UNIVERSIDADE FEDERAL DE MINAS GERAIS
Faculdade de Direito
Programa de Pós-Graduação em Direito

Mariana Krollmann Fogli

AUTOGERENCIAMENTO DA PRIVACIDADE NO ACESSO ÀS REDES DIGITAIS E O USO DA BASE LEGAL DO CONSENTIMENTO: COMPORTAMENTO DOS USUÁRIOS E A PROTEÇÃO LEGAL DOS DADOS PESSOAIS E DA PRIVACIDADE

BELO HORIZONTE/MG

2023

Mariana Krollmann Fogli

AUTOGERENCIAMENTO DA PRIVACIDADE NO ACESSO ÀS REDES DIGITAIS E O USO DA BASE LEGAL DO CONSENTIMENTO: COMPORTAMENTO DOS USUÁRIOS E A PROTEÇÃO LEGAL DOS DADOS PESSOAIS E DA PRIVACIDADE

VERSÃO FINAL

Dissertação de mestrado apresentado ao Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais como requisito para a qualificação ao curso de Mestrado em Direito.

Orientador: orientação do professor Dr. Marcelo de Oliveira Milagres.

BELO HORIZONTE/MG

2023

Ficha catalográfica elaborada pelo bibliotecário Junio Martins Lourenço - CRB-6/3167.

F656a Fogli, Mariana Krollmann
Autogerenciamento da privacidade no acesso às redes digitais e o uso da base legal do consentimento [manuscrito]: comportamento dos usuários e a proteção legal dos dados pessoais e da privacidade / Mariana Krollmann Fogli.-- 2023.
92 f.

Dissertação (Mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito.
Bibliografia: f. 86-91.

1. Direito - Teses. 2. Direito a privacidade - Teses. 3. Proteção de dados - Teses. 4. Redes sociais on-line. 5. Consentimento (Direito) - Brasil. I. Milagres, Marcelo de Oliveira. II. Universidade Federal de Minas Gerais - Faculdade de Direito. III. Título.

CDU: 347.121.1

UNIVERSIDADE FEDERAL DE MINAS GERAIS

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

ATA DA DEFESA DA DISSERTAÇÃO DA ALUNA

MARIANA KROLLMANN FOGLI

Realizou-se, no dia 27 de abril de 2023, às 08:00 horas, Virtual, da Universidade Federal de Minas Gerais, a defesa de dissertação, intitulada *AUTOGERENCIAMENTO DA PRIVACIDADE NO ACESSO ÀS REDES DIGITAIS: COMPORTAMENTO DOS USUÁRIOS E A PROTEÇÃO LEGAL DOS DADOS PESSOAIS E DA PRIVACIDADE.*, apresentada por MARIANA KROLLMANN FOGLI, número de registro 2021654251, graduada no curso de DIREITO, como requisito parcial para a obtenção do grau de Mestre em DIREITO, à seguinte Comissão Examinadora: Prof(a). Marcelo de Oliveira Milagres - Orientador (UFMG), Prof(a). Edgard Audomar Marx Neto (Universidade Federal de Minas Gerais), Prof(a). Marcelo Andrade Feres (UFMG).

A Comissão considerou a dissertação:

(x) Aprovada com autorização para publicação, tendo obtido a nota 75 (setenta e cinco)

( ) Reprovada

Finalizados os trabalhos, lavrei a presente ata que, lida e aprovada, vai assinada por mim e pelos membros da Comissão.
Belo Horizonte, 27 de abril de 2023.

MARCELO DE OLIVEIRA MILAGRES:02377846610 Assinado de forma digital por MARCELO DE OLIVEIRA MILAGRES:02377846610 Dados: 2023.04.28 13:09:31 -03'00'

Prof(a). Marcelo de Oliveira Milagres (Doutor) nota 75

EDGARD AUDOMAR MARX NETO Assinado de forma digital por EDGARD AUDOMAR MARX NETO Dados: 2023.04.28 19:04:13 -03'00'

Prof(a). Edgard Audomar Marx Neto (Doutor) nota 75.

MARCELO ANDRADE FERES:03161492668 Assinado de forma digital por MARCELO ANDRADE FERES:03161492668 Dados: 2023.04.28 19:47:03 -03'00'

Prof(a). Marcelo Andrade Feres (Doutor) nota 75.

Agradeço à minha família, em especial aos meus pais, à minha irmã e aos meus avós, por serem a minha base e a minha fonte de inspirações. Ao meu marido, obrigada pelo seu amor e por todo o companheirismo ao longo deste percurso.
À Carvalho & Furtado, pelo apoio cotidiano.
A todos os amigos que direta ou indiretamente fizeram parte de minha formação, o meu muito obrigada.

RESUMO

Em geral, o usuário não tem meios de conhecer todas as informações geradas por suas interações, nem de obter a certeza de que seus dados estão seguros, tendo em vista a complexidade técnica envolvida na tecnologia utilizada em dispositivos conectados. Com isso, a discussão se concentra na impossibilidade do autogerenciamento pleno pelos titulares do tratamento de dados pessoais em plataformas digitais em face da arquitetura tecnológica envolvida. Essa complexidade tecnológica limita o direito à informação e a observância do princípio da transparência, impedindo, de certo modo, a compreensão acerca dos riscos associados ao tratamento de dados pelos dispositivos. É necessário que o titular consiga exercer o seu direito à privacidade, entendido de forma ampla e integrante conjuntural da dignidade da pessoa humana, envolvendo a autonomia e a liberdade do ser humano para a construção própria de sua esfera pessoal. Mesmo assim, verifica-se a disponibilização crescente de dados pessoais diante das funcionalidades dispostas nas redes digitais e, tal cenário, além do perfilamento e da modulação da sociedade, o que pode enfraquecer atos democráticos, resulta no dilema entre comportamento e a efetiva proteção da privacidade, impasse objeto deste trabalho. O uso do consentimento em dispositivos e plataformas digitais, conforme possibilita a LGPD, para o tratamento de dados não pode ser, nesse contexto, considerado adequado e suficiente, quando se observa as limitações informacionais dos próprios usuários, considerando as garantias fundamentais previstas no ordenamento jurídico pátrio, principalmente o da transparência e da segurança da informação. Deve-se, por meio de uma regulação focada no princípio da transparência e pela conscientização, buscar meios de se alcançar um denominador comum entre o desenvolvimento tecnológico e as regras de proteção de dados pessoais, o que, na atualidade, concentra-se na necessidade de uma mudança cultural acerca da privacidade e, ainda, na gestão de riscos envolvidos no tratamento de dados pessoais em uma estrutura online.

Palavras-chave: Proteção de Dados. Privacidade. Autodeterminação Informativa. Tecnologia. Comportamento. Transparência.

ABSTRACT

In general, the user does not have the means to know all the information generated by their interactions, nor to be sure that their data is safe, since the technical complexity involved in the technology in the connected devices. With that, the discussion focuses on the impossibility of full self-management by the holders of the processing of personal data on digital platforms in view of the technological architecture involved. This technological complexity limits the right to information and the observance of the principle of transparency, preventing, in a way, the understanding about the risks associated with the processing of data by the devices. It is necessary that the holder exercise his right to privacy, understood in a broad and conjunctural way of the dignity of the human person, involving the autonomy and freedom of the human being to build his own personal sphere. Even so, there is a growing availability of personal data in view of the functionalities available in digital networks and, such a scenario, in addition to the profiling and modulation of society, which can weaken democratic acts, results in the dilemma between behavior and the effective protection of privacy, which is the object of this work. The use of consent in the digital platforms, as provided in the LGPD, for processing data cannot, in this context, be considered adequate and sufficient, when observing the informational limitations of the users themselves, considering the fundamental guarantees provided for in the national legal system, mainly that of transparency and information security. It is necessary, through regulation focused on the transparency principle by the user and awareness, to seek ways to reach a common denominator between technological development and the rules for the protection of personal data, which, at present, focuses on the need for a cultural change about privacy and also the management of risks involved in the processing of personal data in an online structure.

Keywords: **Data Protection. Privacy. Informative self-determination, Technology. Behavior. Transparency.**

SUMÁRIO

1. INTRODUÇÃO

A internet, enquanto propulsora da Quarta Revolução Industrial[1], tem como escopo a convergência das tecnologias dos mundos digitais, físicos e biológicos. Isso, pois, é por meio da internet que se possibilita a integração entre dispositivos, proporcionando controle remoto, automações e compartilhamento de informações.

Nesse contexto, visando cada vez mais implementar facilidades no cotidiano humano a partir de um funcionamento personalizado, plataformas digitais, tidas como estruturas criadas para promover interações e transações entre seus usuários por meio do uso de internet, requerem uma abrangente coleta e a vinculação de dados do usuário para fornecer experiências personalizadas.

Desse modo, a coleta e o tratamento de dados com o objetivo de oferecer facilidades no cotidiano das pessoas podem ser considerados um dos pilares da Era dos Dados[2] frente a uma sociedade digital.

Em síntese, quanto maior for o volume, a velocidade de processamento e a variedade de dados, maior é a capacidade de geração de valor (capital). Essa lógica abriu precedentes para um novo tipo de "indústria", que opera por meio do acúmulo e da monetização de dados digitais.

A problemática se lança na vigilância constante que o titular dos dados se submete, sem permissão adequada, prévia e sem limites, refletidos na geração de dados estruturados ou não. Como possível efeito, haverá a invasão da privacidade e da intimidade na tomada das decisões relacionadas ao titular.

De fato, o uso de dados pessoais está intimamente ligado ao conceito vigilância e, no contexto digital, se traduz na verificação constante de usuários e suas interações com os dispositivos. A vigilância cumulada com os aspectos econômicos e comerciais envolvidos na análise de dados inaugura o chamado capitalismo de vigilância.

---

[1] Terminologia inaugurado por Klaus Schwab, fundador do Fórum Econômico Mundial (FEM), que escreveu, em artigo publicado na "*Foreign Affairs*", que: A 1ª Revolução Industrial usou água e vapor para mecanizar a produção entre o meio do século XVIII e o meio do século XIX. A 2ª Revolução Industrial usou a eletricidade para criar produção em massa a partir do meio do século XIX. A 3ª Revolução Industrial usou os eletrônicos e a tecnologia da informação para automatizar a produção na segunda metade do século XX. No século XXI, a 4ª Revolução Industrial é caracterizada pela fusão de tecnologias entre as esferas física, digital e biológica.

[2] Netflix. A Era dos Dados: A Ciência por Trás de Tudo (1ª Temporada). Reino Unido, 2020.

Para Shoshana Zuboff[3], o capitalismo de vigilância, expressão que cunhou para designar esse estágio da economia capitalista, é a consequência de uma nova lógica de acumulação de dados, o *Big Data*[4], e se traduz numa *"nova forma de capitalismo da informação que procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado"*.

Segundo Zuboff, os dados formam os "ativos de vigilância" e os investimentos que esses ativos atraem são denominados de "capital de vigilância". O capitalismo da informação, que a autora reconhece como 'capitalismo de vigilância', torna-se um modelo de negócios, em que as rotineiras estimativas de valor dependem do monitoramento de informações pessoais[5].

Um dos efeitos colaterais desse 'novo' capitalismo é o preço da redução da privacidade. Por haver certa obscuridade dos mecanismos utilizados, não é possível ter certeza da observância dos princípios basilares no que tange o tratamento de dados pessoais, o que, além de oferecer riscos de responsabilização de operadores e controladores, de forma alguma representa uma prática transparente e horizontal.

Diante desse contexto, é perfeitamente racional que as pessoas deixem de fazer boas avaliações dos riscos e não gerenciem sua privacidade de forma eficaz, visando a rápida comunicação e o uso de bens e serviços com as mais diversas funcionalidades.

Gerenciar a privacidade de uma pessoa é um projeto complexo e que não pode ser dimensionado em termos simples e práticos, sendo virtualmente impossível fazê-lo de forma abrangente, abrindo um dilema acerca do autogerenciamento dos riscos envolvidos pelo próprio titular dos dados.

Quando um usuário utiliza uma plataforma digital, suas interações e informações são devidamente coletadas, organizadas e combinadas, podendo revelar, por meio de uma análise algorítmica, perfis comportamentais de cada indivíduo, que são sempre atualizados a partir de novas interações.

---

[3] ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F. et al. (orgs.). Tecnologias da vigilância: perspectivas da margem. Trad. H. M. Cardozo et al. São Paulo: Boitempo, 2018. p. 32

[4] "Big data são grandes e heterogêneas quantidades de dados produzidos rapidamente por uma ampla diversidade de fontes. As inovações tecnológicas vêm permitindo que esses dados sejam coletados e processados, notadamente para conhecimento preditivo. Portanto, o conceito se refere tanto aos dados em si como a sua análise". MPT. *Inteligência artificial, tecnologia digital e discriminação no trabalho*. Direitos e Conceitos Básicos. Disponível em: <https://mpt.mp.br/pgt/publicacoes/cartilhas/inteligencia-artificial-tecnologia-digital-e-discriminacao-no-trabalho/@@display-file/arquivo_pdf>. Acesso em 18 jan. 2023.

[5] ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F. et al. (orgs.). Tecnologias da vigilância: perspectivas da margem. Trad. H. M. Cardozo et al. São Paulo: Boitempo, 2018. p. 32

Importante constar que os algoritmos são sequências de instruções programadas para realizar uma ou várias tarefas. Com o desenvolvimento da tecnologia IA[6], algoritmos de aprendizagem automática passaram a criar, sozinhos, outros algoritmos, o que pode levar a resultados totalmente inesperados, que não poderiam ser antevistos pelos humanos que desenvolveram o código original. Nesse contexto, basicamente, a tecnologia de *Big Data* passa a ser principal fonte para a Inteligência Artificial.

Isso, pois a tecnologia de *Big Data* reúne a imensa quantidade de dados digitais disponível na rede que, quando exposta, permite a criação de modelos que analisam e antecipam o comportamento e a dinâmica de sistemas e interações complexas[7]. Esses dados derivam não só da rotina de navegação dos indivíduos, como também do rastro digital que os indivíduos deixam, muitas vezes sem perceber, na internet. Nesse sentido, à medida que os dados disponíveis são avaliados com rapidez e precisão pela IA, maiores são as possibilidades de uma companhia adotar as melhores práticas para aperfeiçoar processos e iniciativas.

Algoritmos são ferramentas usadas para simplificar decisões, aumentar a eficiência e oferecer conveniência. Mas, quando se observa certo sigilo acerca de seu funcionamento, não é possível entender como eles funcionam ou mesmo se funcionam.

Verifica-se, nesse sentido, a opacidade intrínseca dos algoritmos. Estes controlam diversos aspectos do nosso dia a dia e muitas vezes definem como e se exerceremos alguns dos nossos direitos mais básicos, mas não permitem conhecer como se dá o seu efetivo funcionamento.

Esse monitoramento das predileções pessoais de cada usuário, entretanto, ultrapassa a quantidade e/ou a qualidade dos serviços oferecidos. Há, de fato, um direcionamento dos usuários criado a partir dos rastros digitais deixados. A perfilização, ou seja, o alcance de uma *persona* ou avatar criado a partir da sistematização da infinidade de dados e preferências que um usuário dispõe na internet, permite prever e influenciar comportamentos.

Se um indivíduo é suficientemente conhecido por um algoritmo de uma plataforma digital, é possível a escolha da mais eficaz abordagem para direcioná-lo rumo a determinado comportamento, como, por exemplo, a eleição de um candidato à presidência.

---

[6] ADAMS-PRASSL, Jeremias. What if Your Boss Was an Algorithm? The Rise of Artificial Intelligence at Work. 2019. Comparative Labor Law & Policy Journal 123. Disponível em: <https://ssrn.com/abstract=3661151>. Acesso em 18 jan. 2023

[7] JANNOTI, Claudio; Vasconcelos, Lorena; Emerick, Helena. Discriminação algorítmica no trabalho digital. *Revista de Direitos Humanos e Desenvolvimento Social*. Periódicos Científicos PUC/Campinas. Disponível em: < https://seer.sis.puc-campinas.edu.br/direitoshumanos/article/view/5201>. Acesso em 18 jan. 2023.

Exatamente nesse ponto é que se esbarra no caso emblemático envolvendo a rede social *Facebook* e a empresa de análise de dados *Cambridge Analytica*, que trabalhou na campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos.

No caso, a *Cambridge Analytica* teria comprado o acesso a informações pessoais de mais de 50 milhões de usuários do *Facebook* e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas[8]. A empresa hoje está extinta e, em paralelo ao seu encerramento, foi movida em face da *Meta Platforms Inc.*, controladora do *Facebook*, ações coletivas no estado da Califórnia (EUA) e no Reino Unido para reparação aos danos aos usuários que se sentiram lesados.[9]

No caso, o tratamento e o processamento de dados foi capaz de impulsionar eleitores a escolherem um candidato à presidência específico, interferindo, sem dúvidas, no papel democrático de tais cidadãos. Seja elegendo candidatos ou, até mesmo, levando a sociedade a seguir uma ideologia política, o capitalismo de vigilância pode colocar em xeque o Estado Democrático de Direito na qual o indivíduo se insere, o que ainda não é evidente ou discernível para a maioria dos usuários.

