UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ
INSTITUTO DE ESTUDOS EM DIREITO E SOCIEDADE – IEDS
FACULDADE DE DIREITO – FADIR

ELLYDA LAYANNA DA SILVA LANDIM

LEI GERAL DE PROTEÇÃO DE DADOS:
A VALIDADE DO CONSENTIMENTO E A REAL ANUÊNCIA DO TITULAR DE DADOS FRENTE AO ORDENAMENTO JURÍDICO BRASILEIRO

MARABÁ
2022

ELLYDA LAYANNA DA SILVA LANDIM

LEI GERAL DE PROTEÇÃO DE DADOS:
A VALIDADE DO CONSENTIMENTO E A REAL ANUÊNCIA DO TITULAR DE DADOS FRENTE AO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso, apresentado à Faculdade de Direito do Instituto de Estudos em Direito e Sociedade da Universidade Federal do Sul e Sudeste do Pará, como requisito para obtenção do grau de Bacharel em Direito.

Orientadora: Prof. Dra. Gabriela Natacha Bechara

MARABÁ

2022

Dados Internacionais de Catalogação na Publicação (CIP)
Universidade Federal do Sul e Sudeste do Pará
Biblioteca Setorial Josineide da Silva Tavares

L257l Landim, Ellyda Layanna da Silva

Lei geral de proteção de dados: a validade do consentimento e a real anuência do titular de dados frente ao ordenamento jurídico brasileiro / Ellyda Layanna da Silva Landim. — 2022.

50 f.

Orientador (a): Gabriela Natacha Bechara.

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Sul e Sudeste do Pará, Campus Universitário de Marabá, Instituto de Estudos em Direito e Sociedade, Faculdade de Direito, Curso de Bacharelado em Direito, Marabá, 2022.

1. Proteção de dados - Brasil. 2. Privacidade. 3. Direitos Fundamentais. 4. Brasil. [Lei geral de proteção de dados pessoais (2018)]. I. Bechara, Gabriela Natacha, orient. II. Título.

CDDir: 4. ed.: 341.2732

Elaborado por Miriam Alves de Oliveira – CRB-2/583

Dedicado à minha mãe, Edna. Seu amor, apoio, carinho e dedicação incondicionais acalentam meu coração e me inspiram a sonhar.

AGRADECIMENTOS

Agradeço à Deus pela vida e por todas as bençãos e dons com os quais me agraciou. À minha amada mãe, que sempre esteve ao meu lado, sem seu apoio nada disso seria possível. À minha estimada tia Maria José, cuja distância nunca afastou nossos corações em uníssono. Ao meu pai e irmãos, que sempre torceram por mim e vibraram com minhas vitórias. Aos meus avós, cujo sorrisos sinceros e mãos calejadas me inspiram a seguir em frente. Aos meus caros familiares, de sangue e coração, que lutaram comigo e antes de mim, pelo legado de nossa origem humilde, grata e honesta. Aos meus queridos amigos, que compartilharam o sangue, suor, lágrimas e sorrisos dessa jornada, me incentivando a nunca desistir de mim. Aos meus companheiros de quatro patas, que tanto me enchem de alegria, pura e genuína. À minha orientadora, Professora Gabriela, por seu auxílio, compreensão e companheirismo na elaboração e escrita deste trabalho. A todos os professores que fomentaram minha educação e cidadania, compartilhando sua experiência e conhecimento. Agradeço aos colegas de minha turma originária, 2016, pela partilha, e aos colegas das turmas 2017 e 2018 pela calorosa acolhida. Por fim, e não menos importante, agradeço minha força, persistência e resiliência, que me acompanharam até aqui e que, com sorte, continuarão sendo sempre parte de mim.

Seguiremos sempre juntos em meu coração, nessa bela caminhada da vida.

“A justiça é mesclada de compaixão”

(LEWIS, 1955, p. 285)

RESUMO

A demanda pela proteção de dados e a preocupação com a privacidade são temas recorrentes na atual era da informação. Diante desse contexto, observou-se a ampliação de dispositivos de proteção aos dados pessoais em escala global, destacando-se a criação da Lei Geral de Proteção de Dados (LGPD) como lei específica voltada a proteção de dados e direitos fundamentais de seu titular. Fortalecendo a autodeterminação informativa, a lei em comento estabeleceu o consentimento como um dos principais institutos garantidores dessa proteção. O presente trabalho tem como objetivo analisar se o atual modelo de consentimento está sendo utilizado de maneira válida e eficaz, observando temas que envolvem a base normativa da LGPD, os direitos fundamentais e as inspirações legislativas que a precederam. Faz-se presente também suas estruturas e o instituto do consentimento, presente no ordenamento jurídico brasileiro pela LGPD e outras normas infraconstitucionais. Adotou-se como metodologia a análise bibliográfica e também de outras fontes que competem ao tema, como documentos, notícias extraídas de veículos jornalísticos e dados que permitiram trazer visões referentes ao direito comparado, de forma qualitativa. Propôs-se assim a reflexão de modelos que busquem materializar o consentimento, assegurando ao titular conhecimento e capacitação para o exercício pleno de seus direitos formalmente resguardados, através de modelos de ética e governança de dados mais eficazes.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD); Consentimento; Dados Pessoais; Direitos Fundamentais; Privacidade.

ABSTRACT

The demand for data protection and the concern with privacy are recurrent themes in the current information age. In this context, we have observed the expansion of personal data protection mechanisms on a global scale, highlighting the creation of the General Law of Data Protection (LGPD) as a specific law aimed at protecting data and the fundamental rights of its holder. Strengthening the informative self-determination, the law in question has established consent as one of the main institutes guaranteeing this protection. This paper aims to analyze whether the current consent model is being used in a valid and effective way, looking at issues involving the normative basis of the LGPD, fundamental rights and the legislative inspirations that preceded it. It also presents its structures and the institute of consent, present in the Brazilian legal system through the LGPD and other infra-constitutional rules. The methodology adopted was bibliographic analysis, as well as other sources pertaining to the theme, such as documents, news extracted from journalistic vehicles and data that allowed us to bring comparative law views, in a qualitative way. Thus, it was proposed the reflection of models that seek to materialize consent, assuring the holder knowledge and training for the full exercise of his formally protected rights, through more effective models of ethics and data governance.

Keywords: General Data Protection Law (LGPD); Consent; Personal Data; Fundamental Rights; Privacy.

LISTA DE TABELAS

LISTA DE SIGLAS

APEC	Asia-Pacific Economic Cooperation
CDC	Código de Defesa do Consumidor
CE	Conselho da Europa
CF/88	Constituição Federal de 1988
CoE	Council of Europe
DPO	Data Protection Officer
EU	European Union
FIPPS	Fair Information Practice Principles
GDPR	General Data Protection Regulation
IoT	Internet of Things
LATAM	América Latina
LGPD	Lei Geral de Proteção de Dados
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OEA	Organização dos Estados Americanos
PBD	Privacy by Design
PDPA	Personal Data Protection Act
PL	Projeto de Lei
PIPEDA	Personal Information Protection and Eletronic Documents Act
RGPD	Regulamento Geral de Proteção de Dados
TIC	Tecnology of Information and Communication

SUMÁRIO

1. INTRODUÇÃO

Ao acessar um site, é comum ao usuário de internet ser bombardeado por uma série de perguntas, demandando diversas anuências: se aceita os termos de uso e a utilização de *cookies* ou se concorda com a política de privacidade. Quantas vezes este usuário já fez a leitura desses documentos antes de clicar que concorda ou aceita tais termos e condições? Com o que exatamente ele estava concordando no momento do clique?

A escolha da presente temática surgiu diante de um contexto informacional onde os dados são o novo petróleo, todavia jorrando através de fontes perenes e inesgotáveis: o próprio titular, a quem essas informações tão preciosas pertencem. Não somente por seu teor econômico, mas também pelo fator social e político, fez-se necessária a criação de mecanismos jurídicos que protejam o indivíduo e seus dados, que trazem informações pessoais e sensíveis, colocando-o numa posição de hipervulnerabilidade.

A proteção de dados pessoais não trata tão somente do uso de dados para fins mercantis, como publicidades direcionadas ou contatações indesejadas. É, também, sobre refrear a vigilância estatal, temor catalisador da primeira geração de normativas que visavam disciplinar a proteção de dados pessoais, frente ao próprio Estado que as tutelava. É ainda salvaguarda contra práticas discriminatórias e excludentes. Trata-se de garantia de liberdade, de privacidade, de dignidade, estes direitos fundamentais e constitucionalmente assegurados.

Dada a sua importância e relevância, especialmente no contexto informatizado ao qual a sociedade está atualmente inserida, havia crescente clamor por dispositivos jurídicos que tratassem especificamente da proteção de dados pessoais, iniciando assim o refino de mecanismos já existentes e a criação de novíssimas legislações para adequá-los às demandas hodiernas. No Brasil, o horizonte tornou-se mais próximo com o advento da Lei nº 13.709/18, a Lei Geral de Proteção de Dados (LGPD).

A LGPD, que buscou inspiração no ordenamento europeu, trouxe camada protetiva ao tratamento de dados, não somente em âmbito cibernético, pautada na proteção aos direitos fundamentais e à autodeterminação informativa de seu titular, mas também dando-lhe livre arbítrio quanto ao que pode ou não ser compartilhado e exposto, à medida de sua concordância, devendo esta ser manifestada de forma livre, informada e inequívoca, sendo seus dados tratados com uma finalidade específica e determinada.

Tal posição é passível de questionamentos norteadores para esta pesquisa. O titular tem real condição em consentir com o tratamento de seus dados? Esse consentimento é realmente válido e a anuência real, conforme requisitos dispostos na LGPD e em outros

dispositivos do ordenamento jurídico brasileiro? Este trabalho ocupa-se em questionar se o modelo de consentimento proposto é, de fato, válido e eficaz, dando ao indivíduo um poder que ele não compreende e que tampouco há preocupação em fazer-se compreensível.

Utilizou-se para essa análise pesquisa bibliográfica com diversos e renomados autores, além de fontes que competem ao tema, como documentos, notícias extraídas de veículos jornalísticos e dados que permitiram trazer visões referentes ao direito comparado, de forma qualitativa. Dedica-se, também, a explicar que a lei em si só não se basta, é necessário também que se atrele a ela compromisso de educação e capacitação[1], de conhecimento informacional.

Nesta senda, objetivou-se na primeira seção compreender a base normativa que serviu de fomento à criação da LGPD, trazendo à baila os direitos fundamentais a qual a lei ocupa-se em proteger e também no tocante às inspirações legislativas que a precederam. Na segunda seção, analisa-se a estrutura dos institutos presentes à douta lei, em consonância aos dispositivos jurídicos já vigentes, tanto no ordenamento nacional quanto em esfera internacional. A terceira seção, por sua vez, dedica-se a discutir se o modelo vigente de consentimento é materialmente eficaz, de forma a ratificar ou refutar se a concordância do titular é verdadeiramente válida. Por último, parte-se para as considerações finais deste trabalho.

[1] PINHEIRO, Patrícia Pack. **Proteção de dados pessoais.** São Paulo: Editora Saraiva, 2020. p. 22.

2. A BASE NORMATIVA DOS DADOS PESSOAIS

A civilização humana só se tornou possível por intermédio da habilidade de transmitir memórias ao longo das gerações. Diferentes tecnologias aceleraram esse processo, com sua capacidade de armazenamento, preservação e transmissão de informações e conhecimento. Precipuamente, antes que todo esse volume de conteúdo seja processado e a ele seja atribuído sentido, tem-se um elemento essencial: o dado[2].

Certamente, seu caráter inicialmente anônimo, fragmentado e primitivo pode ser facilmente transmutado, findando sua trivialidade e expandindo seu potencial a partir de processos que permitem correlacioná-lo com outros, condensando-os e indexando-os em tecnologias de bancos de dados, tornando possível prever acontecimentos e comportamentos de indivíduos e da sociedade como um todo.[3]

É importante atentar-se ao fato de que a informação em si se tem mostrado cada vez mais complexa, volúvel e maleável. Seu volume, armazenamento e utilizações se expandem à medida em que formas de manipulação e alteração crescem em igual medida, desde sua apropriação, coleta, tratamento à forma como ela é transmitida. Não há como negar seu potencial como força motriz da evolução tecnológica, diante de sua capacidade de influir em nosso cotidiano.

