativos de GPS, aplicativos de recomendação de músicas, filmes ou até mesmo no controle de estoques em empresas. Todavia são as aplicações mais complexas, como veículos autônomos, sistemas biométricos, sistemas de reconhecimento facial e sistemas de análise de comportamentos pessoais, que capturam e processam maior quantidade de informações, dentre as quais aquelas que representam maior risco de exposição.

Em que pese as inúmeras vantagens destas aplicações, os riscos apresentados no capítulo anterior são alargados com sistemas de IA. Redução do controle humano; remoção da responsabilidade humana; desvalorização de competências humanas e erosão da autodeterminação humana são alguns deles.⁶⁴

A IA facilita que tarefas importantes sejam delegadas a sistemas autônomos independentes, ao mesmo tempo que podem também desvalorizar competências humanas, principalmente em setores de precisão ou em domínios sensíveis.⁶⁵ São capazes também de induzir comportamentos humanos, seja porque tendem se tornar facilitadores de atividades do cotidiano, seja porque podem prever comportamentos, como abordado no tópico anterior – economia de vigilância.

Fabiano Hartmann Peixoto ressalva corretamente que a IA representa apenas uma reprodução parcial da cognição humana, pois, ao contrário do cérebro humano, não é capaz de executar múltiplas tarefas, em múltiplas áreas, como o cérebro humano.⁶⁶

Não se trata, portanto, da IA ficcional, abordada em filmes distópicos, nos quais máquinas se rebelam e subjagam os humanos - o problema é exatamente o oposto. A preocupação com a IA é justamente o fato de os sistemas obedecerem a seus “senhores” sem arrependimentos ou hesitações.⁶⁷

⁶⁴ *Ibid.*, p. 11.

⁶⁵ *Ibid.*, p. 12.

⁶⁶ “A capacidade de aprender regras de um jogo de tabuleiro sofisticado (problema complexo) não tornará a máquina inteligente para sugerir diagnósticos médicos, por exemplo – são problemas distintos”. PEIXOTO, Fabiano Hartmann, **Direito e Inteligência Artificial: referenciais básicos com comentário a resolução CNL 332/2020**, Brasília: Ed. do Autor, 2020. p. 18-19.

⁶⁷ “Não há motivo para supor que a inteligência artificial vá desenvolver consciência, porque inteligência e consciência são muito diferentes. Inteligência é aptidão para resolver problemas. Consciência é a aptidão para sentir coisas como dor, alegria, amor e raiva... Seres humanos resolvem a maioria dos problemas sentindo coisas. Computadores, no entanto, resolvem problemas de maneira muito diversa”. HARARI, Yuval Noah. **21 lições para o século 21**. *Op. cit.*, p. 89-98.

Se os algoritmos de IA são capazes de atrair o usuário por mais tempo, o poder de sugestão é um dos fatores de sucesso destes sistemas. A atividade regulatória deve se preocupar então com este suposto desconhecimento como aspecto natural do mercado de dados. Principalmente pelo fato desta opacidade não ser característica intrínseca do meio digital, mas parte da estratégia deliberada (como segredo de negócios) de certos atores que, na falta de transparência, criam um ambiente que lhes permite classificar indivíduos e inferir sobre suas vidas.⁶⁸

Um segundo obstáculo na regulação desta inteligência artificial é a processo de metrificação da realidade. Esta metrificação pode ser subdividida em três elementos: o reducionismo do modelo, a presunção de racionalidade e autoexecutividade das decisões automatizadas. O primeiro consiste em traduzir a relações humanas em números ou indicadores que sintetizam critérios distintos, como se todas as particularidades pudessem ser quantificadas.⁶⁹

A presunção de racionalidade indica que sistemas de IA, combinados com Big Data, se valem modelos estatísticos, que são associados a uma objetividade mecânica, como se revelassem resultados inquestionáveis. Aliada a esta objetivação, o terceiro elemento, a autoexecutividade das decisões automatizadas, impõe que as decisões não precisem passar por uma instância de avaliação, como é próprio das instâncias jurídicas. Seus resultados são autoaplicáveis.⁷⁰

Frazão entende ainda que, se os dados são fonte destas relações, para que se pudesse ter o mínimo de confiança seria necessário algum tipo de controle sobre:

(i) a qualidade dos dados, a fim de se saber se atendem aos requisitos de veracidade, exatidão, precisão, acurácia e sobretudo adequação e pertinência diante dos fins que justificam a sua utilização quanto sobre (ii) a qualidade do processamento dos dados, a fim de saber se, mesmo a partir de dados de qualidade, a programação utilizada para o seu tratamento é idônea para assegurar resultados confiáveis.⁷¹

Apesar de Frazão corretamente considerar a fundamentalidade em criar mecanismos de transparência e *accountability* para permitir ao Estado definir os meios

⁶⁸ FRAZÃO, Ana. **Capitalismo de vigilância e black box society. A vigilância constante e a ausência de transparência como desafios para a regulação jurídica**. 2019. p. 1-5. Disponível em: <https://www.jota.info/opiniao-e-analise/columnas/constituicao-empresa-e-mercado/capitalismo-de-vigilancia-e-black-box-society-28022019>. Acesso em: 09 abr. 2022.

⁶⁹ FRAZÃO; GOETTENAUER, **O jogo da imitação jurídica...** *Op. cit.*, p. 54-55.

⁷⁰ *Ibid.*

⁷¹ FRAZÃO, Ana. **Fundamentos da proteção...**, *Op. cit.*, p. 38.

e formas que estes tratamentos podem e devem ocorrer⁷², existem outras dificuldades particulares de natureza técnica que precisam ser consideradas.

A própria linguagem de programação é a primeira barreira.⁷³ Seria preciso a tradução para uma linguagem natural para que fosse possível iniciar um processo de avaliação dos modelos de decisão e concretização de uma manifestação a um direito à explicação. O número de critérios de análise e o volume de dados capturados podem ser da ordem de grandeza⁷⁴ que, seria preciso um software para analisar os resultados produzidos por outro software.⁷⁵

Desconstruir as caixas pretas do Big Data não é fácil. Por mais que estivessem dispostos a expor seus métodos ao público, ou fossem obrigados a tal, as conclusões são determinadas por fórmulas complexas elaboradas por equipes de engenheiros e resguardadas por outra de advogados. Algoritmos de inteligência artificial podem ter milhares de linhas de código, combinações de dados internos e externos. “Qualquer pessoa que realmente tente entender o modelo provavelmente terá que processar milhares de páginas de palavreado legal complicado — alguns dos quais podem ser bastante ofuscantes”.⁷⁶

Este processo é em tal grau complexo que diante da multiplicidade de passos necessários para falar-se em transparência de sistemas de inteligência artificial, é

⁷² FRAZÃO, Ana. **Capitalismo de vigilância e black box society**. *Op. cit.*, p. 1-5.

⁷³ Mattiuzo observa que um exame minucioso da própria linguagem de programação seria suficiente para fins de conformidade, resguardados segredos comerciais. A ressalva do estudo é a mesma em relação a Ana Frazão, a barreira linguística destas tecnologias. “*Thus, it appears that a scrutiny of the programming itself would suffice for compliance purposes. Clear information about the decision process and the criteria applied by the algorithm should be provided whenever required, and if that information cannot be shared due to commercial or industrial secrecy reasons, a specialized government agency has the power to audit the algorithm in order to verify any discriminatory outcomes.*” MATTIUZZO, Marcela, “**Let the algorithm decide**”: is human dignity at stake?, *Revista Brasileira de Políticas Públicas*, v. 11, n. 1, 2021. p. 354-360.

⁷⁴ “O modelo chinês foi treinado em 1,75 trilhão de parâmetro... Wu Dao 2.0 revelou Hua Zhibing, o primeiro estudante virtual chinês do mundo. Hua pode aprender, desenhar e compor poesia. ZHAVORONKOV, Alex. **Wu Dao 2.0 - Bigger, Stronger, Faster AI From China**. Disponível em: <https://www.forbes.com/sites/alexzhavoronkov/2021/07/19/wu-dao-20bigger-stronger-faster-ai-from-china/?sh=27f164656fb2>. Acesso em: 14 abr. 2022.

⁷⁵ PEREIRA, Robson Pascoal; LORENZETTO, Andrei Meneses. **Inteligência artificial e modelos de decisão automáticos: o enviesamento dos algoritmos**. Anais da VIII Jornada de Direitos Fundamentais 2021. Rede Interamericana de Direitos Fundamentais e Democracia, 2022. Disponível em: https://red-idd.com/files/2021/2021GT03_008.pdf. Acesso em: 14 abr. 2022. p. 11-12.

⁷⁶ Pasquale utiliza como exemplo o fornecimento de 30 milhões de páginas de documentos, forçando o auditor ou fiscalizador a perder tempo procurando uma informação específica, como uma agulha no palheiro. PASQUALE, Frank. **The black box Society**... *Op. cit.*, p. 6-7.

possível utilizar a expressão “eficácia irracional dos dados”.⁷⁷ Esta irracionalidade faz parte da estratégia para manter as caixas pretas dos algoritmos.

Pasquale elenca três estratégias para manutenção das caixas pretas inverificáveis e incontestáveis: sigilo real, sigilo legal e ofuscação. Enquanto o sigilo real estabelece uma barreira tecnológica de acesso ao conteúdo, como proteções de segurança da informação, o sigilo legal obriga que certas informações sejam mantidas em segredo, como segredos fiscais ou bancários. Já a ofuscação envolve tentativa de ocultação ou dissimulação do segredo comprometido.⁷⁸ O resultado da soma dos sigilos reais e legais com a ofuscação é o que o autor denomina opacidade.

Outra autora crítica em relação aos modelos de dados, suas opacidades, imperfeições e riscos associados é a matemática, cientista de dados Cathy O’Neil. Para O’Neil, sendo um modelo nada mais do que uma representação abstrata de algum processo e tendo em mente que as pessoas alternam de comportamentos, de hábitos, de opiniões e de condutas, todo modelo matemático de previsão comportamental contém inevitavelmente incertezas envolvidas.⁷⁹ Incertezas responsáveis por influenciar diretamente nos bens (não somente materiais) que indivíduos terão ou não acesso.

Se estabelecem modelos até mesmo em atividades rotineiras, que as pessoas executam praticamente diariamente, sem perceber que de fato foram estipuladas escolhas a partir de inferências sobre fatos. Ao ir trabalhar todos os dias, a escolha das ruas, dos horários é feita a partir de um modelo natural. Se está chovendo, antecipa-se a saída de casa, se o horário é de tráfego ou se há obras durante um período, vias alternativas são escolhidas.

Ainda assim, é provável que eventos não previstos possam ocorrer e o trajeto escolhido não seja o mais rápido, econômico ou, de forma geral, o mais eficiente. Um acidente inesperado, uma obra não prevista, uma manifestação pública podem fazer com que o motorista se atrase, mesmo tendo calculado o tempo correto de deslocamento em situação normal. Para as máquinas, há também um limite das habilidades de predição de julgamentos e seu poder de decisão é ruim na ocorrência

⁷⁷ FRAZÃO, Ana. **Fundamentos da proteção...**, *Op. cit.*, p. 39.

⁷⁸ PASQUALE, Frank. *Op. cit.*, p. 6-7.

⁷⁹ O’NEIL, Cathy. **Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça à democracia**. tradução Rafael Abraham. 1. ed. Santo André, SP; Editora Rua do Sabão, 2020. Título original: Weapons of math destruction: how big data increases inequaty and threatens democracy. p. 30-31.

de eventos inesperados ou que tenham ocorridos poucas vezes no passado. “Por esta razão, em que se pesem a utilidade e importância da estatística, há que se tomar cuidado com seu emprego amplo e absoluto, sem que existam mecanismos ou válvulas de escape para correção de resultados”.⁸⁰

Ademais, mesmo neste modelo mais simples, o julgamento do caminho reflete prioridades, medos e incertezas do seu criador. Ao desviar de determinados bairros ou ruas durante a noite, o motorista impõe ao seu modelo que há um risco de assalto em determinado local. Aquele endereço se torna mais perigoso que outro qualquer. O’Neil reforça “apesar de sua reputação de imparcialidade, os modelos refletem objetivos e ideologias”⁸¹. Com o Big Data, estas opiniões, dúvidas e preconceitos são embutidos em matemática.

Quanto mais enraizada estiver a percepção de perigo para o motorista, mais provavelmente o fará mudar de rota. Assim como, quanto mais consolidado for determinado preconceito em determinada sociedade, mais os dados refletirão este padrão de comportamento. Como resultado, é presumível que o sistema de IA que utilize estes dados reflita modelos com tais rótulos.

Quanto mais dados, acredita-se que melhores são modelos. Se policiais são posicionados em locais determinados por modelos matemáticos e treinados para reprimir crimes com maior ocorrência segundo estatísticas, certamente o modelo de abordagem policial não utilizará características individuais, mas sim de localização de crimes, posicionando os policiais novamente nas comunidades mais pobres.⁸²

Algoritmos baseados em dados históricos, repletos de preconceitos, reproduzirão, na mesma medida, os padrões de conduta. A prática baseada em

⁸⁰ FRAZÃO, Ana. **Fundamentos da proteção...**, *Op. cit.*, p. 34.

⁸¹ *Ibid.*, p. 35.

⁸² Cathy O’Neil traz uma série de exemplos de modelos enviesados, os quais classifica como WMD (*Weapon Of Math Destruction*) ou, na sua obra traduzida, ADM (Algoritmos de Destruição em Massa). Um destes algoritmos é conhecido como LSI-R ou *Level Of Service Inventory – Revised* e inclui um longo questionário para o detento preencher com perguntas como: Quantas condenações anteriores você já teve? Qual papel das drogas e álcool? Tem conhecidos presos? Primeira vez que é parado pela polícia? Estas perguntas são utilizadas para medição do risco de reincidência. É razoável imaginar que as respostas variam conforme a origem ou o local que o abordado pela polícia more. Moradores das zonas periféricas da cidade, onde reside a população mais pobre, provavelmente já foram parados pela polícia dezenas de vezes mesmo sem ter feito algo errado e acabam “perdendo pontos” neste modelo. Este questionário inclui questões circunstanciais como local de nascimento, vizinhança a amigos para determinar que a parcela mais pobre da população estatisticamente é mais propensa a crimes. Forma-se um ciclo, no qual o algoritmo determina que as mesmas zonas periféricas merecem mais repressão, novas abordagens são realizadas e a pontuação de periculosidade aumenta. O próprio modelo ajuda a manter o ciclo destrutivo em pé. O’NEIL, Cathy. *Op. cit.*, p. 41-43.

modelos estatísticos presume ainda que atributos como nível de renda, localização e emprego possam ser combinados para determinar aspectos subjetivos como probabilidade de ocorrência de crime. Estas generalizações são práticas comuns em decisões automatizadas e podem gerar discriminação por erro estatístico.⁸³ Algoritmos podem analisar cliques, números, localizações ou histórico de inadimplência, mas tem dificuldade em trabalhar com conceitos mais abstratos como justiça.

Mattiuzzo sublinha, entretanto, que apesar da crítica geral a respeito da tomada de decisão algorítmica e da generalização destes modelos, decisões baseadas em generalizações são amplamente aceitas no ordenamento jurídico. “Portanto, os algoritmos não podem ser considerados ilegais apenas por empregarem a mesma metodologia já utilizada nos mecanismos tradicionais de tomada de decisão”⁸⁴. Dentre as razões apontadas por Mattiuzzo, a principal é que muitas destas generalizações são baseadas em critérios objetivos e, somente executam de forma mais rápida, processos que obteriam o mesmo resultado se fossem executados por humanos.

Outra razão apontada pela autora é que as generalizações são a base de várias políticas públicas, como campanhas de vacinações por idade, estabelecimento de auxílio por grupos de risco, de tal forma que generalizar seria uma forma de viabilizar a tomada de decisão.⁸⁵ Mattiuzzo afirma que o fato de algumas decisões carecerem de participação humana não significa que violam princípios ou garantias fundamentais.

Um exemplo seriam sistemas de inteligência artificial que controlam tempos de semáforos em cidades inteligentes. A decisão algorítmica não requer atomização dos dados coletados e nem a identificação dos motoristas. Desta forma não afetariam direitos individuais dos motoristas caso estes não fossem identificados.

Isso não significa, entretanto, que não haja na visão da autora situações em que as generalizações sejam ilegais ou no mínimo indesejadas, como nos casos em que a lei exija a avaliação individual de condutas (como no direito penal), ou nos casos

⁸³ DONEDA *et al*, **Considerações iniciais sobre inteligência artificial...** *Op. cit.*, p. 3-6.

⁸⁴ MATTIUZZO, “**Let the algorithm decide**”: is human dignity at stake? *Op. cit.*, p. 348.

⁸⁵ “Generalizations are also the basis for several public policies. When the government organizes flu vaccination campaigns, for example, it establishes risk groups that will be the main – if not the only – target of the immunization effort, even if the highlighted characteristics (such as age, underlying health conditions, pregnancy) do not cover all the possible cases of serious complications and lethality.” *Ibid.*, p. 348.

em que seja necessário o exercício de julgamento ou prudência e a interpretação de valores morais ou éticos.⁸⁶

Mattiuzzo concorda também, na linha desta pesquisa, que o resultado é fortemente influenciado pela qualidade dos dados que são capturados. Dados incorretos, desatualizados, tendenciosos ou discriminatórios certamente geram generalizações prejudiciais.

A utilização de características em comum para classificação de grupos de pessoas em “cestas” rotuladas afeta outras áreas como acesso a empregos ou créditos, na medida que partem também de suposições analisadas por Big Data. Na sociedade qualificada por relações remotas, dados pessoais constituem a forma de representação e apresentação destas pessoas para o mundo. São determinantes para abrir ou fechar portas de oportunidades e acessos. Um dado incorreto, um critério mal elaborado ou um modelo enviesado podem equivocadamente afetar a realização de direitos fundamentais, como o da personalidade.⁸⁷

Se algoritmos aprendem pelo exemplo, eles precisam ser treinados. “Estes treinamentos devem ser inclusive para que o algoritmo desaprenda algo que não é mais válido. As variáveis que compõe o resultado da análise, a interpretação dada a uma informação, a resposta apresentada a uma situação nova deve ser avaliada”.⁸⁸ Se o resultado é tão válido quanto os dados que lhe servem, alguns dados devem ser eliminados.

Ao apontar três caminhos para o desenvolvimento da inteligência artificial, Fabiano Hartmann compreende o caráter policontextual da IA, suas vantagens e riscos, direcionando para um caminho de estabelecimento de diretrizes, estimulando hábitos que minimizem riscos e enfrentando danos de forma ética e normativamente consistente.⁸⁹

1.3 INTERNET DAS COISAS E A FUSÃO HOMEM-MÁQUINA

⁸⁶ “The necessary conclusion is that algorithms are extremely useful tools that must be used without losing sight of their limitations. The same way using a hammer to cut paper will likely be ineffective, using algorithms to determine what is “fair” is doomed to failure, or at the very least will yield suboptimal results.” *Ibid.*, p. 354-360.

⁸⁷ DONEDA *et al*, **Considerações iniciais sobre inteligência artificial...** *Op. cit.*, p. 3-6.

⁸⁸ PEREIRA; LORENZETTO. **Inteligência artificial...** *Op. cit.*, p. 12.

⁸⁹ PEIXOTO, **Direito e Inteligência Artificial...** *Op. cit.*, p. 36.

Atualmente a utilização de dispositivos móveis se consolidou como o principal meio de acesso à internet⁹⁰. Ainda que essencialmente trate-se de acesso via telefone celular, outras formas de comunicação, com ou sem intervenção humana, ganham espaço e passam a integrar o cotidiano do ser humano. Televisões com internet e carros conectados não causam mais surpresa, pelo contrário, se tornam requisitos na aquisição destes bens de consumo.

Relógios inteligentes (*smartwatches*), pulseiras inteligentes (*smartbands*) podem monitorar a atividade cardíaca, respiratória, sugerir exercícios diários, controlar a qualidade de sono e conectar pessoas. Estes dispositivos “vestíveis” ou *wearables* mudam a forma de interação com o espaço digital.

Realmente é muito prático que se possa controlar as luzes ou eletrodomésticos com palmas e comandos de voz. Entretanto, ao mesmo que esta interconexão dos dispositivos possa representar um avanço nas facilidades das rotinas diárias dos indivíduos, essencialmente estão recebendo e tratando dados constantemente.⁹¹

Essa interação entre estes objetos através de conexões tem sido denominada Internet das Coisas (Internet of Things – IoT) e abrange não apenas tarefas internas de residências como nos exemplos citados, mas também troca de informações em ambientes externos, como sinais de trânsito, controle de tráfego e monitoramento de câmeras de segurança.⁹²

Esta hiperconexão de tudo e de todos é mais uma das críticas ao dataísmo (tratado no tópico anterior). A maximização do fluxo de dados, a conexão do corpo, da natureza e dos objetos, como os carros na rua, as geladeiras na cozinha são mandamento dos sistemas de IoT. Zuboff ressalta que é impossível imaginar o capitalismo de vigilância sem algo como a internet das coisas.

⁹⁰ Segundo a pesquisa TIC Domicílios 2020, o telefone celular é o dispositivo mais utilizado, de forma geral pelos usuários, para acesso a internet. COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros** - TIC Domicílios 2020. Disponível em: <https://cetic.br/pt/tics/domicilios/2020/individuos/C16/>. Acesso em: 07 mai. 2022.

⁹¹ A apresentação do dispositivo Google Glass sugere esta conexão em tempo real. Pessoas podem “compartilhar a visão”. O Glass pode conectar você a colegas de trabalho em um instante, levando a experiência para onde você estiver. Convide outras pessoas para “ver o que você vê” por meio de uma transmissão de vídeo ao vivo para que você possa colaborar e solucionar problemas em tempo real. (tradução livre). Disponível em: <https://www.google.com/glass/start/>. Acesso em: 07 mai. 2022.

⁹² LEAL, Livia Teixeira, **Internet of Toys : Os brinquedos conectados à internet e o direito da criança e do adolescente**, Revista Brasileira de Direito Civil, Belo Horizonte, v. 12, abr./jun. 2017. p. 176. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/38/32>. Acesso em: 07 mai. 2022.

Todo comando que surge a partir do imperativo de predição requer essa presença material no mundo real, o “saber e fazer”. O novo aparato é a expressão material do imperativo de predição, e representa um tipo de poder inédito animado pela compulsão econômica no sentido da certeza. Dois vetores convergem aí: os ideais iniciais de computação ubíqua e os imperativos econômicos do capitalismo de vigilância. Esse encontro assinala a metamorfose da infraestrutura digital de uma coisa que temos para uma coisa que nos tem.⁹³

Do ponto de vista mais pessimista sobre a conexão de dispositivos, a espécie humana caminha para um processo de fusão com máquinas onde não será mais possível a desconexão. Essa fusão tem duas vertentes, ou pode ser vista de duas perspectivas.

A primeira, mais simples e atualmente mais presente no cotidiano das pessoas, sugere que a fusão homem máquina signifique uma série de facilidades que exigem compartilhamentos de dados constantes. Neste campo estão os citados aplicativos de monitoramento de saúde, aplicativos de localização e preferências pessoais. Como abordado, a imprecisão dos modelos e dos dados capturados podem gerar desvios. Os dados, nestes cenários, tendem a fluir de forma cada vez mais imperceptível e sua utilização pode conflitar com direitos da personalidade e privacidade.

A segunda perspectiva, mais profunda, sugere que esta fusão homem-máquina será mais disruptiva. Implantes cerebrais, softwares de detecção de emoções com base no movimento dos olhos, câmeras embutidas no corpo humano, emulando sinapses e movimentando músculos.⁹⁴ Neste cenário, diferenças sutis no comportamento humano, como gestos e risos, que não seriam perceptíveis a outros humanos, podem ser detectados e classificados por sensores biométricos. Apesar das inúmeras aplicações práticas benéficas (como tratamentos de doenças e neuropróteses) que podem apontar estas soluções⁹⁵, Denis Franco joga luz a possível invasão de aspectos mais internos da privacidade, como pensamentos e sentimentos, “através da invasão do espaço da soberania psicofísica”.⁹⁶

⁹³ ZUBOFF, *Op. cit.*, p. 248.

⁹⁴ *Ibid.*, p. 78.

⁹⁵ “Um grupo de neurocientistas da Suíça e da Alemanha anunciou em um estudo nesta semana ter conseguido pela primeira vez usar um chip cerebral para devolver alguma capacidade de comunicação a um homem que, não fosse por essa tecnologia, seria incapaz de se comunicar. O paciente, vítima de uma paralisia muscular que atinge todo seu corpo, consegue agora transmitir vontades a seus médicos e enfermeiros usando apenas a força do pensamento”. Disponível em: <https://oglobo.globo.com/saude/chip-cerebral-devolve-capacidade-de-comunicacao-paciente-com-paralisia-total-25445618>. Acesso em: 08 mai. 2022.

⁹⁶ SILVA, Denis Franco, **Do humano ao pós-humano: pessoa e autonomia privada no contexto do aperfeiçoamento biônico**, Tese de doutorado. Rio de Janeiro: Programa de Pós-Graduação em

Aplicações na área da neurotecnologia⁹⁷ tem despertado discussões éticas sobre limites da evolução. Na medida que se confundem o mundo real e o digital, os debates acerca da utilização de IA na neurociência apontam para novas pautas. Inicialmente atreladas a uma perspectiva reabilitacional, como nos casos de traumas ou lesões, principalmente no sistema nervoso, os incrementos das pesquisas em neurociência almejam novos sentidos, tanto no prolongamento da vida e produtividade do corpo, quanto no aclaramento do funcionamento das funções cerebrais.⁹⁸

Com a entrada da tecnologia 5G, cuja velocidade estima-se ser aproximadamente 100 vezes mais rápida que a 4G⁹⁹, o volume de dados necessários para produzir modelos matemáticos baseados em leituras cerebrais deixa de ser uma barreira, permitindo que novos dispositivos neurais possam ser conectados à rede, oportunizando a manipulação da experiência mental de indivíduos, ainda que os limites reais dessa manipulação permaneçam no campo da suposição.

Essa arquitetura computacional cada vez mais ubíqua composta de pessoas, dispositivos e espaços “inteligentes” conectados em rede é o que Zuboff classifica como o poder instrumentário dos algoritmos, que conhecem e moldam comportamentos humanos.¹⁰⁰ Martins sinaliza ainda que estes sistemas se tornarão mais interconectados, as interações entre os componentes se expandirão, novos serviços serão criados e a percepção humana da realidade será alterada, ampliando problemas de segurança e proteção destes dados.¹⁰¹

No Brasil, encontra-se em tramitação o projeto de lei 1.229/2021, que modifica a Lei 13.709/2018 – Lei Geral de Proteção de Dados – LGPD, incluindo no rol de dados protegidos, o dado neural. Dentre as modificações sugeridas pelo PL

Direito do Departamento de Direito da PUC-Rio, maio de 2009. Disponível em: <https://doi.org/10.17771/PUCRio.acad.15041>. Acesso em: 08 mai. 2022. p. 106.

⁹⁷ “A neurotecnologia abarca todas as tecnologias desenvolvidas para entender o cérebro, visualizar seus processos e, inclusive, controlar, reparar ou melhorar suas funções...Essa técnica, entre outros fatores, permitiu aos pesquisadores identificar quais áreas do cérebro se ativam ou desativam durante determinadas tarefas... As técnicas não invasivas são aquelas que permitem agir desde o exterior, enquanto as invasivas requerem a implantação de eletrodos por meio de cirurgia”. IBERDROLA. **Neurotecnologia: como revelar os segredos do cérebro humano**, 2022. Disponível em: <https://www.iberdrola.com/inovacao/neurotecnologia>. Acesso em: 08 mai. 2022.

⁹⁸ SARLET, Gabrielle Bezerra Sales, **A Inteligência Artificial no Contexto Atual...** *Op. cit.*, p. 275-277.

⁹⁹ DUFFY, Clare. CNN Business. **The big differences between 4G and 5G**. Disponível em: <https://edition.cnn.com/2020/01/17/tech/5g-technical-explainer/>. Acesso em: 21 mai. 2022.

¹⁰⁰ ZUBOFF, *Op. cit.*, p. 18-23.

¹⁰¹ MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros, **Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais**, Revista do Ministério Público do Estado do Rio de Janeiro, nº 78, p. 157–164, 2020.

1.229/2021 percebe-se a preocupação com a definição e regulamentação de dado neural, assim como a conceituação de interface-cérebro-computador e neurotecnologia. O art. 5º da LGPD passa a vigorar com as seguintes alterações:

XX – dado neural: qualquer informação obtida, direta ou indiretamente, da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador invasivas ou não-invasivas;

XXI – interface cérebro-computador: qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático ou que substitua, restaure, complemente ou melhore a atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo;

XXII – neurotecnologia: conjunto de dispositivos, métodos ou instrumentos não farmacológicos que permitem uma conexão direta ou indireta com o sistema nervoso.¹⁰²

O projeto, de autoria do deputado federal Carlos Henrique Gaguim, justifica que a neurotecnologia abre espaço para uma nova forma de coleta de dados, diretamente do cérebro humano. Apesar de, nos termos da própria LGPD, qualquer dado que possa identificar ou tornar identificável uma pessoa ser enquadrado como dado pessoal (art. 5º, I), razão pela qual naturalmente os dados neurais estariam protegidos, o projeto reforça a preocupação com a intimidade do indivíduo ao classificar dado neural como tipo específico próprio de dado pessoal.

Novamente salienta-se que o campo da ciência que estuda e desenvolve métodos para conectar o sistema nervoso pode trazer inúmeros benefícios a vida de pessoas. Não se trata de criar mecanismos que impeçam tal avanço científico. Todavia, o que se revela é, nos termos do projeto de lei, que, ao mesmo tempo que um computador possa coletar dados para tratamentos médicos, possa “revelar lembranças, pensamentos, padrões comportamentais, emoções, sonhos e mesmo os desejos mais íntimos”.¹⁰³

¹⁰² BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.229/2021**. Modifica a Lei nº 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. Brasília: Câmara dos Deputados, 2021. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2276604>. Acesso em: 21. mai. 2021.

¹⁰³ “Por mais intenso que o tratamento de dados fosse, a coleta até pouco tempo encontrava uma barreira que parecia intransponível: a consciência humana. Os rastros de dados deixados pelo indivíduo na Internet, tais como “likes” e a navegação por diferentes sites ainda dependem de “clicks”, os quais são conscientemente executados. No entanto, quando as informações podem ser coletadas diretamente do sistema nervoso, podem ser obtidos pensamentos que jamais viriam a ser comunicados ou transformados em ações, ou mesmo podem ser registradas informações do nosso subconsciente”. *Ibid.*, p. 4.

Razão pela qual a proposta é de que o tratamento de dados neurais só possa ocorrer quando o titular ou responsável consentir de forma específica. As finalidades do tratamento devem ser detalhadas até mesmo nos casos em que a interface-cérebro-computador possa capturar dados de titulares inconscientes. Ademais, o fato de não se aplicarem as exceções de tratamento no art. 4º da LGPD confirma a opção do projeto de manutenção do dado neural como um dado sensível, que enseja maior proteção do que os demais dados pessoais.