A valer, os indivíduos não relutam tais práticas, principalmente diante de serviços gratuitos, entregando os próprios dados a todo momento, sem qualquer questionamento ou resistência correspondente. E o risco disso está, para além da privacidade, exatamente, na modulação invisível de comportamentos e visões, bloqueando experiências e promovendo o declínio das esferas de debate e da própria criatividade humana, fatores estes que, sem dúvidas, enfraquecem os processos democráticos.

Um comparativo feito por Frank Pasquale no estudo titulado "*The Black Box Society*"[10], traz para a Era da *Big Data* a Alegoria de Platão – O Mito da Caverna[11], que pode ser vista como uma crítica atual aos que, por ignorância, falta de conhecimento ou indisponibilidade, não questionam a realidade e aceitam facilmente as ideias impostas por um grupo dominante, enxergado nas grandes empresas de tecnologia, como *Google* e *Facebook*.

O que se observa é certa condição de ignorância que passam a viver os seres humanos aprisionados pela perfilização, impedindo o conhecimento da verdade.

---

[8] Disponivel em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml

[9] Disponivel em: https://www.infomoney.com.br/negocios/meta-dona-do-facebook-pagara-quase-us-1-bilhao-para-encerrar-acao-coletiva-nos-eua-sobre-cambridge-analytica/

[10] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press: Cambridge, Massachusetts London, England, 2015

[11] PLATÃO.A República. Tradução de Leonel Vallandro.Rio de Janeiro: Nova Fronteira, 2011.

A vida na plataforma digital pode representar um mundo sensível, experimentado a partir das sombras digitais deixadas pelo usuário, onde reside uma percepção modulada da realidade, que aprisiona os seres humanos à ignorância e ao senso comum.

Em verdade, há mecanismos que podem ser capazes de permitir que proteção de dados seja parte integrante do desenvolvimento tecnológico e também da maneira como um produto ou serviço é criado. Todavia, para o uso adequado de tais mecanismos, muitas vezes, não será suficiente atualizar os processos herdados com um verniz de privacidade, mas pode ser necessário construir novos processos e sistemas ou redesenhar significativamente os existentes.

De todo modo, o dilema entre comportamento e proteção dos dados permanece, principalmente, por dependerdo próprio comportamento de usuários ao disponibilizarem informações, gerenciar senhas e acessar em plataformas e dispositivos.

Soma-se a isso o fato de que diante do capitalismo de vigilância presente, não se verifica o interesse crescente no uso de tais processos. E, nesse aspecto, a transparência necessária e o esclarecimento do titular quanto ao funcionamento das plataformas, frente ao capitalismo de vigilância, permanecem limitados.

Ainda que a Lei 13.709 (Lei Geral de Proteção de Dados - LGPD), publicada em 14 de agosto de 2018, acentue o princípio da transparência e da segurança da informação – sugerindo que as plataformas e aplicativos disponham abertamente sobre os possíveis riscos dos sistemas, a existência de ferramentas robustas de obscuridade que permitem aos usuários restringir análises e sobre planos de contingência para mitigar os riscos de privacidade se os sistemas forem comprometidos –, é difícil que se alcance todas as implicações possíveis acerca do tratamento de dados no âmbito digital.

Há uma realidade dinâmica, em que haverá riscos nem sempre previsíveis e deveres acessórios que, no geral, não estarão previstos de forma expressa e compreensível para os usuários das plataformas e aplicativos, ao aceitarem os termos e condições disponibilizadas. Assim sendo, principalmente em relação aos dados pessoais sensíveis, haverá a necessidade de se estudar o consentimento a ser dado pelo usuário, de acordo com as funcionalidades dos aplicativos e plataformas digitais.

Tem-se um contraponto que merece ser estudado para alcance do equilíbrio de interesses e princípios envolvidos, visando ao desenvolvimento da tecnologia e, ao mesmo tempo, a tutela da dignidade da pessoa humana.

Trata-se de um assunto de extrema relevância. Os dados pessoais podem ser considerados elementos nucleares para o desenvolvimento político, social e econômico. Assim, essa nova era, sedimentada na comunicação digital, se constrói a partir da evolução tecnológica

recente, que, conforme ensina Bruno Bioni[12], *"criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imagináveis".*

E, nesse caso, a facilidade de se tratar dados pessoais ainda mais sensíveis, principalmente em relação ao uso em larga escala das redes sociais e plataformas digitais, é preocupante, ao considerar o direito à liberdade, igualdade e, ainda, à intimidade[13].

Como se nota, se propõe neste trabalho um debate acerca da esfera de proteção de dados pessoais e da privacidade no acesso às plataformas digitais, considerando o comportamento de usuários e a busca por funcionalidades dispostas na referida estrutura tecnológica.

Isso é, defende-se a atual impossibilidade de o titular de dados exercer, de forma efetiva, todos os seus direitos assegurados por lei, a partir do controle sobre os seus dados pessoais em face da arquitetura tecnológica complexa das plataformas digitais, conforme possibilidade prevista na Lei Geral de Proteção de Dados, sem a plena conscientização acerca da garantia fundamental da privacidade e da proteção de dados.

Diante desse cenário, o tema a ser desenvolvido tem como objetivo o debate acerca do autogerenciamento das informações pessoais, considerando a utilização da base legal do consentimento para o tratamento de dados pessoais em plataformas digitais, nos termos das nas normas dispostas na Lei 13.709/2018 (LGPD), em especial o art. 7º, inciso I, e art. 8º. Ora, seria a base legal do consentimento a via mais adequada para a proteção de dados pessoais?

Com isso, de forma mais específica, o tema do presente estudo tem foco no não cumprimento dos requisitos previstos no art. 8º da mencionada legislação nacional. A valer, se estuda a impossibilidade de depositar exclusivamente aos controladores e operadores de dados, como faz a legislação atual, um caminho seguro em torno do tratamento de dados.

Assim, o objetivo do texto é estudar a impossibilidade atual de alcance de um consentimento, de fato, livre, inequívoco, informado e específico no tratamento de dados pessoais em plataformas digitais, considerando os riscos envolvidos na disponibilização de informações em razão de um eventual perfilamento.

---

[12] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 4.

[13] Conforme ilustra Bruno Bioni: "Por conseguinte, tais compilações de dados estariam fora do escopo de controle dos cidadãos, abrindo-se uma porta perigosa para a desproteção de dados pessoais. Isto porque, no final das contas, pode haver um volume de informações detalhado sobre uma pessoa a compor um perfil muito preciso sobre a sua personalidade". BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 266.

Tendo como pano de fundo os princípios da transparência e da segurança da informação, previstos na LGPD, uma vez a insuficiência da referida legislação frente à sua aplicação prática, a análise de riscos envolvidos possibilita a elaboração de um trabalho de cunho preventivo, visando a minimização de incidentes. Nesse contexto, um trabalho que proponha tal análise se monstra de especial relevância.

Cabe ressaltar, por fim, que o desenvolvimento de uma abordagem crítica às plataformas digitais não significa a adoção de uma postura contrária ao desenvolvimento tecnológico. Pelo contrário, trata-se, sobretudo, de compreender as ferramentas no âmbito da proteção de dados pessoais, levantando um debate fundamental visando a construção, adequação e atualização da legislação, jurisprudência e doutrina nacional.

2. DA PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

2.1. Da transcendência do direito à privacidade

A discussão acerca da privacidade e do tratamento de dados pessoais não é nova e ultrapassa os limites territoriais brasileiros.

Em verdade, seja na filosofia ou no direito, há inúmeras propostas para o alcance de um denominador comum ao conceituar a privacidade. O uso da palavra "privacidade" constitui as maneiras pelas quais se emprega a palavra na vida cotidiana e, portanto, a concepção de privacidade é um conceito abstrato[14].

Apesar disso, a literatura dominante se esforça para localizar a "essência" da privacidade, isso é, o denominador central que torna as coisas privadas. Nesse sentido, as concepções de privacidade devem ser avaliadas determinando sua precisão em capturar o que é privacidade naquele dado cenário[15], ainda que de forma geral.

Há de se considerar a natureza e o valor conferido à esfera privada em determinadas sociedades, para que se realize a valoração de sua configuração atual. Funções diversas em gênero e amplitude devem ser conhecidas para adequá-las ou não ao momento atual.

Cada ordenamento segue seu próprio caminho ao tratar do tema da privacidade, visto que as particularidades de cada sociedade são determinantes, resultando em consideráveis diferenças de concepção. Ora, a diferença entre público e privado carrega uma variedade de significados correntes que remetem a diversas fases históricas.

A Declaração Universal de Direitos Humanos das Nações Unidas de 1948 dispõe que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques contra sua honra e reputação". No mesmo sentido, Convenção Europeia de Direitos Humanos de 1950 estabelece que "toda pessoa tem direito ao respeito de sua vida privada e familiar, sua casa e sua correspondência".

Tal perspectiva parece ser um consenso mundial[16] sobre a importância da privacidade e a necessidade de sua proteção, como ocorre no Brasil.

Por direitos fundamentais, entende-se os direitos que visam criar e tutelar os elementos essenciais da liberdade e da dignidade da pessoa humana[17]. Sabe-se que os direitos humanos

---

14 SOLOVE, Daniel J..Understanding Privacy. Harvard University Press. Cambridge Massachusettes, 2008.fls.14
15 SOLOVE, Daniel J..Understanding Privacy. Harvard University Press. Cambridge Massachusettes, 2008.fls.14
16 SOLOVE, Daniel J..Understanding Privacy. Harvard University Press. Cambridge Massachusettes, 2008.fls.14
17 BONAVIDES, Paulo. Curso de Direito Constitucional. 15 ed. São Paulo: Malheiros, 2004. P. 560.

tem contornos de ordem universal. E, nesse ponto, os direitos fundamentais seriam a parcela dos direitos humanos que são positivados e reconhecidos pela ordem jurídica do Estado.

Conforme ensina Carl Schmitt, os direitos fundamentais podem ser caracterizados pelos critérios formais e um material: do critério formal, pode-se aduzir que são todos aqueles direitos e garantias especificados na ordem constitucional; já o segundo critério estabelece que os direitos fundamentais são aqueles com grau mais elevado de garantia e segurança, grau esse constitucionalmente estabelecido – são imutáveis ou de alteração dificultosa.

Já os direitos da personalidade são considerados aqueles direitos que representam qualidades mínimas, atributos relacionados à condição de pessoa humana. Por serem direitos inatos, cabe ao Estado apenas reconhecê-los e positivá-los, como é o caso do direito à privacidade.[18]

Carlos Alberto Bittar afirma que "[…]os direitos da personalidade constituem direitos inatos – como a maioria dos escritores ora atesta –, cabendo ao Estado apenas reconhece-los e sancioná-los em um ou outro plano do direito positivo – em nível constitucional ou em nível de legislação ordinária –, e dotando-os de proteção própria, conforme o tipo de relacionamento a que se volte, a saber: contra o arbítrio do poder público ou as incursões de particulares".

Mesmo estando positivados no plano infraconstitucional, enquanto direitos fundamentais devem estar previstos na Constituição, prevalece o entendimento que os direitos da personalidade são direitos fundamentais, não apenas pelo fato de serem direitos decorrentes do princípio maior da dignidade da pessoa humana, mas porque resultam da proteção à subjetividade do ser humano[19].

A Constituição Federal de 1988 ocupou-se do assunto e incluiu, entre as garantias e direitos fundamentais de seu artigo 5° a proteção da "intimidade" e da "vida privada" (inciso X), deixando claro que a proteção da pessoa humana abrange esses aspectos.

A valer, a "vida privada" implica na distinção entre as coisas da vida pública e da vida privada. Já a "intimidade", aparenta se referir a eventos mais particulares e pessoais. De todo modo, a discussão dogmática sobre os limites entre ambos os conceitos, em razão de seu elevado grau de subjetividade, desvia o foco do problema principal, que é exercício dos direitos envolvidos na dignidade da pessoa.

---

[18] MARINONI, Luiz Guilherme. MITIDIERO, Daniel. SARLET, Ingo Wolfgang. Curso de Direito Constitucional. P. 274-277.

19 DINIZ, Maria Helena. Curso de Direito Civil Brasileiro. 1. A Teoria geral do Direito Civil. 29 ed. São Paulo: Saraiva, 2012. P. 129-133.

Tem-se mais frutífero e razoável analisar a privacidade como um conceito guarda-chuva[20], isso é, que guarda um conjunto de direitos à privacidade relacionados à intimidade, sigilo, propriedade e dignidade[21].

Assim como faz Danilo Doneda[22], no presente trabalho a preferência pelo uso do termo privacidade. Razoavelmente, o termo é específico e consegue unificar os valores expressos pelos termos intimidade e vida privada.

De fato, a noção de privacidade remonta, em uma primeira análise, na noção de isolamento físico, estando relacionado à propriedade ou a inviolabilidade desse direito individual. Inclusive, mais recente, no Brasil, a inviolabilidade do domicílio e da correspondência estão presentes em todas as Constituições, desde a Constituição do Império de 1824[23].

De todo modo, o distanciamento da noção de privacidade do direito à propriedade privada é ponto de partida para análise do surgimento da privacidade no âmbito jurídico, apesar de sua importância história e decorrente de uma evolução cultural que tem presença já nas civilizações mais antigas.

Na Grécia Antiga[24], já se distinguia o público do privado. Contudo, não se tratava de uma liberdade pessoal, mas de uma organização social. No Império Romano, o direito à privacidade só poderia ser compreendido se recolocada na sua função social e histórica. Isso é, o sujeito do direito romano não é o indivíduo, mas o complexo produtivo de uma casa, com papel importante do pai de família, detentor da propriedade e que realiza negócios[25].

Já na Idade Média, verifica-se a construção da privacidade traduzida no binômio liberdade-propriedade, diante da emergente classe burguesa, como uma resposta ao absolutismo.

Com o desenvolvimento do Estado enquanto nação, da própria ideia de sociedade civil, submersos em teorias de soberania nos séculos XVI e XVII, há a formação da noção moderna do público, momento em que também se observa a delimitação de uma esfera privada, livre das

---

[20] SOLOVE, Daniel J..Understanding Privacy. Harvard University Press. Cambridge Massachusettes, 2008.fls.45

[21] SOLOVE, Daniel J..Understanding Privacy. Harvard University Press. Cambridge Massachusettes, 2008.fls. 15

[22] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019, fls. 79

[23] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019, fls. 85

[24] Jeffrey Rosen. The unwanted gaze, cit., p. 5. In: DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019

[25] LOPES,José Reinaldo de Lima. O direito na história: lições introdutórias. 4 ed. São Paulo: Atlas, 2012, fls. 16

ingerências desse ente público, principalmente ao fim do feudalismo e, posteriormente, observado na Revolução Industrial[26].

O liberalismo pensado fortemente por John Locke[27] postula a propriedade como elemento essencial ao desenvolvimento da própria pessoa, como realização da personalidade do indivíduo, estando ligada a valores materiais. A segurança do homem para exercício de sua liberdade relaciona-se à sua riqueza, bem como às suas posses e, consequentemente, o direito de propriedade era a condição inafastável para chegar à privacidade[28].

A evolução da privacidade com a mudança de tal paradigma ocorre com a sociedade industrial e com o desenvolvimento da ideia de liberdade diretamente ligada à autonomia privada como uma forma de resistência do homem frente à tendência de massificação da sociedade industrial, buscando, de certa forma, a correção dos rumos do liberalismo[29].

Em paralelo, verifica-se o surgimento dos meios de comunicação em massa, que modifica a expectativa de privacidade, com os mecanismos sociais impactados pela intrusão na vida privada de um cidadão. Destaca-se, nesse sentido, o referencial teórico de Samuel Warren e Louis Brandeis[30], em que direito à privacidade é inaugurado na contemporaneidade no texto "*The Right to Privacy*", impulsionado pelo inconformismo gerado diante de uma publicação detalhada de uma cerimônia de casamento burguês.