Conforme pontuado por Antonio-Enrique Perez Luño[4], "as possibilidades de intromissão na intimidade e a colonização da vida privada através dos meios tecnológicos, tem suscitado constante inquietude cívica nas sociedades avançadas". Com o avanço da tecnologia e das comodidades que ela proporciona, avançam-se também todos novos métodos, "novos fenômenos de agressão aos direitos e liberdades".

---

[2] Outra forma de diferenciação da dicotomia dado e informação que vale a pena ser citada é a trazida por Danilo Doneda (p. 94, 2011): "o conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica certa promiscuidade na sua utilização. Ambos os termos servem para representar um fato, determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser considerado. [...] o dado estaria associado a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. [...]".
DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** V. 12, N. 2. Joaçaba: Revista Espaço Jurídico, 2011.

[3] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 46.

[4] Traduzido pela autora. Original: "Las possibilidades de intromisión en la intimidad y de colonización de la vida privada a través de médios tecnológicos, han suscitado constante inquietude cívica em las sociedades avanzadas. Es sabido que la etapa atual de desarrollo tecnológico, há generado nuevos fenómenos de agresión a los derechos y libertades".
PEREZ LUÑO, Antonio-Enrique. Teledemocracia, ciberciudadania y derechos humanos. **Revista brasileira de políticas públicas.** v. 4. n. 2. p. 8-46. ISSN 2236-1677. Brasília: CEUB, 2014. p. 10.

Destarte, atribui-se grande importância a figura do banco de dados, verdadeiro "banco" no sentido ao que lhe é atribuída a função de guardar tesouros informacionais dos mais diversos, mas no qual atentaremos àqueles relativos à pessoa natural. Nessa perspectiva, a afirmação de Danilo Doneda[5] que " o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo", mostra-se ainda mais contundente nos dias atuais.

Diante de tal perspectiva, o direito de controlar, apagar ou transformar esses rastros coletados tornou-se, definitivamente, uma questão de máxima relevância política e legal, sendo, concomitantemente, tema jurídico inovador e longevo, mas de forma alguma ultrapassado. Especialmente quando se figura à seara digital, de fronteiras tênues e transformações frenéticas, que ultrapassam os esforços mais céleres do legislador.

Com efeito, o anonimato e autonomia dentro do meio digital mostra-se praticamente intangível, especialmente quando a concessão de dados parte de seu titular, que se submete assim a abrir mão de sua privacidade em troca de produtos e serviços, sem por vezes considerar o real valor de tais informações e seu caráter além de pecuniário. Neste mesmo sentido, Zigmunt Bauman aduz sobre a fragilidade à qual essa "escolha" nos é disposta:

> Quanto à "morte do anonimato" por cortesia da internet, a história é ligeiramente diferente: submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir. De uma forma ou de outra, contudo, nos é oferecida, ao menos nominalmente, uma escolha, assim como ao menos a aparência de um contrato em duas vias e o direito formal de protestar e processar se ele for rompido.[6]

Neste sentido, observa-se que a natureza da tutela jurídica dos dados pessoais deve ser diferenciada, dinâmica, pois não se trata tão somente de propriedade do indivíduo, mas de uma extensão de sua personalidade[7]. A liberdade que historicamente permeia o espaço cibernético não é absoluta, tampouco isenta do exercício das forças normativas e de responsabilização, especialmente no que se trata aos dados pessoais, assunto que será abordado na próxima subseção.

---

[5] DONEDA, loc. cit. p. 93.
[6] BAUMAN, Zygmunt. **Vigilância líquida**. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014. p. 12.
[7] DONEDA, 2020, p. 146-147.

2.1 Dados pessoais como direito fundamental: direito à liberdade, dever à proteção

Outrossim, a valoração de tais dados é há muito fruto de análise de juristas como o célebre doutrinador italiano Stefano Rodotà[8], que faz importante alerta ao fornecimento desses dados pela pessoa natural, em qualidade e quantidade, em troca de determinados serviços, e a abertura que isso traz à lucrativos usos secundários. Clarissa Maria de Lima Moura[9] aduz de modo semelhante, em especial à cessão dos dados pessoais sensíveis, no que ela considera inefetivo o atual modo em que se dá o consentimento por parte do titular de dados, "mediante aceite em termos de uso, cuja leitura não é habitual, mitigando de forma latente o poder de autodeterminação dos titulares sob estes".

Constata-se, desse modo, que atribuir exclusivamente ao indivíduo total domínio e principalmente delegá-lo a proteção quanto à "propriedade" de seus dados pessoais, especialmente tratando-se daqueles considerados sensíveis, não se mostra de forma alguma sensato ou adequado, diante da dimensão que tais informações podem atingir e das mudanças econômico-sociais que podem ser geradas mediante a coleta e tratamento desses dados. A disciplina de tal matéria deve partir de resposta legislativa do Estado.

O exercício da democracia digital denota esforço conjunto entre o indivíduo dotado de atitude responsável, resguardando a auto exposição e disponibilização de informações personalíssimas, assim como implica ação conjunta e interventiva por parte dos setores público e privado[10] para garantirem, de fato, garantias à privacidade e ao sigilo, assim como resguardar o livre exercício ao direito de personalidade. Neste mesmo sentido, Garcia mostra-se incisiva na defesa da elevação do *status* da proteção de dados à caráter de direito fundamental:

> [...] proteger os dados sensíveis é uma forma de prevenir ou eliminar a discriminação, o que, por certo, contribuirá para a efetivação do princípio constitucional da igualdade, consagrado no art. 5° da Constituição Federal. Nesta senda, alguns autores passaram a defender a emergência do direito sobre a proteção de dados pessoais como categoria jurídica autônoma, merecedora do mesmo status dos demais direitos fundamentais. Defendem também a necessidade de reconhecimento do direito à autodeterminação informativa por

[8] RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 46.

[9] MOURA, Clarissa Maria Lima. **Dados pessoais como ativo na economia digital:** a tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos. 2019. Trabalho de Conclusão de Curso (TCC) – Faculdade de Direito da Universidade Federal de Pernambuco. Recife, 2019. p. 15.

[10]. DETERMANN, Lothar. **Determann's field guide to data privacy law –** international corporate compliance. 2. ed. Massachusetts: Edward Elgar, 2015. p. 12-13 apud 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 Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021. p. 92.

> parte do titular dos dados, a partir da qual o internauta deve ter a garantia de controlar como e quando suas informações serão recolhidas e utilizadas, determinar quem terá acesso a seus dados pessoais e como eles serão armazenados e tratados.[11]

O conceito de direito fundamental está fortemente atrelado aos direitos humanos, "que consistem em um conjunto de direitos considerado indispensável para uma vida humana pautada na liberdade, igualdade e dignidade"[12]. Estes, quando reconhecidos pela lei maior, a constituição, consagram-se direitos fundamentais, cuja função primordial é a "defesa da pessoa humana e de sua dignidade perante os poderes do Estado"[13]. A constitucionalização dos direitos fundamentais além de garantia ao indivíduo, é essencial para a concretização da democracia, razão pela qual sua proteção judicial é indispensável[14].

Sendo assim, adentrar-se-á ao rol de direitos fundamentais dispostos no art. 5º da Constituição Federal de 1988, dos quais evidenciam-se dois direitos fundamentais constitucionalmente positivados: o direito à privacidade (inciso X) e o direito ao sigilo pessoal (inciso XI e XII). O constructo do constituinte, mesmo que ainda em inobservância à magnificência do aspecto tecnológico e informático que estava por vir, mostra-se bastante vanguardista, embora ainda lacunoso.

2.1.1 O direito à privacidade e sigilo como norteadores da proteção de dados

Considera-se inicialmente o primeiro aspecto, o direito à privacidade, ao qual dispõe, conforme dispositivo *in verbis*, que "são invioláveis a **intimidade**, a **vida privada**, a **honra** e a **imagem** das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" [grifei]. Mesmo não inserido expressamente no texto normativo da carta magna, finca raízes em marcos legais seculares, como a petição redigida pelos advogados americanos Warren e Brandeis em 1890, intitulada "*The Right to Privacy"*, que já o associava intrinsecamente ao direito à vida digna.

> Gradualmente, o escopo desses direitos legais foi ampliado; e agora o direito à vida passou a significar o direito de gozar a vida, - o direito de ser deixado

[11] GARCIA, Keila Lacerda de Oliveira Magalhães. O direito à proteção de dados pessoais e sua lacuna legal no brasil. ed. 94. v. 1. **Revista científica semana acadêmica** ISSN 2236-6717 versão online. p. 4.
[12] RAMOS, André de Carvalho. **Curso de direitos humanos.** 8. ed. São Paulo: Saraiva Educação, 2021. p. 19.
[13] BONAVIDES, Paulo. **Teoria constitucional da democracia participativa:** por um direito constitucional de luta e resistência, por uma nova hermenêutica, por uma repolitização da legitimidade. São Paulo: Malheiros, 2001.p. 407.
[14] MORAES, Alexandre de. **Direitos humanos fundamentais:** teoria geral. 12 ed. São Paulo: Atlas, 2021. p. 2.

> em paz; o direito à liberdade assegura o exercício de amplos privilégios civis; e o termo propriedade cresceu para abranger toda forma de posse – intangível, bem como tangível. [...] Este desenvolvimento do direito foi inevitável.[15]

Segmentar-se-á, aqui, esse verdadeiro guarda-chuva terminológico do qual trata-se a privacidade e o que ela de fato compreende, pondo-se em voga o elemento vida íntima, que por sua vez engloba a intimidade. Conforme conceitua Nathalia Masson[16], a vida íntima "abarca as relações pessoais, familiares, negociais ou afetivas, do indivíduo, incluindo seus momentos de lazer, seus hábitos e seus dados pessoais".

Ademais, não se pode olvidar do segundo e não menos importante sigilo pessoal, no qual se verifica proteção semelhante à presente no tópico anterior, quando disciplina no inciso XII que é "inviolável o sigilo da correspondência e das comunicações telegráficas, de **dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial", ressaltando, mais uma vez, todo um esforço jurídico presente na Constituição para garantir o direito à privacidade e ao sigilo dos dados pessoais da pessoa natural.

Vislumbra-se ainda o *animus* do legislador em também garantir meios necessários de acesso à dados e informações por parte de seu titular, especialmente ao verificar o instituto jurídico do *habeas data*, remédio constitucional cujas hipóteses de aplicabilidade estão expressas nas alíneas *a* e *b* do inciso LXXII do art. 5º da Constituição Federal de 1988.

É também imprescindível compreender o conceito de anonimato frente a liberdade de expressão, com o anonimato inserido no conceito de privacidade. Por vezes posta de forma equivocada em antagonismo com o direito à liberdade de expressão, "assumindo a presunção de que todos podem falar o que pensam",[17], o anonimato é vedado por fazer-se necessário identificável o indivíduo, quando isto ferir parâmetros legalmente estabelecidos. No âmago da privacidade, o anonimato será direito a ser fruído, "respeitado quando o indivíduo estiver livre de identificação e fiscalização"[18].

---

[15] Traduzido pela autora. Original: "Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, - the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession – intangible, as well as tangible. [...] This development of the law was inevitable".
WARREN, Samuel; BRANDEIS, Louis. **The right to privacy.** v. IV, n. 5. Boston: Havard Law Review, 1890.

[16] MASSON, Nathalia. **Manual de direito constitucional.** 8 ed. rev. ampl. e atual. Salvador: Juspodivm, 2020. p. 288.

[17] PINHEIRO, 2021. p. 42.

[18] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 16. ed. São Paulo: Saraiva Educação, 2021. p. 128.

2.2 A construção da autodeterminação informativa

Apesar de mutável à medida que a humanidade segue seu curso e de estar continuadamente passando por profundas transformações, o direito ainda não é capaz de realizar a façanha de prever futuro tão incerto quanto os avanços tecnológicos vindouros. O caminho galgado até aqui teve de ser antes pavimentado por diversas legislações, decantadas e refinadas até extrair-se o sumo de sua melhor aplicabilidade e efetividade diante da materialidade dos temas normativos.