Estes elementos que, de alguma forma, abrem espaços para adaptação de tomada de decisão a partir de leituras neurais e simulação de raciocínios lógico-dedutivo são enfrentadas, no debate contemporâneo, por indagações de caráter ético. Nesta linha, Gabrielle Sarlet menciona a iniciativa europeia que propõe pilares éticos para a governança de dados e controle da inteligência artificial. A iniciativa, que preconiza a promoção do desenvolvimento da inovação, sem perder de vista o interesse público e a manutenção de direitos e garantias fundamentais, esboça um conjunto de padrões éticos de emprego da IA na União Europeia.¹⁰⁴

Danilo Doneda destaca ainda que a preocupação com a ética dos dados sinaliza uma mudança da centralidade da informação para o dado. Este ramo específico da ética (*data ethics*) “definido como um ramo que estuda e avalia problemas morais relacionados aos dados”, direciona os olhares para a privacidade, o anonimato, a transparência, a responsabilidade e principalmente a confiança nos modelos de inteligência artificial.¹⁰⁵

Em 8 de abril de 2019, o grupo de especialistas em IA apresentou diretrizes éticas para inteligência artificial confiável.¹⁰⁶ O grupo objetiva o desenvolvimento de um mercado digital inteligente, porém sustentável e inclusivo. Uma IA confiável, além de respeitar limites da legalidade, ética e robustez, deve, segundo a comissão, possuir como requisitos (supervisão humana; robustez técnica e segurança; privacidade e governança; transparência; diversidade, não discriminação e justiça; bem-estar social e responsabilidade). “É imprescindível que haja uma avaliação dos impactos e uma tentativa de mitigação dos riscos necessários em uma sociedade democrática, com

¹⁰⁴ SARLET, Gabrielle Bezerra Sales, **A Inteligência Artificial no Contexto Atual...** *Op. cit.*, p. 296-297.

¹⁰⁵ DONEDA *et al*, **Considerações iniciais sobre inteligência artificial...** *Op. cit.*, p. 10-11.

¹⁰⁶ EUROPEAN UNION (EU). European Commission. **Ethics guidelines for trustworthy AI**. Report / Study. Publication 08 April 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. Acesso em: 21 mai. 2022.

vistas a não infringir as esferas jurídicas dos indivíduos”.¹⁰⁷ Assim como mecanismos de *feedback* externos aos próprios sistemas de inteligência artificial, a ponto de permitir um diálogo com a sociedade.

A centralidade da supervisão humana como requisito dos sistemas de uma inteligência artificial confiável demonstra o “reconhecimento que, embora tragam grandes facilidades e oportunidades, a inteligência artificial também apresenta riscos que devem ser minimizados de forma adequada, eliminando possíveis distorções”.¹⁰⁸ Contendo ainda princípios gerais de explicabilidade, rastreabilidade ou auditabilidade, o relatório produzido pelo grupo de especialistas da comissão deixa nítido que *data ethics* correlaciona responsabilidades morais com a responsabilidade no desenho dos algoritmos.¹⁰⁹

Publicada em 2020, a resolução n.º 332 do Conselho Nacional de Justiça – CNJ corrobora com a preocupação com a governança e o uso da IA.¹¹⁰ Independentemente de ser voltada à utilização de IA no Poder Judiciário, anuncia princípios que orientam decisões baseadas em sistemas de inteligência artificial. Em seus considerandos, propõe o atendimento a critérios éticos de transparência, previsibilidade, possibilidade de auditoria e garantia de imparcialidade e justiça substancial; promoção da qualidade; da liberdade e da justiça; que os dados utilizados possam ser rastreados e auditados, bem como cuidados com a privacidade dos usuários.¹¹¹

Peixoto destaca também o art. 7º da resolução, que fundamenta que as decisões judiciais que utilizem ferramentas de IA devem preservar a igualdade, a não discriminação, a pluralidade e a solidariedade. Sublinha-se que a resolução evidencia que vieses discriminatórios podem surgir no uso de IA e, na impossibilidade de

¹⁰⁷ SILVA, Gabriela Buarque Pereira; JUNIOR, Marcos Ehrhardt, **Diretrizes éticas para a inteligência artificial confiável na União Europeia e a regulação jurídica no Brasil**, Revista IBERC, v. 3, n. 3, 2020. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/133>. Acesso em: 21 mai. 2022. p. 15-16.

¹⁰⁸ PEREIRA; LORENZETTO. **Inteligência artificial...** *Op. cit.*, p. 14.

¹⁰⁹ Certamente a tecnologia produz uma enorme variedade de fatos ensejadores da responsabilidade civil. Não é objetivo do estudo a responsabilização civil da eventual imprevisibilidade, não explicabilidade ou danos decorrentes da inteligência artificial. Sobre os elementos tradicionalmente exigidos para a configuração do dever de indenizar, recomenda-se a leitura de Guilherme Magalhães Martins e Nelson Rosendal, Responsabilidade Civil e Novas Tecnologias.

¹¹⁰ CONSELHO NACIONAL DE JUSTIÇA. **Resolução n.º 332/2020, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 21 dez. 2022.

¹¹¹ PEIXOTO, **Direito e Inteligência Artificial...** *Op. cit.*, p. 40.

aplicação de medidas corretivas, o modelo deva ser descontinuado com as razões que levaram a tal decisão.

Frazão entende que o meio mais efetivo para lidar com estes princípios, principalmente o da explicabilidade e auditabilidade, requer um processo de testes extensivos, de modo que os resultados indesejados possam ser excluídos toda vez que se mostrarem presentes. Tal exclusão delimitaria listas ou categorias que não poderiam ser criadas sob o risco de agravar categorizações de indivíduos.¹¹² Ainda que não se adentre no aspecto prático sobre quem deva realizar estes testes, qual seu âmbito de proteção e, se incumbe ao Estado esta delimitação, sistemas de IA devem respeito a valores democráticos como intimidade e privacidade de dados. Por mais que essa transparência seja desejada e necessária, a prática parece caminhar no sentido oposto.

Caminho este que, na visão de O’Neil, sustentará diretamente sistemas de inteligência artificial e IoT nos próximos anos. Aos olhos humanos serão apenas sistemas sugerindo itens de compras, rotas de trânsito, definição de preços e anúncios. Programas matemáticos que determinarão como os indivíduos devem ser tratados, em que cesta de humanos se enquadram. A autora é cética quanto a possibilidade de transparência destes modelos matemáticos. Para O’Neil estes algoritmos além de arbitrários são não responsabilizáveis.¹¹³

Frazão resume a necessidade de regulação dos limites de tratamento destes dados. A preocupação não se restringe as deficiências ou insuficiências destes modelos matemáticos. Para a autora,

os algoritmos preocupam tanto quando acertam como quando erram. Preocupam quando acertam, pois podem revelar aspectos íntimos da nossa personalidade que gostaríamos de manter em segredo. Preocupam quando erram, pois desconfiguram a nossa individualidade, atribuindo-nos características que não temos, com o agravante de que tais decisões são baseadas em juízos totalmente equivocados.¹¹⁴

Em ambos os casos, as decisões baseadas unicamente em algoritmos podem restringir acessos, oportunidades e tolher direitos. Estas violações atingem a personalidade da pessoa, sua individualidade, seu direito fundamental à intimidade, à

¹¹² FRAZÃO, Ana. **Fundamentos da proteção...**, *Op. cit.*, p. 42-43.

¹¹³ O’NEIL, Cathy. **Algoritmos de destruição em massa...** *Op. cit.*, p. 268-269.

¹¹⁴ FRAZÃO, Ana. **Fundamentos da proteção...**, *Op. cit.*, p. 34.

vida privada, à imagem, além do, sem atalhos, direito fundamental à proteção dos dados pessoais.

É inegável que as mudanças tecnológicas, que não deixarão de ocorrer, alteraram o fluxo e a dinâmica do tratamento de dados pessoais dos titulares. A expansão das possibilidades e finalidades suscitam atenção para os efeitos, não somente na projeção do livre desenvolvimento de cada indivíduo, mas também em todo o ordenamento jurídico.

Na medida que o direito deve olhar para estas inovações, surge a necessidade de reexame de institutos relacionados a proteção da personalidade e da privacidade, bem como a criação de novos, como propriamente o direito à proteção de dados pessoais. Institutos que umbilicalmente relacionados, devem propiciar abertura para abarcar as noções de desenvolvimento econômico, tecnológico, inovação e, ao mesmo tempo autodeterminação informativa.

2. DIREITO À PERSONALIDADE, DIREITO À PRIVACIDADE E DIREITO À PROTEÇÃO DE DADOS

Em sua definição mais elementar, os direitos da personalidade são aqueles que se relacionam com o indivíduo, cujo componente essencial coloca o ser humano como centro do direito. A despatrimonialização é o ponto de atenção de um direito privado repersonalizado, razão pela qual os direitos da personalidade possuem como característica uma elasticidade.¹¹⁵

Diferente do direito de propriedade, cujo objeto é externo ao sujeito, nos direitos da personalidade o objeto recai sobre seu titular de forma indissociável. Neste ponto, Doneda ressalta a “artificialidade de uso acrítico da categoria de direito subjetivo” por alguns autores. Para Doneda, como as relações jurídicas privadas se constituíam em instrumentos de natureza proprietária, sua consequência era a classificação dos direitos subjetivos à categoria do “ter”. No que lhe concerne, a tutela da personalidade contradiz estes sistemas ao emergir a categoria do “ser”, no qual a pessoa é a merecedora de proteção.¹¹⁶

Adriana Corrêa e José Antônio Gediel também destacam que a proteção do “ser” é o que se tem conferido ao direito da personalidade a partir do século XX. Com contorno ao direito à intimidade e à vida privada, deixa de ser compreendido pelo aspecto patrimonial¹¹⁷, muito embora intimidade e vida privada sejam apenas alguns dos direitos da personalidade, que, como ressaltado, não possuem rol taxativo e comportam uma dinamicidade.

Essa dinamicidade ou elasticidade do direito à personalidade (que além dos direitos citados anteriormente, ligavam-se ao direito ao nome e à imagem) é superada por uma interpretação que conduz a um único direito à personalidade, porém que comporta uma pluralidade de manifestações. Assim, afasta-se uma eventual taxatividade do direito à personalidade, acolhendo como objeto a tutela da pessoa

¹¹⁵ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 51.

¹¹⁶ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 88.

¹¹⁷ CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres, **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado**, Revista Faculdade de Direito - UFPR, v. n. 47, p. 141–153, 2008.

humana e seu livre desenvolvimento, apesar de, como observa Doneda, tais contornos possam dificultar a definição de seus limites e restrições.¹¹⁸

Ainda, na concepção de um poder sobre sua própria pessoa, aventa-se a possibilidade de uma dupla abordagem do direito à personalidade. De um lado, um direito que incide sobre a própria pessoa (*ius in se ipsum*), de outro uma incidência externa de cunho negativo geral. Para Tepedino, ambas são válidas, na medida que o conteúdo da pretensão de respeito aos bens pessoais recai também à coletividade.¹¹⁹

Conclui-se, portanto, que o direito à personalidade passa a almejar uma nova aplicabilidade através de sua constituição como valor juridicamente relevante. Normas como a proteção de dados pessoais passam a integrar esta pluralidade de manifestações, obviamente requerendo necessidades específicas (como controle do acesso, utilização e circulação de dados), mas sem perder a conexão com a proteção ao direito da personalidade.

Busca-se fortalecer a proteção da pessoa inserindo nos poderes do titular desse direito de personalidade o controle não só sobre o acesso, mas também no que se refere ao seu tratamento, à sua utilização e à sua circulação [...] Na sociedade tecnológica contemporânea, dessa forma, a construção da esfera privada passou a ser compreendida pela possibilidade de o indivíduo controlar o acesso e o uso dos dados que constituem sua identidade pessoal e permitem o livre desenvolvimento de sua personalidade (tais como: opinião política, convicções religiosas, vida sexual, dados de saúde e dados genéticos).¹²⁰

Esse alcance da proteção de dados é sem precedentes no âmbito da sociedade tecnológica. Já entendido que a proteção, ou a falta de, afeta todas as esferas da vida social, política e econômica, Laura Mendes, corrobora com a ideia que desenvolvimentos modernos poderiam acarretar novos riscos para o indivíduo e, desta forma, “o direito geral de personalidade serviria para conceder proteção por meio de sua formulação abstrata contra riscos ainda desconhecidos e

¹¹⁸ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 90-91.

¹¹⁹ TEPEDINO, Gustavo, **A tutela da personalidade no ordenamento civil-constitucional brasileiro**, Rio de Janeiro: Renovar, 2008. Disponível em: https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil_constitucional_brasileiro. Acesso em: 16 jun. 2022. p. 6.

¹²⁰ CORRÊA; GEDIEL, **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado**. *Op. cit.*, p. 143.

imprevisíveis”.¹²¹ Analisando decisões do tribunal constitucional alemão, a autora resume que não é possível estabelecer de forma conclusiva o conteúdo deste direito, e que a análise de casos concretos resulta em novas abordagens em termos de direitos fundamentais, inclusive superando concepções clássicas de esfera privada.

Assinala ainda três atributos pertencentes a estes direitos da personalidade: proteção abrangente, autodeterminação e abstração. Tais atributos sintetizam as explicações a respeito do âmbito de proteção, dos poderes dos titulares e da proteção ampliada na sociedade moderna.¹²²

Direitos que Rodotà compreende terem forte ligação com elementos básicos da democracia. Motivo pelo qual critica a expressão ou a afirmação de quem não tem nada a esconder, não tem nada a temer. A preservação da privacidade, da intimidade ou do controle de circulação de informações não pode tornar o indivíduo “inimigo” ou automaticamente suspeito. “Esta lógica é típica dos regimes totalitários e, portanto, contrária à democracia”.¹²³

O fenômeno da proteção de dados, que se insere nestes elementos básicos de uma sociedade democrática, provoca a ordem jurídica a se reorganizar e assegurar proteção adequada, principalmente em um quadro de reequilíbrio de poderes no ambiente digital.

Este quadro normativo de reequilíbrio de poderes, associado a um movimento de afirmação de direitos fundamentais na internet, é o que se tem denominado “Constitucionalismo Digital”. Inicialmente este termo havia sido cunhado para se referir a um movimento de limitação do poder de atores na internet, em oposição ao poder do Estado. Todavia, a corrente contemporânea passou a se orientar pelo reconhecimento de prescrições de normativas comuns entre tais atores.¹²⁴

Tarefa esta que Moura destaca ser complexa, considerando a dificuldade no estabelecimento deste acoplamento do direito constitucional no ciberespaço,

¹²¹ MENDES, Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito**, Revista de Ciências Jurídicas, v. 25, n. 4, 2020. p. 7-10.

¹²² *Ibid.*

¹²³ “Se trata de una lógica típica de los regímenes totalitarios y, por tanto, contraria a la democracia. En efecto, si una persona quiere preservar una esfera, aunque mínima, de privacidad e intimidad, y desea que nadie conozca ciertas informaciones sobre sí mismo, se convierte, según el Estado, en alguien que tiene algo que esconder y, automáticamente, en sospechoso, en enemigo del pueblo”. RODOTÀ, **Democracia y protección de datos**. Op. cit., p. 15-16.

¹²⁴ MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. **Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro**. Justiça do Direito. v. 34, n.2, 2020. Disponível em: <http://seer.upf.br/index.php/rjd/article/view/11038>. Acesso em: 20 mar. 2022. p. 9-10.

principalmente por seu caráter transnacional.¹²⁵ Gilmar Mendes e Fernandes assinalam que a “internet se relaciona de forma ambivalente com a teoria dos direitos fundamentais.”¹²⁶ Na sociedade dos dados, a internet amplia as possibilidades de realização de algumas garantias individuais. Em certos cenários é inclusive condição necessária, como no campo da liberdade de expressão. As novas formas de comunicação digital influenciam na própria reflexão da dimensão normativa de direitos constitucionais, criando oportunidades distintas daquelas que recebem proteção constitucional explícita. Por outro lado, ressaltam que, estes avanços, ao mesmo tempo que ampliam esta capacidade de realização de direitos fundamentais, podem suscitar abusos e violações de outros direitos.¹²⁷ No exemplo da liberdade de expressão, estes são percebidos nos casos de disseminação de desinformação e discursos de ódio.¹²⁸

Essa transição, na visão de Stefano Rodotà, não garante que o resultado seja a entrada na pós-democracia. Por se encontrar na dimensão do inédito não pode ser avaliado com critérios do passado, nem tampouco ter atribuída uma espécie de autoevidência a qualquer evento futuro. Rodotà é crítico em relação à manutenção do poder por grandes empresas de tecnologia que com os dados “governam nossas vidas”. Desta forma, o fortalecimento desta nova dimensão deve considerar não apenas a intromissão do Estado, mas a limitação destes poderes externos.¹²⁹

¹²⁵ MOURA, Ariel. **Constitucionalismo Digital**. IX CONGRESSO INTERNACIONAL DA ABRASD - Associação Brasileira de Pesquisadores em Sociologia do Direito. 2018. Disponível em: https://www.academia.edu/38515467/CONSTITUCIONALISMO_DIGITAL. Acesso em: 03 jun. 2022. p. 934-937.

¹²⁶ MENDES; FERNANDES. **Constitucionalismo Digital**... *Op. cit.*, p-10-12.

¹²⁷ *Ibid.*

¹²⁸ Em relação ao conflito de liberdade de expressão e o discurso de ódio (*hate speech*), recomenda-se a leitura de Daniel Sarmiento. Para o autor, o *hate speech* “tende a produzir dentre as suas vítimas ou o revide violento ou o silêncio humilhado. No primeiro caso, há riscos evidentes para a paz social e para a ordem pública. Ao invés de uma discussão voltada para o bem comum, corre-se o risco de deflagração de uma verdadeira guerra no espaço público. No segundo caso, as vítimas do ódio, oprimidas, humilhadas e sentindo-se deserdadas por um Estado que se recusa a protegê-las, retraem-se e abandonam a esfera pública. O resultado é prejudicial não só a elas, que são privadas do exercício efetivo da sua cidadania, como a toda a sociedade, que perde o acesso a vozes e pontos de vista relevantes, cuja expressão na arena pública enriqueceria e pluralizaria o debate público. Neste sentido, é plausível a afirmação de que a liberação do *hate speech*, no cômputo geral, produz menos discurso do que a sua restrição”. SARMENTO, Daniel. **A liberdade de expressão e o problema do “hate speech”**. Revista de Direito do Estado, Rio de Janeiro, ano 1, n. 4, 2006. p. 33-34.

¹²⁹ RODOTÀ, Stefano. **Perché Internet ha bisogno di una propria Costituzione**. La Repubblica, Italian Tech. 2014. Disponível em: https://www.repubblica.it/tecnologia/2014/03/15/news/perch_internet_ha_bisogno_di_una_propria_costituzione-81045633. Acesso em: 18 jun. 2022.

Repensar como o exercício do poder deve ser legitimado na sociedade da informação, articular os limites do exercício do poder são componentes deste desafio do constitucionalismo digital. Adicionalmente, reconhecer como os valores da governança digital podem ser protegidos¹³⁰, o que demanda uma compreensão mais substantiva dos direitos constitucionais na governança online.¹³¹

Iniciativas que não implicam necessariamente em alterações formais nos textos constitucionais, mas que reconhecem a existências de novos direitos como: direitos de acesso à internet; direitos de esquecimento ou mais recentemente desindexação de conteúdo; direitos de neutralidade da rede, bem como deveres de transparência e uso ético de dados pessoais. Materialmente estas categorias intentam limitar o poder do Estado e dos atores privados em suas relações com usuários.¹³²

Concluem, portando, Gilmar Mendes e Fernandes que a atuação dos Tribunais e as Cortes Constitucionais ainda carregavam a visão arraigada do constitucionalismo digital como forma de oposição ao poder do Estado, explicado pela falsa crença que a difusão da internet implicaria na crise de um modelo de constitucionalismo moderno. Essa posição, que diverge da concepção contemporânea de constitucionalismo digital, era alimentada pelo “ideário de que o estado político moderno não seria mais capaz de responder à complexidade regulatória da sociedade interconectada”¹³³ Esvaziamento relativizado nas decisões recentes ante ao “reconhecimento de que as mesmas formas tradicionais de governo continuam a exercer função política relevante na definição da normatividade do ciberespaço”.¹³⁴

2.1 RECONSTRUÇÃO DA PRIVACIDADE – DA AUTONOMIA DO INDIVÍDUO À MONETIZAÇÃO DE CONTEÚDO

¹³⁰ “No âmbito digital pode-se observar a discussão sobre a privacidade, liberdade e segurança de dados impulsionada pelos vazamentos dos arquivos da Agência Norte-americana de Segurança (NSA) por Edward Snowden, um ex-funcionário terceirizado da mesma, no qual vem à tona um projeto do próprio governo americano chamado “PRISM”, criado com intuito de monitoramento de dados dos particulares desde o atentado às torres gêmeas de 2011”. MOURA, **Constitucionalismo Digital**. *Op. cit.*, p. 936.

¹³¹ SUZOR, Nicolas. **Digital Constitutionalism : Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms**. Queensland University of Technology (QUT) School of Law, 2018. p. 4.

¹³² MENDES; FERNANDES, **Constitucionalismo Digital...** *Op. cit.*, p. 9-15.

¹³³ *Ibid.*, p. 16.

¹³⁴ *Ibid.*, p. 17.

Vida privada, intimidade, sigilo, segredo, espaço particular são termos que já foram, e ainda são utilizados na tentativa de estabelecimento de um conceito de privacidade. Esta tentativa de delimitação do conteúdo do direito à privacidade, na visão de Danilo Doneda, soa, no mínimo, como parcial. Estipular um núcleo duro do que pode ser enquadrado como privacidade é diminuir a multiplicidade de interesses à que se propõe este direito, o qual é a tutela da pessoa humana. Por óbvio que Doneda não quer dizer que tais conceitos não sejam mais aplicáveis, mas simplesmente que não podem ser considerados isoladamente, reafirmando uma continuidade histórica da tutela da privacidade.¹³⁵ Esta indefinição “deve ser tomada mais como uma característica intrínseca da matéria do que um defeito ou obstáculo. Tal indeterminação é uma característica ontológica da própria construção da esfera privada”.¹³⁶

Continuidade histórica que, para a maioria dos autores, tem como referência inicial do debate moderno sobre a privacidade o artigo jurídico escrito em 1890 por Samuel Warren e Louis Brandeis para a revista *Harvard Law Review*.¹³⁷ O conceito de privacidade à época, distinto do atual, associava-se com a possibilidade de ausência de comunicação com outras pessoas, ou o direito de ser deixado só. (*Right to be let alone*)¹³⁸. O que Warren e Brandeis propuseram foi considerar se as leis existentes permitiam oferecer este princípio da privacidade e, em caso afirmativo, qual sua extensão. Esse direito de ser deixado só¹³⁹, como direito da pessoa contra o mundo, afirmava o caráter de inviolabilidade de personalidade.

Essas raízes profundas de proteção à intimidade mudaram de forma e intensidade com o surgimento da internet, aceleradas principalmente pela capacidade

¹³⁵ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 41.

¹³⁶ *Ibid.*, p. 104-105.

¹³⁷ WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. *Harvard Law Review*. v. 4, n. 5 1890, p. 193-220. Disponível em: <https://www.jstor.org/stable/1321160?seq=1>. Acesso em: 19 jun. 2022.

¹³⁸ Ressalta-se que embora amplamente citado como “direito de ser deixado só”, os autores em nenhum momento definem estritamente *right to privacy*, conforme destaca Danilo Doneda. O termo é referenciado pelo magistrado norte-americano Thomas Cooley. DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 104.

¹³⁹ Rodotà exemplifica que a privacidade, inicialmente traduzida como o direito de ser deixado só, possuía uma aplicação muito distinta da atual. Primordialmente foi uma manifestação tipicamente burguesa. “A possibilidade de aproveitar plenamente a própria intimidade é uma característica que diferenciava a burguesia das demais classes”. O isolamento era privilégio de poucos e, aliás, o direito de ser deixado só pode assumir “significado imensamente negativo quando isso implica no desinteresse pelas condições de vida dos menos favorecidos”. RODOTÀ, Stefano, **A vida na sociedade da vigilância - a privacidade hoje**, Rio de Janeiro: Renovar, 2008. p. 27-28.

e velocidade de processamento e transmissão destas informações.¹⁴⁰ O que antes, apesar de protegido, demorava para ser conhecido pelos demais, hoje, tornado público, alcança um número grande de pessoas instantaneamente.

Além disso, o sujeito ativo na violação primeiramente era o Estado e seus centros de processamento de dados. Porém, potencializados pelo crescimento do fluxo de informações, pelo alargamento das possibilidades de usos e pela diminuição dos custos computacionais, exigiu-se que fossem criados meios de proteção da privacidade também contra terceiros.¹⁴¹

Em primeiro lugar, foi o Estado que por primeiro se encontrou na posição de utilizar largamente informações pessoais. Os motivos são razoavelmente claros: um pressuposto para a administração pública eficiente é o conhecimento tão acurado quanto possível da população... Fora da esfera estatal, a utilização de informação era limitada basicamente por um motivo estrutural, a princípio quase que generalizado: a desproporção de meios computacionais dos organismos privados em relação ao Estado.¹⁴²

O aumento do uso de informações não foi somente quantitativo, mas qualitativo. Novos métodos, técnicas de coleta, formas de categorização e novas utilidades em modelos de negócios estruturados mudaram o cenário de processamento de informação, que antes representava uma ameaça do Estado ao indivíduo. Estende-se o poder do processamento de dados para as relações entre indivíduos e entes privados.

A privacidade, neste novo cenário, ganha importância como requisito de exercício de outras liberdades e direitos. Seu conteúdo incorpora a multiplicidade de espécies citada no início do capítulo e passa a ser pressuposto para que o cidadão desenvolva sua individualidade de forma autônoma. Essa compreensão leva ao entendimento da privacidade e de sua violação não somente como um problema de coleta e exposição de dados, mas de proteção de direitos humanos, de limitação da manifestação das liberdades e identidade da pessoa.¹⁴³

¹⁴⁰ OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019. p. 56.

¹⁴¹ OLIVEIRA; LOPES, **Os princípios norteadores da proteção de dados...**, *Op. cit.*, p. 57.

¹⁴² DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 34-35.

¹⁴³ NETO, Elias Jacob de Menezes; Jose Luis Bolzan de Moraes, **A fragilização do Estado-Nação na proteção dos direitos humanos violados pelas tecnologias da informação e comunicação**. Revista Direitos Fundamentais & Democracia, v. 23, n. 3, 2018. p. 244-251.

Partindo deste conjunto de atividades e situações, constata-se que “hoje a sequência quantitativamente mais relevante é “pessoa-informação-circulação-controle”, e não mais apenas “pessoa-informação-sigilo”, em torno da qual foi construída a noção clássica de privacidade”.¹⁴⁴ O objetivo extrapola a esfera do segredo para uma forma mais ampla, de determinação de quais informações serão acessíveis e quem pode acessá-las. Mantém-se, de todo modo, o foco de proteção no indivíduo.¹⁴⁵

Estas esferas são frequentemente citadas como baseadas na “teoria das esferas concêntricas” ou “teoria dos círculos concêntricos” de Heinrich Hubmann. A teoria elaborada em 1953 delimitava a esfera de proteção conforme a área de privacidade afetada. Na camada mais externa (esfera pessoal), estariam as intersecções interpessoais — convivência entre pessoa e sociedade. Na camada intermediária (esfera privada) as informações são restritas a um grupo de pessoas mais próximas e desconhecidas do público. Por fim, na esfera mais profunda (segredo) guardam-se as informações mais íntimas, nunca ou raramente compartilhadas com quaisquer outros indivíduos.¹⁴⁶

Desta forma, quanto mais profunda a camada, mais intocável e protegida deveria estar a informação. Porém, na prática, essa classificação é muito mais complexa do que um puro enquadramento, principalmente pelos motivos já abordados, a multifacetada interpretação da privacidade. Por esta razão, autores como Danilo Doneda consideram infrutífero conceituações que intensifiquem ou atenuem diferenças entre os termos.

Independente da esfera, a ausência clara de uma terminologia da privacidade pela doutrina e jurisprudência “podem ter sugerido ao legislador optar pelo excesso, até pelo temor de reduzir a aplicabilidade da norma”. A tentativa de classificação conceitual desviaria o principal objetivo que é “a aplicação do direito fundamental da

¹⁴⁴ RODOTÀ, **A vida na sociedade da vigilância - a privacidade hoje**. *Op. cit.*, p. 93.

¹⁴⁵ Constata-se tal proteção inclusive no texto constitucional brasileiro, conforme inclusão entre os direitos e garantias fundamentais (art. 5, X) do direito a inviolabilidade da intimidade, da vida privada, da honra e a imagem das pessoas. BRASIL. Constituição 1988. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 19 jun. 2022.

¹⁴⁶ ROSSONI, Caroline; BOLESINA, Iuri, **A teoria dos círculos concêntricos e a proteção à vida privada: análise ao caso Von Hannover vs. Alemanha, julgado pela corte europeia de direitos humanos**. XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea - VII Mostra de Trabalhos Jurídicos Científicos, 2004. Disponível em: <https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/11672>. Acesso em: 19 jun. 2022. p. 3-6.

pessoa humana em questão, em sua emanção constitucional”.¹⁴⁷ Razão pela qual Doneda unifica termos como vida privada, intimidade, segredo e sigilo em “privacidade”.

Essas mudanças e ampliações no entendimento da privacidade levantam uma nova problemática, a análise de conflitos com outros institutos. Reforça-se a necessidade da verificação de limites e restrições, e como a privacidade (na sua acepção mais ampla) se choca com direitos de informação, transparência ou vedação ao anonimato. Além disso, é preciso também analisar os limites e restrições da própria tutela de dados em sentido estrito, como condição prévia de proteção de outros bem jurídicos constitucionais.¹⁴⁸

Um dos casos clássicos no direito brasileiro de resolução de conflitos entre privacidade e liberdade de imprensa, que exigiu a análise de proporcionalidade, foi o da exposição de vídeos íntimos da Daniella Cicarelli. A solicitação da modelo era que os vídeos fossem ser removidos, alegando inexistir interesse público. A ação, julgada improcedente em primeira instância, considerou que a exposição voluntária da intimidade ao público impede exigência de um direito à privacidade futura. A decisão, foi reformada pelo Tribunal de Justiça, com entendimento de que a não autorização de vinculação do vídeo pelo casal, o torna ilícito e a violação a intimidade deveria ser preservada, ainda que notoriamente fossem personalidades públicas. Por fim, a corte constitucional manteve a decisão, exigindo a remoção do vídeo pela plataforma *YouTube*.¹⁴⁹

Ingo Sarlet indica que, especialmente em relação à proteção de dados, a ponderação ou o balanceamento que precisa ser verificado na solução de conflitos ganha especial relevância por conta das disparidades de poder econômico, social e político existentes entre os titulares do direito e as grandes empresas que coletam e processam dados. “É imprescindível ser consistente com as exigências do teste de

¹⁴⁷ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 106-108.

¹⁴⁸ A própria Lei 13.709/2018, em seu art. 7º traz um rol de hipóteses de tratamento de dados mediante o qual não é necessário o consentimento do titular e, neste sentido, operam como condições de legitimação das restrições. Estas hipóteses e suas aplicações serão detalhadas no capítulo seguinte deste trabalho.