Na referida obra, a privacidade encontra-se diretamente ligada ao isolamento do indivíduo e em sua tranquilidade. Ora, naquela época, frente ao capitalismo americano, se demonstrava a privacidade como um direito fundamental relacionado aos interesses e

---

[26] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019, fls. 88

[27] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019, fls. 89

[28] "*If man in the state of Nature be so free as has been said, if he be absolute lord of his own person and possessions, equal to the greatest and subject to nobody, why will he part with his freedom, this empire, and subject himself to the dominion and control of any other power? To which it is obvious to answer, that though in the state of Nature he hath such a right, yet the enjoyment of it is very uncertain and constantly exposed to the invasion of others; for all being kings as much as he, every man his equal, and the greater part no strict observers of equity and justice, the enjoyment of the property he has in this state is very unsafe, very insecure. This makes him willing to quit this condition which, however free, is full of fears and continual dangers; and it is not without reason that he seeks out and is willing to join in society with others who are already united, or have a mind to unite for the mutual preservation of their lives, liberties and estates, which I call by the general name – property*". John Locke. Second Treatise of Government. Cambridge: Hackett, 1980 (facsímile do original publicado em 1690), p. 159 [ed. bras.: Segundo tratado sobre o governo e outros escritos. 2a ed., Petrópolis: Vozes, 1994].

[29] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019

[30] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890) In: Doneda.

comportamentos do indivíduo para com a proteção de suas informações quando utilizados por terceiros, desvinculada do direito de propriedade.

Tais desdobramentos, inclusive, foram atualizados por Alan Westin[31], colocando ênfase na autonomia do indivíduo para controle de suas informações pessoais, compreendendo a privacidade como reivindicações acerca da extensão do tratamento e compartilhamento de dados.

Nesse aspecto, a referida bibliografia fortalece na doutrina o protagonismo da autodeterminação informativa, que se desdobra, na atualidade, no gerenciamento de dados pelo titular e, de forma prática, no uso do consentimento enquanto justificativa válida para fins de tratamento de dados pessoais. Em verdade, a preocupação atual ultrapassa colunas sociais e se torna fruto do estrondoso incremento no fluxo de informações nos últimos anos.

A esfera privada passa a estar relacionada, então, com a liberdade de desenvolver a própria personalidade, livre de ingerências externas, a partir de suas próprias informações tidas como pessoais. Ganha-se um papel ainda mais importante, qual seja o de que a pessoa não está submetida a formas de controle social que, em última análise, anulariam sua individualidade, o que inviabilizaria o livre desenvolvimento de sua personalidade.[32]

Destaca-se, ainda, o texto "A *vida na sociedade de vigilância: privacidade hoje"*, de 2008, em que se observa contribuições valiosas Stefano Rodotá[33] que desloca ainda mais o conceito de privacidade da noção de "*right to be alone*", trazendo, expressamente, o efetivo controle pela própria pessoa de suas informações pessoais.

A privacidade assume, portanto, um papel importante na proteção da pessoa humana, não na lógica da exclusão, mas como elemento indutor da autonomia e dos direitos de liberdade de uma forma geral, o que justifica, inclusive, a dificuldade em sua conceituação pela doutrina. Nesse papel, trata-se de um pressuposto de uma sociedade democrática moderna.

Mais do que o direito subjetivo, o direito à privacidade contorna o direito de administração de escolhas para com o exterior acerca de informações pessoais, não se tratando mais de um isolamento, mas da projeção pessoal frente ao controle público[34].

---

31 WESTIN ,Alan F.Priva cy And Freedom, 25 Wash. & Lee L. Rev. 166 (1968).

32 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019

33 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008.

34 RODOTÁ, Stefano. Tecnologie e diritti. Bologna: 11 Mulino, 1995

2.2. *O desenvolvimento da privacidade para a autodeterminação informativa*

Acompanhando o desenvolvimento tecnológico, Stefano Rodotà[35], em seu texto publicado em 1995, "*Tecnologie e diritti*", inaugura um modelo de equilíbrio entre direito, política e tecnologia, momento em que se passa a buscar na doutrina um alcance da estabilidade entre o digital e as liberdades individuais.

É nesse contexto que a introdução da tecnologia de informação em várias áreas da vida econômica e social ganha importância diante da observação crescente do processamento de dados. Passa-se a observar um consenso internacional relativo à política internacional sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais que resultou no empenho em sistematizar a matéria no âmbito legislativo e em debater o assunto no âmbito judicial.

A temática da privacidade passou a se estruturar em torno de dados e, especificamente, dos dados pessoais. Com isso, o próprio conteúdo do termo privacidade passou a ser verificado com mais clareza pela concepção de direito de acesso a dados processados e armazenados, assim como a autodeterminação informativa, com todas as suas consequências[36].

De fato, já na década de 1960, a tecnologia começou a ser determinante para a definição dos limites do direito à privacidade. A informática traz mudança nos próprios postulados entorno do direito à privacidade, com a concentração do seu objeto cada vez maior nos dados pessoais, deixando de lado o caráter subjetivo das considerações quanto à violação da privacidade.[37]

Mediante a proteção de dados pessoais, garantias, até então, relacionadas exclusivamente com o direito à privacidade, passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses relacionados à personalidade humana devem ser considerados,

---

[35] RODOTÁ, Stefano. Tecnologie e diritti. Bologna: 1l Mulino, 1995

[36] "An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law". E.U.A., Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973, <aspe.hhs.gov/datacncl/1973privacy/c3.htm>.

[37] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: TENDÊNCIAS CONTEMPORÂNEAS DE MATERIALIZAÇÃO. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020. Fls.39

incluindo as diversas formas de controle da esfera pessoal, tornadas possíveis com o tratamento de dados pessoais.

Nesse sentido, verifica-se a garantia constitucional firmada pelo Tribunal Constitucional Federal Alemão no bojo das Reclamações Constitucionais ajuizadas contra o recenseamento geral da população que fora determinado pela Lei do Censo de 1983[38].

A decisão histórica reconheceu, com base no direito geral da personalidade consagrado na *Grundgesetz*, a Constituição Alemã, e, ainda, uma lei federal considerada pioneira em proteção de dados pessoais de 1977, a *Bundesdatenchutzgesetz*, que "*o livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais, assegurando, assim, a proteção à autodeterminação informativa"*.

A partir da referida decisão, o direito à autodeterminação informativa passou a orientar até hoje a proteção de dados pessoais na Alemanha, exercendo grande influência em países do sistema jurídico romano-germânico.

A autodeterminação informativa também é um dos fundamentos da disciplina da proteção de dados no Brasil, pois concebida como um direito fundamental, na esteira do direito geral de privacidade, proporcionando ao indivíduo o direito no controle sobre suas informações.

Nesse cenário, o Supremo Tribunal Federal, também em decisão histórica, teve a oportunidade de reconhecer a existência no ordenamento brasileiro do direito à autodeterminação informativa. O julgamento se deu em apreciação de medida cautelar no bojo da Ação Direta de Inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (ADI 6387) contra a Medida Provisória nº 954/2020.

A Medida Provisória impugnada determinava que as empresas de telecomunicações compartilhassem os dados como nome, telefone e endereço, de todos os seus usuários com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de pesquisas estatísticas, tendo em vista a situação de emergência de saúde pública decorrente do Coronavírus.

A Ordem dos Advogados do Brasil arguiu a inconstitucionalidade da medida, tendo em vista a ausência dos requisitos da relevância e urgência, bem como a violação à dignidade da pessoa humana, diante da presença no ordenamento jurídico pátrio de um direito fundamental à autodeterminação informativa, a ensejar tutela jurisdicional quando sua violação não for devidamente justificada.

---

[38] BVerfG, Order of the First Senate of 15 December 1983 - 1 BvR 209/83 -, paras. 1-214.

Foi arguido, ainda, que na sociedade de informações atual, com o incremento cada vez maior da presença digital, ampliam-se os riscos de invasão à vida privada, enquanto direito de escolha de exercício de sua própria personalidade.

Embora o Supremo Tribunal Federal tenha proferido reiteradas deliberações em proteção aos direitos de intimidade, privacidade, sigilo das comunicações, há uma relevância ímpar no julgamento da ADI 6387[39] pelo Plenário, diante da decisão monocrática da ministra

[39] EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não pode ser invocado como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada.

Rosa Weber, que suspendeu a eficácia da MP 954/2020, por ter sido pela primeira vez reconhecido expressamente a tutela constitucional do direito à autodeterminação informativa, a ser extraída diretamente do texto constitucional.

Na decisão, a relatora fez menção ao artigo *The Right to Privacy*, escrito pelos juízes da Suprema Corte dos Estados Unidos, Samuel D. Warren e Louis D. Brandeis, e consignou que "já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima".

À luz dessas premissas, o Tribunal Pleno do Supremo Tribunal Federal chancelou o entendimento da relatoria, vencido apenas o Ministro Marco Aurélio, proferindo uma decisão histórica que firmou o reconhecimento expresso de que a Constituição Federal de 1988 assegura aos brasileiros o direito à autodeterminação informativa, enquanto direito à privacidade, devendo o uso dos dados e informações pessoais ser controlado pelo próprio indivíduo, ressalvada a existência de norma em consonância com a ordem constitucional.

O julgamento proferido pela Suprema Corte é paradigmático por referendar não apenas uma proteção constitucional autônoma aos dados pessoais em si (e não apenas ao sigilo da comunicação destes), mas também por consagrar, no âmbito constitucional a autodeterminação informativa, citando, inclusive, a sua positivação na legislação infraconstitucional (LGPD).

2.3.Da legislação em torno da autodeterminação informativa

Por muito tempo, em face da ausência de limites e diretrizes para suas operações, as redes digitais se concentraram em coletar dados dos usuários e criar soluções a partir dessas informações, algo que, atualmente, passa a ser questionado em razão dos princípios da proteção de dados e privacidade, positivados, recentemente, em legislações de alguns países.

No contexto atual, de disseminação e hegemonia crescente das tecnologias digitais, a proteção de dados, seguida da autodeterminação informacional, é precondição absoluta para o debate democrático. Dessa forma, regimes de proteção de dados desempenham papel

---

(ADI 6387 MC-Ref, Relator (a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020)

fundamental em países democráticos, que respeitam os direitos humanos, oferecendo mecanismos de proteção à privacidade.

Como ensina Danilo Doneda[40], *"a privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos".*

Em verdade, a regulação voltada para a proteção de dados pessoais surge no Estado Moderno após a Segunda Guerra Mundial, em que há a percepção pelos governos da utilidade das informações pessoais de suas populações para planejamento e coordenação, voltadas para um crescimento ordenado [41].

Ainda assim, com o referencial teórico de Alan Westin[42], a preocupação regulatória inicial se desenvolve e não mais se limita a dados estatais, acobertando também a esfera privada.

Esse desenvolvimento legislativo tem como pano de fundo as *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico – OCDE. Isso pois, a OCDE trata-se de um órgão mundial, criando no pós-segunda guerra, que se dedica à promoção do desenvolvimento econômico e o bem-estar social.

Com o desenvolvimento econômico social, a partir da tecnologia da informação, foram emitidos o *Privacy Guideline*, em 1980, e o *Transborder Data Flows*, em 1985, que, sem dúvidas, influenciaram mundialmente o desenvolvimento da proteção de dados pessoais e privacidade, ao estabelecer padrões normativos, principalmente voltados para a transferência de informações entre países membros[43].

Na década de oitenta, o Conselho da Europa também passou a formular, junto à Cooperação e Desenvolvimento Econômico - OCDE, diretrizes para privacidade. Como consequência, foi iniciada um alto nível de convergência das regras sobre proteção de dados

---

[40] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019, fls. 96

[41] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 110

[42] WESTIN, Alan. Privacy and Freedom. New York: Athenum, 1967

[43] "Em 2013, ambas as *guidelines* sofreram um processo de revisão, tendo sido mantida, no entanto, a sua espinha dorsal". BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls.

pessoais no âmbito transnacional, ganhando escala em organismos internacionais com forte capilarização na Europa continental.

Imperioso destacar a presença de normas facilitadoras para a harmonização das legislações voltadas para a proteção de dados pessoais já na Convenção 108, em 1980, de Strasbourg, evidentemente influenciada pelas guias orientativos da Cooperação e Desenvolvimento Econômico - OCDE.

A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares diz respeito ao tratamento automatizado de dados pessoais, foi o primeiro instrumento jurídico internacional sobre proteção de dados. No documento, há disposição expressa sobre o dever de se garantir a todas as pessoas o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal[44].

Destaca-se que a Convenção nº 108 é aberta à assinatura de Estados que não são membros do Conselho. Contudo, o Brasil não é signatário.

Como se nota, há uma tendência global em que a União Europeia fez frente em questões regulatórias. No âmbito da proteção de dados e da privacidade, em 1995, surge a Diretiva 95/46/CE, estabelecendo uma definição básica de dados pessoais e outras delimitações importantes para a discussão do tema.

Em dezembro 2000, há a publicação da Carta dos Direitos Fundamentais da União Europeia[45], que prevê que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". O texto 2012/C 326/02 alterou a Carta proclamada em 7 de dezembro de 2000 e substituindo-a a partir da data de entrada em vigor do Tratado de Lisboa, passando a ter caráter vinculante.

Esses são pontos de partidas no cenário europeu, se justificam por uma série de fatores, desde o desenvolvimento econômico e tecnológico mais precoce e mais intenso no continente até a própria cultura ligada à privacidade, proporcionando condições para que problemas especificamente ligados à privacidade e a dados pessoais fossem considerados antes e, a partir daí, fossem estabelecidos instrumentos regulatórios e jurídicos de tutela às liberdades individuais afetadas, incluindo o direito à privacidade.[46]

---

[44] COUNCIL OF EUROPE, Chart of signatures and ratifications of Treaty 108. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

[45] Disponível em <https://eur-lex.europa.eu/eli/treaty/char_2012/oj>. Acessado em 20/04/2023.

[46] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: TENDÊNCIAS CONTEMPORÂNEAS DE MATERIALIZAÇÃO. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020. Fls. 40

Após escândalos envolvendo o uso de informações de usuários de redes sociais para campanhas políticas, além da exposição quanto ao monitoramento de grandes autoridades internacionais, há a publicação, em 2018, do Regulamento Geral de Proteção de Dados (GDPR), que assume o lugar da antiga diretiva, sendo aplicada a todos os países-membros da União Europeia.

De fato, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), para além de uma regulamentação econômica no aspecto concorrencial, se apresenta como uma tentativa de encerrar ou, pelo menos diminuir, as desigualdades geradas pelas informações e o seu aproveitamento.

Nesse aspecto, em razão do desenvolvimento da tecnologia, a referida legislação dispõe de certa abertura para que a norma consiga acompanhar juridicamente um cenário tecnológico, ainda repleto de inseguranças e incertezas, no intuito de um trabalho preventivo em que se consiga vislumbrar riscos em tempo hábil e, ainda que de forma, limitada.

Além disso, a proteção de dados é, em primeira instância, a tutela do direito à personalidade, composto pela autonomia, a liberdade e a autodeterminação do indivíduo. Com isso, a legislação busca se contrapor ao esforço de uma ampla definição de perfis, classificação do indivíduo em agrupamentos.

Para além de questões comerciais, países como o Brasil tendem a se consolidar como desenvolvedores, mas também como adquirentes de tecnologias. Tal cenário propicia um ambiente frutífero para a disseminação de parcerias comerciais na área tecnológica, assim como exige novas regulações sobre as relações entre países e suas companhias no que tange ao tratamento de dados pessoais.

3. DA LEGISLAÇÃO NACIONAL E OS PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

3.1. A Lei Geral de Proteção de Dados no Brasil

A legislação pátria, que inaugurou o debate de forma expressa a partir do Marco Civil de Internet, parece ter se inspirado no histórico legislativo europeu com a publicação da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, em 2018, que regula as atividades de tratamento de dados pessoais, com base no que se entende por privacidade, destacando como princípios a segurança da informação e a transparência no uso de dados pessoais.

Nesse contexto, a importância de se observar o tratamento de dados, incluindo o perfil comportamental, está relacionada com os efeitos do tratamento de tais informações, visto que têm conteúdo essencial para a concretização das escolhas individuais acerca da personalidade humana. Além disso, permite-se a efetivação do direito à saúde, da liberdade de expressão, de comunicação, religiosa e de associação.

A proteção de dados pessoais se constrói como uma garantia de caráter instrumental, que deriva, sem dúvidas, da tutela da privacidade como um todo, fazendo referência a um conjunto de garantias fundamentais que já se encontram no ordenamento jurídico brasileiro.

O direito à proteção das informações pessoais encontra-se, hoje, previstos na Lei Geral de Proteção de Dados e amparados na Constituição Federal de 1988, após Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

O inciso XII do artigo 5º, da Constituição Federal, assegura ser inviolável o sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo exceções específicas e o inciso X, por seu turno, assegura, conforme já mencionado, a inviolabilidade da intimidade e da vida privada, da honra e da imagem das pessoas.

Com a inclusão do inciso LXXIX, enquanto presente no rol de direitos e garantias fundamentais, a proteção de dados passa a ter as características como a imprescritibilidade, inviolabilidade, universalidade entre outras, visando a promoção da dignidade da pessoa humana. Mais do que isso, representa a verdadeira integração da personalidade em sua acepção mais completa diante da Sociedade da Informação[47].