Por conseguinte, a construção deste instituto jurídico da proteção de dados não ousou escapar de cenário semelhante, com marcos geracionais ao redor do mundo, tendo inicial foco na liberdade de acesso às informações por parte de órgãos públicos até a ênfase progressiva em regras quanto ao seu acesso, tuteladas sob escrutínio estatal[19].

2.2.1 Primeira geração

Nesse diapasão, inicia-se a primeira geração de leis sobre proteção de dados, que tinham como finalidade responder à possíveis violações de intimidade à privacidade pessoal que poderiam advir da tecnologia vigente à época. O grande foco, aqui, era dar fim à sangria do acesso indiscriminado aos dados pessoais da população por parte do governo.

As grandes criações ficcionais e utópicas presentes do panóptico e *big brother*, nas antológicas obras de Bentham, Focault, Huxley e Orwell pareciam tornarem-se reais com o advento da computação: o fantasma da vigilância estatal. Em 1967, Alan Westin já demonstrava grande preocupação quanto à falta de mecanismos que controlassem a coleta e processamento de dados em sua obra “Privacy and Freedom”, temendo usos além daqueles que poderiam ser utilizados em benefício da população.

> A questão da privacidade levantada pela informatização é se o aumento da coleta e processamento de informações para diversos fins públicos e privados, se não for cuidadosamente controlado, poderia levar a um poder de vigilância por parte do governo sobre vidas individuais e atividades organizacionais. [...] Para planejamento, eficiência e controle social, esses dados governamentais, sistemas informatizados de transações e arquivos centrais de registros do futuro poderiam trazer enormes benefícios à Sociedade. Mas, a menos que sejam colocadas cuidadosamente salvaguardas para a privacidade no planejamento e administração de sistemas que a maioria dos especialistas em informática consideram ser desenvolvimentos inevitáveis das próximas

[19] RODOTÀ, op. cit., p. 44.

> décadas, o crescimento da vigilância de dados será impressionante. Enquanto isso, os presentes dossiês e sistemas de informação computadorizados continuam a aumentar, sem muitas diretrizes legais ou administrativas ainda para lidar com as questões de privacidade que eles levantam. [20]

Foi neste período, mais especificamente na década de 1970, que surgiram as iniciativas pioneiras voltadas a tutelar os dados pessoais, como o *Data Legen 289* ou *Datalag*, o Estatuto para banco de dados sueco, primeira lei nacional de proteção de dados, de 1973, e o *Privacy Act* estadunidense, de 1974. Reflexo do "estado da tecnologia e [d]a visão jurista à época, [...] marcada pela convicção de que direitos e liberdades fundamentais estariam ameaçados pela coleta ilimitada de dados pessoais, então realizada basicamente pelo Estado"[21].

2.2.2 Segunda Geração

A segunda geração veio ainda na segunda metade da década de 1970, após a *Bundesdatebschutzgesetz* da República Federativa Alemã, em 1977. No ano seguinte, a francesa *Informatique et Libertés* se diferencia por sua estrutura, com ensejo voltado à proteção a ser exercida pelo cidadão, carente de mecanismos que pudessem identificar e tutelar seus próprios dados.

A mudança de perspectiva a partir desde ponto, antes do surgimento de redes sociais ou expansão da internet em ambientes domésticos e sua ascensão ao *mainstream*, é pautada pela percepção que "o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social"[22].

Contudo, esta visão voltada à liberdade do usuário de dispor de seus dados estava aquém das consequências dos dados regiamente lançados ao acaso e à disposição de terceiros, sob a frágil responsabilização única de seu alheio titular. Não se eram levados em conta, ainda, os desdobramentos que acarretariam ao coletivo, o que logo faria urgir o clamor por novas mudanças.

---

[20] Tradução da autora. Original: "The issue of privacy raised by computerization is whether the increased colletion and processing of information for diverse public and private purposes, if not carefully controlled, could lead to a sweeping power of surveillance by goverment over individual lives and organizational activity. [...] For planning, efficiency, and social control, these goverment data centers, computerized transaction systems, and central record files of the future could bring enormous benefits to Society. But unless safeguards for privacy are placed carefully in the planning and administration of systems that most computer experts feel to be inevitable developments of the next two decades, the growth in data surveillance will be awesome. Meanwhile the presente dossiers and computerized information systems continue to increase, without many legal or administrative guidelines as yet to cope with the issues of privacy that they raise. (p. 119-131).
WESTIN, Alan. **Privacy and freedom**. Nova York: Athenum, 1967. p. 119-131.

[21] DONEDA, 2020, p. 165-166.

[22] Ibid., 167.

2.2.3 Terceira Geração

A grande mudança trazida pela terceira geração foi a busca pela efetividade da **autodeterminação informativa**, trazida pela primeira vez pelo *Bunderverfassungsgericht*, o Tribunal Constitucional Alemão, em decisão de 15 de dezembro de 1983. Viu-se assim o conflito entre o livre consentimento e o direito à informação de forma transparente, mas também a união da esfera pessoal e política. À título de exemplo, têm-se também as legislações da Finlândia e Noruega, além de emendas realizadas às leis alemã e austríaca.

Tal percepção não deixou de ser notada pelo judiciário brasileiro, conforme está presente em voto proferido pelo Ministro Ruy Rosado de Aguiar, ao qual associa o instituto da autodeterminação informativa com o direito à privacidade presente na CF/88, em fragmento abaixo disposto:

> 1. A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado Moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou concelá-lo [sic]. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, algumas providências já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível das garantias fundamentais, com o direito de autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, [...] com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para a garantia dos limites permitidos na legislação. [...] No Brasil, a regra do art. 5º inc. X, da Constituição de 1988, é um avanço significativo: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.
>
> STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p.6119.

O indivíduo passou a ter liberdade em dispor da privacidade de seus dados à medida em que se sujeita a condições estabelecidas pelo Estado, já que neste marco temporal foi estabelecido que tal exposição "também pode abranger escolhas significativas para a organização social e política, [já que] uma vez mais a disciplina da coleta e tratamento das informações demonstra que não pode ser reduzida somente ao seu valor individual"[23].

2.2.4 Quarta e atual geração

Hodiernamente, as leis de proteção de dados encontram-se em sua quarta geração. A pessoa natural, titular de seus dados, passa a dividir seu protagonismo com a atuação do Estado, que aumenta a proteção e diminui o controle meramente individual dessas informações, podendo atingir grau máximo quando tratar-se de dados sensíveis.

As lições ensinadas pela progressão de leis que sofisticaram a disciplina dessa matéria encontram-se em curso em leis posteriormente elaboradas, como a Constituição Brasileira promulgada em 1988, o Regulamento Geral de Proteção de Dados (RGPD) de 2016 e normas infraconstitucionais brasileiras como a Lei Geral de Proteção de Dados (LGPD) de 2018, que dispõe sobre o "tratamento de dados pessoais, inclusive nos meios digitais, [...] com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoal natural", conforme extraído do *caput* de seu art. 1º.

2.3 As raízes da Lei Geral de Proteção de Dados

Em um momento ao qual a regulamentação de dados na internet era ainda incipiente, a União Europeia já realizava movimentações no escopo de tutelar essa matéria, buscando a "proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados", no qual lê-se pessoas singulares como pessoas naturais.

Assim foi moldada a Diretiva 95/46/CE do Conselho da Europa, texto de referência que abrangeu todos os Estados-membros europeus, sob esforço de garantir um grau adequado de proteção ao usuário diante das novas tecnologias, tratando-o como um direito fundamental[24], estando presentes também na Carta dos Direitos Fundamentais da União Europeia, de 2000, disposta no artigo 8º, que introduz ainda a figura de uma autoridade fiscalizatória.

---

[23] RODOTÀ, op. cit., p. 46.
[24] GARCIA, op, cit., p. 4.

Com novos paradigmas e tecnologias sendo difundidos, expandiu-se ainda mais a necessidade de um esforço conjunto entre o Estado, o indivíduo (pessoa natural) e o setor privado para garantir proteção, transparência e o estabelecimento de novos direitos como o direito ao esquecimento, por exemplo. Em vigor desde 2016, o *General Data Protection Regulation* (GDPR) ou Regulamento Geral de Proteção de Dados (RGPD) traz um conjunto de normas que regulamentam condutas, atribuem direitos, identificam sujeitos e delimitam a licitude do tratamento de dados.

De forma semelhante organiza-se a Lei Geral de Proteção de Dados (LGPD) de 2018, lei brasileira que versa sobre o mesmo tema, em vigor desde 2020, que mesmo aplicando-se também ao ambiente real e tangível, trata-se de significativo avanço à regulação de uso da internet e da democracia digital no Brasil, proeminente em assegurar ao titular de dados o pleno exercício de seus direitos fundamentais[25]. Nota-se, portanto, as influências diversas que incidiram sobre a lei pátria, perpassando principalmente pelo direito à privacidade, com seu fortalecimento e intrínseca ligação com o direito à vida e à dignidade da pessoa humana.

Faz-se importante observar o crescimento expressivo da discussão quanto à proteção de dados ao longo da primeira década do século XX na América Latina, na qual destaca-se esforços para garantir a proteção de dados, muitas vezes atreladas à matéria consumerista, e também ações coletivas voltadas à cibersegurança, como a "Declaração sobre o Fortalecimento da Segurança Cibernética nas Américas", da Organização dos Estados Americanos (OEA), de 2004.

[25] SARLET; RUARO, op. cit. p. 95-96.

Tabela 1 – Proteção de Dados Pessoais – LATAM[26]

PAÍS	*STATUS* LEI OU PL	PAÍS	*STATUS* LEI OU PL	PAÍS	*STATUS* LEI OU PL
Argentina	25.326 – 2000.	El Salvador	Nem em discussão.	Panamá	Desde 2016.
Barbados	Lei de Prot. de Dados – 2005.	Guiana Francesa	A que vigora na França. Lei de Processamento de Dados desde 1978.	Paraguai	1.682 – 2001.
Belize	Nem em discussão.	Guatemala	Em discussão, n. 4090 – 2009.	Peru	29.733 – 2011.
Brasil	13.709 – 2018.	Guiana	Nem em discussão.	Suriname	Nem em discussão.
Chile	19.628 – 1999.	Honduras	Nem em discussão.	Trinidad e Tobago	Em discussão desde janeiro 2011.
Colômbia	1.581 – 2012.	Jamaica	Nem em discussão.	Uruguai	Lei nº 18.331 – 2008.
Costa Rica	Lei n. 8.968 – 2011.	México	Desde 2010	Venezuela	Nem em discussão.
República Dominicana	172 – 2013	Nicarágua	Desde 2012		

Fonte: PINHEIRO, 2020.

Conforme conteúdo exposto na tabela acima de Patrícia Peck Pinheiro, depreende-se que dentre os países da América Latina a desenvolverem leis específicas à proteção de dados, a legislação brasileira é a mais recente. Extrai-se ainda que em alguns dos países considerados menos desenvolvidos economicamente, os passos para a criação dessa normativa ainda caminham lentamente, de forma quase incipiente, conquanto em outros tantos não há sequer vislumbre do início de debate desta imprescindível discussão.

[26] PINHEIRO, 2020, p. 42-43.

3. A LGPD COMO MARCO LEGISLATIVO BRASILEIRO E SEUS INSTITUTOS JURÍDICOS

Após análise do histórico fomentador desse marco legal, faz-se imprescindível compreender o galgar desse marco jurídico, tendo em mente as legislações brasileiras que o precederam, no tocante à sua aplicabilidade junto ao universo digital. Inafastável também são os elementos fáticos, ao redor do globo e em território nacional, que explicam sua grande relevância e popularidade crescente entre não-juristas, especialmente dentre os profissionais das Tecnologias de Informação e Comunicação.

Adentrar-se-á em seus principais institutos e conceituações, a fim de melhor compreender sua aplicabilidade, com ênfase, repisa-se, aos meios digitais, mesmo diante de sua aplicabilidade também ao mundo real. A Lei Geral de Proteção de Dados tem como cerne, de acordo com o que se pode depreender a partir do enunciado presente em seu supracitado art. 1º, "a proteção e tratamento dos dados pessoais", à luz de direitos fundamentais como privacidade, sigilo e personalidade.