¹⁴⁹ HESS, Heliana Maria Coutinho, Apontamentos sobre o princípio da proporcionalidade na Alemanha e no Brasil – aplicações ao Direito midiático, *in*: PRETTO, Renato Siqueira De; KIM, Richard Pae; TERAOKA, Thiago Massao Cortizo (Orgs.), **Interpretação Constitucional no Brasil**, [s.l.]: Escola Paulista da Magistratura, 2017. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ic11.pdf>. Acesso em: 14. abr. 2022 p. 287-289.

proporcionalidade¹⁵⁰, não apenas no sentido de proibição de uma intervenção, mas também, no sentido de proibição de uma proteção insuficiente”.¹⁵¹

A incorporação do constitucionalismo digital, proposto por Gilmar Mendes, implica inclusive, em relação a conflitos de direitos de proteção de dados, na necessidade de redefinição da teoria da eficácia horizontal dos direitos fundamentais. Ao contrário do que propõe a doutrina dos Estados Unidos (*state action*)¹⁵², Mendes reafirma o reconhecimento, no caso brasileiro, da eficácia de aplicação de direitos fundamentais nas relações privadas. Esta perspectiva de proteção passou a orientar o papel do legislador, mediante o dever de proteção “não apenas de proibição do excesso, mas de conformação dos direitos fundamentais na dimensão privada”.¹⁵³

Entretanto, a concepção da teoria da eficácia horizontal dos direitos fundamentais¹⁵⁴, segundo Gilmar Mendes, no ambiente digital tem aplicabilidade limitada, pois, enquanto na versão tradicional a teoria se baseia em uma ótica de “equilíbrio entre direitos individuais dos atores”, nas relações virtuais a dimensão deve ser coletiva-institucional e deve considerar, do mesmo modo, o enorme desequilíbrio de poder entre as plataformas, cujas decisões refletem nas possibilidades de realização de liberdades públicas.¹⁵⁵

¹⁵⁰ O objeto da pesquisa não alcança o estudo aprofundado da exigência de teste de proporcionalidade. Para exame sobre o tema recomenda-se a leitura de: Teoria dos Direitos Fundamentais - Robert Alexy; Colisão de Direitos Fundamentais e Princípio da Proporcionalidade – Wilson Antônio Steinmetz; Direitos Fundamentais: Trunfos contra a maioria – Jorge Reis Novais e Direitos fundamentais: Conteúdo essencial, restrições e eficácia – Virgílio Afonso da Silva.

¹⁵¹ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 53.

¹⁵² “Com base na concepção do Estado Liberal Clássico, uma teoria contrária à horizontalização dos direitos fundamentais ainda é fortemente adotada nos Estados Unidos da América, denominada *state action*, que estabelece uma visão quase universal de que os direitos fundamentais estabelecidos no *Bill of Rights* da Carta estadunidense impõem limitações apenas para os Poderes Públicos”. Diferente do Brasil que estabelece aplicabilidade imediata as normas definidoras de garantias e direitos individuais, ou seja, também ocorre a aplicação de forma direta às relações privadas. CARVALHO, Alexander Perazo Nunes de; LIMA, Renata Albuquerque. **A Eficácia Horizontal dos Direitos Fundamentais**, Revista Opinião Jurídica, v. 13, n. 17, p. 11–23, 2015. Disponível em: <https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/469/187>. Acesso em: 21 jun. 2022.

¹⁵³ MENDES; FERNANDES, **Constitucionalismo Digital...** *Op. cit.*, p. 19-23.

¹⁵⁴ A teoria da eficácia horizontal dos direitos fundamentais envolve outras questões que extrapolam os objetivos da presente pesquisa. Para investigar a vinculação de particulares a direitos fundamentais sugere-se a leitura complementar de: A Eficácia Dos Direitos Fundamentais – Ingo Wolfgang Sarlet; A Eficácia Horizontal dos Direitos Fundamentais - Alexander Perazo Nunes de Carvalho e Renata Albuquerque Lima; Os direitos fundamentais na Constituição Portuguesa de 1976 - José Carlos Vieira de Andrade; Direitos fundamentais e direito privado - Claus-Wilhelm Canaris e Direitos Fundamentais e Relações Privadas – Daniel Sarmento.

¹⁵⁵ MENDES; FERNANDES, **Constitucionalismo Digital...** *Op. cit.*, p. 19-23.

Os direitos à privacidade e proteção de dados claramente não são absolutos e estão sujeitos a limites e passíveis de restrições, mas como recorda Ingo Sarlet, “acionam-se, também nesse caso, os assim chamados limites aos limites dos direitos fundamentais, dentre os quais desponta a necessária observância dos critérios de proporcionalidade e da salvaguarda do núcleo essencial”.¹⁵⁶ Limites aos limites que devem, principalmente considerando a discrepância de forças, repetir que, o que se assume relevo é tutela da pessoa e suas condições básicas de exercício de sua individualidade.

O direito à privacidade ou à proteção de dados, portanto, poderão ser restringidos mediante avaliação da dimensão de peso com outros princípios envolvidos. Para Alexy, esta análise envolve o exame de três máximas: adequação, necessidade e proporcionalidade em sentido estrito (sopesamento).¹⁵⁷ A restrição será proporcional se alcançar um objetivo legítimo e não puder ser igualmente realizada por outra medida menos gravosa.

Pode-se citar ainda que, a utilização de algoritmos afeta também outras esferas das relações privadas, como o direito a anonimização da comunicação, o direito à neutralidade da rede. Todavia, a análise das restrições encontra o mesmo caminho dos direitos à privacidade e proteção de dados em sentido estrito, cabendo utilização de técnicas de proporcionalidade.

2.1.1 – Publicidade direcionada e perfilação do usuário

O exemplo da Cicarelli representa o já exposto afrontamento ao direito à privacidade no âmbito individual, já que o vazamento de vídeos íntimos prejudicou a imagem somente a modelo. Convém, porém, abordar o risco coletivo da proteção da privacidade, em especial alimentado por empresas que coletam informações sobre um grande conjunto de consumidores em numerosas fontes de dados.

Chamados de corretores de dados, ou *data brokers*, estas entidades coletam dados em fontes comerciais, governamentais ou públicas e compilam estes dados

¹⁵⁶ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 55.

¹⁵⁷ Alexy define princípios como mandamentos de otimização em face das possibilidades jurídicas e fáticas. O estudo proposto, de avaliação da dimensão do direito à proteção de dados pessoais, não alcança os detalhes das diferenças de regras e princípios e as minúcias nos casos de colisão de direitos fundamentais. Para tal, aconselha-se a leitura da obra completa do autor. ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros Editores, 2009. p. 117-119.

para comercializá-los. O objetivo final desta comercialização é criar grupos de usuários para os quais os anúncios possam ser mais efetivos. Essa publicidade direcionada, ou comportamental, utiliza a perfilação de pessoas para comunicar em massa, de forma a mitigar a ineficiência (standardização) da comunicação tradicional que atingia públicos não propensos a consumir o bem anunciado.¹⁵⁸

A Federal Trade Commission – FTC¹⁵⁹ realizou estudo (*Data Brokers - A Call for Transparency and Accountability*) aprofundado sobre corretores de dados que coletam informações pessoais sobre os consumidores de uma ampla variedade de fontes e as fornecem para diversas finalidades, como comercialização de produtos e detecção de fraudes. A primeira importante constatação é que os consumidores desconhecem estas empresas, pois os *data brokers*, geralmente, não interagem com o consumidor final. Em seguida, verificou-se que estas empresas utilizam não somente dados brutos dos usuários, mas também dados inferidos sobre os consumidores, baseados no histórico de comportamento e padrões de conduta, como, por exemplo, sites que navega.¹⁶⁰ Estes dados derivados são o que permitem criar segmentos de clientes e por consequência a publicidade comportamental. A classificação dos clientes viabiliza a análise de probabilidade de resposta a esforços de marketing específicos ou a chance de realizarem uma compra em um determinado momento.

Esta classificação, que culmina no *user profiling* ou perfilamento do usuário, consiste na avaliação de dados pessoais para determinar aspectos de uma pessoa singular. É o que Doneda diferencia de “informação base” e “informação-resultado” ou

¹⁵⁸ Bioni subdivide a publicidade em três: publicidade contextual, que correlaciona a temática de um determinado ambiente como anúncios de carro em revistas automotivas. Nesta publicidade o meio é o mais relevante; a publicidade segmentada, na qual não importa o meio, mas o público que acessa. Nesta segmenta-se a camada da massa de consumidores, independentemente da plataforma que será veiculada. Por fim a publicidade comportamental, que personaliza o contato entre consumidores e vendedores, de acordo com o perfil de cada consumidor, sendo esta a mais efetiva. BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**; Editora Forense, 3. ed.; São Paulo, 2021. p. 15-16.

¹⁵⁹ A FTC é uma agência governamental norte-americana de proteção e prevenção de práticas comerciais desleais. Federal Trade Commission - FTC. Disponível em: <https://www.ftc.gov/>. Acesso em: 22 jun. 2022.

¹⁶⁰ Apenas como exemplo, o relatório demonstra que o banco de dados de um dos *data brokers* tem informações sobre 1,4 bilhão de transações de consumidores e mais de 700 bilhões de elementos de dados agregados. O banco de dados de outro data broker cobre um trilhão de dólares em transações de consumidores. RAMIREZ, Edith *et al*, **Data Brokers - A Call for Transparency and Accountability**, Federal Trade Commission, 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 16 jun. 2022.

aplicação de métodos de tratamento para obtenção de inferências¹⁶¹. Desta forma, as características personalíssimas são mensuradas e, como tratado pelo relatório da FTC, a probabilidade de sucesso de venda de um determinado produto ou serviço é maior.¹⁶²

Essa técnica é utilizada também para mitigação de riscos por outros ramos empresariais. Um dos mais simples, ou mais didáticos, é o citado no primeiro capítulo, referente a seguradoras de veículo. Com a utilização de dados singulares rastreáveis, como localização em tempo real (GPS), endereço residencial e comercial é possível medir a probabilidade de acidentes e majorar ou diminuir o risco para o negócio. Obtém-se uma representação virtual da pessoa, numérica e quantificável, cujos parâmetros e resultados são desconhecidos pelo seu representante real.

Ortiz e Silveira destacam que esse trabalho de mineração e cruzamento de dados permitem inferências não imaginadas. A análise combinatória de dados identifica padrões não previstos, mas que fornecem correlações e agrupamentos de tipos comportamentais valiosos para o mercado publicitário. O que os autores denominam modulação do comportamento difere da mera vigilância tratada no capítulo primeiro deste trabalho. “Modular é interferir sutilmente no rumo do actante em ação”.¹⁶³ Assim, mais do que identificar padrões, criam-se demandas.

Schmidt Neto também se alinha com o entendimento ao traduzir o ser humano como uma animal “hackeável”. A utilização de *smartphones* e os aplicativos que as pessoas operam diariamente alimentam hábitos e identificam rotinas. Servem de moduladores de comportamentos naturais.¹⁶⁴

¹⁶¹ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 163.

¹⁶² Um exemplo desta inferência é cita por O’Neil em seu livro. O fornecimento massivo de dados de uma rede de supermercados permitiu estudo de hábito dos consumidores para inferir ou deduzir posicionamentos políticos. Consumidores que compraram produtos de última hora, ou seja, que estavam dispostos ao lado dos caixas foram classificados como impulsivos. Os que pagaram preços mais altos por produtos de marcas conhecidas, foram classificados como consumidores fiéis. Na contramão, os que trocaram produtos de preferência por promoções, são os voláteis. Por mais simples que este modelo possa ser, foi utilizado para verificar como estes consumidores se comportavam na política. Uma das conclusões foi que os voláteis manifestaram comportamentos similares aos eleitores indecisos. Uma vez que a equipe de análise de dados entendeu a correlação e o que era necessário para que mudassem de comportamento, trabalhou em campanhas eleitorais específicas para cada grupos. O que se apresenta neste trabalho como publicidade comportamental. O’NEIL, Cathy. *Op. cit.*, p. 293-295.

¹⁶³ ORTIZ, Elaine; SILVEIRA, Sergio Amadeu da, Redes sociais, censura privada e modulação, *in: Ciberpolítica, ciberativismo e cibercultura*, Águas de Lindóia - SP: Anais do 37º Encontro Anual da Anpocs, 2013. p. 9-10.

¹⁶⁴ SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. *Op. cit.*, p. 160-161.

O exame de cada informação (endereços, trabalhos, remunerações, atividades diárias, condições de saúde e financeira) criam uma narrativa sobre o passado da pessoa e a perspectiva de futuro. O relatório do FTC não indica que estes dados estejam sendo utilizados para fins discriminatórios, entretanto o perfilamento do usuário inevitavelmente gera modelo de tratamento distinto, igualando todos que se encaixam nestas cestas. Isso sugere que tenham as mesmas facilidades e barreiras por conta de suas singularidades.

Mattiuzzo faz um contraponto quanto a coleta de dados individuais pelas empresas e a obrigatoriedade de transparência destes processos. Para a autora, supondo que tal processo fosse realizado corretamente, ou seja, segundo a legislação em vigor e que o resultado atingisse a expectativa do titular, a exigência de transparência da decisão algorítmica poderia ser negativa se, e somente se, esta falta de transparência não violasse outros direitos individuais.

Se um motor de busca criar um perfil para acompanhar o meu comportamento e direcionar anúncios para mim, e por qualquer razão os seus algoritmos chegarem à conclusão que gosto de passar as minhas férias na praia, desde que o único resultado seja um aumento do número de anúncios de viagens ao Rio de Janeiro no meu navegador, em vez de anúncios de viagens a Campos do Jordão, é muito difícil sustentar que um direito foi violado...O cenário poderia ser diferente, no entanto, se o anúncio em questão estivesse relacionado com oportunidades de emprego. Devido à relevância do assunto anunciado, os erros no algoritmo são mais susceptíveis de implicar violações de direitos, caso em que a transparência e a explicabilidade tornam-se cruciais para avaliar se o processo de tomada de decisão é legal. (tradução livre).¹⁶⁵

Em conclusão, para Mattiuzzo a compreensão de quão transparente deve ser a decisão algorítmica está relacionada ao impacto em potencial aos titulares dos dados. O funcionamento interno do sistema será necessário sempre que estiver em jogo direitos fundamentais, pelo risco de enviesamentos e desigualdades.

Tal posição desconsidera que a falta de transparência não se relaciona somente com o perfilamento do usuário, mas com o controle e condicionamento do cidadão, conforme visão de Rodotà. No exemplo do anúncio de viagem, o risco não

¹⁶⁵ "If a search engine creates a profile to track my behavior and direct advertisements to me, and for whatever reason its algorithms come to the conclusion I enjoy spending my holidays at the beach, as long as the only outcome is an increased number of advertisements for trips to Rio de Janeiro showing up on my browser, rather than ads for trips to Campos do Jordão, it is very hard to sustain a right was violated...The scenario could be different, however, if the advertisement in question related to job opportunities. Due to the relevance of the matter advertised – employment –, mistakes in the algorithm are more likely to entail rights violations, in which case transparency and explainability become crucial to assess if the decision making process is lawful." MATTIUZZO, "Let the algorithm decide": is human dignity at stake? *Op. cit.*, p. 359-360.

seria a indicação de um local indesejado, mas o sugestionamento de que o Rio de Janeiro é o melhor lugar para viajar. Ademais, determinar quais decisões algorítmicas podem violar direitos e quais não são relevantes não é uma tarefa elementar.

Não sendo o objetivo da pesquisa detalhar técnicas de rastreamento de dados, cumpre importância a apresentação, ainda que superficial, de uma delas, o *fingerprinting*. Essa técnica, mais invasiva que os mais conhecidos *cookies*¹⁶⁶, criam uma identidade digital, ou uma impressão digital única (sem o conhecimento do usuário) com base nos programas, extensões e características do computador utilizado.¹⁶⁷ Essa impressão digital única possibilita a identificação do usuário na internet e, novamente, abre espaço para a publicidade comportamental.

Estes bancos de impressões digitais são controlados por agente econômicos que, devido à capacidade de armazenamento, intensificam a possibilidade de violação de direitos de personalidade e privacidade, segundo Gilmar Mendes. A isonomia é colocada em risco nos casos de estereotipação de grupos sociais.¹⁶⁸ Esta é uma das razões pelas quais se discutem a ampliação do âmbito de aplicação das legislações de proteção de dados.

Outra discussão que ganha espaço é a commodificação dos dados (utilizando a expressão de Rodotà), ou seja, o tratamento dos dados como direito de propriedade.¹⁶⁹ Para o jurista italiano, a publicidade comportamental transformou os dados pessoais em um novo bem jurídico, dotado de valor patrimonial.¹⁷⁰ Para Bioni, nesta lógica o consumidor torna-se produto comercializável.

No modelo de negócio tradicional, consumidores trocam uma quantia pecuniária por um bem de consumo... Trata-se de uma relação bilateral entre consumidor e fornecedor, cuja transação econômica é aperfeiçoada por uma transferência pecuniária... Sob o novo modelo, consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca

¹⁶⁶ Pequenos trechos de texto usados para armazenar informações em navegadores da web. Os cookies são usados para armazenar e receber identificadores e outras informações em computadores, smartphones e outros dispositivos. Meta, **Central de Privacidade**, 2023. Disponível em: <https://www.facebook.com/policies/cookies/>. Acesso em: 25. jun. 2022.

¹⁶⁷ Mozilla Firefox. **O que é rastreamento de identidade digital?** 2023. Disponível em: <https://www.mozilla.org/pt-BR/firefox/features/block-fingerprinting/>. Acesso em: 25. jun. 2022.

¹⁶⁸ MENDES; FERNANDES, **Constitucionalismo Digital**... *Op. cit.*, p. 7.

¹⁶⁹ Em 2020, o empresário e candidato presidencial de 2020, Andrew Yang, prometeu governar os dados como um direito de propriedade, afirmando que pagaria aos indivíduos comuns por serem rastreados e vigiados. HONG, *Op. cit.*

¹⁷⁰ MAIA, Roberta Mauro Medina, A titularidade de dados pessoais previstas no art. 17 da LGPD: direito real ou pessoal?, in: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 143.

de publicidade direcionada. São os anunciantes de conteúdo publicitário que realizam o arranjo econômico. Desta forma, tal relação torna-se plurilateral, uma vez que envolve, necessariamente, os anunciantes para haver retorno financeiro.¹⁷¹

Não significa, todavia, que Rodotà concorde com essa “patrimonialização” dos dados. A opinião do autor, da qual o presente estudo se alinha, é que o direito à proteção de dados tem mais a ver com a personalidade do que com a propriedade e, portanto, se enquadra como um direito pessoal e não patrimonial, inalienável e intransferível.¹⁷²

Esta convergência da privacidade com um direito pessoal é marcada desde o artigo jurídico escrito em 1890, por Warren e Brandeis. Neste, os autores escreveram que “o princípio que protege os escritos pessoais e todas outras produções pessoais, não contra roubo, mas contra a publicação sob qualquer forma, não é na realidade o princípio da propriedade privada, mas o de uma personalidade inviolável”.¹⁷³

Hoffmann-Riem, apesar de ressaltar, em nota de rodapé, que seu estudo não aborda a questão se há um direito exclusivo comparável ou idêntico ao da propriedade, propõe que “do ponto de vista da política legal, seria justificável, se não necessário, obrigar os provedores a pagar aos usuários uma taxa justa se consentirem na coleta e no uso de dados que são particularmente valiosos para o processamento”.¹⁷⁴ Para o autor faria sentido que só fossem comercializados dados pessoais entre seus titulares e empresas privadas.

Considerar válida estas transações, seria reforçar o poder de vigilância, modulação e controle dos grandes *players* do mercado, por conta da evidente diferença econômica entre estas empresas e as pessoas singulares. Tratar a informação com um bem jurídico negociável, portanto, não afigura ser a solução correta para o uso indevido e irrestrito de dados pessoais. Tais situações não se limitariam a vetores patrimoniais, mas, como trabalhado, afrontariam direitos de personalidade e liberdades individuais.

¹⁷¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 22.

¹⁷² RODOTÀ, **A vida na sociedade da vigilância - a privacidade hoje**. *Op. cit.*, p. 19.

¹⁷³ “*The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality*”. WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**, *Op. cit.*, p. 205.

¹⁷⁴ HOFFMANN-RIEM, Wolfgang, **BIG DATA E INTELIGÊNCIA ARTIFICIAL: DESAFIOS PARA O DIREITO**, Revista Estudos Institucionais, v. 6, n. 2, 2020. p. 471.

Doneda é outro autor que compartilha a visão prejudicial de considerar dados pessoais como direito de propriedade. Estes interesses que não se limitam a vetores patrimoniais seriam prejudicados sob a ótica de seu valor econômico.¹⁷⁵ Assim como a vida e o corpo constituem um estado natural e não podem ser comercializados, a personalidade se comporta da mesma forma, em um domínio distinto do direito à propriedade. Não se renuncia e não se aliena a personalidade.

Além da indisponibilidade e oponibilidade *erga omnes*, Tepedino considera que, como direito subjetivo privado, a personalidade possui generalidade, extrapatrimonialidade e imprescritibilidade. Generalidade, pois são concedidos a todos, indiscriminadamente; extrapatrimonialidade, pois ainda que sua lesão gere danos passíveis de ressarcimento, não podem ser calculados economicamente e imprescritibilidade, pois não perecem com o tempo.¹⁷⁶ Desta forma, em síntese, “A mercantilização dos dados pessoais acarreta a perda da importância de sua dimensão política como instância de proteção da liberdade no espaço público. Relativiza-se, com isso, também a inviolabilidade da intimidade e da vida privada”.¹⁷⁷

A discussão, sobre a “comodificação” ou patrimonialização dos dados pessoais, ganha espaço então a partir de *zero-price advertisement business model*¹⁷⁸, baseados na publicidade de preço zero, onde são os consumidores que pagam, com sua atenção ou com suas informações, pelos conteúdos e serviços que recebem. Neste modelo, em que as preferências do público pelo conteúdo preveem o seu interesse em determinados produtos, a contraprestação é incerta e não fixada pecuniariamente. Diferente das operações econômicas tradicionais, o consumidor não

¹⁷⁵ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 150.

¹⁷⁶ TEPEDINO, **A tutela da personalidade...** *Op. cit.*, p. 10.

¹⁷⁷ CORRÊA; GEDIEL, **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado**. *Op. cit.*, p. 149.

¹⁷⁸ “The story often told about zero-price advertising-based business models (in the online or offline world) is that consumers “pay” something other than money for the content or services they receive. So, for example, the traditional broadcast advertising-based approach is sometimes modeled as one in which consumers pay for television or radio content with “attention” to advertising. The assumption underlying such models is that content recipients experience some disutility from being subjected to broadcast advertising but are willing to incur that cost because it is outweighed by the expected benefit of the programming itself”. STRANDBURG, Katherine J., **Free Fall: The Online Market's Consumer Preference Disconnect** (October 1, 2013). 2013 University of Chicago Legal Forum 95, NYU School of Law, Public Law Research Paper N°. 13-62, NYU Law and Economics Research Paper N°. 13-34. Disponível em: SSRN: <https://ssrn.com/abstract=2323961>. Acesso em: 21 mar. 2022. p. 107.

sabe qual o custo da transação, e nem tampouco como a disponibilização de seus dados poderá lhe afetar.¹⁷⁹

“O *zero-price advertisement business model* consiste, portanto, em um novo modelo de negócios, que esconde uma série de sujeitos para sua operacionalização”.¹⁸⁰ Os *data brokers* são exemplos de atores que, operando nesta entrega direcionada, impedem a identificação pelos titulares dos dados. Para o consumidor mais esclarecido, a percepção de que o produto oferecido consiste em alguma preferência exposta. Para os mais ineptos, a publicidade direcionada chega como uma capacidade de previsão. Para ambos, o caminho é desconhecido. “Como resultado, há um fluxo informacional abundante e difícil de mapear todos os atores neles envolvidos, o que é desafiador para qualquer perspectiva regulatória”.¹⁸¹

Esta entrega da preferência do consumidor pelo uso do bem ou produto é o *trade-off* entre progresso tecnológico e privacidade citado no primeiro capítulo. Entretanto, Frazão adverte que, “direitos fundamentais não podem estar sujeitos, exclusivamente, a juízos de custo-benefício, uma vez que são deontológicos e vinculantes”.¹⁸² As relações no ambiente digital devem preservar a condição existencial de seus titulares. O preço não é zero e a troca entre eficiência e privacidade não é justa.

Assegurar a proteção de dados é também assegurar contra as consequências de uso destes dados por outros. É proteger não somente a coleta, como a sua manipulação. É ainda diminuir as assimetrias de poder nas relações privadas e mitigar os riscos de modelos supostamente gratuitos. Na sociedade dos dados, chamada de sociedade de vigilância por Rodotà, é salvaguardar a individualidade das pessoas e como estas se apresentam.

Pela pressão que a proteção dos dados pessoais sofre dos dois vetores principais: do Estado — para aumentar a quantidade e qualidade de dados dos cidadãos, e do mercado — tendo em vista o valor econômico¹⁸³, o direito à proteção de dados não poderia deixar de fazer parte do catálogo de direitos fundamentais.

¹⁷⁹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 24.

¹⁸⁰ *Ibid.*, p. 29.

¹⁸¹ *Ibid.*

¹⁸² FRAZÃO, Ana. **Objetivos e alcance da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 110-111.

¹⁸³ CORRÊA; GEDIEL, **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado**. *Op. cit.*, p. 145.

2.2 DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

A Constituição Federal Brasileira assegurou em 2022 o direito fundamental à proteção dos dados pessoais, em um inciso distinto da já protegida intimidade e vida privada. Apesar da privacidade servir de elo entre estes direitos, a distinção não é um acaso. A tutela da intimidade e vida privada exterioriza-se essencialmente de forma individual, estática e negativa, prevalecendo o dever de abstenção. Ao contrário, a proteção de dados é dinâmica e, além da abstenção de tratamento em algumas hipóteses, segue os dados em sua circulação.¹⁸⁴

Proteção de dados que alcança condição de direito fundamental autônomo pela primeira vez na Carta de Direitos Fundamentais de União Europeia (CDFUE) no ano 2000.¹⁸⁵ Carta esta que reúne direitos que estavam distribuídos em legislações dispersas dos países membros da União Europeia - UE. Razão pela qual o direito fundamental à proteção de dados, vinculou somente estados integrantes da UE. Na CDFUE, o direito à proteção de dados é estabelecido em seu art. 8º que define como hipóteses de tratamento, o consentimento da pessoa interessada ou outro fundamento legítimo previsto por lei, sujeito a fiscalização por parte de uma autoridade independente.¹⁸⁶

Assim como o respeito a vida privada e familiar, liberdades de expressão e informação, o direito à proteção de dados, na CDFUE está contido no título II, Liberdades. Como cerne da democracia, a proteção de dados tornou-se condição preventiva para gozos de outras liberdades fundamentais.¹⁸⁷

No plano internacional, o respeito a estas liberdades são, acima de tudo, direitos humanos, como na Declaração Universal dos Direitos Humanos de 1948¹⁸⁸. De todo modo, “o direito à proteção de dados pessoais é, simultaneamente, um direito humano e um direito fundamental, o que, calha enfatizar, não afasta situações de tensão e

¹⁸⁴ RODOTÀ, **A vida na sociedade da vigilância - a privacidade hoje**. *Op. cit.*, p. 8.

¹⁸⁵ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 21-24.

¹⁸⁶ UNIÃO EUROPEIA, **Carta dos Direitos Fundamentais da União Europeia**, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 02 jul. 2022.

¹⁸⁷ RODOTÀ, **Democracia y protección de datos**. *Op. cit.*, p. 18-20.

¹⁸⁸ NAÇÕES UNIDAS. Assembleia Geral. **Declaração universal dos direitos humanos**. Rio de Janeiro: UNIC, 2009. Publicado originalmente em 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 7 jul. 2022.

conflitos normativos, de diversa natureza”¹⁸⁹, por mais que inexista expressamente um direito humano no sistema internacional das Organizações das Nações Unidas - ONU.

Embora não haja dissenso sobre tal terminologia, ainda de tangenciando o tema, expressões como “direitos fundamentais” e “direitos humanos” tem naturezas distintas, em que pese a utilização como sinônimos seja corriqueira. José Carlos Vieira de Andrade explica que os direitos fundamentais se aplicam na esfera do direito constitucional positivo de um Estado, enquanto os direitos humanos, ou como o autor denomina, “direitos fundamentais internacionais”, são aqueles reconhecidos no âmbito do sistema internacional, independentemente de sua vinculação com determinada ordem constitucional.¹⁹⁰

No Brasil, a construção do direito fundamental à proteção de dados, que culmina com a inclusão no rol de direitos fundamentais da Constituição Federal, não surge repentinamente. Como é comum entre os direitos fundamentais, é um processo. Processo este que, até chegar na sanção da lei específica, Lei 13.709/2018 - LGPD, encontrava disposições dispersas sobre acesso e proteção de dados na Lei do *Habeas Data*, como Código Civil, no Marco Civil da Internet, na Lei de Acesso à Informação, entre outros.

O primeiro movimento legislativo brasileiro sobre a matéria foi o projeto de Lei n.º 2.796/1970, de autoria da deputada Cristina Tavares, do PMDB, que assegurava aos cidadãos acesso às informações constantes em bancos de dados.¹⁹¹ O projeto, apesar de arquivado, foi importante por resultar, no processo de redemocratização e na presença da ação de *habeas data* na Constituição Federal de 1988.¹⁹² Além de assegurar o conhecimento de informações relativas à pessoa, a ação constitucional de *habeas data* permite a retificação destes dados.

Regulamentada pela Lei n.º 9.507/1997, concedeu-se o manejo da ação constitucional de *habeas data*. No entanto, não conseguiu enfrentar os desafios proporcionados pelo crescimento do tratamento de dados, que ganhou volume com a

¹⁸⁹ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 25.

¹⁹⁰ ANDRADE, José Carlos Vieira de. **Os direitos fundamentais na Constituição Portuguesa de 1976**, 5ª. ed. Almedina: Coimbra, 2012, p. 24-35.

¹⁹¹ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.796, de 4 de novembro de 1980**. Assegura aos cidadãos acesso às informações sobre sua pessoa constantes de bancos de dados e dá outras providências. Brasília: Câmara dos Deputados, 1980. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 7 jul. 2022.

¹⁹² DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais, in: Danilo Doneda ... [et al.]. **Tratado de Proteção de Dados Pessoais**, Editora Forense Ltda. Rio de Janeiro - RJ, 2021. p. 10-15.

evolução tecnológica das décadas seguintes. Apesar de prosperar, o *habeas data* não chegou a identificar um direito à proteção de dados pessoais.¹⁹³

Tal visão é reforçada pelo fato de o *habeas data* ter assumido forma de ação constitucional e não de direito material. Esta opção por não detalhar seu conteúdo material foi baseada na suposição de que os interesses dos particulares pudessem se restringir a simples identificação e retificação de dados, não havendo nenhuma restrição contra a coleta e utilização destes dados. Na análise deste instituto, Doneda faz referência ao Ministro Luís Roberto Barroso, para quem a ação constitucional de *habeas data* chega a possuir uma função simbólica, cuja importância dogmática supera a própria efetividade do instituto.¹⁹⁴

Por mais que o Código Civil de 2002 tenha reforçado a exigência de cessar a ameaça ao direito à personalidade (art. 12º) e a inviolabilidade da vida privada da pessoa natural (art. 21º), foi somente em 2011, com a Lei 12.414/2011 — Lei do Cadastro Positivo¹⁹⁵ — que conceitos de proteção de dados são retomados na esfera federal. Seu objetivo era disciplinar a formação e consulta de banco de dados para formação de histórico de crédito, permitindo ao mercado a identificação de bons pagadores. Em tese, esta identificação propiciaria redução das taxas de juros e proteção ao crédito.

A Lei do Cadastro Positivo trouxe princípios importantes que vieram a se consolidar mais tarde na LGPD. Dentre eles, o princípio da qualidade de dados e o princípio da necessidade (art. 3º, § 1º), ao permitir somente armazenamento de informações objetivas, claras, verdadeiras e de fácil compreensão, assim como necessárias para avaliar a situação econômica do cadastrado.