Isso é, considerando o escopo tanto da Constituição Federal como da legislação ordinária, que traz a tutela da privacidade e da personalidade, a preocupação com dados pessoais traz à tona a ideia de privacidade informacional e, ainda, permite o exercício dos direitos do titular em relação às suas informações, por meio de sua liberdade (autodeterminação informacional), visando a redução do desequilíbrio social e econômico entre titulares e agentes de dados e, consequentemente, a garantia da igualdade e da não discriminação.

A Lei Geral de Proteção de Dados altera os artigos 7º e 16º do Marco Civil da Internet, considerando o seu escopo e seu âmbito de aplicação.

É bem verdade que a construção da LGPD tem como pano de fundo uma série de disposições categorizadas e espaças nas quais algum aspecto da proteção da privacidade assume relevo. Se destacam, nesse âmbito, os preceitos sobre a proteção de dados pessoais no direito

---

[47] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2ª edição de 2019, fls. 28[6]

consumerista, definidos nos artigos 43 e 44 do Código de Defesa do Consumidor e, ainda, na Constituição Federal com a ação de *habeas data*, regulamentada pela Lei 9.507/97.

Nos termos do art. 1º ao dispor sobre regras e limites quanto ao tratamento de dados pessoais, o objetivo da LGPD será o de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com isso, o papel e o alcance da LGPD levantam repercussões nas esferas individuais, além de implicar na restruturação das relações sociais e políticas, principalmente considerando o desenvolvimento tecnológico.

Não há dúvidas de que a proteção de dados pessoais no ordenamento jurídico pátrio trata de uma garantia fundamental que visa resguardar a dignidade da pessoa humana nos termos do art. 1º, inciso III, 5º, caput, ambos da Constituição Federal.

A valer, a ideia de proteção de dados pessoais está relacionada com a garantia à intimidade (art. 5º, X), quanto do direito à informação (art. 5º, XIV), ou do direito ao sigilo de comunicações e dados (art. 5º, XII), assim como da garantia individual ao conhecimento e correção de informações sobre si pelo *habeas data* (art. 5º, LXXII).[48]

Nos termos do artigo 5º, inciso I, dado pessoal é composto por informações relacionadas à pessoa natural identificada ou identificável, podendo ser ele classificado como sensível, nos termos do inciso II do mencionado artigo, se refere à "*origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*".

A importância da previsão acerca de uma categoria especial de dados está relacionada com os efeitos do tratamento de tais informações, visto que tais dados têm conteúdo essencial para a concretização do princípio da igualdade e da não discriminação. Além disso, permite-se a efetivação do direito à saúde, da liberdade de expressão, de comunicação, religiosa e de associação.

Isso é, considerando o escopo da lei, qual seja a tutela da privacidade e da personalidade, a classificação de dados pessoais sensíveis traz à tona a ideia de privacidade informacional e, ainda, permite o exercício dos direitos do titular em relação às suas informações, por meio de sua liberdade (autodeterminação informacional), visando a redução do desequilíbrio social e econômico e, consequentemente, a garantia da igualdade e da não discriminação.

---

[48] MULHOLLAND, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista De Direitos E Garantias Fundamentais, 19(3), 159-180.

A valer, a categorização dos dados pessoais está intimamente relacionada com o princípio da não discriminação, previsto na LGPD, que conforme ensina Caitlin Mulholland[49] é dos mais relevantes no que diz respeito ao tratamento de dados sensíveis. Isso, pois o dado sensível, como vem sendo explorado, carrega certo potencial lesivo, relacionado com a sua capacidade discriminatória, seja por entes privados, seja por entes públicos.

Nesse contexto, para tais dados classificados como sensíveis, a LGPD estabelecerá um regime especial previsto no art. 11.

Já em relação ao conceito de tratamento, nos termos do art. 5º, inciso X, será toda e qualquer operação envolvendo dados pessoais. A lei se apresenta de forma exemplificativa e, nesse sentido, toda e qualquer operação envolvendo dados pessoais estará dentro do escopo da lei, no caso praticada por pessoa natural ou pessoa jurídica em uma atividade econômica, com exceção daquelas com fins jornalísticos, artísticos, acadêmicos, investigação criminal, segurança pública e defesa nacional.

Ou seja, em maior ou menor grau, a LGPD será aplicável a empresas em geral, independente do porte e do ramo de negócio[50].

Isso pois, o uso de dados pessoais está presente em muitos momentos da atividade empresarial: nas relações de trabalho, com execução do contrato, banco de dados e compartilhamento de informações de colaboradores; contratação de Parceiros e Profissionais Autônomos - Revisão e Adequação de Contratos; monitoramento e segurança do ambiente de trabalho; Relações *B2B* (*bussiness to bussiness*) - Abrangência de todos envolvidos no contrato (representantes contratuais, subcontratados e terceirizados); site, uso de *cookies* e uso de formulários online, interações e desenvolvimento de mídias e uso de redes sociais (*marketing*); e, ainda, quando se está diante de novos negócios, com trabalhos de *due diligence* e transações empresariais.

Nesse cenário, os dados pessoais podem ser considerados elementos nucleares para o desenvolvimento político, social e econômico[51], principalmente considerando a presença cada vez mais acelerada da tecnologia em nosso cotidiano. Ora, conforme ensina Bruno Bioni a

---

[49] MULHOLLAND, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista De Direitos E Garantias Fundamentais, 19(3), 159-180.

[50] O artigo 55-J, inciso XVIII, da LGPD, traz a possibilidade de regime diferenciado para Microempresas e Empresas de Pequeno Porte que ainda se encontra pendent de regulação pela Autoridade Nacional de Proteção de Dados – ANPD.

[51] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 4.

tecnologia "*criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imagináveis".*

A facilidade de acessar dados pessoais, principalmente por meio de celulares, é um campo fértil para a produção de uma quantia elevada de informações, até então inimaginável, no qual os dados passaram a ser processados e estruturados com todo tipo de finalidade, com o objetivo de trazer melhorias na oferta de produtos e serviços aos titulares de dados, com a apresentação de propostas individualizadas, experiências personalizadas, de acordo com os interesses demonstrados e, ainda, em tempo real.

E, nesse caso, a facilidade de se tratar dados pessoais, ainda mais sensíveis, principalmente em relação ao uso em larga escala das redes sociais e plataformas integradas, é preocupante, ao considerar o direito à liberdade, igualdade e, ainda, à intimidade[52].

Deve se manter em equilíbrio com interesses e princípios empresariais, visando, ainda, o desenvolvimento econômico, o que também é uma das bases previstas na LGPD, conforme art.1º, incisos V e VI.

Diante da vigência em plenitude da Lei Geral de Proteção de Dados no Brasil, visto que a lei propõe, para além do cumprimento de exigência legal, uma mudança cultural relacionada com a ideia de privacidade e o uso de informações pessoais, há a necessidade urgente de que as empresas implementem as regras dispostas na nova legislação, visando a diminuição de riscos relacionados com as penalidades administrativas, além de demandas impulsionadas pelos próprios titulares de dados, como ações judiciais de indenização.

3.2.Pilares para um tratamento de dados pessoais adequado

O tratamento adequado de dados pessoais se pautará em 3 pilares, sendo eles: (1) a observância dos princípios, (2) exercício dos direitos dos titulares e (3) enquadramento de justificativa legal para cada operação.

Nesse cenário, a legislação brasileira estabelece que aqueles que operam dados pessoais devem garantir o livre exercício dos direitos do titular, que conforme art.18, gera aos controladores de dados pessoais a obrigação de permitir (i) a confirmação da existência de

[52] Conforme ilustra Bruno Bioni: "Por conseguinte, tais compilações de dados estariam fora do escopo de controle dos cidadãos, abrindo-se uma porta perigosa para a desproteção de dados pessoais. Isto porque, no final das contas, pode haver um volume de informações detalhado sobre uma pessoa a compor um perfil muito preciso sobre a sua personalidade". BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 266.

tratamento de dados; (ii) acesso aos dados tratados; (iii) correção dos dados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários; (v) portabilidade; (vi) eliminação de dados tratados sem consentimento, quando esse for necessário ao tratamento; (vii) informação a respeito de compartilhamento; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências de negá-lo; e (ix) revogação do consentimento.

Além disso, será necessário o enquadramento de cada operação envolvendo dados pessoais em uma das hipóteses legais previstas na lei, dispostas nos incisos art. 7º da LGPD[53], sendo elas: Consentimento do titular; Legítimo Interesse; Cumprimento de obrigação legal ou regulatória; Tratamento pela administração pública; Realização de estudos e de pesquisa; Execução ou preparação contratual; Exercício regular de direitos; Proteção da vida e da incolumidade física.

No que tange aos dados pessoais sensíveis, a princípio, é possível observar que deverá ser utilizada a base legal do consentimento e, no caso do seu não fornecimento, abre-se a oportunidade de uso de outras bases legais, no caso de o uso de dados pessoal sensível for indispensável, sendo que as hipóteses de execução de contratos (art. 7º, V) e de proteção do crédito (art. 7º, X) ficam de fora do rol apresentado no inciso II, do art. 11 da LGPD.

No caso de legítimo interesse do controlador (art. 7º, IX), também não há menção expressa a respeito do uso de tal base legal. Contudo, o art. 11, inciso II, alínea "g", da LGPD prevê uma hipótese de tratamento de dados pessoais sensíveis e, conforme discute Caitlin Mulholland[54], a mencionada alínea pode ser considerada a aplicação da base legal do legítimo interesse, de forma mais restritiva, vinculada essencialmente aos interesses dos titulares de dados e se pode ser considerado, ainda, o interesse de terceiros, conforme prevê o art. 7º, inciso IX da LGPD.

Um destaque que se faz da legislação é a permissão quanto ao tratamento de dados sensíveis sem a necessidade de fornecimento do consentimento do titular de dados, quando for indispensável para a execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (artigo 11, II, b, LGPD), além de outras hipóteses em que se tem como pano de fundo os interesses públicos.

No mais, se requer que cada tratamento de dado pessoal tenha como pano de fundo os princípios acerca da matéria que estão dispostos no art. 6º da LGPD.

---

[53] Destaca-se que, para o tratamento de dados sensíveis, é necessário observar o que prevê o art. 1º da LGPD.

[54] MULHOLLAND, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista De Direitos E Garantias Fundamentais, 19(3), 159-180.

A razão de se estruturar princípios em uma legislação instrumental, dirigida aos agentes responsáveis pelo tratamento de dados pessoais, se verifica pela própria complexidade tecnológica.

Ora, a falta de experiências exatas e o elevado uso indiscriminado e sigiloso de informações por plataformas digitais e empresas multinacionais faz com que o próprio legislador tivesse certo receio em dispor acerca de todas as consequências decorrentes do uso de informações no seio tecnológico.

Ainda assim, percebe-se certa dificuldade para o estabelecimento de um sistema rígido e detalhado em razão da velocidade do desenvolvimento tecnológico, o que poderia trazer rapidamente uma legislação ultrapassada, caída ao desuso. A solução que parece ter sido encontrada, na opinião da autora, é o fortalecimento do indivíduo, enquanto titular dos dados pessoais tratados.

Uma vez que o direito à privacidade e proteção de dados dignam a permitir que o titular escolha a apresentação de sua esfera pessoal perante o público, a construção de uma legislação fundada em princípios se torna a valer uma base normativa de sustentação, de onde se pode extrair concepções e intenções para o exercício de direitos, ou encontrar a sua sustentação em caso de lacunas na sua aplicação frente à complexidade e velocidade da tecnologia.

Seguindo essa tendência, a LGPD parece impor uma série de mandamentos que devem ser observados em todas as operações envolvendo o tratamento de dados, independentemente da base legal e do contexto, além de servir como orientação para aplicação da lei em casos difíceis. A instrumentalidade da norma está, justamente, em viabilizar aplicação prática desses princípios em casos concretos, devendo ser observados pelos agentes de tratamento.

A LGPD dispõe de 10 princípios que podem ser vistos como os alicerces que devem embasar todas as operações de tratamentos de dados pessoais no Brasil, ajudando a entender os objetivos da lei e a forma como a legislação foi construída.

Por uma simples leitura da legislação, fica claro que a lei tem como meta trazer mais transparência para os processos envolvendo dados pessoais, dando prioridade ao poder do titular sobre as suas informações. Da mesma maneira, pela leitura dos princípios, resta evidenciado que a LGPD deposita atenção nas atividades econômicas que operam dados pessoais, elencando a necessidade de se comprometer com a segurança dos dados.

Se uma operação de tratamento de dados não segue algum dos princípios, ela pode ser considerada inadequada e ilegal. Portanto, é fundamental que se entenda e incorpore os princípios da LGPD na rotina dos operadores e controladores de dados.

Dessa forma, as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

> *"Art. 6º, inciso I - finalidade: a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*
>
> *art. 6º, inciso II - adequação: a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao (à) titular, de acordo com o contexto do tratamento; (art. 6º, inciso III) necessidade: o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*
>
> *art. 6º, inciso IV - livre acesso: é a garantia dada aos (às) titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;*
>
> *art. 6º, inciso V - qualidade dos dados: é a garantia dada aos (às) titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*
>
> *art. 6º, inciso VI - transparência: é a garantia dada aos (às) titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*
>
> *art. 6º, inciso VII - segurança: trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;*
>
> *art. 6º, inciso VIII - prevenção: compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais; (art. 6º, inciso IX - não discriminação: sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;*
>
> *art. 6º, inciso X - responsabilização e prestação de contas: demonstração, pelo Controlador ou pelo Operador, de todas as*

> *medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas*. ”

De modo geral, quando se observa o direito à proteção de dados pessoais relacionado à autodeterminação informativa, isso é, ao controle pelo titular de seus dados pessoais, constata-se que o princípio da transparência ganha força na medida em que permite o conhecimento pelo indivíduo de como, porque e para que circulam as suas próprias informações. Ou seja, é por meio da transparência que, de fato, o titular terá conhecimento e conseguirá tomar decisões relacionadas à sua esfera pessoal.

A valer, o princípio da transparência relaciona-se com o direito à informação já presente no ordenamento jurídico pátrio para além da LGPD. O Código de Defesa do Consumidor (CDC), por exemplo, estabelece em seu artigo 4º, que os consumidores devem ter as necessidades atendidas com respeito à sua dignidade, saúde e segurança, proteção de seus interesses econômicos, melhoria da sua qualidade de vida, transparência e harmonia das relações de consumo.

Nesse aspecto, o artigo 6º do Código de Defesa do Consumidor (CDC) dispõe como direito básico do consumidor a obtenção de informação adequada sobre diferentes produtos e serviços, como a especificação correta de quantidade, as características, a composição, a qualidade, os tributos incidentes e o preço, incluindo os eventuais riscos que tais produtos ou serviços possam causar.

É válido ressaltar, ainda, que o Código de Defesa do Consumidor (CDC), também prevê o direito dos consumidores ao acesso às informações pessoais, como em cadastros, fichas e registros, estabelecidos no art. 43, § 1º a 6º.

Para o exercício da capacidade decisória, enquanto fundamento da LGPD, os titulares devem possuir o conhecimento prévio quanto aos seus dados pessoais, esclarecendo a finalidade do tratamento, a necessidade do tratamento, a sua justificativa, o tempo do armazenamento, às medidas de segurança adotadas e acerca de eventual compartilhamento.

A ausência dessas informações, sem dúvidas, fere o direito à autodeterminação informativa, impondo a inadequação de eventual tratamento, pois esconde integralmente o titular da realidade, prejudicando qualquer avaliação dos riscos e dos benefícios envolvidos em sua tomada de decisão.

Ocorre que o cumprimento pelos agentes de tratamento da obrigação de dar transparência aos titulares dados pessoais é um dos maiores desafios na atualidade, diante da complexidade tecnológica e do próprio comportamento humano que merecem ser pontuados na presente reflexão.

4. DO CONSENTIMENTO COMO FERRAMENTA DO AUTOGERENCIAMENTO

4.1.Do consentimento como base legal

4.1.1.Do quadro regulatório

A autodeterminação informativa se coloca como um parâmetro normativo para a garantia da privacidade e proteção dos dados pessoais, sendo que a esfera de controle dos dados pessoais deve ser funcionalizada pelo próprio titular.

Nessa perspectiva, entende-se pela importância de propiciar ao titular dos dados pessoais um maior controle de seus dados pessoais em relação à cumulação, transmissão e retificação, autodeterminando as informações que lhes acomete. Somente assim, no entender de Bruno Bioni[55], por exemplo, salvaguardará a privacidade dos consumidores, sendo essa a sua conotação atual na sociedade da informação.