Nessa perspectiva, muito antes do surgimento da legislação europeia que a precedeu e serviu de principal inspiração, o sociólogo espanhol Manuel Castells já discutia sobre tecnologias que emergiram da necessidade de controlar a esfera livre da Internet, no que ele chama de *tecnologias de controle*, classificando-as em três áreas: de identificação, de vigilância e de investigação. Estas estão sob dois pressupostos básicos, do "conhecimento assimétrico dos códigos na rede e a capacidade de definir um espaço específico de comunicação suscetível de controle"[27].

Curioso notar-se que a LGPD permeia todas as esferas das tecnologias de controle propostas por Castells, entrelaçando-se à relação entre a pessoal natural e o campo de batalha digital código *versus* código, internet *versus* liberdade. Em tese, tem-se como função, além de proteger dados e assegurar direitos, neutralizar antagonismos e aparar arestas nas relações digitais. Em um novo contrato social – digital –, abre-se mão de uma suposta liberdade absoluta em favor da proteção do Estado.

3.1 Delimitando conceitos essenciais

Sob os efeitos da contemporaneidade e da hipertrofia do ambiente digital, a sociedade da informação vem se estabelecendo à medida que as tecnologias de informação e comunicação,

[27] CASTELLS, op. cit. p. 175-176.

também conhecidas pela sigla em inglês TIC (Tecnology of Information and Communication), passam a ser elementos essenciais para o desempenho das mais diversas atividades básicas.

Essa inserção massiva de novos elementos causou profundas alterações à dinâmica das relações humanas e sociais, com a inserção de novíssimos conceitos e complexidades com tal rapidez que não é possível ao legislador acompanhar, à mesma velocidade, esta vertiginosa celeridade e vanguardismo. Sarlet e Ruaro dão especial destaque à complexidade do ciberespaço:

> Não se pode desconhecer que, curiosamente, o meio ambiente virtual apresenta facetas muito singulares, vez que as suas dimensões não se circunscrevem ao espaço e tampouco ao tempo. Outro aspecto relevante encontra-se diretamente relacionado com a capacidade de avanço e incremento da tecnologia e, dessa maneira, deve ser considerada a impermanência desse ambiente, pois constantemente se altera o próprio conceito de dados pessoais, sobretudo quando se analisa as condições e os graus de identificabilidade que mudam rapidamente em razão de novos modos de armazenamento, de tratamento e de reidentificação de dados.[28]

Com efeito, o volume massivo de dados e informações sem quaisquer segurança ou proteção demandaram – e continuam a demandar – resposta cada vez mais urgente por parte do Estado, que deu seus primeiros passos regulatórios com o Marco Civil da Internet em 2014, estabelecendo o início de uma era com normas informáticas mais robustas. Tendo como pilar principal o direito fundamental à privacidade, as lacunas presentes na legislação em voga demandaram maior proteção aos dados pessoais através de lei específica, concretizada por meio da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados.

3.1.1 Dados Pessoais e Anonimizados

Adentrando-se à análise da LGPD, faz-se necessário entender o elemento que determina todo o *animus* desse dispositivo jurídico: o dado pessoal. Definido em seu art. 5º, inciso I, o dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável". Na seção anterior, diferenciou-se *dado* de *informação*, sendo este um compilado de dados a quais é atribuído sentido, em resumo.

A conceituação de dados pessoais está presente também em outras legislações nacionais, como o Decreto nº 8.771/16, que em seu art. 14, inciso I, têm redação semelhante à LGPD ao conceitua-lo como "dado relacionado à pessoa natural identificada ou identificável",

[28] SARLET; RUARO, op. cit., p. 83.

todavia é acrescida de rol exemplificativo, ao completar "inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa".

Ainda nesta feita, tem-se ainda a Lei nº 12.527/11, que ao se tratar do acesso à informação, traz o dado pessoal, em seu art. 4º, inciso IV, como "informação pessoal: aquela relacionada à pessoa natural identificada ou identificável". Tem-se em voga a predominância do legislador em trazer caráter expansionista ao conceito e, portanto, o escopo de alargar a qualificação do dado como pessoal, levando-se em conta a fluidez e a necessidade da análise contextual na qual o dado está inserido para que ele seja definido, de fato, como um dado pessoal[29].

Tabela 2 – Tabela comparativa acerca da definição de dados pessoais no direito comparado.

OCDE	**CoE**	**Canadá**	**Argentina**	**APEC**	**EU**
"Dados pessoais" significam qualquer informação relativa a um indivíduo identificável (titular de dados).	"Dados pessoais" significam qualquer informação relativa a um indivíduo identificado ou identificável (titular de dados).	Informações pessoais significam informações sobre um indivíduo identificável.	Dados pessoais: informações de qualquer tipo relacionadas a pessoas físicas ou jurídicas identificadas ou identificáveis.	Informações pessoais significam qualquer informação relativa a um indivíduo identificado ou identificável.	"Dados pessoais" significam qualquer informação relacionada a um indivíduo identificado ou identificável (titular de dados).
Expansionista	Expansionista	Expansionista	Expansionista	Expansionista	Expansionista
1980	1981	2000	2000	2005	1995/2016

Fonte: BIONI, 2020 [grifo da autora] [30].

[29] BIONI, op. cit., p. 79-80.

[30] Esta tabela foi retirada da obra "Proteção de Dados Pessoais", de Rodrigo Bioni (op. cit., p. 84-85), em seus respectivos idiomas de origem, e foi inserida com a tradução livre da autora dos dispositivos jurídicos internacionais referenciados a fim de trazer maior compreensão e fluidez à leitura do texto e seus elementos gráficos. As legislações citadas tratam-se, da esquerda para a direita, junto de seus originais: "Diretrizes para a Proteção da Privacidade e dos Fluxos Fronteiriços de Dados Pessoais" da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que foram adotadas pelos 37 países-membros da Organização, que foram publicadas e entraram em vigor em 1980; original: "personal data" means any information relating to na identified or identifiable individual (data subject). "Convenção para a proteção dos indivíduos com respeito ao

As legislações ao redor do globo que dispõem de tema análogo à Lei nº 13.709/2018 também possuem caráter expansionista ao conceituar o que seriam dados pessoais, visando abranger as nuances do conceito de dados e informações pessoais, termos comumente associados como sinônimos nas legislações correlatas. É possível observar que tais definições assemelham-se às brasileiras, como é possível observar na tabela comparativa anteriormente disposta, na qual mostra-se algumas normas das diferentes gerações de leis de proteção de dados.

Ainda acerca da definição presente no ordenamento jurídico brasileiro e também das legislações internacionais dispostas na tabela acima, o caráter expansionista ao conceituar os dados pessoais segue um critério de razoabilidade, especialmente ao ter-se em conta que o dado pessoal é parte do sujeito, prolongando-o, e sendo, portanto, uma extensão de sua personalidade. Isso é de fundamental importância ao analisar-se até mesmo os dados anônimos e anonimizados, visto seu enorme potencial em transmutar-se em um dado pessoal, recaindo-lhe neste caso e somente assim, a proteção prevista na LGPD.

O conceito de dado anonimizado está disposto no art. 5º da Lei Geral de Proteção de Dados, no inciso III, como o "dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento", não sendo possível, portanto, identificar o sujeito titular do dado. Dessa forma, o dado anonimizado não é, em tese, objeto de proteção, à exclusão da hipótese anteriormente exposta.

3.1.2 Dados pessoais sensíveis e banco de dados

Os dados pessoais sensíveis tratam-se de especial categoria dos dados pessoais, por tratarem-se, conforme redação contida no art. 5º, inciso II da Lei nº 13.709/18, *in verbis*:

---

processamento automático de dados pessoais", do Conselho da Europa (CoE, do inglês *Council of Europe*), que entraram em vigor somente em 1985; original: "personal data" means any information relating to na identified or identifiable individual ("data subject"). *Personal Information Protection and Eletronic Documents Act*, a PIPEDA, do Canadá; original: personal information means information about na identifiable individual. *Ley de Protección de los Datos personales*, a PDPA (*Personal Data Protection Act*) da Argentina; original: datos personales: información de cualquier tipo referida a personas físicas o de existência ideal determinadas o determinables. *APEC Privacy Framework*, da Cooperação Econômica Ásia-Pacífico (APEC, do inglês *Asia-Pacific Economic Cooperation*), fórum econômico regional que abrange atualmente 21 economias globais; original: personal information means any information about an identified or identifiable individual. Por fim, as legislações europeias: Diretiva 95/46/CE, do Conselho Europeu, em referência ao ano de 1995 e o Regulamento Geral sobre a Proteção de Dados (RGPD ou GDPR, do inglês *General Data Protection Regulation*), de 2016, que inspirou a criação da brasileira LGPD; original: "personal data" means any information relating to an identifiable individual ("data subject").
BIONI, op. cit., p. 84-85.

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

Assim como o conceito de dado pessoal, já presente em textos normativos anteriores à LGPD, a definição de dados sensíveis está inserida na Lei nº 12.414/11, a Lei de Cadastro Positivo, estando presente no art. 3º, § 3º, inciso II, sob o vocábulo sinônimo *informações sensíveis*, sendo "consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

A partir da análise desses dois dispositivos, compreende-se que o princípio da não discriminação é o norteador do tratamento dos dados sensíveis, assim como o princípio fundamental da igualdade e isonomia consagrado no art. 5º da Constituição Federal de 1988. O caráter lesivo, discriminatório e de vulnerabilidade a qual pode expor seu titular, por tratar-se de conteúdo que garante um maior potencial de identificabilidade, demanda um regime mais protetivo por parte das leis de proteção de dados, assim como está disposto no ordenamento brasileiro [31].

Destaca-se, ainda, a conceituação apresentada pelo Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, que define de forma mais ampla os dados pessoais sensíveis e, portanto, alarga a extensão da tutela estatal, conforme extrai-se da definição contida em seu art. 9º, 1, que dispõe sobre o tratamento de categorias especiais de dados pessoais, abaixo transcrito:

> 1. É proibido o tratamento de dados pessoais **que revelem** a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. [grifei]

Apesar de preceder a lei brasileira, o RGPD europeu é perspicaz em trazer no texto normativo a possibilidade dos dados *revelarem-se* informações sensíveis, açambarcando a hipótese anteriormente destacada neste trabalho da "fluidez" contextual. Assim como pode aplicar-se à transmutação de dados anonimizados em dados pessoais, esse fenômeno pode

[31] BIONI, op. cit., p. 99.

incidir também nos dados sensíveis, que anteriormente ao tratamento poderiam tratar-se de dado pessoal ou até mesmo um dado anonimizado.

Essa possibilidade mostra-se – com ainda mais intensidade – materialmente latente ao analisar essas informações sob a perspectiva dos *bancos de dados*, também conceituado na LGPD, em seu art. 5º, inciso IV como "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico", ou, como preceitua Danilo Doneda:

> Banco de Dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações. [...] Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos a respeito das informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terc0eiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.[32]

Os dados sensíveis, além de poderem ser utilizados como elemento discriminatório, tem elevado valor econômico por referirem-se à aspectos da vida particular e tratarem-se do mais refinado material a ser utilizado na *perfilização*, ou seja, na construção de um "eu-virtual" criado a partir da coleta de dados. Conforme apresentado por Moura[33], os dados pessoais estabeleceram-se como uma nova fonte de valor econômico, tornando-se ainda mais valiosos após seu tratamento e processamento, aplicando-se a melhorias em experiências de consumo e identificação de tendências.

É a partir da indexação e organização dessas informações que é possível atribuir-lhe valor econômico, *monetizando* esses dados. Sua força como ativo econômico é expressiva, em constatação à análise da conjectura político-econômico-social global, na qual as empresas que os tem como principal insumo consolidam-se com os maiores valores de mercado – como Google, *Meta* (antigo *Facebook*), Amazon e as gigantes da informática *Microsoft* e *Apple*, por exemplo – elevando os bancos de dados a uma das principais *commodities* globais do século.