Também foi a primeira a trazer o princípio da finalidade e o da não discriminação (art. 3º, § 3º). Quanto ao primeiro, ao proibir informações excessivas, limitou a coleta à análise de risco de crédito do cadastrado¹⁹⁶. Quanto a não discriminação, proibiu manejo de informações sensíveis, ou seja, que se relacionam

¹⁹³ *Ibid.*

¹⁹⁴ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 282-300.

¹⁹⁵ BRASIL. **Lei nº 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplimento, 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: 2 jun. 2022.

¹⁹⁶ OLIVEIRA; LOPES, **Os princípios norteadores da proteção de dados...**, *Op. cit.*, p. 69.

com à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Diferente da Lei do *Habeas Data*, que assumiu caráter processual, a Lei do Cadastro Positivo incluiu direitos materiais ao titular, como a possibilidade de cancelamento de cadastro (art. 5º, I) e o direito de não ter seus dados utilizados para finalidades diversas da qual foi coletada (art. 5º, VII), além dos já existentes direitos de informação e retificação de informações. Ao determinar que os gestores de banco de dados disponibilizassem suas políticas de coleta e utilização de dados (art. 7-A, § 1º), ratificou o princípio da transparência, estabelecendo inclusive que tais políticas fossem objeto de verificação. Entretanto, por conta da utilização aquém da esperada e da restrição de coleta para análise e formação de histórico de crédito, sua presença na jurisprudência não foi determinante.¹⁹⁷

Ainda em 2011 outro marco importante para o controle e acesso de informações foi a Lei 12.527/2011 – Lei de Acesso à informação (LAI). Ao dispor sobre procedimentos a serem observados pelo poder público (União, Estados, Distrito Federal e Municípios), regulamenta o direito de todos em receber informações de órgãos públicos de interesse particular, coletivo ou geral.¹⁹⁸ Nos mesmos moldes de atual LGPD, a LAI define informação pessoal como aquela relacionada à pessoa natural identificada ou identificável (art. 4º IV). É ainda extensiva quanto ao rol de ações que configuram tratamento de informação, como coleta, utilização e controle da informação. (art. 4º V).

Ao mesmo tempo que objetiva a transparência dos dados, a LAI não deixa de observar, como fator essencial para sua legitimação, que tal tratamento deva ser feito com respeito a intimidade, vida privada e demais liberdades e garantias fundamentais¹⁹⁹, assegurando a informação autêntica a íntegra²⁰⁰.

Trouxe ainda a previsão legal do consentimento expresso, diferentemente da Lei do Cadastro Positivo que teve removido o dispositivo que exigia o consentimento informado para abertura de cadastro. A remoção da exigência se deu mediante

¹⁹⁷ DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais**. *Op. cit.*, p. 15.

¹⁹⁸ 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 § 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: 4 jul. 2022.

¹⁹⁹ *Ibid.*, Art. 31º.

²⁰⁰ *Ibid.*, Art. 6º.

entendimento de que o STJ já havia publicada a Súmula 550, dispensando o consentimento para utilização de escore de crédito.²⁰¹

Uma das mais importantes normas prévias a LGPD em relação à proteção de dados e mais especificamente na regulamentação do uso da internet é a Lei 12.965/2014, conhecida como Marco Civil da Internet (MCI).²⁰² Estabelece um regime de direitos para os usuários da internet e se alicerça sobre o tripé axiológico da neutralidade, privacidade e liberdade de expressão.²⁰³

Ao mesmo tempo que reconhece a essencialidade da internet para o pleno exercício da cidadania, procura garantir à privacidade dos usuários. Objetiva assegurar a inviolabilidade da intimidade e da vida privada; o sigilo de comunicações na internet; o não fornecimento a terceiros de dados pessoais, salvo mediante consentimento livre, expresso e informado. Com base nestes direitos, a privacidade no MCI, mais do que um princípio enunciativo, passa a ser uma garantia estruturante.²⁰⁴

O MCI inova ao procurar regulamentar a atuação de intermediários quanto ao tratamento de dados pessoais. Longhi destaca o art. 11, que traz a obrigatoriedade dos provedores de localizarem pelo menos um de seus terminais em território brasileiro.²⁰⁵ Por mais legítimos que sejam estes limites e obrigações, a ubiquidade da internet e a possibilidade transfronteiriça na hospedagem de dados tornam determinações neste sentido pouco práticas e tampouco garantem a proteção de dados dos cidadãos.

De certo modo, o MCI conferiu grau de importância à privacidade muito superior que em normas passadas, seja com o estabelecimento de direitos e garantias ou até mesmo com um conjunto de sanções administrativas. Entretanto, ainda persistia a

²⁰¹ BRASIL, Superior Tribunal de Justiça. **Súmula 550**. A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. RSSTJ vol. 45 p. 323, out. 2015. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=550&b=SUMU>. Acesso em: 4 jul. 2022.

²⁰² BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 4 jun. 2022.

²⁰³ LONGHI, João Victor Rozatti, Marco Civil da Internet no Brasil: Breves considerações sobre seus fundamentos princípios e análise crítica do regime de responsabilidade civil, *in*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Orgs.), **Direito Digital: direito privado e internet**, 2 ed. Indaiatuba, SP: Editora Foco, 2019, p. 123–133.

²⁰⁴ *Ibid.*

²⁰⁵ *Ibid.*

visão estática da privacidade, pautada pela concepção de vedação de interferência de terceiros.

O direito fundamental à proteção de dados, acima de tudo, abrange a necessidade de conferência de um poder positivo e dinâmico ao titular. Mais do que impedir a invasão da esfera privada, o âmbito de proteção diz respeito a capacidade de reconhecer o direito à autodeterminação informativa. Neste sentido, extrapola a abordagem exclusiva de privacidade. A autodeterminação informativa visa garantir ao titular a escolha da forma de tratamento de seus dados, ao mesmo que fomenta espaço de livre fluxo de dados.²⁰⁶

Reconhecer a centralidade do controle sobre suas próprias informações é ainda mais relevante no cenário de processamento automatizado que, em conjunto com as técnicas de perfilação, representam todos os riscos abordados no primeiro capítulo.

A autodeterminação informativa, portanto, oferece uma versão dinâmica de gestão²⁰⁷ dos próprios dados, conferindo poderes ao titular sobre a circulação destas informações. Apesar das críticas, explica Rodotà, essas definições passam a fazer parte das legislações de proteção de dados e evidenciam a atribuição de um poder autônomo de controle ou o princípio do “*control of information about oneself*”.²⁰⁸

O reconhecimento de um direito a autodeterminação informativa como um fundamento da proteção dados tem sua origem em 1983, quando a Corte Constitucional da Alemanha reconheceu a inconstitucionalidade da Lei do Recenseamento (*Volkszählungsgesetz*).²⁰⁹ Apesar de a decisão não ter reconhecido propriamente um direito fundamental à proteção de dados, o Tribunal Alemão entendeu que a lei que organizava o censo feria o livre desenvolvimento da personalidade. Ainda, ao dar a prerrogativa de cada cidadão livremente decidir sobre

²⁰⁶ DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais**. *Op. cit.*, p. 3–20.

²⁰⁷ O processo de autogestão dos dados pessoais será abordado no quarto capítulo, em análise conjunta da eficácia do consentimento livre, informado e inequívoco.

²⁰⁸ RODOTÀ, **A vida na sociedade da vigilância - a privacidade hoje**. *Op. cit.*, p. 47.

²⁰⁹ Esta lei previa que cada cidadão deveria responder a 160 perguntas, a serem posteriormente submetidas a tratamento informatizado. Dentre os pontos que geraram controvérsias estava: possibilidade de confrontar os dados com o registro civil para retificação do registro; possibilidade que os dados coletados fossem transmitidos às autoridades federais e existência de multa para aqueles que não respondessem o formulário. DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 170.

a divulgação de seus dados, admitiu um direito fundamental implícito à autodeterminação informativa.²¹⁰

Na decisão, que influenciou outras ordens jurídicas, o Tribunal considerou que os avanços tecnológicos permitiriam (já em 1983) o processamento de dados em massa, ameaçando outros direitos fundamentais, inclusive relacionados com a própria dignidade humana. A forma proposta pela Lei do Recenseamento inviabilizaria que o titular pudesse controlar, além do uso, a exatidão dos dados.²¹¹

Principalmente pela possibilidade prevista na Lei do Recenseamento, de que estes dados fossem transmitidos às autoridades federais, tal utilização ampliaria de forma desproporcional a capacidade do Estado em controlar o comportamento daquela população. “Uma sociedade, na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação, seria contrária ao direito à autodeterminação informativa”.²¹² Mais do que ferir o direito individual à personalidade, permitir tal conduta é contrária ao que se espera de uma sociedade democrática.

Conforme o conceito de *control creep*²¹³ e sua associação com a utilização de dados para finalidades distintas do esperado pelos seus titulares no momento da captura, um dado que a princípio não apresenta importância, combinado com outros dados, podem adquirir um novo e desconhecido valor. A sentença da Corte Alemã, desmistifica a ideia de que alguns dados pessoais não são relevantes e, portanto, não carecem de proteção.²¹⁴

Nesta conjuntura, Laura Mendes considera que, “decisivo para a concepção do direito à autodeterminação informativa é o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados”.²¹⁵ A própria inobservância da finalidade da coleta já apresenta riscos ao cidadão.

²¹⁰ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 30-31.

²¹¹ DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais.** *Op. cit.*, p. 9.

²¹² MENDES, **Autodeterminação informativa: a história de um conceito.** *Op. cit.*, p. 11.

²¹³ Conceito trabalhado no capítulo 1.1. Como outro exemplo, atualmente, o número do telefone é utilizado como chave de identificação no sistema de pagamento PIX. O e-mail é utilizado como chave de identificação em inúmeras plataformas eletrônicas.

²¹⁴ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados.** *Op. cit.*, p. 172

²¹⁵ MENDES, **Autodeterminação informativa: a história de um conceito.** *Op. cit.*, p. 11.

Autodeterminar o fluxo dos dados, impedindo a ingerência ou controle externo é um desafio, principalmente quando a tecnologia torna quase incontável esse domínio. Se os dados pessoais são utilizados para fins diversos dos quais foram coletados, se o cidadão não dispõe de informações sobre quais dados estão em circulação, a “autodeterminação informativa envolve não apenas controlar as informações a que se franqueia acesso a terceiros, mas também a quais informações se deseja ter acesso”.²¹⁶

Assim como a decisão alemã de 1983, a atual interpretação do direito a autodeterminação informativa comporta uma dupla dimensão (individual e coletiva). Apesar do nome sugestivo, o objeto do direito não corresponde somente ao poder de cada indivíduo em decidir sobre acesso e difusão de suas informações, mas constitui uma condição para uma sociedade democrática. Ingo Sarlet coloca a proteção de dados como um direito distante da privacidade isolacionista, entendendo que a atual concepção é espinha dorsal de uma democracia liberal.²¹⁷

Também comporta uma dupla dimensão subjetiva e objetiva. Subjetiva, se desdobrando em uma oponibilidade em face ao Estado, ou seja, um direito em sentido amplo de natureza defensiva ou negativa. Objetiva, pois, estabelecer um dever de atuação do Estado, mediante prestações de natureza fática ou normativa, que garantam o exercício e a fruição deste direito ao titular.²¹⁸

No Brasil, muito antes da sanção da LGPD, o direito à autodeterminação informativa já havia sido compreendido como uma preocupação do Estado, dada crescente vulnerabilidade do cidadão frente a coleta e armazenamento de dados por tempo indeterminado.²¹⁹ No julgamento do REsp. 22.337-8-RS, o Ministro Ruy Rosado de Aguiar (citando o reconhecimento da autodeterminação informativa como uma garantia fundamental no ordenamento alemão) considerou que o cidadão, objeto da

²¹⁶ KONDER, Carlos Nelson; KONDER, Cíntia Muniz de Souza, Transumanismo e inteligência artificial, *in*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (Orgs.), **O Direito Civil na era da inteligência artificial**, São Paulo: Thomson Reuters Brasil, 2020, p. 103–120.

²¹⁷ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 32.

²¹⁸ MENDES, Laura Schertel; JUNIOR, Otavio Luiz Rodrigues; FONSECA, Gabriel Campos Soares da, O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: Rumo a um Direito Fundamental Autônomo, *in*: DONEDA, Danilo *et al* (Orgs.), **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 68–71.

²¹⁹ CUEVA, Ricardo Villas Bôas, A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça, *in*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**, 1 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 88.

indiscriminada colheita de informações, deve dispor de meios eficazes para ter acesso a esta informação, retificá-la ou cancelá-la.²²⁰

2.2.1 – Inclusão da proteção de dados como direito fundamental na Constituição Federal de 1988.

A proteção de dados no ordenamento constitucional brasileiro surge pelo reconhecimento de que a tutela da privacidade, de forma negativa, não era mais suficientemente adequada em razão da amplitude que os dados tomaram na sociedade.

Em maio de 2020, o reconhecimento da natureza autônoma do direito à proteção de dados surge com a medida cautelar em Ação Direita de Inconstitucionalidade – ADI 6387, de relatoria da Ministra Rosa Weber. A decisão suspendeu a Medida Provisória 954/2020, que dispunha sobre o compartilhamento de dados de empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística – IBGE, para fins de estatística durante a pandemia da COVID-19.

Nesse contexto, e a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, defiro a medida cautelar requerida, *ad referendum* do Plenário desta Suprema Corte, para suspender a eficácia da Medida Provisória n. 954/2020, determinando, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia.²²¹

A Ministra ratificou a necessidade de tutela de um direito fundamental à proteção de dados a teor do art. 5º, XII, da CF. Apontou ainda para a existência, no desenho constitucional brasileiro, de um direito fundamental autônomo à proteção de dados, na concepção de um direito à autodeterminação informativa, que decorre do direito da personalidade e do respeito à privacidade, positivados na LGPD, art. 2º, como fundamentos da disciplina da proteção de dados.

²²⁰ BRASIL, Superior Tribunal de Justiça. **REsp. 22.337 / RS**. RSTJ vol. 77 p. 205, mar. 1995. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=22337&b=ACOR>. Acesso em: 7 jul. 2022.

²²¹ BRASIL, Supremo Tribunal Federal. **ADI nº 6.387/DF**. Relator: Ministra Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 8 jul. 2022.

Em seu voto, apontou em síntese que, o compartilhamento de dados produção para estatística oficial, viola dados sigiloso, inclusive telefônicos; que não existiria uma descrição mínima dos procedimentos e finalidades específicas da coleta; que o modo genérico e impreciso comprometeria o exame de proporcionalidade da norma; que não apontava as razões justificadoras da urgência e relevância da medida; e que a ausência de regulação de mecanismos de segurança do IBGE não protegiam as informações dos cidadãos, quanto a eventuais vazamentos ou uso indevidos.²²²

A liminar foi referendada pelo Tribunal Pleno, que destacou ainda que, na proteção constitucional de dados pessoais não existem dados neutros ou insignificantes, refutando o discurso de que dados como nome, endereço e número de telefones poderiam ser compartilhados.²²³

Até mesmo antes da Ação Direta de Inconstitucionalidade – ADI 6.387, o direito fundamental à proteção de dados, como decorrência ou derivação do direito à privacidade, apontava para a admissão de um direito fundamental implícito à proteção de dados. Ingo Sarlet explica que existem direitos fundamentais positivados fora do catálogo, mas também, direitos não positivados, conquanto deduzidos, na condição de direitos implícitos. No sentido etimológico, como um direito subentendido, verifica-se que “a categoria dos direitos implícitos pode corresponder também – além da possibilidade de dedução de um novo direito fundamental com base nos constantes do catálogo – a uma extensão (mediante o recurso à hermenêutica) do âmbito de proteção”.²²⁴

Mas a relevância da matéria conduziu para que, em 2022, ocorresse a promulgação da Emenda Constitucional – EC n.º 115/2022.²²⁵ Ao incluir a proteção de dados no catálogo de garantias e direitos fundamentais, art. 5º, LXXIX, CF, adicionou valor substancial à proteção de dados no Brasil. A EC n.º 115/2022 incluiu ainda a competência dada União em fiscalizar a proteção e tratamento dos dados pessoais

²²² MENDES; JUNIOR; FONSECA, **O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: Rumo a um Direito Fundamental Autônomo**. *Op. cit.*, p. 62-63.

²²³ *Ibid.*

²²⁴ SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais...** *Op. cit.*, p. 69.

²²⁵ BRASIL. Constituição (1988). **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. Brasília, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 jul. 2022.

(art. 21, XXVI, CF) e a competência privativa para legislar sobre proteção e tratamento de dados art. 22, XXX, CF).

Mesmo que já se pudesse reconhecer o direito à proteção de dados, seja como um direito fundamental implícito, seja pela interpretação do STF, fato é que sua positivação formal carrega uma carga valorativa adicional, principalmente pelo estabelecimento de parâmetros mais concretos e mais seguros, devido aos direitos fundamentais possuírem status normativo superior em relação ao restante do ordenamento.²²⁶

Nesta condição, ao menos duas consequências diretas são percebidas. Primeiramente que o direito fundamental à proteção de dados tem aplicabilidade imediata. Segundo que, de acordo com o art. 60, § 4º, IV da CF, os direitos e garantias individuais não podem ser objetos de deliberação de propostas de emenda que tendam a eliminá-los. Tal robustez de proteção e delimitação de limites de reforma formal e material reforçam a assimilação da proteção de dados com elemento básico de uma sociedade democrática.²²⁷

²²⁶ Dentre as razões para a carga positiva adicional que a efetivação do direito fundamental à proteção de dados traz, Ingo Sarlet aponta: “fica assegurada à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio; ao direito à proteção de dados passa a ser atribuído de modo inquestionável o pleno regime jurídico-constitucional relativo ao seu perfil de direito fundamental em sentido material e formal já consagradas no texto da CF, bem como na doutrina e na jurisprudência constitucional brasileira. 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**, Direitos Fundamentais & Justiça, v. n. 42, 2020. p. 186.

²²⁷ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 38.

3. TRATAMENTO DE DADOS NA LEI GERAL DE PROTEÇÃO DADOS

Ao mesmo tempo em que se observou o crescimento de processos de automação e desenvolvimento tecnológico na Europa na metade do século XX, surgiram problemas relacionados à regulação dos dados e consequentemente à privacidade, emergindo a necessidade de instrumentos regulatórios e jurídicos para proteção de liberdades individuais.

O primeiro modelo normativo autônomo de proteção de dados surgiu na Alemanha, no estado de Hesse em 1970.²²⁸ Muito embora, em linhas iniciais, o direito à proteção de dados já pudesse ser extraído da Declaração Universal dos Direitos Humanos de 1948²²⁹, a Lei de Proteção de Dados de Hesse (*Hessisches Datenschutzgesetz*), foi a primeira lei específica a tratar da matéria. Foi a pioneira na proibição de recolhimento, armazenamento e utilização de dados pessoais, na limitação da coleta pelo princípio da finalidade, no estabelecimento do princípio da minimização de dados e da necessidade.

Em 1980, o Conselho da Organização para a Cooperação e Desenvolvimento Econômico – OCDE desenvolveu diretrizes com objetivo de harmonizar as legislações sobre privacidade e, ao mesmo tempo proteger direitos humanos, sem, contudo, interromper ou prejudicar o livre fluxo de dados pessoais. O conselho considerou que algumas restrições poderiam causar sérias perturbações em setores importantes da economia, como bancos e seguros.²³⁰

Ponto fundamental das diretrizes foi a introdução de princípios básicos para aplicação nacional nos instrumentos jurídicos de proteção de dados. Dentre os quais: o princípio da limitação da coleta; o princípio de qualidade de dados; o princípio da

²²⁸ Rede latino-americana de estudos sobre vigilância, tecnologia e sociedade – lavits. **Histórico pelo mundo**. Disponível em: <http://dadospessoais.lavits.org/historico-pelo-mundo/>. Acesso em: 21 jul. 2022;

²²⁹ Artigo 12 - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. NAÇÕES UNIDAS. Assembleia Geral. **Declaração universal dos direitos humanos**. *Op. cit.*

²³⁰ O conselho recomendou que os países membros considerem em suas legislações locais princípios relativos à proteção da privacidade e das liberdades individuais, mas que removam ou evitem criar, em nome da privacidade, obstáculos injustificados aos fluxos de transferências internacionais de dados. OECD - Organisation for Economic Co-operation and Development. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 21 jul. 2022.

necessidade; o princípio da segurança dos dados; o princípio da transparência; o princípio do acesso individual; e o princípio da responsabilidade.²³¹

No ano seguinte, em 1981, o Conselho da Europa publicou a Convenção para a Proteção de Indivíduos em relação ao Processamento Automático de Dados Pessoais (ETS N.º 108).²³² A convenção, além de proteger o indivíduo contra abuso do tratamento de dados pessoais, proíbe o processamento de dados sensíveis (resguardados interesses superiores como segurança do Estado) e consagra o direito de acesso, o direito de retificação e o direito de oposição em relação a informações pessoais armazenadas em bancos de dados. O comitê responsável pela convenção 108, em seu relatório explicativo, deixou claro a estreita colaboração com as atividades da OCDE.²³³

Em relação ao seu âmbito de proteção incluiu ainda o tratamento automatizado, tendo em vista o rápido desenvolvimento da tecnologia de processamento de dados. Importante ainda a referência, na convenção 108, ao conceito de dados pessoais sensíveis, como os suscetíveis a revelar opiniões políticas, crenças religiosas, bem como dados pessoais relativos à saúde ou à vida sexual. Outrossim, este catálogo foi ampliado com incorporação de dados genéticos e biométricos. Reforça a convenção que para este conjunto de dados sensíveis, a proteção foi alargada e o tratamento restringido.²³⁴

Destes dois movimentos (OCDE – 1980 e *Council Of Europe* – 1981) verifica-se a passagem da visão enunciação passiva para uma proteção positiva e dinâmica, pautada na constatação da autonomia individual e ligação com princípios fundamentais, independentemente da existência real de uma violação.²³⁵ A “tutela dos dados pessoais continuou centrada no cidadão, porém passou a abranger mais do

²³¹ *Ibid.*

²³² COUNCIL OF EUROPE. European Treaty Series. **Details of Treaty No.108**. Disponível em: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>. Acesso em: 21 jul. 2022.

²³³ “The committee was instructed to do so in close collaboration with the Organisation for Economic Co-operation and Development, as well as the non-European member countries of that organisation, having regard to the activities which OECD was carrying out in the field of information, computer and communications policy. Close liaison was maintained between the two organisations both at the Secretariat level and at the level of the Council of Europe's committee of experts and the corresponding OECD committee, the Data Bank Panel, which was succeeded in 1978 by an expert group on transborder data barriers. The latter group was instructed by the OECD Council to develop privacy protection guidelines, to facilitate harmonisation of national legislations of the OECD member countries, without this precluding at a later date the establishment of an international Convention”. *Ibid.*

²³⁴ *Ibid.*

²³⁵ RODOTÀ, **A vida na sociedade da vigilância - a privacidade hoje**. p. 59-60.

que a liberdade de fornecer ou não os próprios dados pessoais, preocupando-se também em garantir a efetividade desta liberdade”.²³⁶ A proteção de dados, neste período, passa a ser vista também como o exercício individual livre de decidir sobre o fluxo de acesso aos dados pessoais. Visão esta que se situa na concepção atual do efetivo exercício da autodeterminação informativa.

3. 1 REGULAMENTO GERAL SOBRE PROTEÇÃO DE DADOS – RGPD

Em 1995, o Parlamento Europeu promulgou a Diretiva 95/45/CE.²³⁷ Ao estabelecer uma ação comunitária com vistas à aproximação das legislações e a equivalência de tratamento em todos os estados-membros, objetivou promover a igualdade no nível de proteção de dados na União Europeia. A diretiva estabeleceu a criação de um sistema de autoridades centrais responsáveis pela fiscalização, supervisão e controle das questões envolvendo proteção de dados. Estas autoridades de proteção de dados tiveram na diretiva independência no exercício de suas funções.²³⁸

Consolidando a orientação da Convenção 108 de 1981, a Diretiva 95/45/CE incluiu no seu âmbito de proteção os dados tratados por meios parciais e totalmente automatizados. Em relação aos dados automatizados estipulou ainda o direito de acesso à lógica subjacente ao tratamento. Ademais, proibiu os controladores de aplicarem decisões individuais exclusivamente com base num tratamento automatizado, nos casos que tais decisões afetassem aspectos da personalidade.²³⁹

As similitudes com a Convenção 108 também são percebidas na harmonização das hipóteses de tratamento para além do consentimento. Estas hipóteses denotam a dupla função da Diretiva que, se por um lado estabelece restrições a controladores e tutela a autodeterminação informativa, por outro consagra hipóteses de tratamento que independem do consentimento do titular, cuja função é assegurar o

²³⁶ DONEDA, Danilo, **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, v. 12, n. 2, 2011. p. 97

²³⁷ UNIÃO EUROPEIA. EUR-Lex. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 21 jul. 2022.

²³⁸ MACHADO, Diego Carvalho *et al*, **GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis**, Instituto de Referência em Internet e Sociedade, 2018. p. 6.

²³⁹ DONEDA *et al*, **Considerações iniciais sobre inteligência artificial...** *Op. cit.*, p. 2-3.

funcionamento do mercado interno e a integração econômica resultante do estabelecimento do fluxo transfronteiriço de dados. Doneda salienta que esta dupla matiz não é surpresa, em face da exigência do mercado europeu em diminuir custos de transações, especialmente no mercado tão dependente de dados e com empresas estabelecidas em diferentes Estados-membros.²⁴⁰

Fato é que a promulgação da Diretiva 95/45/CE ensejou a normatização da proteção de dados para vários Estados-membros que não possuíam legislações internas específicas. Foi um importante instrumento de proteção de dados tanto para a esfera privada quanto para a pública. A partir dela, se fortalece a necessidade de justificação do tratamento mediante consentimento ou outro fundamento jurídico.²⁴¹ Após 11 anos de vigência é substituída pelo Regulamento n.º 679/2016, que ficou conhecido como Regulamento Geral de Proteção de Dados – RGPD²⁴².

Por ser um regulamento e não uma diretiva, é considerada uma lei interna diretamente aplicável aos Estados-Membros da UE, não sendo necessária a transposição para cada jurisdição nacional. Esse ponto fortalece a unidade de tratamento de dados na UE e evita diferentes níveis de proteção em cada um dos países europeus.²⁴³

Na mesma esteira de proteção de direitos individuais e contraposição a criação de perfilamento de usuários, o RGPD procura estabelecer mecanismos de preservação da autonomia do titular e de autodeterminação informativa, sem deixar de perceber o direito à proteção de dados também como um direito de regulação econômica. Entretanto, é nítido que o regulamento visa compensar desvantagens

²⁴⁰ DONEDA, **A proteção dos dados pessoais como um direito fundamental**. *Op. cit.*, p. 102.

²⁴¹ DÖHMANN, Indra Spiecker Gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia, *in*: DONEDA, Danilo *et al* (Orgs.). **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 97–113.

²⁴² EUROPEAN UNION (EU). **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04>. Acesso em: 22 jul. 2022.

²⁴³ “The main arguments for GDPR’s rationale support the relevance of a legislation capable of addressing the new issues raised by digital economy and the pervasiveness of information and communication technologies in an equal manner between the different countries of the European Union”. MACHADO *et al*, **GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis**. *Op. cit.*, p. 6.

estruturais resultantes da diferença de poder econômico entre titular e controlador de dados.²⁴⁴

O RGPD, ao conceituar dados pessoais, adotou um conteúdo amplo, se referindo a qualquer informação que possa identificar ou tornar identificável a pessoa, direta ou indiretamente. Machado entende que essa abertura conceitual de dado pessoal é uma estratégia legislativa que parte da premissa de que os dados, ainda que anonimizados, podem ser reidentificados. Para o autor, a possibilidade de anonimização de dados na legislação europeia é controversa. Machado interpreta que a capacidade computacional pode diminuir a eficiência da anonimização de dados.²⁴⁵ Ao mesmo tempo, o RGPD estabelece que os princípios de proteção de dados não são aplicáveis a informações ou dados pessoais tornados anônimos.²⁴⁶

De forma similar ao conteúdo principiológico da Diretiva 95/46/CE, o RGPD adota o princípio da proibição, ou seja, os dados pessoais só podem ser tratados por meio de uma justificação (hipóteses de tratamento de dados). Esta hipótese pode ser o consentimento, fornecido pelo titular para uma finalidade específica, ou um fundamento jurídico, importando sublinhar não haver hierarquia entre tais hipóteses.

O princípio da proibição deve ser lido no sentido de que o tratamento de dados só é lícito para finalidades determinadas no momento da justificação, ou seja, não pode servir de “carta-branca” para tratamentos futuros a vontade do controlador. Devem-se recusar concepções que consideram suficiente uma justificação inicial para tratamentos de dados por tempo indeterminado.²⁴⁷

Outro princípio essencial no RGPD é o princípio da finalidade da coleta, nos termos do art. 5º, par. 1, alínea b. Qualquer dado pessoal só pode ser coletado para fins específicos e determinados, ou seja, veda-se a coleta de dados para utilização incerta ou apenas para formar base de dados do controlador. Döhmman esclarece que a leitura desta alínea, em associação com o art. 6º par. 4 do mesmo regulamento,

²⁴⁴ DÖHMANN, **A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia**. *Op. cit.*, p. 101-102.

²⁴⁵ MACHADO *et al*, **GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis**. *Op. cit.*, p. 7-8.

²⁴⁶ “The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR)**. Recital 26. Disponível em: <https://gdpr-info.eu/recitals/no-26/>. Acesso em: 22 jul. 2022.

²⁴⁷ DÖHMANN, **A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia**. *Op. cit.*, p. 104.

representa uma particularidade em relação à limitação da finalidade, permitindo o uso do dado para finalidade diversa se, e somente se, existir compatibilidade com o propósito para o qual os dados pessoais são inicialmente recolhidos. Para a autora o critério é a estreita conexão entre a antiga e a nova finalidade.²⁴⁸

3.2 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Diante da insuficiência de legislações específicas, vez que até 2018, como abordado, o direito a proteção de dados possuía abrigo somente no Marco Civil da Internet e em legislações reflexas, o Brasil aprova a Lei n.º 13.709/2018, Lei Geral de Proteção de Dados - LGPD²⁴⁹. Sancionada em 14 de agosto de 2018, torna-se o principal instrumento de proteção de dados pessoais no ordenamento jurídico nacional. Objetiva o estabelecimento de regras claras que visam garantir a proteção de dados pessoais, por meio de práticas transparentes aos titulares dos dados, pessoas naturais.

Foi seguramente um esforço dos operadores do direito, com uma articulação política, na medida que os atuais instrumentos, embora versassem sobre o direito à proteção da privacidade, a rigor, não definiram diretrizes cristalinas em relação ao uso indevido dos dados da pessoa natural. Neste aspecto, frente a esta insuficiência, o texto representou um importante avanço na ordem jurídica brasileira na matéria²⁵⁰, principalmente com a positivação do direito fundamental à proteção de dados pela EC n.º 115/2022.

Cabe a ressalva de que, não significa que antes da LGPD não existia nenhuma proteção de dados no ordenamento brasileiro. Contudo, embora houvesse proteção, sua setorização e pulverização em leis e decretos esparsos, por certo, obstaculizava a visualização de um sistema. A LGPD, neste contexto, significa “uma orientação para organização formal deste sistema, a partir da cristalização e reprodução de muitos

²⁴⁸ *Ibid.*, p. 106.