Dessa forma, torna-se imprescindível que se estabeleça o processo de comunicação entre o controlador ou o operarador do banco de dados e o titular. Ora, é a informação a premissa para tal relação intersubjetiva.

No cenário nacional, ganha destaque o Código de Defesa do Consumidor que disciplina no art. 43 os bancos de dados e cadastros de consumidores. Se faz na referida legislação a conferência ao consumidor do direito de controle de suas informações pessoais, seguindo a orientação normativa denominada *Fair Information Practice Princples/FIPPS*, que estabelece um conjunto de oito princípios relacionados ao uso, coleta e privacidade de dados, publicados em 1980 pela Organização para Cooperação e Desenvolvimento Econômico - OCDE.

A diretriz normativa imposta pelo Código de Defesa do Consumidor (CDC) coloca o consumidor no centro do controle de suas informações, exigindo transparência, qualidade dos dados e limitações temporais para o tratamento, além do exercício de direitos básicos, como acesso, retificação e cancelamento de eventual operação envolvendo dados). Isso é, é possível afirmar que o direito consumerista inaugura de forma expressa a autodeterminação informativa no país.

---

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

Seguindo em diante, mister se faz abordar a Lei do Cadastro Positivo, Lei nº 12.414/11, alterada pela Lei Complementar nº 166 (de 8 de abril de 2019), que estabelece no Brasil o uso regulamentado de plataformas de dados de históricos financeiros de consumidores, por meio do qual o comerciante tem acesso a informações que poderão distinguir um indivíduo "bom pagador" e, em razão da baixa probabilidade de risco, poderá ofertar crédito com menores taxas.

Em um primeiro momento, a referida lei estabelecia que o consumidor ou a empresa precisava autorizar a abertura de seu cadastro positivo nos órgãos de proteção ao crédito. Isso é, a legislação estabelecia desde já uma conexão direta entre o controle dos dados pessoais acoplado ao dever de informar, quando pontuava, em seu art. 4º, que a abertura do cadastro exigia consentimento informado.

Ocorre que, de acordo com a Associação Nacional dos *Bureau*s de Crédito, no período de vigência do antigo texto da legislação, somente 15 milhões de brasileiros aderiram ao cadastro positivo de forma espontânea, número pequeno frente à população economicamente ativa do país[56]. Justamente pela falta de informação por parte do consumidor acerca de quem teria acesso aos dados e como essas informações seriam utilizadas, muitos deixaram de aprovar o cadastro no referido sistema.

Com isso, foi elaborado o Projeto de Lei 441/2017, que deu origem à Lei Complementar 166/2019, que contou com a inclusão dos consumidores no sistema de cadastro positivo de forma automática e, assim, passou a não mais depender de autorização, com o intuito de ampliar a base de dados[57].

O objetivo da alteração foi levar a mais pessoas as possíveis vantagens de participar do cadastro, como maior probabilidade de conseguir crédito e taxas de juros menores. Pois, como a inclusão precisava ser solicitada, quem desconhecia a existência do Cadastro Positivo acabava deixando de aproveitar seus potenciais benefícios.

Todavia, ainda assim, o controle das informações permanece focada no titular dos dados. A lei determina que o consumidor deve ser notificado após sua inclusão no Cadastro Positivo, sendo possível solicitar o cancelamento ou reabertura do cadastro a qualquer momento, gratuitamente, pelos canais de atendimento.

---

[56] ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO. Cadastro Positivo para todos. Disponível em: < https://www.anbc.org.br/lermais_materias.php?cd_materias=14>. Acesso em: 13 de março de 2023.

[57]

[10] ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO. Cartilha Cadastro Positivo. Disponível em: < https://www.anbc.org.br/lermais_materias.php?cd_materias=28>. Acesso em: 13 de março de 2023.

Além disso, também se garante à pessoa cadastrada o direito de consultar seus dados no Cadastro Positivo gratuitamente e, do mesmo modo, é garantido o direito à exclusão ou correção de informações incorretas.

No mais, mesmo com a inclusão automática, permanece a necessidade de que a pessoa cadastrada autorize o acesso ao seu histórico de pagamentos. Sem a autorização, somente é possível o uso das informações no cálculo da nota de crédito, que pode ser exibida em consultas.

Nessa mesma toada, o Marco Civil da Internet, Lei n° 12.965, de 23 de abril 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, também dispõe no art. 7º acerca do "consentimento informado" para que os dados pessoais dos usuários possam ser coletados, transmitidos e processados em sentido amplo.

Vale dizer, é a prestação da dita informação que cientificará o usuário da internet a respeito da mera possibilidade de controlar seus dados pessoais, o que perpassa desde a coleta dos dados até a sua destinação, eliminação e/ou retificação.

Assim, na dimensão procedimental da internet, toda e qualquer ferramenta tecnológica utilizada para coleta de dados deve se cientificada ao consumidor, momento em que se verifica que a autodeterminação informativa foi o parâmetro inserido no Marco Civil da Internet para garantia da proteção de dados pessoais.

Na sequência, a Lei Geral de Proteção de Dados (LGPD) fecha o quadro regulatório nacional no que se refere à autodeterminação informativa, com o protagonismo do consentimento, visando o livre desenvolvimento da personalidade do indivíduo.

4.1.2. Do consentimento como base legal para o tratamento de dados pessoais

Em um primeiro momento, o consentimento era a única hipótese prevista na lei para o tratamento de dados pessoais, nos termos do anteprojeto da lei colocada para consulta pública em 2010. Em 2015, outras bases legais foram incluídas no texto, mas sua utilização dependeria da dispensa do consentimento.

Após o envio do texto ao Congresso Nacional, o texto aprovado e sancionado acabou desconstruindo qualquer hierarquia entre as hipóteses de tratamento de dados, estabelecendo o consentimento apenas como uma das bases legais, conforme se verifica da leitura do art. 7º da LGPD.

De fato, a construção normativa sobre proteção de dados ganhou contornos mais definidos após a Segunda Guerra Mundial[58], em que, conforme dito, os dados pessoais dos cidadãos passaram a auxiliar na reconstrução das cidades. É exatamente nesse tal contexto que surgem as primeiras leis de proteção de dados, as quais compõem a chamada primeira geração de normas de proteção de dados, com uma atuação regulatória sobre os bancos de dados.

Com o avanço tecnológico, esse tipo de controle governamental se tornou inviável. Dessa forma, uma segunda geração de normas de proteção de dados, passou a transferir ao próprio titular a incumbência de proteger seus dados.

Aos poucos, se amplia ainda mais o protagonismo do consentimento, definindo o cidadão como responsável pelo controle e autorização do que acontece com seus dados pessoais durante toda a trajetória deles.

Tal modelo, consideradas normas de terceira geração, porém, passou a ser questionado pois o seu exercício pleno acabaria em uma completa exclusão ou abstenção da vida em sociedade. Ora, se toda a lógica de proteção dos dados pessoais é centrada na responsabilidade de controle do titular sobre o ciclo de vida de tais dados, a única forma de efetivamente proteger dados seria a proteger a esfera individual.

A atual e quarta geração de normas de proteção de dados é composta por comandos que buscam cobrir essa deficiência, seja a partir da atuação por meio da criação de autoridades fiscalizadoras e/ou reguladoras para atuar ao lado do titular na proteção de seus dados pessoais ou por meio da ampliação das hipóteses de tratamento de dados pessoais, para além do consentimento.

Isso é, o titular não está mais "sozinho" na proteção de seus dados pessoais e nem precisa se abster de participar da vida em sociedade. Da mesma forma, o exercício das atividades econômicas não mais depende exclusivamente da discricionariedade do titular.

A legislação brasileira parece ter seguido tal caminho. A disposição de um conjunto de bases legais para o tratamento de dados pessoais, trazido pela quarta geração de normas, não tem o intuito de tirar completamente o protagonismo do consentimento, mas evita a exclusão do indivíduo.

---

[58] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 109

Ao citar Mayer-Schoneberger, o autor Bruno Bioni destaca que "somente os eremitas alcançariam a proteção plena de seus dados, já que, como decorrência da sua recusa em fornecê-los, amargariam o custo social decorrente da exclusão de tais atividades"[59].

Mesmo diante de um cardápio de bases legais, percebe-se uma legislação fortemente preocupada com o consentimento, justamente pela carga principiológica envolvida de que o titular de dados deve estar e permanecer no controle de suas informações e, ainda, na sua autonomia da vontade.

Assim, justifica-se não tratar o consentimento como um negócio jurídico autônomo, já que essa opção reforçaria uma determinada vantagem obtida por aquele que consente[60]. Há de se garantir a proteção da pessoa como valor preponderante, o que remete à ideia de uma ação espontânea e livre, mas com efeitos desejados.[61]

Por outro lado, Juliana Dantas e Eduardo Henrique Costa[62] se posicionam no sentido de que o consentimento, conforme previsto na LGPD, seria negócio jurídico. Para eles, o consentimento para tratamento de dados pessoais, dentro da teoria do fato jurídico, deve ser classificado como negócio jurídico, visto que não implica, de forma alguma, prejuízo aos interesses do titular dos dados pessoais. Pelo contrário, pode trazer um número ainda maior de tutelas protetivas.

Os atos jurídicos *lato sensu*, como colocado por Pontes de Miranda, "são os meios mais eficientes da atividade inter-humana, na dimensão do direito. Neles e por eles, a vontade, a inteligência e o sentimento inserem-se no mundo jurídico, edificando-o".[63]

Dividem-se em ato jurídico *stricto sensu* e negócio jurídico.

O ponto em comum entre ambos é justamente a presença da vontade como elemento do seu suporte fático.

Marcos Bernardes de Mello caracteriza o Negócio Jurídico "como o fato jurídico cujo elemento nuclear do suporte fático consiste em manifestação ou declaração consciente de

---

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

[60] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei geral de proteção de dados pessoais – e suas repercussões no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 293.

[61] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020. p. 301.

[62] DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados: ensaio à luz da teoria do fato jurídico. In: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (coord.). Direito Civil e tecnologia. Belo Horizonte: Fórum, 2020. p. 86

[63] PONTES DE MIRANDA. Tratado de direito privado: parte geral. Rio de Janeiro: Borsoi, 1954. Tomo 2. p. 446.

vontade, em relação à qual o sistema jurídico faculta às pessoas, dentro de limites predeterminados e de amplitude vária, o poder de escolha de categoria jurídica e de estruturação do conteúdo eficacial das relações jurídicas respectivas, quanto ao surgimento, permanência e intensidade no mundo jurídico".[64]

Nessa definição, tem-se que o traço distintivo entre o ato jurídico *stricto sensu* e o negócio jurídico está na a possibilidade de escolha da categoria jurídica e de estruturação do conteúdo eficacial a partir da exteriorização de vontade.

Sendo a exteriorização da vontade parte do suporte fático para ato ou negócio jurídico, o consentimento, na teoria do fato jurídico, já se apresenta como um ato jurídico *lato sensu*. Dentro do gênero, poderia ser ato jurídico *stricto sensu* ou negócio jurídico. A distinção aqui se faz porque, enquanto no primeiro não haveria possibilidade de modificação de sua eficácia, tal modificação seria possível no segundo [65].

O consentimento para tratamento de dados pessoais traz, em sua essência, a possibilidade de modificação de sua eficácia, até nos termos da própria LGPD ao possibilitar a revogação do consentimento. Se isso não se dá na prática, não se deve à natureza do ato de consentir, mas sim à estrutura contratual em que ele se insere, ou seja, o fato de se apresentar como sendo de adesão [66].

Admite-se uma estrutura dinâmica, em que se exige uma cooperação entre os sujeitos do vínculo obrigacional, em razão dos interesses estarem canalizados para um fim comum: proteção de dados e garantia da privacidade. Trata-se, portanto, de uma visão solidarista que tem o princípio da boa-fé em sua gênese, enquanto uma coordenação recíproca de deveres e direitos.

Nesse momento, nota-se que o consentimento funciona mais como um instrumento, por excelência, da autodeterminação, sem implicar na inviabilidade do desenvolvimento social da pessoa humana ou na própria atividade econômica.

---

[64] MELLO, Marcos Bernardes de. Teoria do fato jurídico: plano da existência. 14. ed. São Paulo: Saraiva, 2007. p. 189.

[65] MELO, Marco Aurélio Bezerra. Curso de Direito Civil: responsabilidade civil. São Paulo: Atlas, 2015. v. 4.

[66] REQUIÃO, Maurício. A natureza jurídica do consentimento para tratamento de dados pessoais. In: REQUIÃO, Maurício (Org.). Proteção de dados pessoais: novas perspectivas. Salvador: EDUFBA, 2022, p.26

4.2. Dos requisitos legais para uso do consentimento como base legal para o tratamento de dados pessoais

À luz da LGPD, o consentimento é conceituado no artigo 5º, inciso XII, como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Esse conceito pode ser destrinchado em quatro critérios para a sua eficácia e validade, pelos quais o consentimento deve ser: livre, informado, inequívoco e, ainda, utilizado para uma finalidade determinada.

Pela leitura da legislação, é possível constatar que não há, de forma expressa, a definição específica de cada um desses critérios. A saída encontrada no presente trabalho foi recorrer ao Regulamento Geral de Proteção de Dados da União Europeia (GDPR), bem como às orientações emitidas pelo Conselho Europeu de Proteção de Dados (*European Data Protection Board*), ao considerar a *Guideline* 05/2020 emitida pelo antigo Grupo de Trabalho do Artigo 29[67].

No caso, o conceito básico de consentimento previsto no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) é o mesmo ao previsto Diretiva 95/46/CE, permanecendo como um dos fundamentos jurídicos em que o tratamento de dados pessoais tem de se basear, nos termos do artigo 6º do Regulamento Geral de Proteção de Dados da União Europeia (GDPR)[68].

No caso, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) fornece as orientações suplementares no artigo 7º e nos considerandos 32, 33, 42 e 43 sobre a forma como o responsável pelo tratamento deve atuar para cumprir os principais elementos do requisito do consentimento.

O critério livre implica uma escolha espontânea dos titulares dos dados. Isso é, se o titular dos dados não puder exercer escolha de livre-arbítrio, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não poderia ser considerado válido.

O trabalho envolve a verificação de algum tipo de subordinação ou assimetria de poder que possa, de alguma forma, eliminar a voluntariedade do consentimento, nos termos do artigo 14 do Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

---

[67] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt

[68] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt

A avaliação de que o consentimento foi dado livremente dependerá de uma análise contextual específica, principalmente quando subordinado à execução de um contrato ou à prestação de um serviço, tal como dispõe o artigo 7º, nº 4, do Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Em termos gerais, busca-se evitar qualquer hipótese em que se verifique alguma pressão, coação ou influência inadequada sobre o titular dos dados, que o impeça de exercer livremente a sua vontade.

Imperioso destacar que um serviço pode envolver múltiplas operações de tratamento, que irá abranger mais de uma finalidade. Nesses casos, os titulares dos dados devem poder escolher quais são as finalidades que aceitariam ou não e, assim, dar consentimento para um conjunto de finalidades determinadas.

O consentimento não é dado de livre vontade se o processo/procedimento para obter o consentimento não permitir aos titulares dos dados autorizem separadamente para cada operação de tratamento de dados pessoais. O que remete a outro critério, o da especificidade.

Isso é, o consentimento do titular dos dados deve ser dado em relação a uma ou mais finalidades específicas, momento em que o titular de dados tem escolha em relação a cada uma delas. O requisito de que o consentimento deve ser específico serve para garantir um maior controle do agente de tratamento e, ainda, maior transparência em relação ao tratamento de dados.

Há de se evitar qualquer desequilíbrio para que se garanta uma manifestação verdadeiramente livre. Tanto é assim que no Considerando 43 do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) há a vedação do uso do consentimento pelas autoridades públicas para o tratamento, uma vez que existe frequentemente um desequilíbrio de poder na relação entre o responsável pelo tratamento e o titular dos dados.

No mesmo sentido, verifica-se, por exemplo, o desinteresse em utilizar essa base legal nas relações trabalhistas. De fato, parte da doutrina tem questionado se esse consentimento é, verdadeiramente, livre e – a depender do colaborador – de fácil compreensão, especialmente quanto à necessidade de tratamento daqueles dados.

Em verdade, a LGPD não foi pensada para as peculiaridades do trâmite de informações entre empregador e empregado e, com isso, ainda existe um debate quanto à aplicação da legislação no âmbito trabalhista.

Nesse sentido, por exemplo, o Regulamento Europeu de Proteção de Dados (GDPR), norma referência para a criação da LGPD, prevê que a proteção de dados nas relações de emprego deve ter regulação própria, reconhecendo, portanto, a especificidade dessas relações.

De todo modo, esse entendimento não significa que os empregadores nunca possam utilizar o consentimento como fundamento jurídico para eventual tratamento de dados. Pode haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente ou, a depender do contexto, fazer o uso de outras bases legais.