Diante de tamanho potencial, a exploração massiva de dados para fins econômicos, mesmo diante do inchaço de regulamentos e leis que buscam tutelar as relações quanto a coleta

[32] DONEDA, 2011, p. 92.
[33] MOURA, op. cit., p. 13.

e tratamento de dados entre pessoas naturais e jurídicas, sejam de direito público ou privado, é utilizada também para fins pouco nobres, atentando-se inclusive a tão cara democracia.

> Dados não são o novo ouro, são o novo urânio. Às vezes pode-se fazer dinheiro a partir deles, mas podem também ser radioativos, perigosos de armazenar, têm usos militares e geralmente você não os quer concentrar em grande quantidade, e são regulamentados. Porque manter urânio quando não lhe é necessário?[34]

Um dos maiores escândalos recentes de coleta e tratamento ilegal de dados é o da empresa britânica de análise de dados *Cambridge Analytica*, que se utilizou de uma lacuna presente nos termos de uso do *Facebook* para coletar dados de milhões de usuários sem conhecimento e, portanto, sem consentimento prévio, "usando dos artifícios das redes sociais para atingir uma massa de indivíduos com publicidade especialmente direcionada a eles", através de "manipulação de dados durante eleições com intuito de favorecer determinadas figuras políticas"[35].

Revelado com exclusividade pelo *The Guardian* e *The New York Times* em 2015, a campanha presidencial do senador e candidato republicano Ted Cruz utilizou-se da estratégia de transformar *likes* em votos[36], ao traçar perfis psicológicos que permitiam traçar perfis de eleitores assim como traçavam os perfis de consumidores, com base em seu comportamento, direcionando propagandas políticas de acordo com o público alvo, conforme afirma o periódico britânico *The Gardian*[37]. A estratégia desenvolvida pela *Cambrigde Analytica*, supervisionada por Steve Bannon, foi também utilizada para outros fins políticos, sendo empregadas na campanha de Donald Trump à eleição presidencial americana de 2018, a saída do Reino Unido

---

[34] VALSORDA, Fillipo. Disponível em < https://twitter.com/filosottile/status/1162404848073170944>. Acesso em: 05 maio 2020. Tradução livre da autora. Original: Data is not the new gold, data is the new uranium. Sometimes you can make Money from it, but it can be radioactive, its dangeros to store, has militares uses, you generally don't want to concentrate it too much, and it's regulated.Why keep uranium you don't need?

[35] ANASTASIA, Vittoria Alvares; LARA, Caio Augusto Souza. **O escândalo cambridge analytica:** a manipulação de dados na era digital. Percurso – Anais do IV Conlubradec (Congresso Luso-Brasileiro de Direito Empresarial e Cidadania). v.4. n. 31. Curitiba: Congresso Luso-Brasileiro de Direito Empresarial e Cidadania, 2019. p. 165.

[36] LAPOWSKY, Issie. **How cambridge analytica sparked the great privacy awakening:** repercussions from the scandal swirling aroud the data analytics firm continue to be felt across the tech industry. Disponível em: < https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>. Acesso em 5 de maio de 2022.

[37] DAVIES, Harry. **Ted cruz using firm that harvested data on millions of unwitting facebook users.** Disponível em: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>. Acesso em 5 de maio 2022. passim.

SOLON, Olivia; GRAHAM-HARRISON, Emma. **The six weeks that brought Cambridge Analytica down.** Disponível em < https://www.theguardian.com/uk-news/2018/may/03/cambridge-analytica-closing-what-happened-trump-brexit>. Acesso em 5 de maio 2022. passim.

da União Europeia, popularmente conhecido como *Brexit*, e também na campanha eleitoral de Jair Bolsonaro à campanha presidencial brasileira de 2018[38].

A manipulação de dados que tornavam possíveis expor o posicionamento político, infringindo a privacidade dos usuários ao tratar de informação tão sensível, foi elemento propulsor do Regulamento Geral de Proteção de Dados europeu, promulgado em 2016 e também da Lei Geral de Proteção de Dados de 2018, ampliando a alçada da tutela jurídica de proteção de dados, consolidando ainda mais seu *status* como direito fundamental autônomo.

3.2. Tratamento de dados e seus agentes

Conforme exposto, os dados permeiam todas as esferas da sociedade, com algoritmos organizados de forma a construir perfis e identidades digitais em bancos de dados, utilizando-os para os mais diversos fins. A regulação proporcionada pela Lei nº 13.709/18 "consagra a obrigatoriedade do gerenciamento seguro do início até o fim da operação que envolve os dados pessoais"[39], tornando-a um freio à extração quase predatória de dados sem consentimento ou ciência do usuário. De forma semelhante posicionam-se Tepedino, Frazão e Oliva, ao afirmarem que:

> Tal aspecto é fundamental para a compreensão da LGPD, porque os valores e objetivos por ela reconhecidos representam um importante contraponto à tendência de monetização dos dados, considerando-os como *commodities* e objeto de livre-extração ou negociação. De forma contrária, os princípios da LGPD mostram que dados não são meros bens de cunho patrimonial, o que revela a insuficiência das soluções de mercado para qualquer disposição a respeito deles. [...] Por essa razão, [...], a disciplina do consentimento não deve ser tratada sob viés negocial, mas sim a partir do poder de autodeterminação e a consideração dos direitos fundamentais em questão.[40]

No ordenamento jurídico brasileiro, o tratamento de dados encontra amparo legal no art. 5º, inciso X da LGPD, transcrito a seguir:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]

---

[38] SANCHES, Mariana. **Aliado de trump e bolsonaro, steve bannon é liberado após entregar passaporte a autoridades americanas.** Disponível em < https://www.bbc.com/portuguese/internacional-59270676>. Acesso em 5 maio 2022. passim.
[39] SARLET; RUARO. op. cit., p. 86.
[40] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p.

> X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avalição ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

O Regulamento Geral de Proteção de dados possui redação semelhante em seu art. 4º, 2:

> 2. <<Tratamento>>, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;[41]

Presentes em inúmeras legislações que tratam da proteção de dados pessoais ao redor do mundo, os princípios que regem, também, o tratamento de dados, dispostos nos incisos do art. 6º da LGPD – **finalidade**, adequação, necessidade, livre acesso, qualidade dos dados, **transparência**, segurança, prevenção, não discriminação, responsabilização e prestação de contas, além do difundido princípio jurídico da boa-fé –, estabeleceram-se ao longo das gerações de normas que buscavam tutelar essa disciplina.

Definidos pela terminologia em inglês *Fair Information Practice Principles (FIPPS)*, os princípios presentes em diversos diplomas legais "formam a espinha dorsal de inúmeras normas existentes atualmente, [...] sendo importante ressaltar que os princípios deverão ser cumpridos, independentemente das bases legais para o tratamento de dados pessoais"[42].

Esses princípios devem ser especialmente observados pelos agentes de tratamento, que, conforme o inciso IX do art. 5º da LGPD, são compostos por dois elementos: o controlador e o operador de dados, à qual recaem responsabilidades e deveres nas relativas às operações de tratamento de dados, definidos nos incisos VI e VII, respectivamente:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

---

[41] UNIÃO EUROPEIA. **Regulamento (eu) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[42] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (cord). **LGPD:** lei geral de proteção de dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 127-128.

> VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Tem-se ainda outras figuras importantes a serem observadas na lida do tratamento de dados, como o encarregado (art. 5º, VIII), equivalente ao DPO (*Data Protection Officer*) da RGPD, que atua como canal de informação entre os agentes de tratamento, e os titulares de dados e a Autoridade Nacional de Proteção de Dados, prevista no inciso XIX, como o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei [Lei n. 13.709/18] em todo o território nacional".

Tabela 3 – O tratamento, seus agentes e o controlador de dados

Tratamento (X)	Agentes de Tratamento (IX)	Controlador (VII)
Toda operação realizada com dados pessoais [...];	Controlador (VI); Operador (VII)	A quem competem as decisões referentes ao tratamento de dados pessoais;

Tendo em foco a discussão de coleta e tratamento de dados por agentes privados, não se pode olvidar o poder massivo do poder público diante do tratamento de dados, devendo este ser objeto de especial regulação, razão pela qual a LGPD reserva um capítulo especial para tratar desta temática. A caminhada rumo à proteção à privacidade, como abordado em seção anterior, iniciou-se ainda no século XVIII, frente ao temor da supervigilância estatal do indivíduo.

Essa realidade não se restringe à história, conforme pode-se constatar frente aos escândalos expostos ao público por Edward Snowden e Julian Assange, que envolviam a vigilância de indivíduos em escala global por parte do governo estadunidense[43], que feriram de morte a já frágil fé do cidadão na capacidade do Estado de tutelar a proteção fundamental à privacidade, já que era ele o principal agente invasor. Curiosamente, a enxuta Constituição

[43] A exposição de documentos secretos sobre a vigilância por parte do governo americano, desde cidadãos comuns à líderes mundiais, tanto por parte do ex-agente da NSA (National Security Agency) quando por Julian Assange, através do site *Wikileaks*, gerou uma crise diplomática sem precedentes nos EUA. A presidenta do Brasil à época, Dilma Roussef, também foi alvo de espionagem. Dentre os desdobramentos causados, pode-se citar a "Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da América por países da Região", aprovada em julho de 2013 e aprovada por cinco países membros do Mercosul: Argentina, Bolívia, Brasil, Uruguai e Venezuela).
G1. **Entenda o caso edward snowden, que revelou espionagem dos eua,** passim.
WELLE, Deutsche. **Entenda o caso assange e wikileaks fato a fato.** passim.
GREENWALD, Glenn; MACASKILL, Ewen. POITRAS, Laura. **Edward snowden:** the whistleblower behind the nsa surveillance revelations. passim.

Americana não se utiliza da expressão "privacidade" explicitamente. A proteção da privacidade e, por analogia, dos dados, é essencial ao exercício pleno da liberdade do indivíduo, conforme extrai-se do posicionamento de Daniel J. Solove: "quando protegemos a privacidade, nos protegemos contra interrupções de certas atividades. Uma invasão de privacidade interfere com a integridade de certas atividades e até mesmo destrói ou inibe algumas atividades"[44].

Se tal violação deu-se diante de um Estado democrático de direito, no qual o consentimento é requisito básico para a coleta de dados[45], em países governados de forma ditatorial, a coleta de dados é utilizada de forma a superar distopias ficcionais, como a apresentada no episódio intitulado "Queda Livre", da série britânica *Black Mirror*[46], que aborda a superexposição e *oversharing*, o compartilhamento de informações "a mais" que o necessário, como forma de garantir benefícios e popularidade entre seus pares, mas servindo também como elemento punitivo.

Caso semelhante ocorre na China[47], onde o governo chinês criou o *Sesame Credit* ou *Zhima Credit*, um sistema de score de crédito semelhante ao brasileiro Serasa, que avalia o histórico financeiro do consumidor. Todavia, no sistema chinês, essas informações são utilizadas para compor um banco de dados com hábitos, padrões de consumo e comportamentos, estes fornecidos por grandes multinacionais, para punir ou recompensar os cidadãos diretamente em seu *score* de crédito.

---

[44]Traduzido pela autora. Original: "when we protect privacy, we protect against disruptions to certain activities. A privacy invasion interferes with the integrity of certain activities and even destroys or inhibits some activities". SOLOVE, Daniel J. **Understanding privacy.** Cambridge: Havard University Press, 2008. p. 9.

[45] A necessidade de consentimento é prevista em legislações estadunidenses que tratam de proteção de dados e privacidade, como a *California Consumer Privacy Act (CCPA)*, que trata de mecanismo de proteção e autonomia ao consumidor sobre a coleta de dados, traz o conceito de consentimento, 1798.140., *h*: "*'Consent' means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent*.
ESTADO DA CALIFÓRNIA. **California consumer privacy act of 2018.** Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>. Acesso em 8 maio 2022.

[46] QUEDA livre (temporada 3, ep. 1). Black Mirror [Seriado]. Criação: Charlie Brooker. Direção: Joe Wright. Roteiro: Michael Schur e Rashida Jones. Publicado em: 21 de outubro de 2016. Duração: 63 minutos. Netflix. Disponível em: <https://www.netflix.com/watch/80104627 >. Acesso em: 7 maio 2022.