²⁴⁹ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jul. 2022.

²⁵⁰ SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências, *in*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 368.

destes dispositivos esparsos, inclusive com status principiológico em alguns casos”.²⁵¹ Ainda, na visão de Doneda, existia um hiato entre a proteção constitucional da privacidade e a tutela de informações pessoais em sentido estrito. Este hiato poderia deixar de proteger os indivíduos em certas situações de utilização abusiva de suas informações pessoais.²⁵²

É preciso destacar que a LGPD foi fortemente influenciada pela legislação de proteção de dados europeia, o RGPD. O regulamento europeu, de forma positiva, pressionou os países de outros continentes, que dependem de relações comerciais com a Europa, a editarem normas próprias que garantissem o efetivo direito individual de proteção de dados.

O cenário de incerteza quanto à compatibilidade entre a aplicação do RGPD e as regulamentações nacionais sobre o assunto transcende o território europeu, como se pode observar pelos próprios princípios de aplicação extraterritorial das suas disposições legais. A prossecução da globalização dos mercados de serviços digitais no século XXI corrobora a concepção de um sistema internacional cada vez mais interligado por empresas e utilizadores que operam em vários mercados, sujeitos a diferentes jurisdições. No contexto da aplicação extraterritorial do RGPD, a partir de um dos mais importantes mercados globais de prestação e consumo de serviços digitais, é natural que outras economias também procurem adaptar-se ao atual regime jurídico, de modo a manter a sua competitividade no comércio internacional. (tradução livre)²⁵³

Muito embora o Brasil não esteja vinculado ao direito europeu, em razão da integração global típica da internet se exige o atendimento a parâmetros, que por si só implicam em certas simetrias entre os marcos regulatórios.²⁵⁴

Um ano após a sanção da LGPD, a Lei 13.853/2019 é publicada²⁵⁵. Além de promover algumas alterações na LGPD, cria a Autoridade Nacional de Proteção de

²⁵¹ OLIVEIRA; LOPES, **Os princípios norteadores da proteção de dados...**, *Op. cit.*, p. 72.

²⁵² DONEDA, **A proteção dos dados pessoais como um direito fundamental**. *Op. cit.*, p. 106.

²⁵³ “*The scenario of uncertainty as to the compatibility between the application of the GDPR and national regulations on the subject transcends the European territory, as one can observe from the very principles of extraterritorial application of its legal provisions. The pursuit of market globalization of digital services in the 21st century corroborates the design of an international system increasingly interconnected by companies and users that operate in several markets, subject to different jurisdictions. In the context of GDPR’s extraterritorial application, from one of the most important global markets for digital services provision and consumption, it is natural that other economies also seek to adapt itself to the current legal regime in order to maintain their competitiveness on international*”. MACHADO et al, **GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis**. *Op. cit.*, p. 20.

²⁵⁴ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 26-27.

²⁵⁵ BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 23 jul. 2022.

Dados – ANPD. A autoridade nacional é umas das várias alternativas que o Estado dispõe para dar conta do seu dever de proteção. Como órgão central na interpretação da LGPD, é responsável, dentre outros, por zelar pela proteção de dados, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, estabelecer normas e diretrizes para sua implementação e deliberar, na esfera administrativa, sobre a interpretação da lei e sobre as suas próprias competências e casos omissos.²⁵⁶

Uma das fragilidades da ANPD, segundo especialistas na área²⁵⁷, era a sua vinculação como órgão da administração pública federal, integrante da Presidência da República. A independência de uma autoridade de fiscalização é elemento central para sua institucionalização e no caso na ANPD esta vinculação poderia comprometer em partes sua atuação.

Esta independência surge com a Lei n.º 14.460/2022 que, dentre outras medidas, revogou o art. 55-A § 1º da Lei 13.853/2019 que previa a transitoriedade da natureza jurídica na ANPD. Esta lei representa um avanço na autonomia técnica e decisória da autoridade de fiscalização, pois autarquias de natureza especial não são subordinadas hierarquicamente a ministérios ou à Presidência.²⁵⁸

Cumprir destacar que a LGPD trouxe fundamentos novos na tutela dos dados pessoais que não se resumem na absorção de elementos anteriormente presentes. São percebidos na lei novos princípios e direitos que se integraram aos paradigmas relacionados à proteção de dados. Fundamentos novos, disciplinados no art. 2º da LGPD. Além do histórico respeito à privacidade e inviolabilidade da intimidade, a LGPD tem como alguns dos fundamentos: à autodeterminação informativa; liberdades individuais; desenvolvimento econômico e tecnológico; a livre iniciativa e o livre

²⁵⁶ ANPD – Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público - Guia Orientativo**. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 17 jul. 2022. p. 5.

²⁵⁷ FILHO, Carlos Edison do Rêgo Monteiro; CASTRO, Diana Paiva de, Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709/2018), *in*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 334.

²⁵⁸ BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em: 21 dez. 2022.

desenvolvimento da personalidade.²⁵⁹ Frazão infere que tais objetivos denotam a clara posição da LGPD em proteger cidadão e as situações existenciais derivadas do tratamento de seus dados.²⁶⁰ Objetivos valorizados pelo estabelecimento de obrigações do gerenciamento seguro do início até ao fim da operação manipule dados pessoais.²⁶¹

Apesar da similitude (com o RGPD) das definições de dados pessoais ou dados sensíveis, constantes no art.º 5 da LGPD, importa a verificação dos princípios que a legislação brasileira optou por trazer de forma explícita em seu art. 6º: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. Gabrielle Sarlet e Regina Ruaro relembram que esta constelação principiológica é emoldurada por princípios constitucionais, além de serem amparados por outros instrumentos jurídicos para além do direito digital.²⁶²

Ainda que outros possam ser derivados ou implicitamente estabelecidos, como o princípio da boa-fé ou do interesse público, a preocupação com o equilíbrio entre a proteção da pessoa e os coletividade é percebida.²⁶³ O primeiro, e talvez mais importante²⁶⁴ princípio do art. 6º da LGPD, é o princípio da finalidade. Fundamental para limitar o acesso a terceiros, o princípio da finalidade determina que os propósitos devem ser específicos, explícitos e informados ao titular, ou seja, não se admite finalidades amplas ou genéricas.

Ao estabelecer uma limitação ao tratamento ulterior, “eventual uso secundário dos dados pessoais somente pode ser realizado para uma finalidade que seja compatível com a finalidade original do tratamento dos dados”.²⁶⁵ Lido em conjunto com o princípio da adequação (art. 6º, II), a compatibilidade estabelece-se de acordo

²⁵⁹ Art. 2º. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jan. 2023.

²⁶⁰ FRAZÃO, Ana. **Objetivos e alcance da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 102.

²⁶¹ SARLET, Gabrielle Bezerra Sales;; RUARO, Regina Linden, A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018, **Revista de Direitos Fundamentais e Democracia**, v. 26, p. 81–106, 2021.

²⁶² *Ibid.*, p. 85-86.

²⁶³ OLIVEIRA; LOPES, **Os princípios norteadores da proteção de dados...**, *Op. cit.*, p. 57-61.

²⁶⁴ O termo importante não denota uma hierarquia entre os princípios de tratamento de dados pessoais na LGPD, mas tão somente que é um dos mais trabalhados e sua incidência na LGPD é percebida em outros trechos como: direitos de acesso; legítimo interesse; requisitos do consentimento; término de tratamento de dados e transferências internacionais de dados.

²⁶⁵ ANPD – Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público - Guia Orientativo**. *Op. cit.*, p. 13.

com o propósito e o contexto do tratamento, que devem sempre ser informados ao titular.

O princípio da finalidade (art. 6, III) estabelece uma limitação quantitativa no tratamento de dados. A ideia é que todas as operações utilizem o mínimo necessário para a realização de suas finalidades. Deduz-se deste à proporcionalidade e a frase: “Depois decide-se como o dado será utilizado”, não encontra guarida neste princípio. Impõe-se a menor quantidade possível de dados à coleta ou ainda, que se deixe de coletar se a finalidade pode ser atingida por outros meios.²⁶⁶

O princípio da não-discriminação (art. 6, IX) veda a realização do tratamento para fins discriminatórios ilícitos ou abusivos, tendo em vista que alguns dados, especialmente os dados sensíveis (definidos no art. 5º, II), são suscetíveis a uma abordagem diferenciada e potencialmente discriminatória. Já o princípio do livre acesso (art. 6, IV) garante o exercício da liberdade de informação facilitada e gratuita sobre a forma e a duração do tratamento.

Mais do que um direito de consulta, Filho e Castro depreendem deste princípio uma forma capaz de suprir o desnível de poder entre titular e controlador, relativamente à falta de informação. Admitem os autores que inclusive o titular pode ser assistido por profissional qualificado, de forma mitigar a disparidade de conhecimento técnicos e jurídicos entre as partes.²⁶⁷

Ainda que observados todos os princípios, a LGPD especifica os fundamentos jurídicos ou hipóteses de tratamentos de dados. Assim como no RGPD, o consentimento é o primeiro deles (apesar de não haver hierarquia entre si). Os incisos II ao X do art. 7º da LGPD elencam um rol taxativo de hipóteses de tratamento de dados que dispensam o consentimento do titular.²⁶⁸

²⁶⁶ O guia orientativo de tratamento de dados pessoais pelo poder público traz um exemplo elucidativo quanto a coleta de dados além da estrita necessidade. “A Secretaria de Educação de um Município contrata, por licitação, uma empresa para fornecer merenda nas escolas. Para firmar o contrato com a Secretaria, tanto o representante da empresa quanto o servidor público que assinará o contrato fornecem os seus dados, como nome, profissão, CPF, RG, estado civil e endereço residencial. Para atender a outros dispositivos legais e dar publicidade à contratação da empresa, o contrato é divulgado no sítio eletrônico da Secretaria de Educação. É possível que dados como estado civil e endereço residencial não sejam necessários para a identificação dos responsáveis pela contratação e para viabilizar o exercício do controle social sobre a atividade do órgão público. Assim, a fim de limitar o tratamento ao mínimo necessário para a realização de suas finalidades, o ideal é não coletar esses tipos de dados”. *Ibid.*, p. 14.

²⁶⁷ FILHO, Carlos Edison do Rêgo Monteiro; CASTRO, Diana Paiva de. **Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados...** *Op. cit.*, p. 330-331.

²⁶⁸ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou

O consentimento será detalhado no capítulo seguinte desta pesquisa, porém em alguns casos não será nem indispensável, nem o mais apropriado. Nos casos de existência outra base legal de tratamento, alguns autores indicam adequado e seguro para os agentes de tratamento que não seja utilizado o consentimento, ainda que seja possível obtê-lo. De todo modo, não sendo via consentimento, é fundamental ocorrer um encaixe em pelo menos uma das hipóteses legais, sob o risco de o tratamento de dados ser considerado ilícito.²⁶⁹

Ainda que não detalhados todos os princípios e hipóteses legais de tratamento, observa-se que o direito à proteção dados não se trata de direito patrimonial. Frazão concorda com Doneda e Rodotà ao afirmar que a LGPD pode ser vista como um “freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas”.²⁷⁰ Permitir a comercialização seria renunciar ao livre desenvolvimento individual e desconsiderar direitos fundamentais em questão. Renúncias que são inválidas tanto sob a ótica da LGPD como a partir de outros diplomas legislativos.²⁷¹

Partes destes “freios” estão no capítulo III da LGPD, que enuncia os direitos dos titulares, em particular o art. 18, que confere o direito de o titular requisitar ao

regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; 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); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros; VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jan. 2023.

²⁶⁹ VIOLA, Mario; TEFFÉ, Chiara Spadaccini de, Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7.º e 11, *in*: DONEDA, Danilo *et al* (Orgs.), **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 120-127.

²⁷⁰ FRAZÃO, Ana. **Objetivos e alcance da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 103-104.

²⁷¹ Frazão cita como exemplo o art. 11 do Código Civil – Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária. *Ibid.*

controlador, a qualquer momento: o acesso; a correção; eliminação; e a portabilidade dos seus dados, dentre outros. A interpretação deste rol de direitos deve ser exemplificativa, pois representam algumas das possibilidades jurídicas de manifestação de autonomia sobre seus próprios dados.²⁷²

Ingo Sarlet evidencia que as posições jurídicas subjetivas, que a LGPD atribui ao titular dos dados, delimitam o próprio âmbito de proteção do direito fundamental à proteção de dados. Mais do que somente uma posição negativa ou um direito de defesa, o catálogo de direitos do capítulo III associa-se à dupla função dos direitos fundamentais, projetando também em direitos positivos.²⁷³

Outro direito do titular que a LGPD consubstancia é o direito de revisão de decisões tomadas unicamente com base em tratamento automatizado (art. 20). Entende-se que decisões algorítmicas podem definir perfis e limitar acessos ou afetar aspectos da personalidade do titular. Razão pela qual se exige uma explicação sobre seu funcionamento, observados os segredos comercial e industrial.²⁷⁴ A respeito destes segredos, Frazão frisa que:

o dever do controlador é fornecer subsídios que tornem compreensível a passagem dos seus objetivos, consolidados no artefato algorítmico em critérios matemáticos, até a decisão automatizada. Não se torna imperativo que as minúcias técnicas da decisão sejam reveladas, protegido assim o segredo comercial e industrial; mas deve o controlador demonstrar, em linguagem natural, porque ele mesmo acredita que a decisão automatizada é a que melhor atende suas pretensões.²⁷⁵

No regulamento europeu, mais do que o direito de explicação, o titular tem o direito de não ficar sujeito a uma decisão baseada exclusivamente no tratamento automatizado, resguardadas as exceções do parágrafo 2, que incluem a inaplicabilidade da vedação quando autorizada pela legislação da União ou do Estado-

²⁷² Ingo Sarlet demonstra um possível exemplo desta não taxatividade do art. 18 da LGPD e o rol de posições jurídicas associadas. “Espaço para o reconhecimento de outras posições jurídicas, como se dá, em caráter ilustrativo, com o assim chamado direito ao esquecimento...Nesse contexto, o melhor exemplo talvez seja o de um direito à desindexação relativamente aos provedores de pesquisa na internet, que, a despeito da controvérsia que grassa em torno do tema, tem sido objeto de reconhecimento em diversas decisões judiciais”. SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental...** *Op. cit.*, p. 197.

²⁷³ *Ibid.*, p. 196.

²⁷⁴ Em relação a este assunto, tratado no capítulo 1.2 do presente trabalho, entende-se que, apesar da fundamentalidade em criar mecanismos de transparência, existem dificuldades de ordem técnica que precisam ser consideradas. O trabalho destacou ao menos duas, quais sejam: a linguagem de programação e o volume de dados capturados. Somados conclui-se que em determinados casos, seria preciso um software para analisar os resultados produzidos por outro software.

²⁷⁵ FRAZÃO; GOETTENAUER, **O jogo da imitação jurídica...** *Op. cit.*, p. 58.

Membro, ou ainda quando baseada no consentimento explícito do titular dos dados. O considerando 71 deixa explícito que a preocupação com a perfilação do usuário é, além de revelar aspectos individuais da pessoa, prever desempenhos, comportamentos ou outras características que afetem a pessoa de forma significativa.²⁷⁶

3.3 DISTINÇÕES APLICÁVEIS ENTRE OS DADOS ANÔNIMOS E OS DADOS SENSÍVEIS

Se por definição a LGPD entende como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável e por dado anonimizado considera o dado relativo ao titular que não possa ser identificado, por silogismo os dados anonimizados não estão protegidos pela lei. Esta dedução lógica não é só implícita nas conceituações da LGPD, conforme expressa em seu art. 12, que descreve que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização puder ser revertido. Assim como no regulamento europeu, a legislação brasileira, em uma extensão da interpretação de Machado²⁷⁷, admite certa controvérsia ao reconhecer que um dado possa perder sua característica de anônimo e, desta forma, seus titulares reidentificados.

²⁷⁶ “The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR)**. Recital 71. Disponível em: <https://gdpr-info.eu/recitals/no-71/>. Acesso em: 22 jul. 2022.

²⁷⁷ Ver nota de rodapé 245.

De toda sorte, a LGPD traz, não no rol de definições do art. 5º, mas na seção de tratamento de dados, a conceituação de dados pseudonimizado (conceito idêntico ao constante no regulamento europeu)²⁷⁸. Para a lei, consiste “no meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro”.²⁷⁹ Diferente dos dados anonimizados que não são alcançados pela norma, os pseudonimizados podem levar a reidentificação do titular, razão pela qual são protegidos pelos mesmos princípios e fundamentos jurídicos.²⁸⁰

Dentre as técnicas mais comuns de anonimização destacam-se a supressão, a generalização e a pseudoanonimização.²⁸¹ A supressão consiste na substituição de algumas informações por valores fixos ou caracteres que impedem a identificação. Um exemplo simples seria, em um banco de dados, a substituição do nome da pessoa pelos caracteres “XYZ”. Seria o equivalente, no meio físico, a colocar uma tarja no texto. Poderia a supressão traduzir-se na simples eliminação de parte dos dados. No mesmo exemplo, seria a remoção da coluna com o nome do titular.

A generalização corresponde ao agrupamento de dados em categorias ou faixas genéricas. Ao invés da data de nascimento, por exemplo, um cadastro conteria uma faixa de idade (20 a 30 anos; 30 a 40 anos; acima de 40 anos). Na generalização, modifica-se a escala ou a ordem de grandeza dos dados. A randomização ou aleatorização baseia-se no mascaramento de dados, por meio da adição de ruídos, que podem ser dados fictícios ou combinações entre os próprios dados. Por fim, na pseudoanonimização o dado perde sua possibilidade de associação senão pelo uso de informação adicional, ou seja, essa técnica consiste em separar os dados em dois ou mais grupos. A informação adicional ou a “chave” para esta ligação deve ser mantida pelo controlador e ambiente seguro.²⁸²

Quanto maior a combinação destas técnicas, menor a possibilidade de reidentificação e consequentemente a possibilidade de utilização para além das

²⁷⁸ O conceito de pseudonimização inexistia na Diretiva 95/45/CE. É no RGPD uma medida mitigativa que visa assegurar a não identificação do titular dos dados.

²⁷⁹ Art. 13 § 4º LGPD. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.**

²⁸⁰ CUEVA, Ricardo Villas Bôas, **Anonimização e pseudonimização de dados pessoais no processo eletrônico**, Revista dos Tribunais, 2020. p. 249-252.

²⁸¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**; Editora Forense, 3. ed.; São Paulo, 2021. p. 61-62.

²⁸² RODRIGUES, Juciana. **Anonimização como forma de proteção de dados**. Associação Brasileira de Ciências de Dados – ABRACD. 2020. Disponível em: <https://abracd.org/anonimizacao-como-forma-de-protecao-de-dados/>. Acesso em: 28 jul. 2022.

hipóteses previstas na LGPD. A análise de quais técnicas deve ser fática, variando de acordo com o contexto de utilização dos dados. “Por isso não há um único método ou uma combinação perfeita *ex-ante* para parametrizar o processo de anonimização”.²⁸³ Bioni destaca ainda que a impossibilidade de reidentificação deve atingir inclusive o controlador ou operador que procedeu à sua anonimização. Garantir a desvinculação dos dados à pessoa é romper o elo entre o dado e o titular.²⁸⁴

Se o intuito da anonimização é remover quaisquer elementos que possam reidentificar o titular do dado, a questão que se levanta, principalmente com a evolução tecnológica dos processos de agregação do Big Data é: existe um dado totalmente anonimizado? Martins afirma que “a confiabilidade de tais mecanismos não podem ser atestada de forma cabal no atual estado da arte das estruturas tecnológicas da ciência da computação”.²⁸⁵ Se um dado anônimo pode ser reidentificado, é possível diferenciar juridicamente estas categorias na LGPD? A questão é relevante posto que, conforme apresentado, os dados anonimizados não são considerados dados pessoais e, desta forma, não são protegidos.

Gabrielle Sarlet e Regina Ruaro apontam que de fato não há uma metodologia de anonimização total. Para as autoras todas as formas de anonimização podem sofrer uma engenharia reversa e todo processo é precarizado em face do desenvolvimento de novas técnicas, “tratando-se de um mito que se impõe de uma maneira geral para o engendramento da proteção sistemática da pessoa na sociedade informacional e que exige uma atenção redobrada e contínua”.²⁸⁶ Pela possibilidade de combinação de dados mantidos em bancos de dados distintos e, pela probabilidade de reidentificação do titular, a anonimização total é tida como um mito ou uma ficção jurídica.

Mito da anonimização que também é aduzido por Bioni ao expor estudo que demonstram a falibilidade do processo de anonimização. “A agregação de diversos pedaços de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito

²⁸³ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais....** *Op. cit.*, p. 63.

²⁸⁴ CUEVA, **Anonimização e pseudonimização de dados pessoais no processo eletrônico.** *Op. cit.*, p. 252.

²⁸⁵ MARTINS, Guilherme Magalhães; JUNIOR, José Luiz de Moura Faleiros, **PROTEÇÃO DE DADOS E ANONIMIZAÇÃO: PERSPECTIVAS À LUZ DA LEI Nº 13.709/2018**, Revista Estudos Institucionais, v. 7, 2021. p. 378.

²⁸⁶ SARLET; RUARO, **A proteção de dados sensíveis...** *Op. cit.*, p. 90-91.

mosaico”.²⁸⁷ Este exemplo demonstra que um dado anonimizado têm o risco de se tornar dado pessoal se a “engrenagem” que correlaciona os dados puder ser encontrada em outra base de dados.

Partindo destes pressupostos, qualquer dado anonimizado é um dado pessoal. Admitir essa afirmação seria reconhecer que tanto o RGPD como a LGPD apresentam uma redundância normativa e falham ao atribuir tratamentos distintos para os mesmos tipos de dados. A saída, na visão de Bioni, é a adoção do critério de razoabilidade. As duas normas indicam o conceito de “esforços razoáveis” como custo e tempo necessários para reverter a anonimização. Se a exigência destes dois atributos for acima do razoável para que ocorra a reidentificação do titular, ainda que possível, o dado não será considerado pessoal. Nestas situações, serão tratados como anônimos por ambas as legislações. Esse critério da razoabilidade é o amparo para o estabelecimento de definições distintas e sobretudo de tratamentos jurídicos distintos.²⁸⁸

Martins observa que a dificuldade é justamente aferir o que é um “esforço razoável” no exercício do estabelecimento do grau de identificabilidade de um dado pessoal. O resultado desta complexa avaliação conduz ao correto enquadramento nos marcos regulatórios de proteção de dados.²⁸⁹

Além dos dados anonimizados, outro conjunto de dados que possuem definições e hipóteses de tratamento especiais são os dados sensíveis. A LGPD considera dado pessoal sensível como 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”.²⁹⁰ A partir destas definições,

²⁸⁷ Ao criar um concurso para melhorar seu algoritmo de sugestão de filmes, a Netflix disponibilizou sua base de dados com todas as avaliações de filmes de seu catálogo, suprimindo o nome do usuário, mantendo somente a data de avaliação e a nota do filme. Utilizou ainda técnicas de randomização para dificultar a identificação do usuário. Mesmo assim, os pesquisadores combinaram as análises da plataforma de *streaming* com o site da IMDB (onde pessoas compartilham suas impressões sobre filmes). Ao cruzar estas duas bases de dados, correlacionando as datas e avaliações (notas) encontraram os nomes dos usuários do Netflix. BIONI, Bruno Ricardo. **Proteção de Dados Pessoais....** *Op. cit.*, p. 63-65.

²⁸⁸ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais....** *Op. cit.*, p. 66-67.

²⁸⁹ MARTINS, Guilherme Magalhães; JUNIOR, José Luiz de Moura Faleiros, **PROTEÇÃO DE DADOS E ANONIMIZAÇÃO...** *Op. cit.*, p. 389.

²⁹⁰ Art. 5º, II LGPD. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm. Acesso em: 21 jan. 2023.

ao menos quatro categorias de dados pessoais sensíveis são percebidas: dados pessoais sensíveis de origem; dados pessoais sensíveis de crenças; dados pessoais sensíveis corporais e dados pessoais sensíveis sexuais.²⁹¹

Essas categorias são frutos de observações práticas de que algumas espécies de informação possuem potencial de causar maiores danos aos seus titulares, em caso de usos indevidos. Essa maior lesividade ensejou a diferenciação no tratamento nas legislações sobre proteção de dados pessoais. Assim como se observou que o direito à proteção de dados ampliou conceitos tradicionais de privacidade, antes atrelados a vida privada e intimidade, percebeu-se que os preceitos de tratamentos deveriam ser mais estreitos para os dados sensíveis.²⁹²

Na mesma esteira, Teffé e Fernandes entendem que os dados sensíveis devem ser protegidos de forma mais rígida, pois são essencialmente relevantes para garantias de direitos e liberdades fundamentais.²⁹³ Esta relevância e a possibilidade de serem utilizados de forma discriminatória torna imperiosa a aplicação de princípios da precaução e da prevenção a este conjunto de dados.²⁹⁴ Os dados sensíveis estão, neste sentido de proteção a outros direitos fundamentais, tão conectados à privacidade quanto à igualdade.

Repercute-se, do mesmo modo que em relação aos dados anonimizados, se o processo de agregação e combinação de dados pode tornar um dado que, a princípio não se enquadraria como dado sensível, poder ganhar tal característica. A pergunta seria a mesma: Há algum dado não sensível? Quanto mais inclinada estiver a resposta a negação, menor é a diferença nas hipóteses de tratamento. Essa questão é significativa na avaliação, por exemplo, do tratamento de dados para proteção do crédito ou para atender os legítimos interesses do controlador, já que estes dois fundamentos não se aplicam a esta categoria especial de dados.

²⁹¹ TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad, Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites, In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). **O Direito Civil na era da inteligência artificial**. 1 ed. São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2020. p. 289-290.

²⁹² DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 147.

²⁹³ TEFFÉ; FERNANDES, *Op. cit.*, p. 285.

²⁹⁴ Relativamente ao princípio da prevenção, este se diferencia do princípio da precaução, vez que reside no grau estimado de probabilidade de ocorrência do dano. No princípio da prevenção tem-se a “verdade sabida” e o potencial lesivo já é conhecido. Pelo princípio da precaução, não se tem como seguro de que haverá impacto, mas se pode vislumbrar a existência de um problema desta ordem o que caracteriza um dos pressupostos para a aplicação do princípio da precaução. SARLET; RUARO, **A proteção de dados sensíveis...** *Op. cit.*, p. 87-87.

Teffé e Fernandes afirmam que “a linha distintiva entre dados pessoais de caráter geral e dados sensíveis, espécie do primeiro, pode não ser tão nítida, diante da dinamicidade das relações e contextos traçados”.²⁹⁵ Dados que em princípio não pareçam sensíveis ou relevantes, uma vez combinados ou transferidos para outros controladores, podem determinar características sensíveis a respeito de seus titulares.²⁹⁶ Torna-se cada vez mais complexo antecipar os efeitos da coleta de algumas informações.

Nesse sentido, pode-se compreender que o conteúdo da categoria dos dados sensíveis não é estático, sendo essencial a verificação concreta do uso que deles se faça. Para a adequada tutela da informação pessoal, é fundamental que se verifique o contexto de sua utilização, além das relações que possam ser estabelecidas com as demais informações disponíveis, e a potencialidade de seu tratamento servir como instrumento de estigmatização ou discriminação da pessoa.²⁹⁷

Portanto, o entendimento é que a definição de dado pessoal sensível na LGPD é exemplificativa, aceitando uma perspectiva mais ampla, onde primordial para determinação do rótulo de sensível é o risco de danos a direitos fundamentais de seus titulares.

Neste universo de riscos dos dados sensíveis, Teffé e Fernandes trabalham com o reconhecimento fácil. Ao ser integrado a sistemas de vídeo, os algoritmos de reconhecimento fácil permitem a identificação da pessoa, ainda que o identificado desconheça que esteja sendo vigiado. Além de informações biográficas (como idade, sexo e etnia) essas tecnologias possibilitam a qualificação de emoções (felicidade, raiva, nervosismo), vez que a face está intimamente ligada à identidade e ao estado emocional dos indivíduos.²⁹⁸ Essa identidade é revelada através do cruzamento da imagem com bancos de dados selecionados.

²⁹⁵ TEFFÉ; FERNANDES, *Op. cit.*, p. 285.

²⁹⁶ Ao coletar e processar dados de histórico de compras de cartão de crédito, podem-se revelar convicções religiosas, orientação sexual ou estado de saúde. O exemplo da empresa *Target* trabalhado do capítulo 1.2 é válido neste ponto. Um endereço pode identificar uma nacionalidade e, ainda que a nacionalidade não seja à primeira vista um dado sensível, pode ser utilizada para estigmatizar, classificar ou pré-julgar. O nome do cônjuge, também em tese não sensível, pode revelar a orientação sexual e, da mesma forma, ser utilizado para discriminar.

²⁹⁷ TEFFÉ; FERNANDES, *Op. cit.*, p. 288.

²⁹⁸ “Na França e na Suécia, foi proibida a utilização de reconhecimento facial nas escolas; nos Estados Unidos, cidades como Berkeley, San Francisco, Oakland, Cambridge e Summerville baniram imagens coletadas por dispositivos de reconhecimento facial por autoridades públicas... Nessa direção, algumas empresas já anunciaram que estão evitando lançar esse tipo de tecnologia ou mesmo que cancelaram suas pesquisas no tema”. *Ibid.*, p. 294-302

O reconhecimento facial não é uma exceção, mas apenas um exemplo de como dados pessoais sensíveis podem ser utilizados sem o consentimento dos titulares, violando direitos de liberdade e igualdade. Não se olvida que tais tecnologias podem ser utilizadas para a segurança pública, não se aplicando a LGPD nestes casos ou ainda, que possam ser utilizados pela administração pública na execução de políticas públicas, eliminando a exigência do consentimento. O que se pretende levantar é, em um primeiro momento, como o titular é informado sobre o recolhimento destes dados. Segundo, como estes dados são tratados e com quem são compartilhados.

Neste cenário, de amplo conhecimento dos dados pessoais, é indispensável o exame das hipóteses de tratamento de dados pessoais, especialmente o consentimento. Esta manifestação de vontade, que configura um dos pilares do respeito à privacidade e a autodeterminação informativa e, ao mesmo tempo, uma base autorizativa de tratamento de dados pessoais, deve impor responsabilidades aos agentes de tratamento que, além de prevenir abusos e vazamentos, garanta a liberdade de escolha, a informação clara, precisa e inequívoca.

4. CONSENTIMENTO DO TITULAR DOS DADOS

O consentimento é definido no art. 5º, XII da LGPD como uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.²⁹⁹ Essa definição dialoga com o regulamento geral europeu de proteção de dados que, em seu artigo 4 n.º 11, estabelece (além dos adjetivos livre, informado e inequívoco) que a declaração deve ocorrer mediante ato positivo específico.³⁰⁰

O cenário de elevada circulação de informações pessoais, como detalhado no primeiro capítulo, e o inafastável fornecimento destas informações no ambiente digital, sugere a compreensão do consentimento como um processo, como uma ferramenta de controle a favor de seu titular.