Nesse ponto, ressalva-se aos dados pessoais sensíveis, que são os derivados étnicos, religiosos, político, filiação sindical, genético ou biométrico. No caso, a LGPD prevê uma hierarquia da utilização das bases legais.

O tratamento destes pelo empregador deve se prender apenas às bases legais estabelecidas no art. 11, que dispõe quanto à necessidade de consentimento específico do titular e, somente quando não for fornecido, passa-se a permitir a utilização de outras bases legais, como cumprimento de obrigação legal ou regulatória.

Nesse sentido, caso o empregado se negue a consentir com esse tratamento de dados, será possível, nos termos expressos da lei, a utilização de outra base legal. Nessa hipótese, considerando serem os dados pessoais efetivamente necessários para a execução do contrato, o consentimento deixa de ser o fundamento jurídico.

Em relação aos dados de saúde, especificamente, entende-se ser necessária à coleta do consentimento e, não sendo fornecido, é possível a utilização da base legal da execução de contrato (Contrato de Trabalho e Contrato de Prestação de Serviços) e do cumprimento de obrigação legal (Consolidação das Leis do Trabalho, Convenção Coletiva de Trabalho/Acordo Coletivo de Trabalho – art. 7º, inciso XXVI da Constituição Federal/88).

Mesmo entendimento se aplica aos dados relacionados à filiação sindical e à biometria. Dessa maneira, o caminho mais seguro, por enquanto, é exigir o consentimento legal da coleta e transferência dos dados pessoais do empregado, considerando o tratamento de dados sensíveis.

Não sendo possível, como no caso de o colaborador não consentir, sugere-se à utilização das bases legais do cumprimento de obrigação legal, nos termos do art. 8º, XXVI, da Constituição Federal/88 e os artigos 611 e 611-A da Consolidação das Leis do Trabalho ou da execução contratual, considerando o próprio Contrato de Trabalho e os benefícios estabelecidos em acordos coletivos.

Dando sequência, seguindo o que dispõe o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), entende-se pela necessidade de se exigir do titular dos dados uma declaração ou um ato positivo inequívoco, conforme art. 8º, caput e § 1º, da LGPD. Ou seja, o consentimento para tratamento de dados deve se dar por meio de uma ação positiva ou declaração expressa.

Isso é, o consentimento válido exige uma manifestação explícita mediante declaração ou ato positivo inequívoco, em que o titular dos dados age deliberadamente para consentir com o tratamento objeto.

Nesse ponto, é imperioso ter cuidado com o fato do consentimento não poder ser obtido mediante a mesma ação de aceite do contrato. Como tal, pode ser que a recusa consentimento, que não se confunde com aceitação do contrato, possa interromper a experiência de utilização de um serviço ou o próprio negócio jurídico.

Talvez a forma mais literal de cumprir o critério especificidade seja garantir que o titular dos dados tenha acesso a todo o detalhamento do tratamento envolvido e, após, escreva uma declaração ou redija um termo ao agente pelo tratamento explicando exatamente com o que concorda.

Contudo, trata-se de algo que frequentemente não é realista. Inclusive, no âmbito do direito europeu, chegou-se a entender pela impossibilidade de uso de disposições já pré-selecionadas, por representarem um silêncio por parte do titular do dado. Contudo, atualmente, tal prática é vista como uma ferramenta operacional, que proativamente, sinalizada as configurações do serviço acessado.

As declarações escritas podem ter muitos formatos e muitas dimensões que podem estar em conformidade com a legislação. Como se nota da leitura do art. 8º da LGPD, o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

Caso o consentimento seja obtido por declaração oral gravada, embora importe ter devidamente em atenção quais as informações à disposição do titular dos dados antes de este manifestar o consentimento, há um ato de aprovação por parte do titular. O silêncio ou a inatividade da parte do titular dos dados, bem como a mera utilização de um serviço, não podem ser encarados como manifestação ativa de escolha.

A valer, os responsáveis pelo tratamento têm liberdade para cumprirem os requisitos dispostos, de maneira que atenda às suas operações quotidianas. Todavia, surgirá o dever de demonstrar que obteve um consentimento válido. Cabe ao responsável pelo tratamento provar que o consentimento válido foi obtido junto do titular dos dados, conforme § 2º, art. 8º.

A LGPD não prevê exatamente como é que isso deve ser feito. Contudo, basta o agente conseguir provar que o titular de dados deu o seu consentimento em determinada situação. Enquanto a atividade de tratamento de dados perdurar, a obrigação de demonstrar o consentimento existe.

Quando terminar a atividade de tratamento, a prova do consentimento não deve ser conservada mais, uma vez que a partir daí, surgem outras bases legais, como o cumprimento de um dever legal e/ou exercício ou defesa de direitos.

Todavia, é importante destacar que o término da atividade envolvendo o tratamento de dados difere da revogação do consentimento, ainda que seu efeito prático, ao final, se reduza no mesmo.

O § 5º do art. 8º da LGPD, da mesma forma como se prevê na legislação europeia, determina a possibilidade de revogação da mediante manifestação expressa do titular, por procedimento gratuito e facilitado, momento em que deve ser ratificado todos tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Pela natureza do instituto do consentimento, deve-se reconhecer a possibilidade de revogação do ato pelo qual uma pessoa consente no tratamento de seus dados pessoais, visto que nesse seu poder encontra-se o próprio sentido de autodeterminação em relação à construção de sua esfera privada. Esse poder, ligado ao livre desenvolvimento da personalidade, merece, portanto, a tutela do ordenamento jurídico.[69]

Isso é, se o consentimento for revogado pelo titular, todas as operações de tratamento de dados baseadas nesse consentimento e que ocorreram antes da retirada do consentimento permanecem lícitas. Contudo, o agente de tratamento deve parar as ações de tratamento em causa após revogação. Caso não exista qualquer outro fundamento jurídico que justifique a permanência do tratamento dos dados, estes devem ser apagados.

Como se nota, o instituto do consentimento é marcado por uma gradual adjetivação, com base no ordenamento jurídico europeu. Contudo, verifica-se, em verdade, uma ausência na legislação nacional acerca da sua operacionalização.

No exercício de sua autodeterminação, o sujeito não está restrito aos efeitos vinculantes de natureza obrigacional resultantes do consentimento anteriormente oferecido e, consequentemente, não se pode associar tal ato a um inadimplemento de qualquer espécie.

Torna-se, dessa forma, importante que os agentes de tratamento avaliem especificamente as finalidades para as quais os dados são efetivamente tratados e os fundamentos jurídicos em que se baseia cada operação envolvendo dados.

De qualquer forma, ante o necessário atendimento dos requisitos para um consentimento válido, há de se questionar se o consentimento é, de fato, a melhor alternativa para o tratamento

---

[69] Doneda, 315

regular de dados pessoais, principalmente considerando que o consentimento pode ser retirado pelo titular a qualquer momento.

Não existe uma única resposta correta para tal questionamento. É preciso analisar o caso concreto para estabelecer a base legal mais apropriada para um determinado tratamento. A depender da situação, o consentimento pode, de fato, ser a base mais adequada, com a observância de todos os critérios aqui delineados.

4.3. *A operacionalização do consentimento*

A operacionalização do consentimento pode realizar-se por meio da sua interpretação à luz de alguns princípios da proteção de dados pessoais. Destes, destacam-se os princípios da finalidade e o da informação.

O princípio da finalidade pode informar a disciplina do consenso restringindo a sua generalidade. Estipula o Art. 6º, inciso I, da LGPD, que a realização do tratamento deve ter propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Assim, o consentimento deve ser lido restritivamente em relação a sua finalidade.

Para a aplicação correta do princípio da finalidade, evoca-se, ainda, o princípio da informação, que deve ser observado em torno desse consentimento.

Isso é, o consentimento válido depende da completa consciência do titular sobre o tratamento de seus dados pessoais. Essa informação inclui todos os detalhes necessários em uma determinada situação para que o interessado possa formar sua convicção, livre e consciente, para realizar o ato de autodeterminação.

5. DA ARQUITETURA TECNOLÓGICA

De fato, as novas tecnologias digitais prometem trazer grandes benefícios ao bem-estar social no futuro, promovendo melhores condições de vida, de saúde, entre outros. No entanto, a economia das plataformas digitais traz também desafios relevantes, o que compromete potencialmente a capacidade de agência dos indivíduos em relação aos seus dados, o que favorece o capitalismo de vigilância.

De acordo com o que descreve o autor Maurício Requião[70], é superficial simplesmente pretender usar o consentimento no tratamento de dados pessoais, uma vez que se ignoraria todos os nuances e aspectos relevantes envolvidos em tal relação jurídica.

Isso, porque é evidente a situação de vulnerabilidade do usuário frente ao tratamento de dados nas plataformas digitais, em especial considerando a tecnicidade do tema e também o formato em que os serviços e produtos se apresentam no mundo virtual.

Os principais desafios criados pelas plataformas digitais, concentram-se no próprio (i) direito de cada indivíduo saber e, de fato, entender o que é feito com seus dados e, ainda, (ii) no segredo comercial envolvido e (iii) nos prós e os contras da promoção da transparência.

5.1. *Do desenvolvimento tecnológico e a privacidade*

O primeiro desafio diz respeito à dificuldade de impor às plataformas digitais critérios para o uso consentimento informado dos usuários a respeito do uso de seus dados pessoais. Ora, os processos de gestão e tratamento pelas plataformas digitais se complexificam a cada dia, incluindo o uso de ferramentas de inteligência artificial e algoritmos avançados.

Toma-se como base a Internet das Coisas, que tem como escopo a convergência das tecnologias dos mundos digitais, físicos e biológicos. Isso, pois a Internet das Coisas possibilita a integração entre dispositivos que possuem conexão à Internet, proporcionando controle remoto, automações e compartilhamento de informações.

O termo *Internet of Things* (Internet das Coisas) foi criado em 1999, por Kevin Ashton, um dos pioneiros da tecnologia britânica, que ajudou a desenvolver o conceito ao denominar a infraestrutura de *hardware* e *software* que viabiliza a conectividade entre dispositivos que possuem conexão à internet.

A IoT ganha papel de destaque na busca pela hiper conectividade e facilidade no acesso à informação, direcionando o cotidiano humano, visto que proporciona controle remoto, automações e compartilhamento de dados, desde lâmpadas, eletrodomésticos, veículos, entre outros.

Na atualidade, há grande heterogeneidade de equipamentos, tais como TVs, Laptops, automóveis, smartphones, consoles de jogos, webcams conectados à rede, e a lista de dispostivos aumenta a cada dia.

---

[70] REQUIÃO, Maurício. A natureza jurídica do consentimento para tratamento de dados pessoais. In: REQUIÃO, Maurício (Org.). Proteção de dados pessoais: novas perspectivas. Salvador: EDUFBA, 2022, p.22

Com a pluralidade de equipamentos crescente e com a elevação na disponibilização de novos recursos nesses objetos, torna-se possível detectar seu contexto, controlá-lo, viabilizar troca de informações uns com os outros, acessar serviços da Internet e interagir com pessoas. Concomitantemente, uma gama de novas possibilidades de aplicações surge, como as cidades inteligentes e casas inteligentes e, por óbvio, os desafios, como regulamentações, segurança, padronizações, também crescem.

Considerando o que tecnologia pode oferecer à sociedade, bem como os benefícios econômicos envolvidos, os países, no geral, têm investido cada vez mais na sua implementação. No Brasil, em 25 de junho de 2019, foi publicado o Decreto nº 9.854, que institui o Plano Nacional de Internet das Coisas no Brasil, o qual estabelece conceitos, diretrizes e dispõe sobre a Câmara de Internet das Coisas.

O Decreto considera IoT como "*a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade*".

Essa interoperabilidade, pode ser entendida como a capacidade de diversos sistemas e instituições trabalharem em conjunto (interoperar) de modo a garantir a interação entre os equipamentos para trocar informações de maneira eficiente. Essa característica proporciona, em conjunto com inteligência artificial, que plataformas façam diagnósticos médicos prévios, de maneira rápida e sem a necessidade de se aguardar pelo resultado de um exame de saúde.

Não existe, a princípio, um acordo único e geral sobre a arquitetura da interoperabilidade da IoT que seja convencionado no mundo inteiro e também pelos pesquisadores[71].

Há quem proponha um modelo de 3 camadas, mas também há aqueles que defendam modelos com 4 ou 5 camadas. Essa discussão da quantidade de camadas na arquitetura IoT está relacionada à segurança da rede. Na maioria dos casos, os desafios dos objetos inteligentes são a capacidade de processamento reduzida e a sua fonte de alimentação, isso traz a esses dispositivos fragilidades que podem ser exploradas por invasores.

A arquitetura de três camadas é formada basicamente pela Camada de Percepção, Camada de Network e Camada de Aplicação.

A camada de percepção é a camada física. Ela é responsável por, mediante uso de sensores, coletar e juntar informações sobre o ambiente. A camada de Network é a camada

[71] (BURHAN et al., 2018, p. 6)

intermediária, sendo responsável por conectar os objetos aos serviços de redes e aos servidores. Pode-se dizer que ela é uma camada responsável pelo transporte de informação.

E por último, haverá a camada de aplicação. Essa camada é responsável por entregar o resultado desejado. Ou seja, é nessa camada que será gerada uma resposta dizendo ao comando dado pelo usuário em sua experiência na primeira camada.

Em caso de demandas mais complexas, com um maior volume e circulação de dados, se verifica a necessidade de uma arquitetura mais avançada e, dessa forma, haverá a arquitetura de cinco camadas. Nessa arquitetura, são adicionadas as camadas de processamento, que se localizada entre as camadas de Network e Aplicação e a de negócios que se localiza acima da camada de Aplicação.

Nessa arquitetura, as camadas de percepção e aplicação mantém suas características. Entretanto, a camada de Network se tornou a camada de transporte, verificando responsável por apenas conduzir as informações para a camada de processamento, por meio de redes como 5G, LAN, Bluetooth, RFID, entre outras.

A camada de processamento, nova componente da arquitetura, é responsável por armazenar, analisar e processar a grande quantidade de dados da melhor forma possível, utilizando banco de dados, computação em nuvem e módulos de *Big Data*.

E por fim, a camada de negócios. Essa camada é responsável por administrar todo o processo, desde a aquisição e processamento de dados, até a geração de uma resposta que possa ser utilizada na prática.

Como se nota, os ecossistemas de IoT e as cadeias de entrega estão cada vez mais entrelaçados e avançando de maneira contínua, o que cria uma frequência sem precedentes de mudança, tamanho e complexidade nos ambientes em que esses sistemas são construídos. Desse modo, acaba sendo colocada em foco questões relacionadas à segurança da rede e como, por exemplo, e em qual camada devem ser executados os protocolos de segurança e privacidade, e se existe a necessidade ou não de uma camada específica para realizar tais operações.

Para se ter como base, o uso de tecnologia inteligente na área de saúde tem avançado continuamente nos últimos anos. Entre algumas das aplicações que podem ser citadas, como o monitoramento por *Smart Watches*. Essa tecnologia, consiste na utilização de relógios, que além de monitorar o sono, exercícios físicos, são capazes de esquematizar ecocardiogramas e verificar a presença de ritmos cardíacos irregulares.

Existem riscos associados à integração de muitas ferramentas e recursos com um relógio inteligente, pois eles podem ser menos precisos, fazer com que os consumidores tratem

condições que podem não existir ou ser graves, ou impedi-los de buscar verdadeiras avaliações médicas com o equipamento adequado.

Por outro lado, é possível argumentar que tornar essas ferramentas mais comuns pode se tratar de uma medida preventiva e eficaz ao aparecimento de condições mais graves, considerando que eventuais sintomas são descobertos precocemente.

Contudo, há a questão da privacidade e do tratamento de dados. Questiona-se se os consumidores deveriam colocar tanto de sua saúde e dados biométricos nas mãos de não especialistas em saúde como *Google*, *Apple* e *Samsung*, enquanto controladoras dos sistemas de tais equipamentos. O *Google*, por exemplo, já esteve envolvido em vários incidentes envolvendo a transferência inadequada ou secreta de dados.

Do ponto de vista do usuário, opera-se o princípio da abstração. Isso, pois toda a complexidade deve ser invisível e o uso deve ser tão simples que não exija um manual de instruções. O usuário não precisa se preocupar com o fato de que por trás de um clique ou botão há, na realidade, uma gama de equipamentos e instituições conectadas.

A partir disso, o usuário não tem meios de conhecer todas as informações geradas por suas interações com as plataformas integradas em dispositivos, nem tão pouco obter a garantia de que seus dados estão em segurança, tendo em vista a grande complexidade técnica envolvida nas rotinas de segurança da informação de grandes plataformas.