[47] CAMPBELL, Charlie. **How china is using "social credit scores" to reward and punish its citizens.** Disponível em: < https://time.com/collection/davos-2019/5502592/china-social-credit-score/>. Acesso em 7 maio 2022. passim.
LAZARINI, Maria Teresa. **Muito mais que um score de crédito:** conheça o score social da china. Disponível em: < https://www.iq.com.br/financas-pessoais/artigos/score-social-china>. Acesso em 7 maio 2022. passim.

Essa conduta colide frontalmente com o previsto na Lei Geral de Proteção de Dados, no que tange ao tratamento de dados pessoais sensíveis, já que a situação exemplificada se trata do emprego de dados pessoais sensíveis como fomentares de uma prática discriminatória. O tratamento de dados pessoais sensíveis é disciplinado na seção II da Lei nº 13.708/18, a quais são passíveis de tratamento somente diante de consentimento do titular, com exceção expressa em rol taxativo disposto no inciso II do art. 11.

3.2.1 O titular de dados

Classificar o titular como *proprietário* dos dados a ele relativos tratar-se-ia de grande equívoco, visto que em sua natureza jurídica, os dados não se delimitam a um bem, propriedade a ser tutelada pelo Estado, mas à extensão do próprio indivíduo, de sua personalidade. Com amparo no art. 5º, inciso V da Lei Geral de Proteção de Dados, o titular é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

Sendo assim, são necessárias uma série de garantias que visem a proteger os direitos do titular de dados através de princípios relacionados ao tratamento de dados pessoais, protegendo também, por extensão, os limites dos direitos fundamentais[48]. Neste sentido:

> O **titular dos dados pessoais é o núcleo da existência de uma Lei Geral de Proteção de Dados Pessoais**, afinal, a preocupação sobre eventuais violações aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade está umbilicalmente vinculada à pessoa natural [grifei].[49]

Dotado de protagonismo diante da supracitada Lei, que orbita em volta da proteção aos direitos fundamentais, especialmente a privacidade e personalidade, o titular possui uma série de direitos dispostos no capítulo III da LGPD, que lhe permitem, por exemplo, acessar os dados coletados que são objeto de tratamento, corrigi-los, anonimizá-los e excluí-los. Esses direitos serão por ele exercidos a qualquer momento, mediante requisição.

Garantidores de uma espécie de controle, esses direitos são fundamentais aos esforços de garantir, ao menos formalmente, paridade entre agentes e titulares, sendo este elo mais fraco nessa relação, hipossuficiente. Salvo em exceções também expressas em rol taxativo pela lei, a

[48] PINHEIRO, 2020, p. 81.
[49] MALDONADO; BLUM, 2019, p. 95.

coleta, momento inicial do tratamento, se dará a partir do consentimento do titular, de "forma livre, informada e inequívoca", como dispõe o art. 5º, inciso XII da LGPD.

Faz-se mister diferenciar a terminologia entre *titularidade* e *propriedade*. A propriedade é espécie da qual a titularidade é gênero, o que denota a intenção do legislador em tutela mais ampliada que aquela destinada às relações proprietárias:

> O conceito de titularidade exprime, portanto, não apenas a ideia de poder de controle sobre um bem jurídico mas, também e consequentemente, o sentido de atribuição do mesmo, com regras claras disponíveis acerca de seus modos de utilização e disposição. Se dados pessoais são hoje bem jurídicos – daí a inequívoca necessidade de tutelá-los –, precisava o legislador determinar a quem pertencem, fosse acerca de seus aspectos extrapatrimoniais – principal justificativa da crítica dirigida por Daniel Solove aos que enxergavam a privacidade dos dados pessoais apenas como o objeto de um direito de propriedade –, fosse relativamente a seus aspectos patrimoniais, decorrentes do valor econômico que lhes foi atribuído pela sociedade digital.[50]

Fazendo-se entender o porquê da adoção do termo *titularidade* pelo legislador, observa-se que estes conceitos não são antagônicos, e sim pertencentes à uma mesma categoria, estando atrelados aspectos tanto patrimoniais – em se tratando da mercantilização dos dados, transformando-os em bens digitais – quanto extrapatrimoniais, à exemplo da aplicabilidade da responsabilidade civil como forma de reparar danos morais sofridos pelo titular, conforme art. 42 da LGPD[51].

[50] TELEPEDINO; FRAZÃO; OLIVA, 2019, p. 65.

[51] A LGPD não traz com clareza em seu texto normativo se a responsabilidade civil a ser aplicada trata-se da objetiva ou subjetiva. Pode-se afirmar, somente e com certeza, que quando envolver relação de consumo, a responsabilidade civil objetiva será aplicada, conforme previstos nos art. 12 e 14 do Código de Defesa do Consumidor (CDC).

4. A VALIDADE DO CONSENTIMENTO E A REAL ANUÊNCIA DO TITULAR DE DADOS

A proteção a qual a tutela estabelecida pela LGPD recai orbita na concessão de controle sobre os dados pessoais ao seu titular, a autodeterminação informativa. Conforme preceitua Viviane da Silva Coelho Vasques[52], "o dever de informação sobre a utilização e destinação destes dados e necessidade de consentimento informado concede controle ao titular sobre os dados, protegendo-os contra usos indevidos e identificando os responsáveis".

Dessa forma, para que o tratamento de dados seja lícito, é necessário antes haver o consentimento por parte de seu titular, conforme inciso I, art. 7º. Essa premissa é essencial quando tratar-se de dados pessoais e imprescindível ao tratamento de dados pessoais sensíveis. Para ser considerada adequada, essa anuência deve ser fornecida "por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (art. 7º, § 8º da LGPD), em documento denominado termo de consentimento.

De forma semelhante à RGPD, a definição do consentimento está presente no art. 5º, inciso XII da Lei nº 13.709/18, devendo tratar-se de "manifestação **livre**, **informada**, e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma **finalidade determinada**" (grifei). O consentimento é um dos requisitos necessários à licitude do tratamento, sendo trazido ainda de forma extensa no art. 7º da RGPD, que trata das condições a ele aplicáveis.

4.1 Manifestação livre, informada, inequívoca e de finalidade determinada

Tabela 4 – Esquematizando a manifestação do consentimento

Livre	Informada	Inequívoca	Finalidade Determinada
Assegura-se ao titular a escolha de consentir ou não à cessão de seus dados;	O titular tem direito de compreender a mensagem transmitida pelo controlador, de forma esclarecida;	O consentimento deve ser dado de forma expressa, através de ação ou declaração do titular;	Garantia de licitude. Trata-se do limite de atuação do tratamento de dados;

[52] VASQUES, Viviane da Silva Coelho. Considerações sobre a proteção de dados pessoais sensíveis no ambiente virtual. **Cibernética jurídica:** estudo sobre o direito digital. Cláudio Joel Brito Lóssio; Luciano Nascimento; Rosangela Tremel (Organizadores). Campina Grande: EDUEPB, 2020. P. 252-261. p. 560.

Sendo o elemento central para a permissão de uso de dados pessoais, o consentimento em ambiente informático já havia sido disciplinado no ordenamento jurídico, quando o Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, trouxe, em seu art. 7º, inciso IX, o direito ao "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais", atribuído ao usuário de internet.

Com o advento da LGPD, em 2018, essa concordância passou a ser dotada de uma série de pressupostos de validade, devendo esta ser livre, informada, inequívoca e com finalidade determinada, de acordo com a supracitada lei. Ao solicitar o consentimento ao titular, os agentes de tratamento de dados devem estar atentos ao cumprimento de tais requisitos, sob pena de invalidade pelo consentimento estar, de certa forma, viciado, especialmente quando houver desequilíbrio entre estes dois atores[53]. Esse entendimento está expresso no art. 8º, §3º da Lei nº 13.709/18, *in verbis*:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> [...]
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

Destarte, adentra-se a esses pressupostos. Quanto ao quesito liberdade, deve ser assegurado ao titular a escolha de consentir ou não à cessão de seus dados, excluindo-se as exceções de inexigência de consentimento previstas na Lei nº 13.709/18, de forma que a anuência se atenha somente ao necessário para a finalidade por ele ensejada, para a execução de contrato ou serviço a que se refere o tratamento. "Qualquer elemento capaz de exercer influência ou constrangimento ao titular de dados pessoais acarretará a invalidez de seu consentimento ao tratamento de informações"[54], causando, portanto, a invalidade da anuência do titular.

[53] NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da. O consentimento na lei geral de proteção de dados: autonomia privada e o consentimento livre, informado, específico e expresso. p. 29.
[54] Ibid., p. 28.

A manifestação informada interliga-se não somente à simples observância de políticas de privacidade e termos de uso[55] que antecedem seu consentimento. Trata-se da compreensão da mensagem que o controlador quer transmitir ao usuário, dando-lhe , de fato, real noção do procedimento ao qual seus dados serão submetidos. Nesse sentido:

> [...] a mera utilização de farta documentação esparsa, ainda que abordando os diversos tratamentos efetuados pelo controlador – mas sem fornecer ao titular uma noção completa e clara daquilo que, efetivamente, será feito –, pode não se mostrar efetiva para a satisfação ao pleno direito à informação, o que caracteriza uma política de tratamento pouco transparente.[56]

É necessário fazer-se entendido de fato, utilizando-se de *legal design*[57] que busque democratizar o conhecimento tecnológico, mesmo diante das complexidades dos procedimentos e operações que envolvem o tratamento de dados. Apenas atribuir responsabilidade ao titular sobre seus próprios dados sem preocupar-se em democratizar conhecimentos tecnológicos mostra-se ineficiente e injusto, além de cindir a confiança do cidadão em serviços na sociedade da informação[58]. Dar total controle ao titular sobre algo que ele não sabe ao certo não muda tal situação[59].

O consentimento inequívoco deve ser dado de forma expressa, como também preceitua o Marco Civil da Internet[60], por meio de "uma ação positiva ou mediante declaração por escrito" destacando-se que, quando tratar-se desta última modalidade, deve constar "cláusula contratual destacada das demais, com fim de atestar uma manifestação de vontade expressa do titular"[61]. Em âmbito cibernético, essa anuência comumente se dá através de cliques, quando o usuário concorda com os termos de uso e política de privacidade de determinado sítio eletrônico; há

---

[55] As Políticas de Privacidade e Termos de Uso são documentos que, respectivamente, explicam como cada plataforma vai coletar, tratar e usar dados pessoais e que também indicam como o serviço funciona, qual a finalidade, quais recursos são acessados pelo dispositivo do titular, e as responsabilidades da plataforma e do usuário titular de dados.

[56] NOGUEIRA; FONSECA. op. cit., p. 30.

[57] *Legal Design* é, conforme definição dada por Maia, Nybø e Cunha (p. 15, 2020) "a aplicação de princípios e elementos de *design* e a experiência do usuário na concepção e na elaboração de documentos ou produtos jurídicos."
MAIA, Ana Carolina; NYBØ, Erik Fontenele; CUNHA, Mayara. **Legal design:** criando documentos que fazem sentido para os usuários. São Paulo: Saraiva Educação, 2020. Edição Kindle.

[58] BARROS, Juliano Napoleão de. Big data, proteção de dados e transparência: desafios para a consolidação da confiança e garantia dos direitos do cidadão. **Revista culturas jurídicas.** Vol. 7. Num. 17, maio/ago. p. 244.

[59] BACHLECHNER, Daniel; FORS, Karolina La; SEARS, Alan M. **The Role of privacy-preserving technologies in the age of big data.** 13th Pre-ICIS Workshop on Information Security and Privacy, São Francisco, 13 dez. 2018. p. 9.