O direito à proteção de dados pessoais, como uma das manifestações do livre desenvolvimento da personalidade (em sua pluralidade apontada no segundo capítulo), aponta que o consentimento e sua multiplicidade de adjetivos detém por finalidade demonstrar uma tomada de decisão do titular

Esta noção do consentimento envolve uma relação entre o titular (pessoa natural a quem se referem os dados pessoais) e o destinatário (pessoa natural ou jurídica, de direito público ou privado), a quem compete as decisões e o tratamento dos dados pessoais. Ainda que o direito à proteção de dados tenha por titulares apenas pessoas naturais, Ingo Sarlet ressalva que os dados de pessoas jurídicas são protegidos na perspectiva fundamental por outras garantias, como sigilo comercial, industrial e de propriedade.³⁰¹

Sarlet complementa o dever de proteção de dados que incumbe aos destinatários, a partir do exame da dimensão objetiva dos direitos fundamentais e sua eficácia irradiante. Ao verificar que os dados pessoais são novos valores

²⁹⁹ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jul. 2022.

³⁰⁰ “‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR)**. Art. 4. Disponível em: <https://gdpr-info.eu/art-4-gdpr/>. Acesso em: 04 jan. 2023.

³⁰¹ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 49.

constitucionais e que devem iluminar toda a ordem jurídica, tais parâmetros de proteção devem se aplicar nas relações jurídicas entre atores privados.³⁰²

Porém, os destinatários não se resumem a particulares e vinculam também os atores estatais. Tais atores têm a obrigação de aplicar e concretizar o direito à proteção de dados e, respeitando suas atribuições e competências, assim como observando os “deveres de proteção e o critério da proibição de proteção insuficiente”, devem assegurar sua efetividade concreta.³⁰³

De todo modo, a definição expressa de proteção à pessoa natural reforça a centralidade do indivíduo acerca do processo decisório sobre seus dados. Nos casos em que o tratamento não está explicitamente autorizado por alguma base normativa, o consentimento torna-se, portanto, vetor dominante da autonomia do titular dos dados.³⁰⁴

Maia destaca que este vetor dominante é expresso pela opção da titularidade na LGPD. Assume não somente a ideia de controle sobre um bem jurídico, mas demonstra (no capítulo dos direitos dos titulares) o sentido de atribuição de regras claras acerca do seu modo de uso.³⁰⁵

Essa multiplicidade de adjetivos da LGPD, na busca por um consentimento válido, intenta apontar para o fato que, a partir de uma perspectiva obrigacional, deve haver uma cooperação entre agentes de tratamentos de dados, com objetivo de ampliar a capacidade (além de um dever de informação) de tomada de decisão do titular acerca de seus dados.³⁰⁶

O ponto que se levanta é justamente se o consentimento, ao invés de servir de abrigo ao direito fundamental à proteção de dados pessoais, pelo contrário, não

³⁰² SARLET, **Proteção de dados pessoais como direito fundamental...** *Op. cit.*, p. 206.

³⁰³ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais...** *Op. cit.*, p. 50.

³⁰⁴ MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da, Proteção de dados para além do consentimento: tendências contemporâneas de materialização, **Rei - Revista Estudos Institucionais**, v. 6, n. 2, 2020. p. 513.

³⁰⁵ MAIA, **A titularidade de dados pessoais previstas no art. 17 da LGPD...** *Op. cit.*, p. 148-149.

³⁰⁶ “Na medicina, o dever de informação passa a ser delineado pelo direito de autodeterminação do paciente, que só poderia ser exercido com o fornecimento das informações necessárias para tanto [...] No âmbito judicial da responsabilidade civil médica, o consentimento acabou por ser reduzido a dois elementos: o dever de informar e de obter o consentimento por parte dos médicos [...] No contexto da economia de dados, o potencial conferido ao tratamento de dados pessoais de causar danos aos titulares, reacendeu o debate em torno da coleta do consentimento como processo. Um diálogo dinâmico em que as informações necessárias à autodeterminação informacional do titular são fornecidas e atualizadas, e o fornecimento do consentimento deste é garantido e [...] transcendem o dever de informação”. BIONI, Bruno Ricardo; LUCIANO, Maria, O consentimento como processo: Em busca do consentimento válido, *in*: DONEDA, Danilo *et al* (Orgs.), **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 149–161. P. 151-154.

legítima o tratamento de dados pelo Estado e pelo mercado. Corrêa e Gediel sinalizam que o modelo de regulação jurídica do consentimento não só impede este controle por parte do titular, como também viabiliza e legitima o uso de seus dados. As razões do Estado e o mercado são justificadas, com hipóteses vagas e genéricas, como interesse público (no caso do primeiro) e autonomia privada (no caso do segundo).³⁰⁷

Alguns autores, dentre os quais Danilo Doneda, destacam que o consentimento é um dos pontos mais sensíveis na disciplina de proteção de dados pessoais. A partir da formatação do consentimento como autonomia da vontade, Doneda ressalta a necessidade de estruturar a proteção de dados não sob a base patrimonialista (o que acarretaria a legitimação do tratamento de dados), mas a partir de um sistema que privilegie a privacidade como liberdade negativa (proporcionando que a autodeterminação informativa sirva de instrumento para o exercício de poder de escolha do titular).³⁰⁸

Se o consentimento figura como núcleo da legitimidade de tratamento de dados pessoais e representa a expressão da autonomia individual e do controle do titular sobre seus dados, é preciso analisar a eficácia desta autonomia para efetivação deste direito. Laura Mendes e Gabriel Fonseca levantam algumas insuficiências do paradigma do consentimento, que comprometem a manifestação livre, informada e inequívoca, tais como: limitações dos titulares em avaliar o custo/benefício da cessão de seus dados; a lógica do “*take it or leave it*”, ou “tudo ou nada”, na qual a dependência do serviço obriga o aceite do titular; assim como modernas técnicas de agregação de dados (tratadas no capítulo primeiro), que enfraquecem o gerenciamento dos dados pelos titulares.³⁰⁹

A limitação cognitiva parte do pressuposto que sopesar os custos e benefícios em ceder seus dados pessoais ou avaliar riscos e prejuízos é uma tarefa substancialmente complexa para o titular no momento da coleta. Sobretudo online, onde a tomada de decisão dos indivíduos deve considerar políticas de privacidade ou termos de uso complexos, em linguagem de difícil acesso, com conceitos

³⁰⁷ CORRÊA; GEDIEL, **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado**. *Op. cit.*, p. 149-150.

³⁰⁸ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 310-311.

³⁰⁹ MENDES; FONSECA, **Proteção de dados para além do consentimento...** *Op. cit.*, p. 513-519.

demasiadamente técnicos e jurídicos. Para Mendes e Fonseca, a opção pelo consentimento, em muitos casos, é uma medida ineficaz.³¹⁰

Por sua vez, a agregação de dados torna o destino do dado pessoal indeterminado e imprevisível. O que para o titular, no momento da coleta, não aparentava acarretar invasão de sua privacidade ou danos a sua personalidade, combinado com outros dados, pode ter um efeito diverso. O indivíduo sequer tem conhecimento do complexo ecossistema de atores, trocando e manipulando informações, através de práticas de mineração. O fluxo informacional torna-se completamente volátil. Pequenos pedaços agrupados podem formar um perfil dos hábitos do titular.³¹¹

Razão pela qual Adriana Corrêa entende que o consentimento, como uma adequação das categorias existentes de manifestação de vontade do direito civil, não é adequado. Traz a autora uma reflexão sobre os paradoxos e as contradições desse conceito, apontando para uma “impossibilidade de expressão autônoma da vontade pessoal em uma sociedade marcada pelo avanço crescente e acelerado da tecnologia”.³¹² Situações concretas em que a alternativa de não revelação de seus dados pessoais costuma significar a renúncia a determinados bens ou serviços. Danilo Doneda se refere, nestes casos, ao “consentimento como ficção na pretensão de ser instrumento de livre construção da esfera privada”.³¹³ O autor também trabalha com o conceito de assimetria de poder como insuficiência do consentimento.

Gabrielle Sarlet e Regina Ruaro adicionam a esta lista de aspectos que enfraquecem a reafirmação da autonomia, o volume e a velocidade do fluxo de informações, além do excesso de dados ou “pegadas” digitais geradas por todos os indivíduos.³¹⁴ Itens que se encaixam em uma sociedade marcada pelo aumento exponencial do uso de dados como fonte de publicidade e direcionamento de conteúdo.

Apontar limitações ou entraves do consentimento na LGPD não significa, de forma alguma, deslegitimar tal instrumento, como se a melhor solução fosse sua

³¹⁰ *Ibid.*

³¹¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento.** *Op. cit.*, p. 143.

³¹² CORRÊA, Adriana Espíndola. **Consentimento livre e esclarecido: o corpo objeto de relações jurídicas.** 1. ed. Florianópolis: Conceito, 2010. p. 17.

³¹³ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados.** *Op. cit.*, p. 312.

³¹⁴ SARLET; RUARO, **A proteção de dados sensíveis...** *Op. cit.*, p. 98.

ruptura completa. Pelo contrário, as insuficiências do modelo sugerem a exigência de uma revisão do papel do consentimento como protagonista na proteção de dados pessoais e o exame detalhado de cada uma de suas adjetivações.

A fundamentalidade do ato de consentir deve ser precedida pelo esclarecimento, pela adequação dos termos e pela compreensibilidade da linguagem empregada. Deve ainda se destinar a propósito específico, pela necessidade ao tempo da coleta e substancialmente pela liberdade de escolha.³¹⁵ Não pode ser uma carta-branca para o compartilhamento de dados de forma irrestrita. O ato de consentir não pode estar relacionado a ideia de ausência de interesse na proteção. Não se renuncia o direito à proteção de dados pessoais com o consentimento.³¹⁶

4.1 CONSENTIMENTO LIVRE - MANIFESTAÇÃO DE VONTADE E LIVRE-ARBÍTRIO

Adriana Corrêa assinala que a garantia do convívio social, que se dá através das normas jurídicas, constitui um traço distintivo da subjetividade moderna. A forma como o indivíduo se autodetermina e se relaciona significa, em termos de autonomia, a compreensão da liberdade.³¹⁷

Existe mais de uma vertente de escolha a respeito dos fundamentos que a autonomia, ou a liberdade de agir conforme nossa vontade, pode ser analisada. André Perin, em seu livro (o livre-arbítrio na era do Big Data) o faz segundo raízes filosóficas, pois sua abordagem aponta para o fato que a massificação de tratamentos de dados por tecnologias de Big Data permite manipular a consciência, vontades e desejos dos indivíduos.³¹⁸

Ao analisar a obra “Ética” de Spinoza, observa que apesar de se considerarem livres, os homens desconhecem as causas pelas quais são conduzidos a acreditar

³¹⁵ 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, 2019. p. 12-14.

³¹⁶ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 315.

³¹⁷ CORRÊA, Adriana Espíndola. **Consentimento livre e esclarecido: o corpo objeto de relações jurídicas**. *Op. cit.*, p. 23.

³¹⁸ SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. *Op. cit.*, p. 18-20.

que realmente desejam algo. Ao crer na liberdade de suas vontades, apetites e limitações ignoram as causas que os dispõe a ter essas vontades.³¹⁹

Assim, pode-se afirmar que quando percebemos a decisão adotada, ela já havia sido tomada, pois os sentidos remetem a informações depois da reação entre as substâncias. Tudo reage conjuntamente, mas só percebemos o que já ocorreu. Daí conjecturar-se que, quando a escolha é feita, o sujeito dela ainda não está consciente.³²⁰

O filósofo alemão Schopenhauer, atribuía ao livre-arbítrio a ausência de obstáculos físicos ou materiais, de modo que as ações dos homens obedecessem exclusivamente a sua vontade. Subsequentemente, o autor questiona se a própria vontade é livre. Presume, de forma muito resumida, que todo ato volitivo dependa de um ato volitivo anterior, sendo impossível estabelecer uma conexão entre o conceito empírico da liberdade e o conceito de livre-arbítrio. Conclui que a liberdade, portanto, consiste na ausência de força necessitante.³²¹

O conceito de liberdade pode assumir uma gama de significados, a depender do espectro de análise. Para o objeto da pesquisa (consentimento livre), a ausência de força necessitante representa a possibilidade de escolha ou recusa de utilização dos seus dados pessoais, sem circunstâncias que, de qualquer forma, impeçam, dificultem ou limitem sua opção. É sob este viés que se se estabeleceu, no art. 8º da LGPD, a vedação ao tratamento de dados pessoais mediante vício de consentimento.³²² Representa a base como instrumento de autodeterminação e construção da esfera privada.³²³

Liberdade que, para Ricardo Bioni, representa a ideia “de uma ação espontânea, que não é objeto de pressão, mas, pelo contrário, de livre-arbítrio, caracterizado pela tomada de uma escolha em meio de tantas outras que poderiam ser feitas por alguém”.³²⁴ Ao exemplificar a tomada de decisão livre sobre dados pessoais, o autor aponta alguns requisitos como: inexistência de desequilíbrio entre o

³¹⁹ SCHMIDT NETO, André Perin. *Op. cit.*, p. 30-35.

³²⁰ SCHMIDT NETO, André Perin. *Op. cit.*, p. 53.

³²¹ SCHOPENHAUER, Arthur. **O livre-arbítrio**. Biografia e prefácio de Afonso Bertagnoli; tradução de Lohengrin de Oliveira. Ed. Especial. Rio de Janeiro: Editora Nova Fronteira, 2012. Disponível em: <https://amz.onl/6oPyhGD>. Acesso em: 10 jan. 2023.

³²² VIOLA; TEFFÉ. **Tratamento de dados pessoais na LGPD...** *Op. cit.*, p. 122.

³²³ TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de, **O consentimento na circulação de dados pessoais**, Revista Brasileira de Direito Civil - RBDCivil, v. 25, p. 83–116, 2020. p. 92.

³²⁴ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 189.

titular dos dados e o responsável pelo tratamento; granularidade para diferentes operações de tratamento; e prestação do serviço independente do consentimento.

A proposta de apresentação de requisitos para a tomada de decisão permite tangibilizar o consentimento livre e, ao mesmo tempo, escapar da armadilha do ciclo dos atos volitivos originários. Ao propor uma análise do consentimento livre, moldado no direito civil e em especial na LGPD, reconhece-se que a causa formal da manifestação da vontade é que ela seja livre de vícios e emanada por um sujeito capaz. Exclui-se, portanto, os motivos abstratos que levaram a escolha para determinação da qualificação jurídica e validade.³²⁵

O consentimento livre, portanto, implica em considerar as opções do titular sobre o destino de seus dados pessoais, a quem se destina, seus possíveis usos, para que o interessado possa formar sua convicção.³²⁶ Para Doneda, assume a característica de um ato jurídico unilateral, sem efeitos vinculantes de natureza obrigacional.³²⁷ O art. 18, IX da LGPD comprova esta característica ao prever a revogação do consentimento como um direito do titular.

Além de não possuir esta característica vinculante, o Regulamento Geral Proteção de Dados Europeu (art. 7º, n.º 4)³²⁸ dispõe que o consentimento dado livremente deve evitar estar condicionado à execução de um contrato ou prestação de um serviço, para tratamento de dados além do necessário para sua execução. Hoffmann-Riem observa, todavia, que o texto não veda expressamente e não deixa claro em que medida deve ser entendida como uma proibição de vinculação.³²⁹

A LGPD não traz tal proibição, apesar de enunciar o princípio da necessidade (art. 6º, III) como “limitação do tratamento ao mínimo necessário para a realização de suas finalidades”. Na leitura do art. 9º § 3º firma apenas que, nos casos de condição para o fornecimento de produto ou de serviço, a informação ao titular deva ser destacada.

³²⁵ CORRÊA, Adriana Espíndola. **Consentimento livre e esclarecido: o corpo objeto de relações jurídicas**. *Op. cit.*, p. 40-43.

³²⁶ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 189.

³²⁷ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 317-318

³²⁸ “*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR)**. Art. 7. Disponível em: <https://gdpr-info.eu/art-7-gdpr/>. Acesso em: 22 jul. 2022.

³²⁹ HOFFMANN-RIEM, **BIG DATA E INTELIGÊNCIA ARTIFICIAL...** *Op. cit.*, p. 469.

O problema do consentimento livre reside exatamente neste condicionamento, uma vez que, ainda que a informação seja destacada, a recusa em fornecer o aceite pode inviabilizar acesso a serviços essenciais para o cidadão, especialmente no âmbito digital. Na sociedade cada vez mais dependente de serviços digitais, canais de acesso para comunicação ou plataformas de negócios online, é improvável conceber que algum cidadão não tenha, ora ou outra, que se deparar com algum tipo de aceite. A recusa poderia implicar no custo social de exclusão de tais cidadãos de atividades por vezes elementares, inclusive na realização de outros direitos fundamentais.³³⁰

Hoffmann-Riem entende que o consentimento perde a natureza se determinados serviços forem indispensáveis e não haja ofertas concorrentes de qualidade comparável.³³¹ O’Neil serve-se do exemplo da entrevista de emprego. Alguns empregadores utilizam algoritmos de escore de crédito para recrutamento. Não se espera de um candidato a recusa do consentimento para consulta, pois, ainda que não declarada de forma expressa, tal negativa resultaria na sua rejeição/desclassificação imediata.³³²

As políticas de privacidade giram em torno da ficção de que os consumidores podem e irão barganhar por privacidade, ou irão desistir de acordos que considerem muito invasivos à privacidade [...] As pessoas clicam automaticamente em “concordo” quando confrontadas com acordos de “termos de serviço”, totalmente cientes de que não há chance de modificar os termos. Além disso, nem mesmo está claro se vale a pena examinar os próprios termos de serviços. O mais novo truque das corporações é incluir uma cláusula de “modificação unilateral” que permite que elas alterem o contrato posteriormente, sem aviso prévio às pessoas afetadas. É forma de mercado, substância feudal: todos nós sabemos quem dá as cartas nesses “acordos”. (tradução livre)³³³

Rui Carlos Bittencourt e Marco Berberi destacam outro exemplo: os trabalhadores em plataformas digitais. Nestes casos, agravam-se os problemas, pois, além do monitoramento ser constante, não é facultada ao trabalhador a possibilidade

³³⁰ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 116.

³³¹ HOFFMANN-RIEM, **BIG DATA E INTELIGÊNCIA ARTIFICIAL**... *Op. cit.*, p. 469.

³³² O’NEIL, Cathy. **Algoritmos de destruição em massa**... *Op. cit.*, p. 230.

³³³ “The bulk of online privacy policies are a great example of a failed disclosure regime. They revolve around the fiction that consumers can and will bargain for privacy, or “opt out” of deals or jobs they deem too privacy invasive [...] People mechanically click “I agree” when confronted with “terms of service” agreements, fully aware that there’s no chance they can modify the terms. Moreover, it’s not even clear that the terms themselves are worth perusing. Corporations’ newest trick is to include a “unilateral modification” clause that lets them change the agreement later, with no notice to the persons affected. It’s market form, feudal substance: we all know who calls the shots in such agreements.”. PASQUALE, Frank. **The black box Society**... *Op. cit.*, p. 143-144.

de não ceder seus dados no momento de instalação do aplicativo.³³⁴ O consentimento nestes casos é puramente uma formalidade.

O consentimento como condição *sine qua non* para acesso ao serviço retira a possibilidade efetiva de rejeitar a condição imposta nos termos de serviços de privacidade. “O que se verifica na prática é a obediência do titular à vontade das empresas, o que facilita práticas de controle e de uso indiscriminado de dados pessoais”.³³⁵ Nos casos concretos, os indivíduos não têm a oportunidade de negociar as políticas de privacidade das plataformas.

O RGPD frisa, no considerando 43, que o consentimento não constitui fundamento jurídico válido nas relações com evidente desequilíbrio entre o titular dos dados e o responsável pelo tratamento.³³⁶ Apesar disso, a presunção de que os usuários possam estabelecer as cláusulas de tratamentos de dados desconsidera a vulnerabilidade (informacional, técnica e econômica) e a assimetria de poder existente entre estes atores. Nestas situações, a decisão individual se origina de uma imposição estabelecida por terceiro.³³⁷

Além de impossibilidade de estabelecer os termos, os usuários têm poucos recursos legais para reclamações sobre como as plataformas são governadas. A resposta para estes usuários que não aceitam “voluntariamente” as condições propostas é, em grande parte: “se você não gosta, saia”.³³⁸ Laura Mendes afirma que, o respeito à autonomia do titular dos dados “decorre não apenas um dever de proteção contra o conhecimento não autorizado por terceiros, mas também um dever de proteção contra o consentimento meramente aparente”.³³⁹ Ao titular deve ser dada a opção de discordar daquele tratamento.

³³⁴ BITTENCOURT, Rui Carlos Sloboda; BERBERI, Marco Antônio Lima, Do compartilhamento da economia à fragmentação da privacidade do trabalhador 4.0, *in*: CALOMENO, Cassiana Gomes; BERBERI, Marco Antônio Lima (Orgs.), **Direitos Fundamentais e Tecnologia**, Curitiba: Editora Íthala, 2020, p. 22.

³³⁵ TEPEDINO; TEFFÉ, **O consentimento na circulação...** *Op. cit.*, p. 95.

³³⁶ “In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR)**. Recital 43. Disponível em: <https://gdpr-info.eu/recitals/no-43/>. Acesso em: 22 jul. 2022.

³³⁷ MENDES; FONSECA, **Proteção de dados para além do consentimento...** *Op. cit.*, p. 516.

³³⁸ SUZOR, *Op. cit.*, p. 3.

³³⁹ MENDES, **Autodeterminação informativa: a história de um conceito.** *Op. cit.*, p. 15.

Alguns autores, como Ingo Sarlet³⁴⁰, Lia Camurça e João Matias³⁴¹, avaliam que este modelo se assemelha a contratos de adesão, cujas cláusulas foram estabelecidas unilateralmente. A obrigação fática de contratar esvazia o direito fundamental à livre autodeterminação informativa. Sublinham ser preciso, além do conhecimento, que haja uma compreensão prévia sobre o que o titular dos dados está concordando.

Um dos exemplos mais nítidos de impossibilidade de rejeição das condições impostas em política de privacidade é a ferramenta de comunicação *WhatsApp*. A política estabelece que os dados dos usuários podem ser utilizados para aprimorar, entender, personalizar e ainda comercializar ofertas de serviços, inclusive com outros produtos da empresa do grupo econômico *Meta*, tais como (Facebook, Messenger, Instagram).³⁴² Se o usuário não consentir com a política, não poderá utilizar a ferramenta. Com a dependência deste aplicativo para tarefas cotidianas, declarar que quem não concorde com os termos deva procurar outra ferramenta de mensagem instantânea é ignorar os impactos econômicos e sociais, ignorar a assimetria de poder de barganha entre o indivíduo e a gigante do ramo. Logo, não há como falar em consentimento livre neste caso. A proteção da vontade interna do cidadão deve incluir o combate a indução mascarada da liberdade de escolha.³⁴³

4. 2 CONSENTIMENTO INFORMADO E O PRINCÍPIO DA FINALIDADE

Para Mario Viola e Chiara Teffé, na LGPD, o vocábulo informado significa que o titular dos dados deve receber “informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados”.³⁴⁴ Fator determinante, a informação deve ser prestada pelo agente de tratamento de modo claro, adequado e em linguagem acessível. Deve apontar os riscos e implicações do tratamento de dados. Os autores destacam a importância dos princípios da

³⁴⁰ SARLET, **Proteção de dados pessoais como direito fundamental...** *Op. cit.*, p. 209.

³⁴¹ CAMURÇA, LIA CAROLINA VASCONCELOS, João Luís Nogueira Matias, Direito à privacidade e à proteção de dados pessoais: Análise das práticas obscuras de direcionamento de publicidade consoante a Lei n.º 13.709, de 14 de agosto de 2018, **Revista de Direitos Fundamentais e Democracia**, v. 26, 2021. p. 10-11.

³⁴² Meta Platforms, Inc. **Política de Privacidade do WhatsApp**. Disponível em: https://www.whatsapp.com/legal/privacy-policy/?locale=pt_BR. Acesso em: 14 jan. 2023.

³⁴³ SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. *Op. cit.*, p. 116.

³⁴⁴ VIOLA; TEFFÉ. **Tratamento de dados pessoais na LGPD...** *Op. cit.*, p. 123.

transparência, adequação e finalidade. Berberi complementa ao reiterar que só é possível pensar em autodeterminação informativa com o necessário esclarecimento dos alcances e limites impostos a quem realiza a coleta de dados.³⁴⁵

Este dever-direito de informação é o mecanismo responsável por capacitar o titular a respeito do controle eficaz de seus dados pessoais. Os motivos para coleta, as formas de tratamentos e potenciais compartilhamentos com terceiros (em quantidade e qualidade suficiente) são pressupostos de tomada de decisão por parte do cidadão. Bioni ressalva, no entanto, ser desnecessário ao cidadão receber as minúcias do tratamento dos dados. Esse tipo de detalhamento, ao invés de informar, prejudicaria a compreensão do titular. Para a tomada de decisão, sobre consentir ou não, interessa saber as consequências que tal atividade pode trazer na sua esfera privada.³⁴⁶

Ao exigir informações específicas e explícitas ao titular, o princípio da finalidade (art. 6º, I, LGPD) veda o consentimento para aprovações genéricas, nas quais o consentimento careceria do dever de informação. Embora seja um desafio extrair a camada adicional de proteção do qualificador “específico”, uma das alternativas dos agentes de tratamento é adotar mecanismo que chamem a atenção do titular, tais como alertas, que isolem a declaração de vontade à situação na qual é exigido o consentimento.³⁴⁷ Diferentemente do RGPD que adotou o termo “expresso”, na LGPD a conjugação dos qualificadores “específico” e “explícito” carregam mesma carga semântica e têm sido interpretadas da mesma forma.

O art. 9º da LGPD, reforça que será considerado nulo o consentimento em caso de informações que não tenham sido apresentadas de forma clara, inequívoca e transparente. Adiciona ainda que mudanças nas finalidades de tratamento (não compatíveis com o consentimento original) requerem informação prévia ao titular,

³⁴⁵ BERBERI, Marco Antonio Lima, Disrupção tecnológica e privacidade: algumas reflexões sobre o amanhã, *in*: ALVITES, Elena Cecilia *et al* (Orgs.), **Direitos Fundamentais & Democracia: novas abordagens na perspectiva interamericana**, Porto Alegre, RS: Editora Fundação Fênix, 2022, p. 353–365.

³⁴⁶ Bioni cita como exemplo de informação demasiadamente específica a lógica de protocolos de segurança dos algoritmos do sistema. Esse tipo de informação, por seu caráter eminentemente técnico, obstaculizaria a correta compreensão do titular de dados. BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 185-186.

³⁴⁷ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**; Editora Forense, 3. ed.; São Paulo, 2021. p. 193-194.

facultando a possibilidade de revogação do consentimento.³⁴⁸ Gustavo Teppedino e Chiara Teffé defendem que este artigo deve ser interpretado de forma restritiva, ao vedar ao agente estender autorizações de tratamento para momentos futuros, contextos diversos ou compartilhamento com terceiros distintos dos pactuados inicialmente.³⁴⁹

Ao mesmo tempo que o consentimento para compartilhamento de dados do *WhatsApp* não se enquadram em um consentimento livre (conforme tópico anterior), tampouco é informado, pois, em concordância do que foi tratado, o consentimento informado requer mecanismos que tornem claro que a finalidade da coleta se destina a fins publicitários (nos moldes do que foi aludido como publicidade comportamental).³⁵⁰ Apesar do exemplo se referir ao *WhatsApp*, a mesma lógica se aplica a *Google* e seus resultados de buscas.

O problema em se referir ao dever de esclarecimento ao titular, pelo agente de tratamento de dados está, para Gabrielle Sarlet, em considerar que a sociedade estruturada sob a forma de rede se trata de um ambiente absolutamente neutro. As oportunidades de controle e vigilância fazem parte do negócio das grandes empresas que coletam dados. Ao ceder sem maior zelo seus dados pessoais, reforça-se a tese de que, para se sentirem incluídos, é uma ficção achar que o cidadão vai exigir as informações necessárias para proteger sua privacidade.³⁵¹

Por mais que o titular dos dados exigisse esse esclarecimento, Bioni acrescenta que, as evoluções tecnológicas e as mudanças na forma de manipulação e agregação originariam novas barreiras para estes cidadãos.³⁵² Trata-se do problema da *Privacy Self-Management and the Consent Dilemma* (Autogestão da privacidade e o dilema do consentimento). Hoffmann-Riem é crítico em relação ao modelo de autogerenciamento da privacidade, pois é ilusório achar que o nível adequado de

³⁴⁸ Art. 9º §1º e §2º LGPD. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 21 jan. 2023.

³⁴⁹ TEPEDINO; TEFFÉ, **O consentimento na circulação...** *Op. cit.*, p. 93.

³⁵⁰ NETO, **A fragilização do Estado-Nação na proteção dos direitos humanos...** *Op. cit.*, p. 12-13.

³⁵¹ SARLET, Gabrielle Bezerra Sales, **Notas sobre a identidade digital e o problema da herança digital: uma análise jurídica acerca dos limites da proteção póstuma dos direitos da personalidade na internet no ordenamento jurídico brasileiro**, Revista de Direito Civil Contemporâneo, v. 17, n. 5, 2018. p. 36.

³⁵² BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 151.

proteção contra violações de direitos seja uma tarefa usuários individuais.³⁵³ Outro crítico e autor de livro específico sobre o tema é Daniel Solove. O autor afirma que:

esses problemas cognitivos prejudicam a habilidade dos indivíduos de fazer escolhas informadas e racionais sobre os custos e benefícios de consentir na coleta, uso e divulgação de seus dados pessoais [...] mesmo indivíduos bem-informados e racionais não podem autogerenciar adequadamente sua privacidade devido a vários problemas estruturais [...] A cada sinal de falha do autogerenciamento da privacidade, no entanto, a resposta típica dos formuladores de políticas, acadêmicos e outros é pedir mais e melhor autogerenciamento da privacidade. (tradução livre)³⁵⁴

Portanto, para Solove as leis de proteção de dados oferecem um conjunto de direitos ao titular, porém não fornecem um controle efetivo, pois é virtualmente impossível para as pessoas uma compreensão dos possíveis usos posteriores dos dados. O autogerenciamento de privacidade, apesar de amplamente aceito, se refugia no consentimento. Ao invés de concentrar-se em saber se certas formas de coletas são adequadas ou prejudiciais ao cidadão, se esforçam em saber se estes cidadãos concordam ou não com o uso de seus dados, legitimando praticamente qualquer forma de coleta.³⁵⁵

4. 3 CONSENTIMENTO INEQUÍVOCO – SOBRECARGA DE INFORMAÇÕES E OBSCURIDADE DAS POLÍTICAS DE PRIVACIDADE

Não basta informar o usuário a respeito do uso de seus dados se a informação não for clara. O teor da comunicação deve desembocar em uma declaração de vontades que não deixe dúvidas sobre a intenção do titular. O adjetivo inequívoco, no consentimento, deve ser visto desta forma e integrado a outras bases legais. Os atributos do consentimento (livre, informado e inequívoco) devem se complementar.³⁵⁶

³⁵³ HOFFMANN-RIEM, **BIG DATA E INTELIGÊNCIA ARTIFICIAL**... *Op. cit.*, p. 489.

³⁵⁴ “*These cognitive problems impair individuals’ ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data [...] even well-informed and rational individuals cannot appropriately self-manage their privacy due to several structural problems [...] With each sign of failure of privacy self-management, however, the typical response by policymakers, scholars, and others is to call for more and improved privacy self-management*”. SOLOVE, Daniel J, **INTRODUCTION: PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA**, Harvard Law Review, v. 126, 2013. p. 1881-1882.

³⁵⁵ *Ibid.*, p. 1882-1893.

³⁵⁶ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 190-192.