Para qualquer tomada de decisão, o usuário precisaria entender o modelo básico de dados que suporta a criação de experiências de uso de tecnologias novas e inovadoras. Até mesmo técnicos da área deixam de compreender totalmente o funcionamento interno dos dispositivos e protocolos de comunicação. Ao criar o dispositivo, há um trabalho de ocultar a complexidade do *hardware* e, ao mesmo tempo, garantir a segurança e a estabilidade do produto a longo prazo.

Entende-se, na verdade, que o sucesso de um produto de IoT depende de sua usabilidade. Por se tratar de uma ferramenta facilitadora, os clientes não compram ou usam produtos muito complicados. Por isso, é natural que se crie *software* apenas para produtos simples, divertidos de trabalhar e comercialmente atraentes.

Colocando o problema em termos econômicos, é possível dizer que a estratégia regulatória tradicional, que poderia consistir na promoção da transparência está sujeita, no contexto digital, a diversas limitações, tendo em vista o problema das externalidades de dados, a racionalidade limitada dos usuários e os altos custos de transação associados à formulação de um consentimento informado.

Na Alegoria do Mito Caverna, prisioneiros acorrentados assistem sombras lançadas por um incêndio atrás deles. Eles não podem entender as ações daqueles que criam as imagens, em razão de representar tudo que eles conhecem da realidade. Como aqueles que se contentam em usar tecnologia sem entendê-la, tais indivíduos podem se ver hipnotizados pelos resultados, sem ter como se protegerem da manipulação ou exploração.

O protagonista na alegoria da transformação da sociedade nesse contexto da Era da *Big Data* foi o *Google*[72].

O *Google* foi fundado em 4 de setembro de 1998 na Califórnia/EUA pelos seus criadores são Larry Page e Sergey Brin, dois estudantes do curso de doutorado da Universidade de Stanford. Hoje, a empresa é uma das três mais valiosas do mundo, juntamente com *Apple* e *Amazon*, possuindo hoje um grande repertório de produtos que vão muito além da Busca na web, que ainda é seu carro-chefe.

Brin e Page decidiram dedicar ao estudo das propriedades matemáticas da *World Wide Web*, o nome "oficial" da internet. Eles assinaram uma dissertação com o título "*The Anatomy of a Large-Scale Hypertextual Web Search Engine*" ("A anatomia de um mecanismo de pesquisa da Web hipertextual em grande escala", em tradução livre). O texto descrevia, em resumo, as propriedades técnicas de um buscador capaz de rastrear a web inteira e listar as páginas com base na sua relevância.

Para colocar em prática as ideias da dissertação, Page e Brin criaram o *BackRub*, um buscador que usava a tecnologia, criada por eles, chamada de *PageRank*, que depois passou a se chamar *Google*. Originalmente, o buscador online ficava lotado nos servidores da Universidade de Stanford e era acessado pela URL *google.stanford.edu*. O domínio *google.com*, porém, só foi registrado em 15 de setembro de 1997.

Ao final da década de 90, início dos anos 2000, apesar das manifestações contrárias dos criadores da plataforma, foi projetado um sistema da *Google* de anúncios por Eric Veach. O sistema *AdWords*, a princípio, não previa uma compra de melhores propagandas e em melhores posições pelos anunciantes. Em um primeiro momento, os anúncios que conseguissem fazer mais cliques por usuários, garantindo, então, uma maior utilidade, recebiam melhores posições.

Contudo, se observou uma suposta manipulação com a realização de cliques pelos próprios anunciantes. Dessa forma, iniciou na plataforma uma prática de leilão de anúncios.

---

[72] VELIZ, Carissa. Privacdade é o poder: por que e como você deveria retomar o controle de seus dados. Tradução Samuel Oliveira – 1 ed. São Paulo: Editora Contracorrente, 2021. Fls. 54

Não foi um sucesso instantâneo, mas se tornou a principal fonte de renda da empresa e responsável por levantar alguns bilhões de dólares para o *Google* todos os anos. Isso permitiu que a empresa continuasse oferecendo produtos gratuitos para usuários. A valer, nesse momento, os usuários estes deixaram de ser os clientes do *Google*, tornando-se os próprios produtos.

Se antes os dados dos usuários serviam, exclusivamente, para melhorias nos sistemas de buscas, aos poucos, em razão da necessidade de se calcular as interações dos anúncios, as informações dos usuários passaram a ser fundamentais para a personalização de propagandas.

À medida que os usuários pesquisavam sobre o que desejavam, o *Google* passava a coletar milhões de dados sobre eles. Assim, o *AdWords*, complementado pela *AdSense*, deu o pontapé inicial na economia de vigilância. [73]

Ocorre que a sociedade romantizada pelo desenvolvimento tecnológico e ainda, embebedada pela possibilidade de alcance facilitado de serviços, principalmente gratuitos, nada fez. A narrativa em torno da troca de dados pessoais pela utilização de plataformas digitais foi observada anos depois que os negócios foram feitos.

Apesar da preocupação no final dos anos 90 pela Comissão Federal de Comércio nos Estados Unidos, a matéria deixou de ser o foco em razão dos ataques terroristas em 2001, que mudaram o rumo no aspecto informacional, colocando a segurança como uma demanda emergencial, envolvendo público e privado.

Essa cooperação pública e privada vigora na atualidade. Países, de forma geral, utilizam o apoio das grandes empresas de tecnologia para fins de vigilância. Durante crises, essa parceria jamais poderá ser desconsiderada, a partir da análise de prós e contras. As instituições privadas e as agências governamentais se engajam na tomada do poder e as liberdades civis são enfraquecidas e, na maioria das vezes, jamais reestabelecidas após a passagem de uma crise.

Esse cenário se altera a partir do episódio americano ocorrido no dia 11 de setembro de 2001, em que, em razão dos ataques terroristas, se passou a observar a missão de se garantir a segurança nacional a qualquer custo. Desde então, qualquer discussão no âmbito estadunidense acerca da privacidade foi arquivada[74].

Foi apresentada uma oportunidade governamental para que agentes de inteligência expandisse poderes de vigilância, com o auxílio de gigantes da tecnologia. Ocorre que a maior

---

[73] ELIZ, Carissa. Privacdade é o poder: por que e como você deveria retomar o controle de seus dados. Tradução Samuel Oliveira – 1 ed. São Paulo: Editora Contracorrente, 2021. Fls. 59

[74] Zubboff, 112-21

parte do tráfego mundial da internet circula na infraestrutura sob o controle dos Estados Unidos, o que importa na vigilância de dados em todo o mundo.

O terrorismo ou uma crise sanitária, como a Pandemia do Covid-19, trazem dificuldades para o pensamento da privacidade, dada a emergência de tais fatos. Contudo, basta entender se todo esse controle, de fato, consegue excluir ou, pelo menos, minimizar ataques terroristas.

A valer, as perdas da privacidade também podem ser letais. É mais adequado que pensemos em proteger os nossos dados, mesmo diante de uma crise, se o indivíduo tiver em mente que a privacidade também importa.

5.2. A problemática entorno do segredo comercial

O *Google*, assim como outras gigantes da tecnologia, no caso, com base na legislação comercial e concorrencial, preferiu manter o sigilo, adotando uma postura de ocultação das tecnologias evolvidas, tratando-as como segredos comerciais.

Em verdade, a proteção ao segredo industrial e comercial, utilizado pelo *Google* e pelas demais *bigtechs*, nasce das normas de proteção à propriedade intelectual, originadas com a Revolução Industrial, por meio da qual a produção artesanal cedeu lugar a uma produção industrial e a sociedade começou a perceber que o "como fazer" poderia ser monetização, a partir de seu valor econômico real.

Com isso, a proteção por meio de leis e regulamentos nacionais passou a ser uma demanda concreta, incrementando no comércio internacional. Assim, começaram a surgir convenções internacionais tratando da proteção à propriedade industrial.

Cita-se, como exemplo, a Convenção da União de Berna[75], no *Trade Related Aspects of Intellectual Property Right*, que teve por objeto "*as patentes de invenção, os modelos de utilidade, os desenhos ou modelos industriais, as marcas de fábrica ou de comércio, as marcas de serviço, o nome comercial e as indicações de proveniência ou denominações de origem, bem como a repressão da concorrência desleal"*. O intuito era garantir às empresas a recuperação de investimentos na pesquisa e desenvolvimento tecnológico, ao determinar a exclusividade de comercialização de um produto ou serviço

No Brasil, as normas sobre concorrência desleal também sempre estiveram ligadas à proteção ao segredo industrial, como se observa do o Decreto nº 24.507/1934.

---

[75] BRASIL. DECRETO No 75.699, DE 6 DE MAIO DE 1975. Convenção de Berna para a Proteção das Obras Literárias e Artísticas. 9 de setembro de 1886, revista em Paris, a 24 de julho de 1971.

Na mesma linha, há o Decreto n° 7.903/1945 e, mais tarde, a Lei nº 9.279/1996. Verifica-se pela análise da legislação que o conceito de propriedade industrial parte de construção doutrinária, que estabelece quais as características desse instituto.

Seguindo o direito internacional, a Lei nº 9.279/199618 adotou um conceito mais amplo de "segredo industrial", incluindo aqui os segredos utilizados na indústria, comércio ou prestação de serviços.

Para que se possa estar diante de um segredo industrial ou comercial, é estabelecido como requisito que se trate de uma novidade envolvendo uma informação que não tenha sido objeto de divulgação. Soma-se a essas características a existência de um valor econômico, implicando em uma vantagem competitiva, podendo ser suscetíveis de transações comerciais.

Pode-se estar diante do desenvolvimento de uma tecnologia, algum processo de fabricação, o desenho de um algoritmo ou o substrato que o alimenta, um modo de atuação, algum conhecimento específico ou até mesmo uma estratégia negocial. Certamente, a inexistência de proteção ao segredo industrial e comercial poderia ser de extrema lesividade para o desenvolvimento econômico e tecnológico do país.

Contudo, é importante que se entenda de quem seria o benefício do referido sigilo, considerando que o seu impacto é inerente à natureza, visto a sua função de construir ou moldar a sociedade. E, nesse ponto, ganha importância o papel da legislção.

Todavia, imperioso trazer à tona que os segredos industrial e comercial foram inseridos na LGPD e podem ser vistos como um limite ao direito de acesso à informação e ao princípio da transparência. Isso significa, portanto, que em diversas situações, a exceção trazida aos segredos industrial e comercial pode se tornar uma verdadeira carta branca, carta esta que pode estar legitimando a lesão a um direito fundamental.

Frank Pasquale parte, então, da metáfora da Caixa Preta, "*The Black Box Society*", que pode referir-se a um dispositivo de gravação, como os sistemas de monitoramento de dados em aviões, trens e carros. Ou pode significar um sistema cujo funcionamentos são misteriosos, em que podemos observar suas entradas e saídas, mas não podemos dizer como um se torna o outro.

Enfrentamos esses dois significados diariamente: rastreados cada vez mais de perto por empresas e governos e, ao mesmo tempo, não se tem ideia de quão longe esta informação pode viajar, o seu uso ou suas consequências.

Como visto, ainda que a LGPD estabeleça diversas disposições que trazem a transparência e o acesso à informação dos titulares dos dados como princípios fundamentais à serem observados para o tratamento de dados pessoais, bem como a imposição de mecanismos

para exercício direto pelos titulares, observa-se que quando se tratar da proteção aos segredos industriais e comerciais, os titulares são deixados de lado de certa maneira.

A valer, o declínio da privacidade, nesse aspecto, deveria, ao contrário, ser acompanhado por níveis comparáveis de transparência pelas instituições privadas e, ainda, pelo próprio governo. Mas, não é o que ocorre. Não se verifica uma tentativa clara de apurar os algoritmos envoltos na internet das coisas ou na inteligência artificial, exceto nas raras ocasiões em um que uma ameaça ou, de fato, a ocorrência de litígio, como o vazamento de dados pessoais.

Há, por evidência, certa incompatibilidade entre o exercício de forma direta pelo titular, como a sobreposição do seu direito de transparência e autodeterminação informativa em detrimento dos segredos industriais e comerciais dos agentes de tratamento. E é nesse ponto que o efetivo debate se inicia: a ausência de uma relação de confiança quando há o tratamento de dados pessoais.

A publicização de um segredo industrial ou comercial descaracteriza a sua própria natureza. Mas, o que se percebe é que não apenas aos titulares não foi dado referido poder, mas igualmente os órgãos de fiscalização e controle permaneceram sem ferramentas suficientes para verificar nas situações concretas o interesse que deve prevalecer e, assim, a possibilidade ou não de compatibilização entre os diferentes interesses.

E, nesse ponto, serão observadas, conforme ensina Pasquale, 3 estratégias para a manutenção das caixas pretas fechadas: o sigilo real, o sigilo legal e a ofuscação[76].

O sigilo real estabelece uma barreira entre conteúdo e eventual acesso não autorizado a ele. Usamos sigilo real por meio de senhas ou, fisicamente, quando diariamente se tranca portas de casa.

Já o sigilo legal, trata-se de uma obrigação, isso é, um dever daqueles que têm acesso a certas informações em mantê-las em segredo, como um funcionário ocupando um cargo de confiança ou um advogado em respeito à ética de sua profissão.

No caso, a ofuscação envolverá tentativas deliberadas de ocultação quando o sigilo já foi comprometido. Por exemplo, uma empresa pode responder a um pedido de informações, entregando 30 milhões de páginas de documentos, forçando seu investigador perder tempo procurando uma agulha no palheiro.

---

[76] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. Harvard University Press: Cambridge, Massachusetts London, England, 2015

O ponto de partida é, sem dúvidas, aprender mais sobre o que os agentes de tratamento estão fazendo com os dados e definir padrões mais rígidos e melhores práticas de auditoria em que se permita uma regulação mais substantiva do setor privado e público.

Mesmo que o segredo comercial seja visto como uma estratégia de negócio, ele é capaz de aniquilar a nossa habilidade de entender o mundo e, ainda, a sociedade que está sendo criada. A ideia de opacidade cria oportunidades para esconder condutas anticompetitivas, discriminatórias ou descuidadas sob um manto de limitação técnica e complexidade tecnológica.

Neste sentido, os arts. 10 e 38 da LGPD estabelecem que a Autoridade Nacional de Proteção de Dados pode solicitar o relatório de impacto à proteção de dados pessoais para os agentes de tratamento, devendo ser observados os segredos comercial e industrial. Diante da ausência de maiores esclarecimentos na própria legislação e da própria ANPD até a presente data, levanta-se, por uma leitura literal da norma, um questionamento se empresas poderiam omitir dos seus relatórios entregues à ANPD informações importantes sobre o tratamento realizado com os dados, mas, que possam se enquadrar sob o manto dos segredos comerciais ou industriais.

Na mesma linha de entendimento, o art. 55-J, ao tratar das competências da ANPD, dispõe que cabe a ela "zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º" da LPGD.

Pode-se pensar que os segredos comerciais ou industriais servem como um escudo, impedindo que o titular e também a fiscalização tivessem, efetivamente, a devida transparência ou conhecimento real sobre o tratamento de dados.

Uma ponderação diferente foi feita no art. 20 da LGPD, que trata do direito de revisão de decisões tomadas unicamente a partir de algum tratamento automatizado de dados pessoais. Isso ocorre, pois, apesar relativizar o princípio da transparência no § 1º, o § 2º dispõe que "em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais".

Aqui, portanto, resta claro que a ANPD poderá intervir e fiscalizar para verificar a conduta do agente. Não obstante, esse dispositivo parece ser insuficiente ao permitir à ANPD apenas realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Ou seja, apenas nestes casos, quando o argumento para a não transparência for o segredo industrial ou comercial e houver suspeita de um tratamento automatizado discriminatório, é que se abre a possibilidade de verificação da ocorrência ou não da lesão ao titular do dado pessoal.

O segredo industrial ou comercial não deveria ser excepcionado e passível de auditoria por parte da ANPD apenas quando diante de decisões automatizadas. Sem a possibilidade de verificação ampla por parte da ANPD dos tratamentos feitos pelos agentes – sejam eles automatizados ou não – e havendo ou não a suspeita de uma discriminação, o argumento de um segredo industrial ou comercial se torna um coringa.

Tal lacuna legislativa tem como pano de fundo a autorregulação do mercado, com o uso de políticas de privacidade como uma resposta a demanda regulatória. Ora, a base legislativa tem fundamento na transparência e no direito à informação.

5.3. Das Políticas de Privacidade e Proteção de Dados

Sendo a transparência e o direito à informação elementos legitimadores do consentimento, as Políticas de Privacidade e Proteção de Dados assumem relevância especial e, com isso, tais documentos passaram a ser base para o tratamento de dados pessoais em plataformas digitais.

Na ótica das Políticas de Privacidades disponibilizadas, o indivíduo é guiado pelos seus interesses diante dos custos e benefícios envolvidos em consentir com o tratamento de dados e seguir na plataforma digital, a partir dos termos que lhe são apresentados. Assim, com o amplo conhecimento acerca de como é o tratamento de dados pessoais, poderá sopesar os custos envolvidos e contrapô-los em face dos benefícios trazidos.