[60] O Marco Civil da Internet qualifica que o consentimento deve ser **expresso**, conforme o inciso IX do art. 7º: "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

[61] NOGUEIRA; FONSECA, op. cit., p. 34.

ainda a concordância tácita com a política de *cookies*,[62] pelo simples ato de permanecer navegando no site. Tamanha facilidade é objeto de crítica por Nogueira e Fonseca, que alertam sobre a banalização deste importante instituto:

> Em suma, é fato que, diante das exigências da LGPD, cada vez mais os titulares serão obrigados a manifestar a sua concordância expressamente para diversos tipos de tratamentos, por vários e distintos controladores. No contexto digital, em especial, é grande a demanda diária por consentimento, o que acaba por acarretar num fenômeno conhecido por "fadiga do consentimento". É que, ao lidar com uma profusão de "cliques" – todos com o intuito de obter algum tipo de autorização – , o alerta dos mecanismos de consentimento termina por dispersar, já que informações relevantes sobre os termos da anuência passam a não ser lidas na sua totalidade.[63]

Presente na parte final do inciso XII, art. 5º da LGPD, a finalidade determinada é importante garantia de licitude por tratar-se do limite de atuação do tratamento de dados, sendo relativa "tanto ao limite de informações a serem coletadas quanto à finitude do procedimento no tempo"[64], assegurando ao titular de dados liberdade de escolha e transparência, além de assegurar certo grau de controle ao utilizador, correlacionando-se diretamente ao consentimento informado[65].

4.2. O consentimento dentro das relações de consumo

A ampliação do acesso de dispositivos informáticos, desde o celular à eletrodomésticos e eletroeletrônicos interligados à sistemas de IoT (internet das coisas)[66] e *softwares* diversos,

---

[62] Conforme a SaferNet Brasil, "um *cookie* é um pequeno arquivo robô usado por servidores de Internet para diferenciar seus usuários e para capturar os dados relacionados à navegação de cada usuário em um site. Serve tanto para armazenar os dados de um usuário no momento de efetuar comprar online, como para dar permissão de acesso a um determinado usuário do site.
Os cookies rastreiam o comportamento dos internautas no momento da navegação e geram informações valiosas sobre os usos e costumes de cada internauta, o que facilita lançamento de campanhas publicitárias, vendas de determinados produtos, etc.
SAFERNET Brasil. **Você sabe o que são cookies e como eles interferem em sua privacidade?** Disponível em: <https://new.safernet.org.br/content/você-sabe-o-que-são-cookies-e-como-eles-interferem-em-sua-privacidade#mobile>. Acesso em: 21 maio 2022.

[63] NOGUEIRA; FONSECA, op. cit., p. 35-36.

[64] PINHEIRO, 2020, p. 96.

[65] NOGUEIRA; FONSECA, op. cit., p. 33.

[66] A Internet das Coisas, do inglês *Internet of Things*, pode ser descrita como a rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet". Através da "computação de baixo custo, nuvem, big data, análise avançada e tecnologias móveis, coisas físicas podem compartilhar e coletar dados com o mínimo de intervenção humana. Nesse mundo hiperconectado, os sistemas digitais podem gravar, monitorar e ajustar cada interação entre itens conectados. O mundo físico encontra o mundo digital, e eles trabalham em conjunto", o que torna a IoT uma das mais importantes tecnologias do século.

trouxe a democratização da tecnologia, mas não necessariamente de *conhecimentos* tecnológicos. Com o aumento do fluxo informacional e da demanda por tecnologias cada vez mais personalizadas, o indivíduo, de bom grado e passivamente, cede "gratuitamente" seus dados em troca de experiências personalíssimas online.

Diante dessa perspectiva, mesmo diante da inobservância dos usuários, que por vezes não demonstram qualquer óbice em utilizar-se do escambo entre dados e serviços aparentemente vantajosos, recai ao Estado a responsabilidade de proteção e tutela do usuário, visto que, conforme preceitua Doneda[67], "as consequências que dele podem advir podem ser pouco nítidas e difíceis de serem identificadas".

> A necessidade de proteger juridicamente o cidadão é oriunda do fato de que os dados pessoais detêm teor econômico tendo em vista à possibilidade de sua comercialização. Isso geralmente é usado por empresas que realizam negócios "online". Os dados pessoais de um consumidor traduzem aspectos de sua personalidade e revelam comportamentos e preferências, tornando-o um alvo fácil de mensagens publicitárias dirigidas.[68]

Quando se aborda o tratamento de dados sob ótica consumerista, eles contam com dupla camada de proteção, sendo protegidos também pela Lei nº 8.078/90, o Código de Defesa do Consumidor, além da própria LGPD. Ao disciplinar as relações entre o consumidor[69] e o fornecedor[70], o CDC traz uma série de direitos básicos do consumidor em seu art. 6º, dos quais podemos destacar o direito à liberdade de escolha e igualdade nas contratações, à informação adequada e clara, à proteção contra publicidade enganosa e cláusulas abusivas e também à facilitação da defesa de seus direitos.

Se na relação assimétrica de poder frente ao fornecedor o consumidor é tido como vulnerável, sendo-lhe necessária proteção específica, ao somar-se o grau de exposição ao qual

---

ORACLE. **O que é iot?.** Disponível em: <https://www.oracle.com/br/internet-of-things/what-is-iot/>. Acesso em: 21 maio 2022.

[67] DONEDA, 2020, p. 293-294.

[68] GARCIA, op. cit. p. 3.

[69] Consumidor, conforme o art. 2º do CDC, "é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final", equiparando-se ao consumidor, de acordo com o parágrafo único, "a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo".

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 21 maio 2022.

[70] A figura do fornecedor é disciplinada pelo CDC, em seu art. 3º, como "todo pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços".

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 21 maio 2022.

está submetido o mercado informacional, ele será hipervulnerável[71]. É comum ao consumidor a concessão de dados pessoais diversos, inclusive de dados pessoais sensíveis, para a celebração de toda sorte de contratos consumeristas. Por conseguinte, é comum também que o consumidor seja a vítima mais recorrente quanto a violação desses dados, estando inclusive previsto na LGPD, art. 45, que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

4.3 A revogação do consentimento

O consentimento é a manifestação da vontade do titular. Nesta senda, não é incomum que o termo de consentimento se dê em formato de contrato de adesão[72], o que torna deveras limitada a forma com a qual o titular pode dispor das condições atreladas à sua anuência: ou concorda com tudo ou discorda de sua totalidade, consequentemente abrindo mão também do que adviria através do consentimento do tratamento de dados.

Esta recusa pode ocorrer prontamente à solicitação do consentimento ou em momento posterior à concordância, sendo retirada sem que isso acarrete ilicitude ao tratamento previamente consentido, mas impossibilitando sua continuidade. Quanto ao procedimento de revogação do consentimento, a LGPD se posiciona, em seu art. 8º, §5º, que "o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado". A RGPD se posiciona neste mesmo sentido, pontuando que tal anuência "deve ser tão fácil de retirar quanto de dar (art. 7º, 3, RGPD).

> Relativamente ao sistema proposto pela LGPD, se o consentimento para o uso dos dados equivale a uma forma de deles dispor, e a realidade mostra que estes podem ser sucessivamente cedidos a terceiros sem a devida autorização, é razoável considerar que o controle sobre eles, assegurado por lei ao seu titular, possa ser oponível *erga omnes*[73].

Se os dados são uma extensão da pessoa natural, seu eu-virtual, nada mais coerente que inserir essa proteção em perspectiva equivalente aos direitos de personalidade, atribuindo-

---

[71] BIONI, op. cit., p. 186.

[72] Conforme disposto no art. 54 do Código de Defesa do Consumidor, o contrato de adesão é "aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo".
BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em 21 maio 2022.

[73] TELEPEDINO; FRAZÃO; OLIVA, op. cit., p. 66.

lhe também as características a ele conferidas, como a oponibilidade *erga omnes*, conforme defendido por Tepedino *et. al*, com efeitos que irradiam em todos os campos, impondo à coletividade o dever de respeitá-los[74], fazendo do controle do titular um direito absoluto. Absoluta, porém, não é a liberdade no ciberespaço, razão pela qual o particular ou o próprio Estado devem ser responsabilizados por eventuais danos causados ao titular e à exposição de dados pessoais[75].

4.4. Em busca do consentimento eficaz, válido e legal

Em consonância aos avanços legislativos internacionais, ratificando os meios de tutela de dados pessoais já existentes, inseriu-se no ordenamento jurídico brasileiro lei específica de forma a assegurar a autodeterminação informativa ao titular de dados, resguardando e protegendo os direitos fundamentais do titular à privacidade e personalidade: a Lei nº 12.709/18, a Lei Geral de Proteção de Dados. Entretanto, o atual modelo de consentimento mostra-se falho, e em realidade, a grande maioria da população continua a não saber com o que de fato está consentimento, carentes de informações e conhecimentos necessários para compreender os intrincados termos de uso e políticas de privacidade com os quais anuiu.

Diante do fenômeno de superexposição na internet cada vez mais comum através das redes sociais e o compartilhamento de informações além das necessárias – *oversharing* –, a dispensa de consentimento prevista no art. 7º, § 4º[76] da LGPD, por exemplo, mostra significativa abertura às já abundantes violações de dados, mesmo após o início da vigência da Lei Geral de Proteção de Dados. O consentimento, mesmo que aplicado de forma eficaz, cumprindo os requisitos trazidos pela LGPD, seria ficto. Neste sentido, Magrani e Oliveira pontuam contundente crítica:

> O modelo de consentimento do usuário como elemento central para a permissão do uso de seus dados pessoais tem se mostrado ineficaz diante de recorrentes abusos contidos nos termos de uso dos provedores e seu descompasso com os direitos humanos. [...] Ademais, ainda que esse modelo fosse eficazmente aplicado, no cenário de internet das coisas e de inteligência artificial, em que a comunicação de dados é feita de forma acelerada e

[74] STOLZE, Pablo; PAMPLONA FILHO, Rodolfo. **Manual de direito civil.** 4. ed. São Paulo: Saraiva Educação, 2020. p. 130.
[75] GARCIA, op. cit., p. 4.
[76] Art. 7º, § 4º da LGPD: "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei."
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 21 maio 2022.

> constante entre máquinas e humanos, a necessidade de ter a todo momento um consentimento expresso verdadeiramente informado para o tratamento de dados irá impor um desafio enorme na prática para que seja realmente eficaz".[77]

À vista do conteúdo até aqui disposto, questiona-se então, se seria necessário mais uma vez inflar o ordenamento pertinente ao tema, com um novo modelo de consentimento positivado na lei pátria, de forma a garantir-lhe real eficácia diante da necessidade de torná-lo válido e legal.

Abre-se assim espaço para testar novos modelos de forma a garantir o consentimento manifesto de forma livre, informada e inequívoca por parte de seu titular, com finalidade específica delimitada pelo controlador de dados. Uma possível solução já se encontra inserida no RGPD[78] europeu e também na LGPD, ao longo de seus princípios e de forma expressa no art. 46[79], o modelo denominado *privacy by design* (PBD), desenvolvido pela canadense Ann Cavoukian (2011), especialista em dados, comissária de informação e privacidade à época, no fim dos anos 90.

Mesmo não se tratando de modelo novíssimo, a diretriz[80] composta por sete princípios norteadores contradiz a obsolescência do modelo massivamente aplicado. De forma a colocar

---

[77] MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A internet das coisas e a lei geral de proteção de dados: reflexões sobre os desafios do consentimento e do direito à explicação. **Revista do Advogado**, São Paulo, n. 144, nov. 2019, p. 82.

[78] O conceito de *privacy by design* e *privacy by defalult* está inserido em todo o art. 25 da RGPD, que trata da proteção de dados desde a concepção e por defeito, *in verbis*:

"1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.

2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares."

[79] A conceito de PBD pode ser encontrada de forma expressa na LGPD:

"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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei".

§ 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

[80] CAVOUKIAN, Ann. Information & privacy: 7 foundational principles. **Internet architecture board**. 2011. passim.

a tecnologia a serviço da privacidade[81], Cavoukian criou um modelo na qual a proteção à privacidade deve ser uma diretriz a ser estabelecida desde a concepção de projetos que envolvam o tratamento de dados, por padrão (*privacy by default*).