Essa manifestação inequívoca, sem ambiguidades e evidente não pode ser extraída de uma omissão do titular. Requer-se um ato comissivo que revele claramente a real vontade do cidadão.³⁵⁷ Esta indicação expressa é requisito, conforme art. 8º da LGPD, que indica que o consentimento deve ser fornecido “escrito ou por outro meio que demonstre a manifestação de vontade do titular”.³⁵⁸ O regulamento europeu é ainda mais específico ao detalhar que, além da necessidade de ser prestado por meio de ato afirmativo claro que estabeleça uma indicação expressa, não pode se constituir pelo silêncio, por caixas pré-marcadas ou pela inatividade do titular.³⁵⁹

Por esta razão, não são consideradas adequados termos e políticas de privacidade pré-selecionadas, muito menos que a omissão do titular em concordar com estes termos represente uma aceitação tácita.³⁶⁰ A questão que se levanta é se o aceite nas políticas de privacidade significa necessariamente a demonstração de um consentimento inequívoco.

Apesar da premissa básica de que todas as circunstâncias do tratamento devem ser bem explicadas, a ponto de o usuário possuir condições suficientes para autorizar o tratamento de seus dados, ao navegar pela internet é comum que se encontre, principalmente depois da publicação do RGPD, termos de uso com a opção “li e aceito”. Geralmente são complexos, extensos, em linguagem técnica e por esta razão, não raras vezes, sequer são lidos pelos usuários.

Certamente a transparência é condição para uma escolha clara e válida. Contudo, apesar da aparência de adequação, na prática, o modo como as informações sobre tratamento de dados é entregue aos titulares, na oferta da maioria

³⁵⁷ VIOLA; TEFFÉ. **Tratamento de dados pessoais na LGPD...** *Op. cit.*, p. 124.

³⁵⁸ Art. 8º LGPD. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jan. 2023.

³⁵⁹ “Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. 2This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. 3Silence, pre-ticked boxes or inactivity should not therefore constitute consent. 4Consent should cover all processing activities carried out for the same purpose or purposes”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR)**. Recital 32. Disponível em: <https://gdpr-info.eu/recitals/no-32/>. Acesso em: 22 jul. 2022.

³⁶⁰ TEPEDINO; TEFFÉ, **O consentimento na circulação...** *Op. cit.*, p. 97-98.

de serviços online, não garante transparência. Inequívoco, como requisito do consentimento, não é satisfeito por estes processos.³⁶¹

Para Helen Nissenbaum o fato de “quase todas as políticas de privacidade serem longas, obscuras e legalistas aumenta o fardo irreal de verificar as respectivas políticas dos sites que visitamos, os serviços que consideramos e usamos e o conteúdo que absorvemos” (tradução livre).³⁶² A professora da Universidade de Stanford acrescenta que, o fato das políticas enunciarem que podem sofrer alterações sem que estas sejam comunicadas, agrava o problema. Exige-se que o indivíduo leia a política não só uma única vez, mas o faça repetidamente.

Crítica a respeito da melhoria dos termos de uso, Nissenbaum registra que políticas de privacidade mais claras e práticas não são suficientes, pois a falha está no modelo, ao supor que os “indivíduos podem entender todos os fatos relevantes para a verdadeira escolha no momento de contratação em pares com coletores de dados”. (tradução livre)³⁶³ Este esforço ineficaz é denominado pela autora de “paradoxo da transparência”. Quanto mais esforços forem depreendidos para simplificar as políticas de privacidade e, desta forma, torná-las mais simples e fácil de ler, mais detalhes do tratamento dos dados seriam ocultados. Resumir as políticas reduz detalhes que fazem a diferença. Quanto mais detalhadas forem, menos transparente.³⁶⁴

Solove corrobora com a concepção de que transformar os avisos de privacidade em textos mais compreensíveis, por mais que aparente ser uma solução correta, não resolve o problema. Para o autor, ainda persiste uma desconexão do valor expresso do direito à privacidade no meio digital. Embora as pessoas relatem que se preocupam com a privacidade, seus comportamentos digitais mostram o contrário. Essa desconexão deriva de certos impedimentos à tomada de decisão,

³⁶¹ POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves, **Governança Global da Internet, Conflito de Leis e Jurisdição**, Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. p. 34-35.

³⁶² “Privacy policies as enactments of notice fare no better. That almost all privacy policies are long, abstruse, and legalistic adds to the unrealistic burden of checking the respective policies of the websites we visit, the services we consider and use, and the content we absorb”. NISSENBAUM, Helen, A Contextual Approach to Privacy Online, **New York University; Cornell Tech**, 2011. p. 35.

³⁶³ “Proposals to improve and fortify notice-and-consent, such as clearer privacy policies and fairer information practices, will not overcome a fundamental flaw in the model, namely, its assumption that individuals can understand all facts relevant to true choice at the moment of pair-wise contracting between individuals and data gatherers”. *Ibid.*, p. 32.

³⁶⁴ “An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance”. *Ibid.*, p. 36.

como a racionalidade limitada em adquirir, memorizar e processar todas as informações relevantes.³⁶⁵

Portanto, os obstáculos da autogestão da privacidade se resumem em: as pessoas não leem os termos de uso e políticas de privacidade; quando leem, não a compreendem, pois carecem de conhecimentos e bases técnicas suficientes para uma escolha adequada; e por fim, quando leem e a compreendem, simplesmente concordam, ou porque não há outra opção, ou porque não podem avaliar adequadamente os custos e benefícios do aceite.³⁶⁶

Estas adversidades ganham proporções maiores quando o usuário tem que lidar com vários agentes de tratamento de dados diariamente. Com o exponencial crescimento dos serviços sendo prestados *online*, gerir a privacidade significa ler não só uma, mas inúmeras políticas de privacidade cotidianamente. A sobrecarga de informação (*overload information*) advém da massificação de produção, coleta, armazenamento e, principalmente, do compartilhamento de dados.³⁶⁷ Como citado no primeiro capítulo, na medida que o Big Data e a IA, ao agregarem dados, podem conferir novos significados, exigir a avaliação dos terceiros com quem o agente compartilha os dados pessoais é sobrecarregar o indivíduo com todo o peso de proteger sua privacidade.

Helen Nissenbaum sugere a articulação de normas substantivas específicas que restrinjam quais informações podem ser coletas ou compartilhadas que desafiam a dinâmica tradicional da autodeterminação informacional. Não se baseia no consentimento específico, pois este consentimento demanda um conhecimento prévio do titular. Para o indivíduo é impossível presentificar o futuro nas relações contratuais. Ao invés, fundamenta-se na chamada *theory of contextual integrity* ou teoria da integridade contextual.³⁶⁸

A partir da análise do contexto do uso dos dados pessoais, a privacidade como integridade contextual, que possui como um dos vetores o princípio da boa-fé, se

³⁶⁵ SOLOVE, *Op. cit.*, p. 1887-1888.

³⁶⁶ Daniel Solove argumenta que a passagem para um regime de obtenção do consentimento mais explícito e afirmativo não são resolver o problema da privacidade. A sofisticação das organizações que manipulam dados pessoais eleva as taxas de “aceite”, criando botões e formulários que, ao invés de proteger dos titulares, são na prática novas versões dos mesmos problemas adjacentes. Na medida que os usuários têm que lidar com inúmeras caixas de avisos sobre privacidade, o aceite ou recusa ocorre independentemente da compreensão dos impactos. *Ibid.*

³⁶⁷ MENDES; FONSECA, **Proteção de dados para além do consentimento...** *Op. cit.*, p. 517.

³⁶⁸ NISSENBAUM, **A Contextual Approach to Privacy Online.** *Op. cit.*, p. 37-40.

concentra da avaliação da razoável expectativa de privacidade do titular dos dados. Esta teoria estrutura-se sob a premissa de que o fluxo informacional deve ser apropriado conforme as suas respectivas esferas sociais. O contexto de coleta e fluência dos dados deve estar alinhada à legítima expectativa do titular. O objetivo é entender de que forma o titular de dados consentiria para este fluxo de informações, determinando, assim, sua integridade.³⁶⁹

A teoria da integridade contextual oferece um caminho mais curto e sistemático até este ponto, invocando a sabedoria aprendida de sistemas maduros de normas informacionais que evoluíram para acomodar diversos interesses legítimos, bem como princípios morais, políticos e valores específicos do contexto... A vida online não é apenas integrada à vida social e, portanto, não produtivamente concebida como um contexto distinto, é radicalmente heterogênea, compreendendo vários contextos sociais, não apenas um, e certamente não é apenas um contexto comercial onde proteger a privacidade equivale a proteger a privacidade do consumidor e informações comerciais. (tradução livre)³⁷⁰

Bioni exemplifica a integridade contextual, ou sua derivação, consentimento contextual, nos contratos de seguro saúde. Estes prolongam-se no tempo, não sendo possível determinar todo o complexo conjunto de procedimentos que podem se modificar pelos avanços da medicina e técnicas de tratamentos. À medida que são descobertas novas técnicas, estas são incorporadas no contrato securitário. Assim como os dados pessoais, o alcance da cobertura de tratamentos não é estático e unitemporal. “Diversas aplicações mantêm não só uma relação contínua com seus consumidores, mas, sobretudo, de alta intensidade. E com isso, o fluxo informacional torna-se de longa duração e exponencial”.³⁷¹ Estes elementos inviabilizam, aos agentes de tratamento, informar ao titular todas as variações dos dados. O consentimento específico ou seria falho, ou insuficiente.

³⁶⁹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. Op. cit., p. 231.

³⁷⁰ “The theory of contextual integrity offers a shorter and more systematic path to this point by invoking learned wisdom from mature systems of informational norms that have evolved to accommodate diverse legitimate interests as well as general moral and political principles and context-specific purposes and values....Not only is life online integrated into social life, and hence not productively conceived as a discrete context, it is radically heterogeneous, comprising multiple social contexts, not just one, and certainly is not just a commercial context where protecting privacy amounts to protecting consumer privacy and commercial information.” NISSENBAUM, **A Contextual Approach to Privacy Online**. Op. cit., p. 37-38.

³⁷¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. Op. cit., p. 233.

Apesar de aceitar certa elasticidade no tratamento, o consentimento contextual não significa, de nenhuma forma, que os princípios da atividade de tratamento de dados pessoais possam ser suprimidos ou ignorados. Persiste o direito do titular de manifestar sua vontade para cessar ou limitar o tratamento, pois, ainda que não se recorra ao consentimento explícito para situações ulteriores dentro do contexto inicial da coleta, não se perde de vista o direito ao controle sobre o seu fluxo informacional.³⁷²

Embora a LGPD, como principal diploma na tutela da proteção de dados pessoais, se dedique a criar situações que conduzam a autodeterminação informativa, ainda considera que o titular, como sujeito racional, tenha condições de valer sua proteção de dados pessoais, sem ponderar a constelação de circunstâncias para um consentimento pleno e válido.³⁷³ Grande parte destas soluções normativas estabelecidas na LGPD, nas palavras de Gabrielle Sarlet e Carlos Molinaro, são relacionadas a uma perspectiva “pré *big data*”. Muito embora, reconheçam os autores, alguns princípios básicos do direito à proteção de dados pessoais são realmente de difícil conciliação com estas novas tecnologias.³⁷⁴

4. 4 LIMITAÇÃO DO CONSENTIMENTO E TECNOLOGIA COMO APRIMORAMENTO DO RESPEITO À PRIVACIDADE

A tutela dos dados pela via tradicional de proteção contratual repressiva, qual seja, pela via das tutelas indenizatórias, apesar de necessária e presente no art. 42 da LGPD³⁷⁵, nem sempre será a mais eficaz na proteção da privacidade. Essencialmente este tipo de proteção possui um controle *ex post*, em razão do dano causado e exigência de reparação.

Ocorre que, na proteção de dados pessoais, a racionalidade exige também um controle *ex ante*, ou preventivo. Esta abordagem impõe uma avaliação dos riscos desde a concepção de um novo serviço (*privacy by design*), até sua efetiva prestação

³⁷² BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. *Op. cit.*, p. 234-238.

³⁷³ SARLET; CALDEIRA, **O consentimento informado...** *Op. cit.*, p. 18-23.

³⁷⁴ 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**, Revista Brasileira de Direitos Fundamentais & Justiça, v. 13, n. 41, 2020. p. 196-200.

³⁷⁵ Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**.

ao usuário final. Este paradigma passa a abraçar as noções de responsabilização ou prestação de contas³⁷⁶ (*accountability*) e privacidade por padrão (*privacy by default*).

Apesar de não mencionar explicitamente *privacy by design* e *privacy by default*, a LGPD impõe estes requisitos (art. 46) ao exigir o dever de adoção de medidas de segurança, técnicas e administrativas que possam impedir o acesso a dados não autorizados do titular. Medidas estas que devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.³⁷⁷

Pensar na proteção de dados desde a concepção do produto ou serviço requer a implementação de soluções tecnológicas que assegurem que o tratamento de dados pessoais durante todo o ciclo de vida de desenvolvimento de um software. Exige a mudança de respostas reativas para uma abordagem de adoção de medidas que previnam ocorrências de danos. O sistema deve ser projetado visando não apenas a garantia contra defeitos ou acessos indevidos, mas arquitetado para cada finalidade de tratamento de dados. O artigo 42 do RGPD cita como exemplo mecanismo de certificação como elementos de cumprimento de tais requisitos.³⁷⁸ Já a LGPD estabelece que a autoridade nacional pode designar organismos semelhantes.

Pautando-se na transparência, estes mecanismos podem tornar seus procedimentos mais verificáveis quanto a exclusão de incoerências sistêmicas ou conformidades de tratamento de dados, como tempo de retenção, técnicas de

³⁷⁶ A responsabilização e prestação de contas está incorporada no conjunto de princípio da LGPD. Art. 6º, X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jan. 2023.

³⁷⁷ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jan. 2023.

³⁷⁸ “The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account [...] A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56”. Intersoft Consulting. **GENERAL DATA PROTECTION REGULATION (GDPR).** Art. 42. Disponível em: <https://gdpr-info.eu/art-42-gdpr/>. Acesso em: 21 jan. 2023.

anonimizações e outras garantias, aumentando a confiança nas respectivas organizações e processos.³⁷⁹

Apesar de questionamentos a respeito destes processos de certificação e eventual interferência na proteção dos segredos comerciais, Hoffmann-Riem retrata que não se trata de divulgar o design tecnológico e os sistemas algorítmicos, mas prescrever procedimentos técnicos que podem ser igualmente sigilosos, principalmente na utilização de dados sensíveis.³⁸⁰

Tema semelhante é abordado na Resolução n.º 332 do CNJ³⁸¹. Estes processos de governança e boas práticas, assim como mecanismos de auditoria e certificação, também são requisitos de transparência e validação de modelos apoiadas em ferramentas de Inteligência Artificial. A ideia, segundo Fabiano Hartmann, está alinhada aos estudos dos efeitos desta crescente utilização da tecnologia de *Big Data* e IA na concepção de produtos ou serviços.³⁸²

Doneda ressalva corretamente que, evidentemente, a tecnologia por si só não pode ser entendida como um meio de tutela. Pode, porém, servir de instrumento de atuação, tanto na esfera pública como na privada, se encarada como meio para regulação da proteção de dados pessoais.³⁸³ É neste contexto que se encaixa o conceito das chamadas PET's (*Privacy Enhancing Technologies*).

As PET's ou tecnologias de aprimoramento da privacidade consistem na utilização de técnicas que possibilitem a utilização do dado pessoal, sem que este esteja em seu estado puro, ou diretamente vinculado a um titular identificado ou identificável. Sem perder a funcionalidade, permite aumentar a privacidade dos usuários ao incluir estratégias de mascaramento, adição de ruídos, truncamentos, etc. Seu propósito é garantir o consumo dos dados e, ao mesmo tempo, reforçar a segurança dos dados pessoais, mitigando a estratégia regulatória caracterizada pelo foco no consentimento.³⁸⁴

³⁷⁹ SARLET; MOLINARO, **Questões tecnológicas, éticas...** *Op. cit.*, p. 190-193.

³⁸⁰ HOFFMANN-RIEM, **BIG DATA E INTELIGÊNCIA ARTIFICIAL...** *Op. cit.*, p. 487-488.

³⁸¹ CONSELHO NACIONAL DE JUSTIÇA. **Resolução n.º 332/2020, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 21 dez. 2022.

³⁸² PEIXOTO, **Direito e Inteligência Artificial...** *Op. cit.*, p. 44.

³⁸³ DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 308-309.

³⁸⁴ MENDES; FONSECA, **Proteção de dados para além do consentimento...** *Op. cit.*, p. 521.

Bioni menciona como um dos exemplos de PET's o DNT (*Do not track*). Esta solução permite ao titular, ainda no plano da coleta, escolher quais os tipos de informações podem ser coletados no seu navegador. Ao invés de controlar, aceitando, rejeitando ou deletando cookies em cada site, “bastaria o consumidor acionar um botão DNT para que automaticamente fosse exteriorizada sua escolha em barrar ou não a coleta dos seus dados”.³⁸⁵ Este tipo de tecnologia, entretanto, dependeria de uma abordagem de privacidade por concepção dos navegadores de busca. Considerando que dois, dos três mais utilizados (*Chrome* e *Edge*), pertencem a duas das maiores empresas de tratamento de dados (Google e Microsoft), existe séria descrença neste tipo de implementação.

Ademais, seria preciso que, além dos navegadores, os provedores de acesso também respeitassem este tipo de parametrização. Bioni finaliza que a falta cogência neste tipo de solução e que movimentos neste sentido requerem regulação para ter efeito.³⁸⁶ Ana Frazão acrescenta que os problemas relacionados à privacidade são tanto políticos e jurídicos como tecnológicos. O equacionamento requer a inclusão de múltiplos atores, estruturas e ferramentas. Empresas responsáveis por processos de tratamentos de dados devem auxiliar na criação de condições de gerenciamento da demanda de dados.³⁸⁷

Condições que para Hoffmann-Riem poderiam ser interfaces programáveis pelas quais os usuários pudessem administrar seus próprios dados. Os responsáveis pelos tratamentos seriam obrigados a fornecer estas customizações em seus sistemas.³⁸⁸ Recai-se, porém, no problema já citado da dificuldade da autogestão da privacidade e o dilema do consentimento. O usuário teria que administrar esses painéis com cada agente que troca dados pessoais. Em linha com o posicionamento de Daniel Solove, a forma isolada de gestão traz mais complexidades do que proteção à privacidade.³⁸⁹

A proposta, para escapar da complexidade da fragmentação do consentimento, seria a criação de *proxies* de interface, ou interfaces intermediárias, capazes de agrupar as preferências dos usuários, substituindo o gerenciamento individual por

³⁸⁵ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento.** *Op. cit.*, p. 174-175.

³⁸⁶ *Ibid.*

³⁸⁷ FRAZÃO, Ana. **Objetivos e alcance da Lei Geral de Proteção de Dados.** *Op. cit.*, p. 116-126.

³⁸⁸ HOFFMANN-RIEM, **BIG DATA E INTELIGÊNCIA ARTIFICIAL...** *Op. cit.*, p. 490.

³⁸⁹ SOLOVE, *Op. cit.*, p. 1882-1893.

meio de uma administração programática, tecnicamente viável, na qual o titular comporia suas decisões acerca dos tipos de dados e fluxos permitidos.³⁹⁰

A gestão global da privacidade, que valeria para todos os agentes de tratamento, reduziria o custo em micro gerenciar cada elemento de forma apartada. Ao mesmo que Daniel Solove apresenta esta proposta de autogestão parcial da privacidade, um questionamento surge: É possível um conjunto uniforme de opções de privacidade que faça sentido para qualquer agente de tratamento de dados? ³⁹¹

Crete da dificuldade em viabilizar este tipo de solução, uma alternativa, em linha oposta, é a redução da atribuição da responsabilidade ao indivíduo, ante o estabelecimento de regulações mais paternalistas que promovam o arranjo jurídico-normativo da autodeterminação informativa com a realidade latente, reconhecidamente de assimetria entre agente de tratamento e titular.

Solução que não passa ilesa a críticas, pois esta abordagem, segundo Solove, ignora o fato que alguns usuários podem desejar renunciar parte de sua privacidade na análise custo-benefício ao expor seus dados. O autor utiliza as próprias redes sociais como exemplo, apontando que, embora a autoexposição possa gerar consequências desastrosas, muitas pessoas recorrem a estes espaços com considerável sucesso e produtividade.³⁹²

Laura Mendes e Gabriel Fonseca corroboram ao afirmarem que o déficit do consentimento não pode servir de justificativa para uma posição puramente paternalista, uma vez que, além de violar a liberdade individual do titular, “a adoção desse raciocínio pode inviabilizar todo um mercado personalizado e inovador, no âmbito digital, e até mesmo a construção de políticas públicas balizadas por evidências empíricas”.³⁹³ Propõe os autores uma forma de autonomia para além de uma acepção formal.

Não se pode olvidar a existência de uma economia de vigilância e a dificuldade de controle do fluxo informacional pelo titular (como já debatido). Neste sentido, é razoável compreender que alguns autores enxerguem a viabilidade de uma solução mais paternalista. Plausível são também as objeções a este modelo, especialmente

³⁹⁰ SARLET; MOLINARO, **Questões tecnológicas, éticas...** *Op. cit.*, p. 193-194.

³⁹¹ SOLOVE, *Op. cit.*, p. 1902.

³⁹² *Ibid.*, p. 1895-1896.

³⁹³ MENDES; FONSECA, **Proteção de dados para além do consentimento...** *Op. cit.*, p. 519.

ao considerar os princípios e fundamentos das legislações de proteção de dados, como o direito à autodeterminação informativa.

Surge então a possibilidade de encaixe no que Cass Sunstein e Richard Thaler conceituaram como “paternalismo libertário”. Sob a ótica de que em muitos casos as preferências não são claras ou são fortemente influenciadas pelo contexto e, sem perder de vista a liberdade das escolhas individuais, o paternalismo libertário considera legítimo que instituições possam guiar as escolhas das pessoas. Enfatiza a possibilidade de que, sob determinadas circunstâncias, as pessoas podem tomar decisões piores para si próprias.³⁹⁴

Para os autores, é falsa a presunção de que as pessoas sempre fazem escolhas melhores do seu ponto de vista. Estas falhas comportamentais, que podem prejudicar o próprio bem-estar, são maiores em contextos em que os indivíduos são inexperientes, como, por exemplo, nos impactos e destinos futuros dos dados pessoais. Assim, estas instituições (no exemplo, o Estado) poderia auxiliar no processo de definição do melhor caminho.³⁹⁵ Ainda, ressaltam ser errada a concepção de que o paternalismo sempre envolve coerção.

Por meio de estudo de comportamento, Sunstein e Thaler demonstram que as pessoas fazem escolhas diferentes, sob o mesmo tema, dependendo do contexto e enquadramento oferecido. Também tendem a decidir com base em eventos recentes. “após um terremoto, a quantidade de seguros contra terremotos aumenta acentuadamente – mas declina regularmente a partir desse ponto, conforme as memórias mais frescas vão se apagando”.³⁹⁶ Por analogia, notícias de vazamentos de dados podem sugerir um comportamento mais reativo, ao passo que, com o passar do tempo, a permissão da coleta e tratamento aumente novamente.

O Estado poderia então utilizar ferramentas que direcionassem, estreitando os limites do consentimento em prol de um resultado mais benéfico ao titular. Esta interferência no processo da escolha não pode impedir as escolhas individuais, mas pode mover na direção que, por algum motivo, o titular teria dificuldade em enxergar sozinho.³⁹⁷

³⁹⁴ SUNSTEIN, Cass S.; THALER, Richard H. **O paternalismo libertário não é uma contradição em termos**. Trad. Fernanda Cohen. Civilistica.com. Revista eletrônica de direito civil. Rio de Janeiro: a. 4, n. 2, 2015. Disponível em: <http://civilistica.com/o-paternalismo-libertario-nao-e-uma-contradicao>. Acesso em: 27 jan. 2023. p. 3-4.

³⁹⁵ *Ibid.*, p. 5-8.

³⁹⁶ *Ibid.*, p. 12.

³⁹⁷ *Ibid.*, p. 17-20.

A independência funcional da Autoridade Nacional de Proteção de Dados – ANPD, promovida pela Lei n.º 14.460, permite que esta autarquia seja o ente responsável por estes controles e pela manutenção dos direitos dos titulares, principalmente nas situações em que o titular tenha ameaçada a tutela adequada. A dificuldade em estabelecer o nexo causal entre o tratamento dos dados e seus efeitos, a desproporção no tratamento e a exclusão dos acessos a serviços e bens, no caso de recusa em fornecer os dados, devem ser os imperativos de uma ANPD preocupada com a concretização da autodeterminação informativa.³⁹⁸ Isso pode incluir criação de limites e restrições para situações ou grupos específicos, sem que estas medidas sejam encaradas como diminuição ou violação da liberdade individual.

A LGPD, ao prever a necessidade de elaboração de relatórios de impactos, contendo a descrição de processos que podem gerar riscos às liberdades civis e aos direitos fundamentais, busca distribuir as responsabilidades aos controladores. Para Mendes e Fonseca, estas medidas, mais do que documentações de processos, representam a mentalidade regulatória voltada para prestação de contas na proteção de dados pessoais.³⁹⁹

Além disso, a criação destes limites materiais exerce a função de não permitir que os ideais do consentimento assumam características puramente formais, ou se tornem meio de legitimar o tratamento de dados pessoais. Pelo contrário, desempenham a função de revitalizá-lo como instrumento legítimo.⁴⁰⁰ Reforça-se novamente que não se trata de diminuir o papel protagonista do consentimento como instrumento de exercício de liberdade do titular, mas de permitir a criação de mecanismos que o assistam.

Limitações que, mais do que instrumentos técnicos de apoio a redefinição de forma de coleta e controle de fluxos, limitem opções de armazenamento ou até mesmo proibam tratamentos a tipos especiais de dados.⁴⁰¹ Considerando a relevância e proporcionalidade, assim como o princípio da boa-fé, deve-se prestar atenção

³⁹⁸ Doneda realça a importância de uma Autoridade Nacional de Proteção de Dados atuante ao afirmar que “o recurso a uma tutela baseada na responsabilidade civil não é, por si só, capaz de proporcionar proteção eficaz para o direito fundamental que representa a proteção de dados pessoais - como não o é, igualmente, a tutela exercida somente pela provocação do interessado ou a autorregulamentação pelo mercado. A ação de uma autoridade para a proteção de dados pessoais representa, portanto, a realização de uma garantia institucional”. DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. *Op. cit.*, p. 333-334.

³⁹⁹ MENDES; FONSECA, **Proteção de dados para além do consentimento...** *Op. cit.*, p. 522-523.

⁴⁰⁰ *Ibid.*, p. 525.

⁴⁰¹ HOFFMANN-RIEM, **BIG DATA E INTELIGÊNCIA ARTIFICIAL...** *Op. cit.*, p. 488.

particular ao propósito específico do processamento de dados. Análise de proporcionalidade e razoabilidade que é fundamental, pois em alguns momentos o uso de tais dados será tão legítimo como necessário.⁴⁰²

Outra preocupação em relação ao consentimento é sua perenidade. Apesar da LGPD possuir mecanismos de revogação, mediante manifestação do titular, ou até mesmo elencar hipóteses de término do tratamento de dados pessoais, a análise da conveniência fica a cargo do controlador, ou seja, o sujeito a quem a manutenção e controle dos dados beneficiam. Esse mecanismo de eliminação de dados precários favorece os agentes de tratamento na manutenção do *status quo* do controle e vigilância do indivíduo.⁴⁰³

O estudo da Federal Trade Commission – FTC mostrou que alguns *data brokers* não possuem a prática de eliminar dados, pois para estes mercados a finalidade de tratamento nunca se encerra. Na pesquisa, alguns rebatem que a manutenção do dado pessoal por tempo indeterminado é importante para construção de uma base histórica e conseqüentemente de mais precisão na análise do cliente.⁴⁰⁴ Este comportamento, além de gerar riscos de segurança para os titulares, viola a determinação de término de tratamento de dados, não respeita o direito do titular em receber do controlador a forma e duração do tratamento e não observa princípios das legislações de proteção de dados.⁴⁰⁵

A criação destes processos de determinação da duração ou da renovação do consentimento, apesar de alinhar-se a concepção da liberdade de escolha individual,

⁴⁰² Os autores citam um nítido exemplo de aplicação correta do critério de razoabilidade, qual seja, a obtenção de dados de geolocalização de celulares visando encontrar pessoas desaparecidas em desastres ou que possam ter sido sequestradas ou estar desaparecidas. TEFFÉ; FERNANDES, *Op. cit.*, p. 301-310.

⁴⁰³ O *Facebook*, em sua política de privacidade, divulga que mantém os dados pessoais pelo tempo necessário para oferecer seus produtos, cumprir as obrigações legais, proteger seus interesses ou os de terceiros. A empresa determina o tempo de armazenamento conforme o tipo de dado. Menciona como exemplo que mantém pelo prazo de seis meses históricos de pesquisa. Em outros casos, e por razões especificadas pela empresa, mantém as informações por um período prolongado. Este período não é determinado e dentre as razões estão algumas genéricas como segurança e integridade. Meta. **Central de Privacidade**, 2023. Disponível em: <https://www.facebook.com/about/privacy>. Acesso em: 31 jan. 2023.

⁴⁰⁴ RAMIREZ *et al*, **Data Brokers - A Call for Transparency and Accountability**. *Op. cit.*, p. 14.

⁴⁰⁵ O guia orientativo da ANPD, ao abordar a duração do tratamento, determina que “o instrumento que autoriza ou formaliza o compartilhamento deve estabelecer, de forma expressa, o período de duração do uso compartilhado dos dados, além de esclarecer, conforme o caso, se há a possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento”. ANPD – Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público - Guia Orientativo**. *Op. cit.*, p. 18-19.

podem recair no mesmo problema da dificuldade do titular em medir os custos de certas formas de coleta, devido ao mencionado grau de incertezas sobre o uso dos mesmos dados no futuro. Por outro lado, o consentimento para uso eterno do dado pessoal é igualmente indesejável. Para Solove, é necessária alguma forma de delimitação para utilização futura. Algumas hipóteses deveriam ser restringidas, algumas limitadas e outras deveriam ser precedidas de um novo aceite do titular do dado.⁴⁰⁶

Ressignificar o consentimento, no intuito de acomodar os parâmetros inconstantes e complexos destas novas relações na sociedade, é papel do Estado.⁴⁰⁷ Reafirma-se a necessidade do debate a respeito do poder associado ao acesso dos dados pessoais. Compete ao poder público mitigar o poder de influência e consequente controle que possa limitar as liberdades civis. O direito deve ser usado como meio para fornecer e conceder proteção.

⁴⁰⁶ “What is needed is for the law to weigh in and provide guidance about the types of new uses at the time they are proposed. Perhaps some ought to be restricted outright, some ought to be limited, some ought to require new consent, some ought to be permitted but with a right to revoke consent, and some ought to be permitted without new consent. Perhaps an agency should review proposals for new uses as they arise.” SOLOVE, *Op. cit.*, p. 1902.

⁴⁰⁷ SARLET; MOLINARO, **Questões tecnológicas, éticas...** *Op. cit.*, p. 207.

CONCLUSÃO

O inegável impacto das tecnologias nas liberdades individuais e a percepção da inevitabilidade da vida sem os serviços digitais fazem emergir a necessidade de uma leitura sob o prisma dos direitos fundamentais envolvidos. O efeito sobre a privacidade dos indivíduos ganha novos contornos com sua robustez, transversalidade e ubiquidade.