> Privacy by Design é sobre como um projeto deve ser desenvolvido. [...] Desde o início de qualquer projeto envolvendo dados pessoais, é necessário considerar a segurança e privacidade dos dados, antecipando problemas e reduzindo o risco de furto e vazamento de dados. Os projetos gerados por meio desse conceito são proativos. Eles oferecem controle para que as pessoas alterem as configurações padrão do sistema, optando por fornecer os dados ou não. Quando falamos sobre Privacy by Default, é necessário entender que "por padrão" significa que as configurações mais seguras são aplicadas por padrão assim que o produto ou serviço é lançado ao público. Ou seja, as pessoas não precisam escolher as configurações de privacidade e proteção, pois essas configurações são pré-configuradas considerando a privacidade. Todas as informações pessoais fornecidas são coletadas apenas para a entrega do serviço ou produto. Mesmo com Privacy by Design e Privacy by Default, todos os dados necessários devem ser informados às pessoas, bem como a finalidade de cada um deles. [...] É possível entender que a Privacy by Default é uma consequência da Privacy by Design. Ambas são estratégias que, quando bem executadas, garantem a privacidade, ponto fundamental hoje em dia.[82]

Mostra-se, aqui, um modelo de consentimento mais eficaz ao trazer, além da autodeterminação informativa, recaindo ainda ao titular o controle e consentimento em relação aos seus dados pessoais, a adoção da privacidade como padrão de ética e governança de dados, e não como uma escolha banal a ser tomada diante de termos que não se fazem compreender. A inovação deve-se ser atrelada à garantia de proteção jurídica e ao livre exercício de direitos fundamentais. A tecnologia deve estar a favor da privacidade e orientada pelo direito, não o contrário. O Estado de Direito, com seus valores e princípios, deve ser o responsável por regular a forma com a qual a tecnologia molda o comportamento dos indivíduos[83], em vista de proteger direitos fundamentais e o bem maior que é a dignidade da pessoa humana[84].

---

[81] As tecnologias voltadas à proteção de dados são chamadas de PETs (do inglês Privacy-Enhancing Technologies), sendo a prática do PBD uma dessas tecnologias.

[82] SIMONETE, Marcel. Privacy by design e privacy by default. **Centro de estudos sociedade e tecnologia.** Vol. 6. N. 6. São Paulo: USP, 2021. p. 2.

[83] MAGRANI; OLIVEIRA, op. cit., p. 85.

[84] Sobre a dignidade da pessoa humana, pontua Flávia Piovesan (2018, p. 109-110): "Sustenta-se que é no princípio da dignidade humana que a ordem jurídica encontra o próprio sentido, sendo seu ponto de partida e seu ponto de chegada, para a hermenêutica constitucional contemporânea. Consagra-se, assim a dignidade humana como verdadeiro superprincípio, a orientar tanto o Direito Internacional como o Direito interno. [...] a dignidade da pessoa humana é princípio que unifica e centraliza todo o sistema normativo, assumindo especial prioridade. A dignidade humana simboliza, desse modo, verdadeiro superprincípio constitucional, a norma maior a orientar o constitucionalismo contemporâneo, nas esferas local e global, dotando-lhe de especial racionalidade, unidade e sentido.

PIOVESAN, Flávia. **Direitos humanos e direito constitucional internacional.** 18. ed. rev. e atual. São Paulo: Saraiva Educação, 2018.

CONSIDERAÇÕES FINAIS

Em vista dos aspectos expostos, não se tem intenção de esgotar todas as discussões sobre o presente assunto, mas de apresentar reflexões, propor estudos futuros e ampliar a discussão sobre temática tão importante a qual se trata a materialidade do atual modelo de consentimento e a real anuência do titular de dados trazida pela Lei Geral de Proteção de Dados, presente também em dispositivos diversos do ordenamento jurídico pátrio.

Sob o fomento de garantir ao titular o exercício pleno de seus direitos fundamentais, vislumbra-se um futuro no qual a proteção de dados e a autodeterminação informativa também fará parte do distinto rol dos direitos constitucionalmente consagrados, não meramente enunciados, mas positivados sob intenção do constituinte de que sua aplicabilidade seja plena e *erga omnis*.

Levando-se em conta o que foi observado, faz-se necessário concomitantemente firmar compromisso com a geração de conhecimento e capacitação, e também com a autodeterminação informacional do indivíduo, para que ele saiba, de fato, como dispor de seus dados e exercer seus direitos de forma plena e digna, sendo-lhe assegurada a privacidade, a qual repousa o direito de ser deixado em paz, conforme apontam Samuel Warren e Louis Brandeis (1890). A democracia em âmbito digital depende da proteção e tutela do eu-virtual, que se encontra em permanente estado de suscetibilidade, no qual seus dados são exigidos como moeda de troca pela inclusão digital.

Diante dessa perspectiva, é imprescindível garantir ao titular de dados mecanismos que tornem possível o exercício desses direitos, que se darão somente através da eficácia do consentimento manifestamente livre, informado e inequívoco. Mesmo diante da falha do modelo atual, faz-se possível alternativas que não representarão hipertrofias legislativas, como os conceitos de *privacy by design* e *privacy by default*, já inseridos na LGPD, sendo necessário tão somente aos controladores e autoridades responsáveis cumprir, de forma ética e guiados por boa-fé, a intenção maior prevista pela LGPD, disposta em seu art. 1º: a proteção dos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

REFERÊNCIAS

ANASTASIA, Vittoria Alvares; LARA, Caio Augusto Souza. O escândalo cambridge analytica: a manipulação de dados na era digital. **Percurso** – Anais do IV Conlubradec (Congresso Luso-Brasileiro de Direito Empresarial e Cidadania). v.4. n. 31. p. 164-167. Curitiba: Congresso Luso-Brasileiro de Direito Empresarial e Cidadania, 2019.

BACHLECHNER, Daniel; FORS, Karolina La; SEARS, Alan M. **The role of privacy-preserving technologies in the age of big data.** 13th Pre-ICIS Workshop on Information Security and Privacy, São Francisco, 13 dez. 2018. Disponível em: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=wisp2018>. Acesso em: 19 maio 2022.

BARROS, Juliano Napoleão de. Big data, proteção de dados e transparência: desafios para a consolidação da confiança e garantia dos direitos do cidadão. **Revista culturas jurídicas.** vol. 7. num. 17, maio/ago. 2019. p. 240-254.

BAUMAN, Zygmunt. **Vigilância líquida**. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

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

BONAVIDES, Paulo. **Teoria constitucional da democracia participativa:** por um direito constitucional de luta e resistência, por uma nova hermenêutica, por uma repolitização da legitimidade. São Paulo: Malheiros, 2001.

BRASIL. **Constituição da república federativa do brasil**: promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm >. Acesso em 27 mar. 2022.

_____. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em 27 mar. 2022.

_____. **Lei nº 12.414, de 9 de junho de 2011:** disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 27 mar. 2022.

_____. **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: 3 maio 2022.

_____. **Lei nº 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: 20 maio 2022.

_____. **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 29 mar. 2022.

CASTELLS, Manuel. **A galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade. Brasil, Zahar, 2003.

CAVOUKIAN, Ann. Information & privacy: 7 foundational principles. **Internet architecture board**. 2011. Disponível em: <https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf >. Acesso em 22 maio 2022.

DETERMANN, Lothar. **Determann's field guide to data privacy law –** international corporate compliance. 2. ed. Massachusetts: Edward Elgar, 2015 apud 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 Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** V. 12, N. 2. Joaçaba: Revista Espaço Jurídico, 2011, p. 91-108.

_____. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

ESTADO DA CALIFÓRNIA. **California consumer privacy act of 2018.** Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>. Acesso em 8 maio 2022.

GARCIA, Keila Lacerda de Oliveira Magalhães. **O direito à proteção de dados pessoais e sua lacuna legal no brasil**. ed. 94. v. 1. Revista Científica Semana Acadêmica. ISSN 2236-6717 versão *online*. Disponível em <https://semanaacademica.org.br/artigo/o-direito-protecao-de-dados-pessoais-e-sua-lacuna-legal-no-brasil>. Acesso em: 25 set. 2019.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. **Proteção jurídica de dados pessoais:** a intimidade sitiada entre o estado e o mercado. N. 47. Curitiba: Revista da Faculdade de Direito – UFPR, 2008, p. 141-147.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A internet das coisas e a lei geral de proteção de dados: reflexões sobre os desafios do consentimento e do direito à explicação. **Revista do Advogado**, São Paulo, n. 144, nov. 2019, p. 80-89.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (cord). **LGPD:** lei geral de proteção de dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020.

MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. Trabalho de Conclusão de Curso (Mestrado) – Faculdade de Direito da Universidade de Brasília, Brasília, 2016. Disponível em: <https://repositorio.unb.br/bitstream/10482/34290/3/2018_ClarissaMenezesVazMasili.pdf>. Acesso em: 26 mar. 2022.

MASSON, Nathalia. **Manual de direito constitucional.** 8 ed. rev. ampl. e atual. Salvador: Juspodivm, 2020.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 16. ed. São Paulo: Saraiva Educação, 2021.

MORAES, Alexandre de. **Direitos humanos fundamentais:** teoria geral. 12 ed. São Paulo: Atlas, 2021.

MOURA, Clarissa Maria Lima. **Dados pessoais como ativo na economia digital:** a tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos. 2019. Trabalho de Conclusão de Curso (TCC) – Faculdade de Direito da Universidade Federal de Pernambuco. Recife, 2019. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/37157/1/Dados%20Pessoais%20Como%20Ativo%20na%20Economia%20Digital%20-%20A%20tutela%20jurídica%20na%20legislação%20nacional%20e%20europeia%20acerca%20da%20manipulaçao%20de%20dados%20sensíveis%20para%20fins%20econômicos%20-%20Clarissa%20Maria%20Lima%20Moura.pdf >. Acesso em: 22 mar. 2022.

NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da. O consentimento na lei geral de proteção de dados: autonomia privada e o consentimento livre, informado, específico e expresso. **Lei geral de proteção de dados:** uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Bernardo Menicucci Grossi (org.). Porto Alegre: Editora Di, 2020. p. 15-44.

PEREZ LUÑO, Antonio-Enrique. Teledemocracia, ciberciudadania y derechos humanos. **Revista brasileira de políticas públicas.** v. 4. n. 2. p. 9-45. ISSN 2236-1677. Brasília: CEUB, 2014.

PINHEIRO, Patrícia Pack. **Direito digital.** 7. Ed. São Paulo: Editora Saraiva, 2021. 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 15 mai. 2022.

_____. **Proteção de dados pessoais.** São Paulo: Editora Saraiva, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553613625/. Acesso em: 15 mai. 2022.

RAMOS, André de Carvalho. **Curso de direitos humanos.** 8. ed. São Paulo: Saraiva Educação, 2021.

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

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 Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021.

SIMONETE, Marcel. Privacy by design e privacy by default. **Centro de estudos sociedade e tecnologia.** vol. 6. n. 6. p. 1-2. São Paulo: USP, 2021. Disponível em: <http://www.cest.poli.usp.br/wp-content/uploads/2021/08/Privacy-By-Design-e-Default_pt_final.pdf >. Acesso em 22 maio de 2022.

SOLOVE, Daniel J. **Understanding privacy.** Cambridge: Havard University Press, 2008.

STOLZE, Pablo; PAMPLONA FILHO, Rodolfo. **Manual de direito civil.** 4. ed. São Paulo: Saraiva Educação, 2020.

TELEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

UNIÃO EUROPEIA. **Regulamento (eu) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Gerak sobre a Proteção de Dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e1554-1-1>. Acesso em 5 maio 2022.

VALSORDA, Fillipo. “Data is not the new gold, data is the new uranium. Sometimes you can make money from it, but it can be radioactive, it's dangerous to store, has military uses, you generally don't want to concentrate it too much, and it's regulated. Why keep uranium you don't need?”. Twitter: @FiloSottile. 11:44 p.m., 16 ago 2019. Disponível em: <https://twitter.com/filosottile/status/1162404848073170944>. Acesso em: 05 maio 2020.

VASQUES, Viviane da Silva Coelho. Considerações sobre a proteção de dados pessoais sensíveis no ambiente virtual. **Cibernética jurídica:** estudo sobre o direito digital. Cláudio Joel Brito Lóssio; Luciano Nascimento; Rosangela Tremel (Organizadores). Campina Grande: EDUEPB, 2020. P. 252-261.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy.** v. IV, n. 5. Boston: Havard Law Review, 1890.

WESTIN, Alan. **Privacy and freedom.** Nova York: Athenum, 1967.