O reconhecimento de um direito fundamental à proteção de dados é condizente em um cenário de riscos de coleta, análise e compartilhamentos de dados pessoais. Ao se valer do conceito de capitalismo de vigilância de Shoshana Zuboff como um processo que reivindica as experiências humanas como matéria-prima, surge o mercado comportamental, no qual o consumidor atua como um assistente de vendas sem custo. Suas transações, preferências e opiniões são transacionadas. As tecnologias avançadas de *big data* e inteligência artificial passam a ter capacidade de acumular estas experiências e delas extrair resultado.

Panorama que pode revelar detalhes mais íntimos da esfera privada e que não aponta para uma diminuição destes tratamentos. Pelo contrário, tendem a crescer e produzir resultados mais inesperados. Crítica destes modelos, Cathy O'Neil afirma que estes programas podem restringir acessos, oportunidades e tolher direitos. Violações que atingem, além do direito fundamental à proteção dos dados pessoais e o direito à privacidade, o direito à personalidade.

A influência destes fenômenos no direito à personalidade parte da premissa que nos direitos da personalidade o objeto recai sobre seu titular de forma indissociável. Assim, os dados pessoais não só se caracterizam como um prolongamento do indivíduo, mas interferem na dimensão social do ser humano. Ato contínuo, a privacidade também comporta uma elasticidade, com a compreensão de que não se trata mais somente de uma visão negativa e estática. Dentre sua pluralidade de manifestações, está poder do indivíduo em determinar quem terá acesso e qual o fluxo de suas informações pessoais.

Por isso, o direito à proteção dos dados pessoais reclama uma construção jurídica própria, que não se reduz a uma evolução do direito à privacidade. Provoca a ordem jurídica a se reorganizar e assegurar proteção adequada, dado o quadro assimétrico de poder entre titulares e agentes de tratamento. Razão pela qual, torna-

se inadequado atribuir natureza comercial aos dados pessoais. Tal direcionamento somente reforçaria a vulnerabilidade do titular frente as grandes empresas do mercado tecnológico.

Ao elevar o direito à proteção de dados pessoais à categoria de direito fundamental, a Emenda Constitucional n.º 115/2022 adicionou valor substancial à proteção de dados no Brasil, reconhecendo que a tutela da privacidade, de forma negativa, não era mais suficientemente adequada em razão da amplitude que os dados tomaram na sociedade. Abraçou ainda o direito à autodeterminação informativa ao admitir um poder positivo e dinâmico ao titular em controlar seus dados pessoais.

Nessa direção, a Lei Geral de Proteção de Dados, como principal instrumento de proteção de dados pessoais no ordenamento jurídico nacional, disciplina o uso e a integridade dos dados pessoais, que são aqueles que permitem identificar ou tornar identificável uma pessoa. Esta caracterização permite a LGPD diferenciar dados pessoais de dados anonimizados. Ponto este que a pesquisa apresentou uma nova problemática.

Ao admitir que novas técnicas de agregação de dados com tecnologia de *big data* possam reidentificar o sujeito, a diferenciação jurídica destas categorias na LGPD não poderia existir. A saída adotada por alguns autores como Ricardo Bioni é a adoção do critério de razoabilidade, uma vez que a própria LGPD alude que o processo de anonimização deve considerar os esforços razoáveis, como tempo e custo, necessários para reverter o processo de anonimização.

Por mais que a LGPD não possa endereçar todos os problemas resultantes da manipulação de dados indevidas pelos agentes de tratamento, oferece um conjunto de regras e princípios sólidos para proteção dos seus fundamentos, dentre os quais, o respeito à privacidade, e à autodeterminação informativa.

Dentre os pontos que suscitam dúvidas quanto a eficácia da proteção de dados de seus titulares, a pesquisa objetivou analisar a hipótese de tratamento de dados mediante o fornecimento de consentimento pelo titular. Este consentimento é adjetivado (no art. 5º, XII da LGPD) como uma manifestação livre, informada e inequívoca. Esta exigência, ao mesmo tempo que reforça a centralidade acerca do processo decisório no indivíduo, também pode assumir um papel meramente formal.

O ponto levantado é se o consentimento, ao invés de servir de abrigo ao direito fundamental à proteção de dados pessoais, pelo contrário, não legitima o tratamento

de dados pelo Estado e pelo mercado, diante de algumas insuficiências que comprometem que a manifestação seja livre, informada e inequívoca.

Dentre elas, as limitações de avaliação dos riscos e benefícios na cessão dos dados pessoais, a lógica do mercado “*take it or leave it*”, pela qual o titular concorda com o compartilhamento de suas informações ou é impedido de ter acesso ao serviço e, ainda, as técnicas de agregação de dados, que dificultam a tomada de decisão do titular pela insuficiência de informações técnicas a respeito das possibilidades de combinações futuras de dados.

De antemão, a pesquisa mostrou que não tem por finalidade desconstruir a importância do instituto do consentimento, mas avaliou cada um de seus adjetivos com a intenção de identificar em que circunstâncias, o direito do titular não tem sido suficientemente atendido, na medida que um consentimento adequado é aquele em que se respeita a autonomia na autorização ou não do tratamento de dados.

O consentimento livre foi definido como aquele resultante da possibilidade de escolha ou recusa de utilização dos seus dados pessoais, sem circunstâncias que, de qualquer forma, impeçam ou limitem a decisão. A ideia de uma ação espontânea que poderia ser tomada frente a tantas outras disponíveis ao titular. Portanto, quando condições de uso são impostas aos usuários e o não aceite implica na exclusão dos serviços oferecidos, o consentimento perde a característica de livre, principalmente quando o bem é essencial para exercícios de outros direitos ou liberdades.

O consentimento será considerado informado quando o titular receber, previamente a coleta, informações necessárias e suficientes para avaliar a forma como serão tratados seus dados. Este dever-direito se estende com a exigência de capacitação do cidadão para que um controle efetivo seus dados. Uma das dificuldades neste ponto está em supor que o titular possa realizar a autogestão de sua privacidade ao nível adequado, diante das inúmeras interações no ambiente digital. Está ainda em presumir que, conforme Gabrielle Sarlet, a sociedade estruturada sob a forma de rede se trata de um ambiente absolutamente neutro.

Por fim, o consentimento inequívoco reclama que não paire dúvidas sobre a declaração de vontade do titular. Políticas de privacidade complexas, extensas, em linguagem técnica dificultam sua leitura pelo cidadão e, não raras vezes, sequer são lidas, implicando na necessidade de busca por novas formas de comunicação e obtenção do aceite.

Diante deste contexto, em que a racionalidade da proteção de dados exige um controle prévio ao tratamento, os diplomas específicos de proteção de dados trouxeram noções de responsabilização, prestação de contas e privacidade por padrão. Combinadas com tecnologias de privacidade, algumas propostas de estabelecimento do chamado consentimento contextual ganham espaço, entendendo que o estreitamento dos limites pode ser uma alternativa viável, sem que impeça escolhas individuais, mas conduza o direito à proteção de dados pessoais para caminhos que o titular teria dificuldade em enxergar sozinho.

Acomodar estes parâmetros inconstantes e complexos destas novas relações na sociedade significa compreender a dinamicidade da proteção de dados. Contudo, não se pode perder de foco que, persiste o direito do titular ao controle sobre o seu fluxo informacional. Este discurso de ambivalência, ora apostando na autogestão da privacidade, ora criando uma zona de interferência, deve ser mediada por princípios da boa-fé, pela proporcionalidade e razoabilidade.

Essa dificuldade no estabelecimento de formulação de perspectivas mais complexas, que conduzam a um direito à proteção de dados pessoais mais eficaz, abre espaço para ampliação do campo de pesquisa. Estratégias adequadas que mitiguem as insuficiências mencionadas ao longo de pesquisa podem ser objetos de novos estudos. O aprimoramento das legislações, ainda em estágios iniciais, a adaptação de novas tecnologias e a criação de parâmetros específicos para limitação do tratamento (temporais ou substantivos) carecem e merecem aprofundamento.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros Editores, 2009.

ANDRADE, José Carlos Vieira de. **Os direitos fundamentais na Constituição Portuguesa de 1976**, 5ª. ed. Almedina: Coimbra, 2012.

ANPD – Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público - Guia Orientativo**. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 17 jul. 2022.

BERBERI, Marco Antonio Lima, DISRUPÇÃO TECNOLÓGICA E PRIVACIDADE: ALGUMAS REFLEXÕES SOBRE O AMANHÃ, in: ALVITES, Elena Cecilia et al (Orgs.), **Direitos Fundamentais & Democracia: novas abordagens na perspectiva interamericana**, Porto Alegre, RS: Editora Fundação Fênix, 2022, p. 353–365.

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: Em busca do consentimento válido, in: DONEDA, Danilo *et al* (Orgs.). **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 149–161.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**; Editora Forense, 3. ed.; São Paulo, 2021.

BITTENCOURT, Rui Carlos Sloboda; BERBERI, Marco Antônio Lima, Do compartilhamento da economia à fragmentação da privacidade do trabalhador 4.0. In: CAMOLENO, Cassiana Gomes; BERBERI, Marco Antônio Lima (coord.). **Direitos fundamentais e tecnologia**. Curitiba: Editora Íthala, 2020. p. 11-26.

BRASIL. IBGE - Instituto Brasileiro de Geografia e Estatística. **Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua**. Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2019. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf. Acesso em: 25 mar. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei n.º 2.796, de 4 de novembro de 1980**. Assegura aos cidadãos acesso às informações sobre sua pessoa constantes de bancos de dados e dá outras providências. Brasília: Câmara dos Deputados, 1980. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 7 jul. 2022.

_____. Constituição 1988. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 19 jun. 2022.

_____. **Lei n.º 12.414, de 09 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: 2 jun. 2022.

_____. **Lei n.º 12.965, de 23 de abril de 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: 4 jun. 2022.

_____. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jul. 2022.

_____. **Lei n.º 13.853, de 8 de julho de 2019.** Altera a Lei n.º 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 23 jul. 2022.

_____. **Lei n.º 14.460, de 25 de outubro de 2022.** Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em: 21 dez. 2022.

_____, Superior Tribunal de Justiça. **Súmula 550.** A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. RSSTJ vol. 45 p. 323, out. 2015. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?livre=550&b=SUMU>. Acesso em: 4 jul. 2022.

_____, Superior Tribunal de Justiça. **REsp. 22.337 / RS.** Serviço de proteção ao crédito. Cancelamento do registro. Prazo (cinco anos). O registro de dados no SPC deve ser cancelado após cinco anos. Art. 43, parágrafo 1, do Código de Defesa do Consumidor (Lei 8.078/90). RSTJ vol. 77 p. 205, mar. 1995. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=22337&b=ACOR>. Acesso em: 7 jul. 2022.

_____, Supremo Tribunal Federal. **ADI n.º 6.387/DF.** Relator: Ministra Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 8 jul. 2022.

_____. Câmara dos Deputados. **Projeto de Lei n.º 1.229/2021.** Modifica a Lei n.º 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. Brasília: Câmara dos

Deputados, 2021. Disponível em:

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2276604>. Acesso em: 21. mai. 2021.

_____. Constituição (1988). **Emenda Constitucional n.º 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. Brasília, 2022. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 jul. 2022.

CAMURÇA, Lia Carolina Vasconcelos; MATIAS, João Luís Nogueira, **Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a lei n.º 13.709, de 14 de agosto de 2018**. Revista Direitos Fundamentais & Democracia, v. 26, p. 6–23, 2021. Disponível em: <https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1590/692>. Acesso em: 10 mar. 2022.

CARVALHO, Alexander Perazo Nunes de; LIMA, Renata Albuquerque. **A Eficácia Horizontal dos Direitos Fundamentais**, Revista Opinião Jurídica, v. 13, n. 17, p. 11–23, 2015. Disponível em: <https://periodicos.unichristus.edu.br/opiniojuridica/article/view/469/187>. Acesso em: 21 jun. 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros - TIC Domicílios 2020** (Edição COVID-19 - Metodologia adaptada). Disponível em: <https://www.cetic.br/pt/tics/domicilios/2020/domicilios/A4/>. Acesso em: 25 mar. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução n.º 332/2020, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Diário da Justiça do Conselho Nacional de Justiça, Brasília, DF, n. 274, p. 4-8, 25 ago. 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 21 dez. 2022.

CORRÊA, Adriana Espíndola. **Consentimento livre e esclarecido: o corpo objeto de relações jurídicas**. 1. ed. Florianópolis: Conceito, 2010.

CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado**. Revista Faculdade de Direito - UFPR, v. n. 47, p. 141–153, 2008.

COUNCIL OF EUROPE. European Treaty Series. **Details of Treaty No.108**. Disponível em: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>. Acesso em: 21 jul. 2022.

CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo digital na implementação de serviços públicos para a**

concretização de direitos sociais no Brasil. Sequência: Estudos Jurídicos e Políticos, v. 41, n. 84, p. 209–242, 2020. Disponível em: <https://doi.org/10.5007/2177-7055.2020v43n84p209>. Acesso em: 25 mar. 2022.

CUEVA, Ricardo Villas Bôas, A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça, in: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**, 1 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 85–98.

_____. **Anonimização e pseudonimização de dados pessoais no processo eletrônico.** In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). O Direito Civil na Era da Inteligência Artificial. 1 ed. São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2020. p. 249-260.

DÖHMANN, Indra Spiecker Gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia, in: DONEDA, Danilo et al (Orgs.). **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 97–113.

DONEDA, Danilo, **A proteção dos dados pessoais como um direito fundamental**, Espaço Jurídico, v. 12, n. 2, p. 91–108, 2011.

_____. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**, 3 ed. São Paulo: Thomson Reuters Brasil, 2021.

_____. Panorama Histórico da Proteção de Dados Pessoais, in: Danilo Doneda et al. **Tratado de Proteção de Dados Pessoais**, Editora Forense Ltda. Rio de Janeiro - RJ, 2021. p. 3–20.

DONEDA, Danilo Cesar Maganhoto et al. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal.** Pensar - Revista de Ciências Jurídicas, Fortaleza, v. 23, n. 04, p. 1–17, 2018. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257>. Acesso em: 16 jul. 2022.

EMPOLI, Giuliano Da. **Os engenheiros do caos**; tradução: Arnaldo Bloch. 1. ed.; 3. reimp - São Paulo; Vestígio, 2020. Título original: Les ingénieurs du chaos.

EUROPEAN UNION (EU). European Commission. **Ethics guidelines for trustworthy AI.** Report / Study. Publication 08 April 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. Acesso em: 21 mai. 2022.

_____. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04>. Acesso em: 22 jul. 2022.

FILHO, Carlos Edison do Rêgo Monteiro; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709/2018), in:

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019, p. 323–345.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019. p. 23-52.

_____. **Capitalismo de vigilância e black box society. A vigilância constante e a ausência de transparência como desafios para a regulação jurídica**. 2019. p. 1-5. Disponível em: <https://www.jota.info/opiniao-e-analise/columnas/constituicao-empresa-e-mercado/capitalismo-de-vigilancia-e-black-box-society-28022019>. Acesso em: 09 abr. 2022.

_____. Objetivos e alcance da Lei Geral de Proteção de Dados, in: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 99–129.

FRAZÃO, Ana; GOETTENAUER, Carlos. O jogo da imitação jurídica: o direito à revisão de decisões algorítmicas como um mecanismo para a necessária conciliação entre linguagem natural e infraestrutura Matemática. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). **O Direito Civil na era da inteligência artificial**. São Paulo: Revista dos Tribunais, 2020. p. 45-63.

FUCHS, Christian, **Mídias Sociais e a Esfera Pública**, Revista Contracampo. Niterói, Rio de Janeiro v. 34, n. 3, ed. dez/2015-mar/2016. Disponível em: <https://periodicos.uff.br/contracampo/article/view/17552>. Acesso em: 23 mar. 2022.

HAN, Byung-Chul. **Infocracia: digitalização e a crise da democracia**. tradução de Gabriel S. Philipson. Petrópolis, RJ: Editora Vozes, 2022.

HARARI, Yuval Noah. **Homo Deus: Uma breve história do amanhã**. Tradução de Paulo Geiger. 1ª ed. São Paulo: Companhia das Letras, 2016. Título original: Homo Deus: A Brief History of Tomorrow.

_____. **21 lições para o século 21**. Tradução de Paulo Geiger. 1ª ed. São Paulo: Companhia das Letras, 2018. Título original: 21 Lessons for the 21st Century.

HESS, Heliana Maria Coutinho. Apontamentos sobre o princípio da proporcionalidade na Alemanha e no Brasil – aplicações ao Direito midiático. In: PRETTO, Renato Siqueira De; KIM, Richard Pae; TERAOKA, Thiago Massao Cortizo (Orgs.). **Interpretação Constitucional no Brasil**. [s.l.]: Escola Paulista da Magistratura, 2017, p. 271–296. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ic11.pdf>. Acesso em: 14. abr. 2022.

HOFFMANN-RIEM, Wolfgang, **BIG DATA E INTELIGÊNCIA ARTIFICIAL:**

DESAFIOS PARA O DIREITO, Revista Estudos Institucionais, v. 6, n. 2, p. 431–506, 2020.

HONG, Sun-há. Control Creep: **When the Data Always Travels, So Do the Harms**. Center for International Governance Innovation, 2021. Disponível em: <https://www.cigionline.org/articles/control-creep-when-data-always-travels-so-do-harms/>. Acesso em: 01 abr. 2022.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. **Measuring digital development: Facts and figures 2021**. Place des Nations CH-1211 Geneva Switzerland, 2021 Disponível em: <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx> Acesso em: 25 mar. 2022.

KONDER, Carlos Nelson; KONDER, Cíntia Muniz de Souza. Transumanismo e inteligência artificial. In: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (Orgs.). **O Direito Civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, p. 103–120.

LEAL, Livia Teixeira. **Internet of Toys: Os brinquedos conectados à internet e o direito da criança e do adolescente**. Revista Brasileira de Direito Civil, Belo Horizonte. v. 12, p. 175-187, abr./jun. 2017. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/38/32>. Acesso em: 07 mai. 2022.

LONGHI, João Victor Rozatti, Marco Civil da Internet no Brasil: Breves considerações sobre seus fundamentos princípios e análise crítica do regime de responsabilidade civil, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Orgs.), **Direito Digital: direito privado e internet**, 2 ed. Indaiatuba, SP: Editora Foco, 2019, p. 123-154.

MACHADO, Diego Carvalho et al. **GDPR and its effects on the Brazilian Law: First impressions and a comparative analysis**. Institute for Research on Internet and Society: Belo Horizonte, jun 2018. Disponível em: <https://irisbh.com.br/en/publicacoes/gdpr-and-its-effects-on-the-brazilian-law/>. Acesso em: 23 mar. 2022.

MAIA, Roberta Mauro Medina, A titularidade de dados pessoais previstas no art. 17 da LGPD: direito real ou pessoal? in: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.), **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 131–156.

MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. **Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais**. Revista do Ministério Público do Estado do Rio de Janeiro, n.º 78, p. 157-164, 2020.

_____. **PROTEÇÃO DE DADOS E ANONIMIZAÇÃO: PERSPECTIVAS À LUZ DA LEI Nº 13.709/2018**. Revista Estudos Institucionais, v. 7, p. 376–397, 2021.

MATTIUZZO, Marcela, “**Let the algorithm decide**”: is human dignity at stake? Revista Brasileira de Políticas Públicas, v. 11, n. 1, p. 343–370, 2021.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. **Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro**. *Justiça do Direito*. v. 34, n.2, 2020. Disponível em: <http://seer.upf.br/index.php/rjd/article/view/11038>. Acesso em: 20 mar. 2022.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. **Proteção de dados para além do consentimento: tendências contemporâneas de materialização**. *Rei - Revista Estudos Institucionais*, v. 6, n. 2, p. 507–533, 2020.

MENDES, Laura Schertel; JUNIOR, Otavio Luiz Rodrigues; FONSECA, Gabriel Campos Soares da, O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: Rumo a um Direito Fundamental Autônomo, in: DONEDA, Danilo et al (Orgs.), **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 61–71.

MENDES, Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito**, *Revista de Ciências Jurídicas*, v. 25, n. 4, p. 1–18, 2020.

MOURA, Ariel. **Constitucionalismo Digital**. IX CONGRESSO INTERNACIONAL DA ABRASD - Associação Brasileira de Pesquisadores em Sociologia do Direito. 2018. p. 925-938. Disponível em: https://www.academia.edu/38515467/CONSTITUCIONALISMO_DIGITAL. Acesso em: 03 jun. 2022.

NAÇÕES UNIDAS. Assembleia Geral. **Declaração universal dos direitos humanos**. Rio de Janeiro: UNIC, 2009. Publicado originalmente em 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos> Acesso em: 7 jul. 2022.

NETO, Elias Jacob de Menezes; MORAIS, Jose Luis Bolzan de. **A fragilização do estado-nação na proteção dos direitos humanos violados pelas tecnologias da informação e comunicação**. *Revista Direitos Fundamentais & Democracia*, v. 23, n. 3, 2018. Disponível <https://doi.org/10.25192/issn.1982-0496.rdfd.v23i31135>. Acesso em: 10 fev. 2022.

NISSENBAUM, Helen. **A Contextual Approach to Privacy Online**. New York University; Cornell Tech, p. 32–48, 2011. Disponível em: <https://ssrn.com/abstract=2567042>. Acesso em: 30 nov. 2022.

NUNES, Luiz Felipe, **Os desafios da democracia participativa: o desenvolvimento da sociedade da informação e a necessária inclusão de grupos sociais desfavorecidos ou marginalizados**. *Anais da VII Jornada de Direitos Fundamentais*, v. 1, 2020. Disponível em: <https://unifor.br/web/pos-graduacao/jornada-de-direitos-fundamentais/atual>. Acesso em: 03 jun. 2022.

OECD - Organisation for Economic Co-operation and Development. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 21 jul. 2022.

OLK, Christopher; GRAFENSTEIN, Max von; WERNICK, Alina. **Data Governance: Enhancing Innovation and Protecting Against Its Risks**. Intereconomics. v. 54, n.4, 2019. p. 228–232. Disponível em: <https://www.intereconomics.eu/contents/year/2019/number/4/article/data-governance-enhancing-innovation-and-protecting-against-its-risks.html>. Acesso em: 01 abr. 2022.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019. p. 53-83.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. tradução Rafael Abraham. 1. ed. Santo André, SP; Editora Rua do Sabão, 2020. Título original: Weapons of math destruction: how big data increases inequity and threatens democracy.

ORTIZ, Elaine; Sergio Amadeu da Silveira. Redes sociais, censura privada e modulação. In: **Ciberpolítica, ciberativismo e cibercultura**. 37º Encontro Anual da ANPOCS. Águas de Lindóia, 2013. Disponível em: <https://anpocs.com/index.php/papers-37-encontro/st/st27/8579-redes-sociais-censura-privada-e-modulacao/file>. Acesso em: 20 fev. 2022.

PASQUALE, Frank. **The black box society : the secret algorithms that control money and information**. Cambridge, Massachusetts London, England: Harvard University Press, 2015.

PEIXOTO, Fabiano Hartmann. **Direito e Inteligência Artificial: referenciais básicos com comentário a resolução CNL 332/2020**. Brasília: Ed. do Autor, 2020.

PEREIRA, Robson Pascoal; LORENZETTO, Andrei Meneses. **Inteligência artificial e modelos de decisão automáticos: o enviesamento dos algoritmos**. Anais da VIII Jornada de Direitos Fundamentais 2021. Rede Interamericana de Direitos Fundamentais e Democracia, 2022. Disponível em: https://reddidd.com/files/2021/2021GT03_008.pdf. Acesso em: 14 abr. 2022.

POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. **Governança Global da Internet, Conflito de Leis e Jurisdição**. Instituto de Referência em Internet e Sociedade, Belo Horizonte. 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/Governanca_global_da_internet_IRIS.pdf. Acesso em: 20 mar. 2022.

RAMIREZ, Edith et al, **Data Brokers - A Call for Transparency and Accountability, Federal Trade Commission**, 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 16 jun. 2022.

RIBEIRO, Claudio José Silva. **Big Data: os novos desafios para o profissional da**

informação. Informação & Tecnologia (ITEC): João Pessoa/Marília, v.1. p. 96-105, jan./jun., 2014. Disponível em: https://www.brapci.inf.br/_repositorio/2015/12/pdf_616d318e35_0000015108.pdf. Acesso em: 03 abr. 2022. p. 99.

RODOTÀ, Stefano, **Democracia y protección de datos**, Cuadernos de Derecho Público, v. 19–20, 2003.

_____. **A vida na sociedade da vigilância - a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

_____. **Perché Internet ha bisogno di una propria Costituzione.** La Repubblica, Italian Tech. 2014. Disponível em: https://www.repubblica.it/tecnologia/2014/03/15/news/perch_internet_ha_bisogno_di_una_propria_costituzione-81045633. Acesso em: 18 jun. 2022.

RODRIGUES, Juciana. **Anonimização como forma de proteção de dados.** Associação Brasileira de Ciências de Dados – ABRACD. 2020. Disponível em: <https://abracd.org/anonimizacao-como-forma-de-protecao-de-dados/>. Acesso em: 28 jul. 2022.

ROSSONI, Caroline; BOLESINA, Iuri, **A teoria dos círculos concêntricos e a proteção à vida privada: análise ao caso Von Hannover vs. Alemanha, julgado pela corte europeia de direitos humanos.** XI Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea - VII Mostra de Trabalhos Jurídicos Científicos, 2004. Disponível em: <https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/11672>. Acesso em: 19 jun. 2022.

SARLET, Gabrielle Bezerra Sales. **Notas sobre a identidade digital e o problema da herança digital: uma análise jurídica acerca dos limites da proteção póstuma dos direitos da personalidade na internet no ordenamento jurídico brasileiro.** Revista de Direito Civil Contemporâneo, v. 17, n. 5, p. 33–59, 2018.

_____. **A Inteligência Artificial no Contexto Atual: uma Análise à Luz das Neurociências Voltada para uma Proposta de Emolduramento Ético e Jurídico.** Revista de Direito Público, v. 18, 2022. p. 272–305. Disponível em: <https://doi.org/10.11117/rdp.v18i100.5214>. Acesso em: 30 mar. 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, 2019. Disponível em: https://run.unl.pt/bitstream/10362/94969/1/O_consentimento_informado_e_a_protecao_de_dados.pdf. Acesso em: 20. out. 2022.

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.** Revista Brasileira de Direitos Fundamentais & Justiça, v. 13, n. 41, p. 183–212, 2020. Disponível em:

<https://dfj.emnuvens.com.br/dfj/article/download/811/964>. Acesso em: 30. nov. 2022.

SARLET, Gabrielle Bezerra Sales; Regina Linden Ruaro. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018**. Revista de Direitos Fundamentais e Democracia, v. 26, p. 81–106, 2021. Disponível em: <https://revistaeletronicardfd.unibrazil.com.br/index.php/rdfd/article/view/2172/694>. Acesso em: 10 mar. 2022.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 11. ed. rev. atual. Porto Alegre: Livraria do Advogado Editora, 2012.

_____. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**, Direitos Fundamentais & Justiça, v. n. 42, 2020. p. 179–218.

_____. Fundamentos Constitucionais: O direito fundamental à proteção de dados, in: Danilo Doneda et al. **Tratado de Proteção de Dados Pessoais**, Editora Forense Ltda. Rio de Janeiro - RJ, 2021. p. 21–59.

SARMENTO, Daniel. **A liberdade de expressão e o problema do “hate speech”**. Revista de Direito do Estado, Rio de Janeiro, ano 1, n. 4, 2006.

SCHMIDT NETO, André Perin. **O livre-arbítrio na era do Big Data**. 1. ed. São Paulo: Tirant lo Blanch, 2021.

SCHOPENHAUER, Arthur. **O livre-arbítrio**. Biografia e prefácio de Afonso Bertagnoli; tradução de Lohengrin de Oliveira. [Ed. Especial]. Rio de Janeiro: Editora Nova Fronteira, 2012. Disponível em: <https://amz.onl/6oPyhGD>. Acesso em: 10 jan. 2023.

SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências, in: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters, 2019, p. 367–415.

SILVA, Denis Franco, **Do humano ao pós-humano: pessoa e autonomia privada no contexto do aperfeiçoamento biônico**, Tese de doutorado. Rio de Janeiro: Programa de Pós-Graduação em Direito do Departamento de Direito da PUC-Rio, maio de 2009. Disponível em: <https://doi.org/10.17771/PUCRio.acad.15041>. Acesso em: 08 mai. 2022.

SILVA, Gabriela Buarque Pereira; JUNIOR, Marcos Ehrhardt, **Diretrizes éticas para a inteligência artificial confiável na União Europeia e a regulação jurídica no Brasil**, Revista IBERC, v. 3, n. 3, p. 1–28, 2020. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/133>. Acesso em: 21 mai. 2022.

SOLOVE, Daniel J. **INTRODUCTION: PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA**. Harvard Law Review, v. 126, 2013. p. 1880–1903.

SUNSTEIN, Cass S.; THALER, Richard H. **O paternalismo libertário não é uma contradição em termos**. Trad. Fernanda Cohen. Civilistica.com. Revista eletrônica de direito civil. Rio de Janeiro: a. 4, n. 2, 2015. Disponível em: <http://civilistica.com/o-paternalismo-libertario-nao-e-uma-contradicao>. Acesso em: 27 jan. 2023.

SUZOR, Nicolas. **Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms**. Queensland University of Technology (QUT) School of Law, 2018.

STRANDBURG, Katherine J., **Free Fall: The Online Market's Consumer Preference Disconnect** (October 1, 2013). 2013 University of Chicago Legal Forum 95, NYU School of Law, Public Law Research Paper N°. 13-62, NYU Law and Economics Research Paper N°. 13-34. Disponível em: SSRN: <https://ssrn.com/abstract=2323961>. Acesso em: 21 mar. 2022.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad, Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites, In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). **O Direito Civil na era da inteligência artificial**. 1 ed. São Paulo: Thomson Reuters Brasil – Revista dos Tribunais, 2020. p. 283-315.

TEPEDINO, Gustavo; GUIA SILVA, Rodrigo da. **Desafios da inteligência artificial em matéria de responsabilidade civil**. Revista Brasileira de Direito Civil – RBDCivil. Belo Horizonte, v. 21, p. 61-86, jul./set. 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **O consentimento na circulação de dados pessoais**. Revista Brasileira de Direito Civil - RBDCivil, v. 25, p. 83–116, 2020.

TEPEDINO, Gustavo, **A tutela da personalidade no ordenamento civil-constitucional brasileiro**, Rio de Janeiro: Renovar, 2008. Disponível em: https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil_constitucional_brasileiro. Acesso em: 16 jun. 2022.

UNIÃO EUROPEIA, **Carta dos Direitos Fundamentais da União Europeia**. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 02 jul. 2022.

UNIÃO EUROPEIA. EUR-Lex. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 21 jul. 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: Estudo sobre as bases legais dos artigos 7.º e 11, in: DONEDA, Danilo et al.

(Orgs.). **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Editora Forense, 2021, p. 117–148.

YOUNAS, M. **Research challenges of big data**. SOCA v. 13, p. 105–107, 2019. Disponível em: <https://doi.org/10.1007/s11761-019-00265-x>. Acesso em: 03 abr. 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução: George Schlesinger. 1. ed. - Rio de Janeiro: Intrínseca, 2020. Título original: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review. v. 4, n. 5 1890, p. 193-220. Disponível em: <https://www.jstor.org/stable/1321160?seq=1>. Acesso em: 19 jun. 2022.