Em consequência, tomará uma decisão, em seu melhor interesse, após ler os termos de privacidade disponibilizados. Partindo dessas premissas, o procedimento se tornou comum foi o de informar o titular dos dados pessoais acerca do tratamento de dados pessoais e, na sequência, permitir com que ele decidir se aceita, ou não, os referidos usos de seus dados pessoais[77]. Com base nas informações disponibilizadas, portanto, pressupõe-se que o indivíduo estaria, de fato, apto a tomar decisões efetivamente autônomas.

Contudo, trata-se de uma ferramenta ineficiente para controle do fluxo de dados pessoais, dada a opacidade e assimetria que marca o tratamento dos dados pessoais,

[77] SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. Harvard Law Review, v. 126, pp. 1880-1903, 2013, fls. 1883

principalmente em plataformas digitais. Em verdade, trata-se de um documento que não capacita efetivamente o titular[78] para exercer o seu direito de controlar suas informações pessoais.

Estudos empíricos têm demonstrado que tais pressupostos nem sempre são adequados, especialmente em face de limitações cognitivas em face da arquitetura tecnológica.

As Políticas de Privacidade funcionam como documento que explicita as práticas e processos adotados por um site, aplicativo ou plataforma em relação à privacidade e segurança de seus usuários, trazendo os termos e condições relacionadas ao tratamento de dados pessoais.

Por óbvio, não se reduz em tratar o titular como incapaz de decidir por si. Porém, o foco excessivo na obtenção de seu consentimento informado deixa de lado a real capacidade do titular dos dados pessoais de compreender e avaliar os riscos e prejuízos que poderão advir de seu consentimento, sobretudo online. De fato, essas limitações cognitivas podem arruinar os pressupostos do "*notice and consent*"[79].

Nota-se, por uma leitura das políticas de privacidade usualmente utilizadas, que tais instrumentos se tratam, por excelência, de um contrato de adesão. Ao titular de dados, resta aderir ou não com a política imposta, exprimindo a pratica da técnica de contratação por adesão. O consentimento então será meramente uma ilusão, uma vez que o indivíduo carece de efetiva autonomia decisória para se proteger dos possíveis perigos e danos à sua personalidade. Nessas situações, a decisão individual de consentir não é livre e autônoma, oriunda da avaliação de todos os ônus e dos bônus envolvidos.

Essas políticas de privacidade não podem ser vistas como um mecanismo ideal para a proteção dos dados pessoais, pois não garantem um controle prévio ao indivíduo de suas informações. Trata-se de uma ação paliativa, que jamais gera o empoderamento do titular de dados. [80]

Além da ausência do poder de barganha, não sendo possível que o usuário dite, de forma completa, as suas preferências em torno da privacidade, muito das vezes serão observados textos longos, complexos, genéricos e obscuros. Dessa forma, além do descumprimento do princípio da finalidade e da informação, não é estabelecida qualquer comunicação adequada com o titular.

---

78 B BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 162

79 SOLOVE, Daniel J..The Myth of the Privacy Paradox, 2020.fls.12

80 BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls.165

Apesar da apresentação de informações pelo agente responsável pelo tratamento de dados, considerando os princípios previstos na LGPD, estudos indicam que, ao tomar decisões sobre sua privacidade e sobre seus dados, os indivíduos deixam de ler regularmente as "Políticas de Privacidade" que lhe são disponibilizadas[81].

Mais do que isso, tendo em vista a complexidade e sofisticação do tratamento de dados na tecnologia, envolvendo vários conceitos técnicos e jurídicos ou quando se considera a extensão dos textos, as informações disponibilizadas costumam ser de difícil compreensão.

Em verdade, o próprio excesso de informações pode ser considerado prejudicial, sobrecarregando a cognição do titular.

Frequentemente, há um debate pelo ativismo entorno da transparência como uma solução questões da metáfora da caixa preta. Em muitos casos, pode ser que a claridade se apresente realmente como a melhor saída. No entanto, a transparência pode simplesmente provocar complexidade que é tão eficaz em derrotar a compreensão quanto à realidade ou o próprio sigilo jurídico. A transparência não é apenas um fim em si mesmo, mas um passo intermediário no caminho para a inteligibilidade, que depende da sociedade.

Nessas situações, o próprio consentimento deixa de corresponder com a vontade real do titular, pois esse sequer há a compreensão dos efeitos que eventual decisão pode causar à sua personalidade, tornando a excessiva na obtenção do consentimento expresso dos titulares inadequada para alcançar o objetivo de conferir efetiva autonomia no âmbito do autogerenciamento informacional.

6. PLATAFORMAS DIGITAIS E O AUTOGERENCIAMENTO PELOS USUÁRIOS

Como foi possível verificar, há um complexo ecossistema tecnológico em que as informações são agregadas, a partir de uma teia de compartilhamento, tornando o fluxo informacional completamente volátil. Nesse cenário, o indivíduo deveria ter consciência a respeito de todos os atores envolvidos e as respectivas práticas de gerenciamento de informações pessoais.

A valer, diante das limitações do entendimento da tecnologia pelo ser humano, é pouco provável que, de fato, esse esteja capacitado para a tomada de decisões acerca de suas informações. Observa-se, por exemplo, a problemática envolta no uso em massa das redes sociais e a disponibilização das mais variadas informações pessoais pela sociedade.

[81] https://www.estudosinstitucionais.com/REI/article/view/521/510

De fato, as empresas utilizam informações pessoais e comportamentais para o alcance de um público-alvo, com a finalidade de definir estratégias comerciais e principalmente de *marketing*. Tais campanhas são direcionadas para uma massa de consumidores com características em comum.

Indo além da segmentação de consumidores pelo público-alvo, atualmente, tem-se utilizado uma definição ainda mais específica. Trata-se da *Persona* (*buyer persona* ou avatar) que pode ser conceituada como uma personagem baseada em dados reais e comportamentais, que representa o cliente ideal de uma marca, produto ou serviço específico.

Isso é, ocorrerá um filtro de interesses comportamentais e dados pessoais envoltos à publicidade, tornando o comercial e *marketing* da empresa cada vez mais direcionado e eficaz.

Destaca-se que, se utilizada a base legal do consentimento, em cada tipo de ação de *marketing* será necessária uma permissão diferente. Desse modo, aconselha-se uma licença para promoções, outra para informativos, entre outros conforme os objetivos.

A recomendação, em verdade, é evitar esse tipo de ação. A sugestão, então, é aplicar ações que visam atrair os clientes de maneira mais transparente e que traz resultados satisfatórios a longo prazo.

Isso é, a ideia não é ir atrás do cliente, mas despertar um interesse para que a pessoa venha até a empresa e se interesse pelo o que essa oferece. Essa atração é feita mediante de conteúdos de qualidade para pessoas certas.

No meio digital, os usuários têm o poder de decidir por onde navegam, o que buscam e o que consomem. A partir dessa liberdade, o modo de atrair novos clientes se dá por meio da produção de conteúdos relevantes e que levam à compra do produto final, por exemplo. Isso é, um *lead* é levado em um processo de nutrição até se tornar um cliente.

A ideia é o uso de um método de abordagem que procura personalizar a comunicação social e, considerando que as redes sociais acumulam um volume elevado dos mais diversos dados pessoais de seus usuários, a sua utilização ganha força para a realização de um *marketing* direcionado, visto a possibilidade de se extrair informações de pessoas ao longo de toda a sua interação com a plataforma.[82]

Tem-se um *marketing* direcionado que visa atrair os clientes e apoiadores de maneira mais transparente e que traz resultados satisfatórios a longo prazo. Isso é, a ideia desse tipo de

[82] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls.18.

comunicação não é ir atrás do cliente, mas despertar um interesse para que a pessoa venha até a instituição e se interesse pelo o que esta oferece.

Essa atração é feita por meio de conteúdos de qualidade para pessoas certas, sendo necessário então o estudo desse público e de seus interesses. Nesse âmbito, ganha força o uso das redes sociais como fonte de dados para esse relacionamento publicitário e de *marketing*, visto que, com o avanço da tecnologia, cada vez mais pessoas usam as redes sociais e, em meio a tais sistemas, disponibilizam conteúdos, interações e sentimentos.

Todavia, a lei é aplicável a todo e qualquer dado pessoal em que seja possível a identificação de uma pessoa natural, o que incluiu o perfil comportamental, nos termos do art. 12, parágrafo 2º da LGPD. Dessa forma, com a simples segmentação de um público-alvo ou com a criação de uma *Persona* estamos lidando com dados pessoais e, por óbvio, tem-se a necessidade de aplicar a LGPD.

Nesse ponto, a LGPD dispõe no art. 7º, parágrafo 4º que fica dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo próprio titular, sem deixar de considerar os direitos e princípios previstos na legislação.

Nesse cenário, apesar de ser desnecessária a utilização da base legal do consentimento, importando na escolha das demais bases legais dispostas na LGPD, para o tratamento de dados pessoais, cujo acesso se torna público pelo titular, não se autoriza o uso indiscriminado dessas informações.

Em verdade, tais dados encontram-se sob o escopo da lei. Assim, é de suma importância cautela na utilização de redes sociais e, ainda, a escolha de uma base legal para tal tipo de tratamento de dados.

Para além disso, tem-se a necessidade de uma análise contextual[83]. A utilização de dados dispostos em redes sociais, manifestamente públicos, deve ser compatível com a finalidade não só da plataforma em si, como, principalmente, da razão pela qual tais dados são públicos.

Na origem, as redes sociais serviam para relacionamentos e integração de círculo social. Por isso, a princípio, terceiros não poderiam usar dados de uma rede social, mesmo que de perfil público, para fins de *marketing*. Contudo, essa finalidade se altera no contexto atual[84].

O *Google* e o *Facebook* (enquanto Grupo - incluindo o *Instagram*) dispõem de Política de Dados que define como são tratados os dados pessoais de seus usuários, de acordo com o

---

[83] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, fls. 257.

[84] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, fls. 257.

que prevê a LGPD e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que devem ser aceitas pelos usuários, utilizando-se, portanto, a base legal do consentimento.

No documento disponibilizado pelo *Facebook*, é estabelecido de forma clara a possibilidade de utilização de dados pessoais (em consonância com as escolhas feitas pelos usuários) para fornecer e viabilizar a operação de seus produtos e para ajudar os anunciantes e outros parceiros a mensurar a eficácia e a distribuição de anúncios e serviços deles, e também para entender os tipos de pessoas que usam tais serviços e como elas interagem com os respectivos sites, aplicativos e serviços[85].

Inclusive, fica expresso no referido documento que, apesar do usuário ter o controle sobre seus dados e ainda haver disposição clara da atuação do *Facebook* enquanto controlador e operador de informações pessoais, as instituições que utilizam das ferramentas do *Facebook* podem continuar usando as Plataformas e soluções do *Facebook* da mesma forma. Todavia, cada instituição será responsável pela conformidade com a LGPD.

Além disso, o *Google*, em sua Política de Privacidade, dispõe que aqueles que usam os produtos de publicidade e avaliação do *Google* precisarão obedecer à Política de consentimento para usuários da União Europeia e receber uma permissão dos usuários para anúncios personalizados e uso de *cookies*/armazenamento local nos sites e apps. Portanto, a utilização dos serviços de publicidade e avaliação do *Google* exige medidas para garantir que as preferências dos usuários sejam respeitadas.

Atualmente, no documento disponibilizado pelo *Facebook*, é estabelecido a possibilidade de utilização de dados pessoais (em consonância com as escolhas feitas pelos usuários) para fornecer e viabilizar a operação de serviços e produtos e para ajudar os anunciantes e outros parceiros a mensurar a eficácia e a distribuição de anúncios e serviços deles, e também para entender os tipos de pessoas que usam tais serviços e como elas interagem com os respectivos sites, aplicativos e serviços.

---

[85] "[...] Os Parceiros que usam nossos serviços de análise
As pessoas contam com nossos Produtos, como contas empresariais, ferramentas profissionais e Páginas do Facebook, para administrar e promover os negócios. As empresas usam nossos serviços de análise para entender melhor como as pessoas estão usando os conteúdos e os recursos delas.Recebemos informações sobre como as pessoas interagem com as publicações, os classificados, as Páginas do Facebook, os vídeos, as Lojas e outros conteúdos das empresas dentro e fora dos nossos Produtos. Em seguida, colocamos essas informações em relatórios agregados. Assim, elas podem ver o desempenho do conteúdo que produzem.Esses relatórios agregam informações como as seguintes: Quantas pessoas interagiram com o conteúdo da empresa. Os dados demográficos e os interesses gerais das pessoas que interagiram com o conteúdo. Os Parceiros que publicam anúncios conosco também recebem outras informações.[...]." Disponível em: https://www.facebook.com/privacy/policy/

Nesse sentido, é plenamente possível a utilização de dados dispostos no *Facebook* e no *Google* quando observada a finalidade expressa nas Políticas de Privacidade das Plataformas, as permissões garantidas pelos usuários, devendo ser observado ainda os parâmetros previstos em lei, o que engloba o regime especial conferido para o tratamento de dados sensíveis.

Assim, mesmo que o titular tenha consentido com Plataforma para exposição de suas manifestações na rede social, isso não implica, em um primeiro momento, que esse cidadão, tenham consentido em ter seus dados analisados e comparado com o de outras pessoas ou ter sua opinião pessoal classificada, ou moldada por meio de uma perfilização.

Uma pesquisa realizada pela *Pew Research Center*[86] concluiu, a partir da realização de entrevistas, que muitos americanos têm pouco ou nenhum entendimento sobre o que as empresas de tecnologia estão fazendo com os dados coletados sobre elas e, mesmo assim, consentem com o tratamento de dados.

Ao mesmo tempo, a maioria informou que se depara com as políticas de privacidade das empresas em algum momento, mas nem todos lêem completamente as referidas políticas e, de fato, entendem sobre o tratamento de dados ali envolvidos.

Foi verificado que 81% dos americanos entendem possuir pouco controle sobre os seus dados coletados pelas grandes empresas. Ocorre que, apesar de 79% manifestarem que se preocupam com o destino de suas informações, ainda assim, poucos apresentaram interesse na leitura das políticas de privacidade que lhe são fornecidas antes de consentirem com o tratamento de dados.

A título de exemplo, apesar de 97% dos americanos afirmarem que usualmente precisam aprovar os termos de uso, apenas 1 a cada 5 informam que sempre (9%) lê as políticas de privacidade antes de consentir, enquanto 36% dos adultos admitiram que, mesmo com os riscos inerentes, nunca leem a política de privacidade disponíveis.

Cerca de dois terços dos entrevistados que, de fato, leem as políticas de privacidade disponibilizadas dizem que normalmente entendem muito (13%) ou parte (55%) das políticas. Mas nem sempre a leitura significa conhecimento. Pela pesquisa[87] realizada, cerca de um terço desse grupo tem uma compreensão menor das políticas de privacidade que leem, incluindo 29% que dizem entender muito pouco e 3% que não entendem nada.

---

[86] Pew Research Center, November 2019, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information

[87] Pew Research Center, November 2019, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information

A valer, entre todos os entrevistados americanos, 8% dizem que entendem bastante as políticas de privacidade, 33% entendem parcialmente, 18% entendem muito pouco e 2% não entendem nada.

Desse modo, é possível entender o instituto como um instrumento ineficaz de controle dos dados pessoais pois, ao consentir, os indivíduos deixam de refletir sobre as consequências decorrentes da coleta de suas informações, o que resulta em uma insegurança jurídica quanto à concretização do direito à proteção dos dados pessoais e da privacidade.

Cumpre salientar que o ser humano tende a priorizar benefícios imediatos, deixando de avaliar, em um primeiro momento, os possíveis danos à privacidade que, por ora, estão distantes, conforme leciona Bruno Bioni[88], a partir da teoria da decisão da utilidade subjetiva.

É sabido que os indivíduos só terão consciência da perda do controle sobre suas informações pessoais após a concretização de dano. Cita-se como exemplo o indivíduo que, ao cadastrar seu cpf em uma loja, recebeu um desconto em sua primeira compra, mas, ao final, teve seus dados pessoais compartilhados com terceiros.

Ou seja, apesar dos prejuízos à privacidade, colocasse na balança um ganho aparentemente significativo, razão pela qual o indivíduo acaba por minimizar qualquer lesão resultante do tratamento dos dados. Com isso, as pessoas deixam de enxergar as consequências que decorrem do uso indevido dos seus dados pessoais.

Dessa forma, após o prejuízo sofrido, o ser humano procura uma "zona de conforto", como entende Bruno Bioni, visando não sofrer pelo incômodo anteriormente suportado. Nesse quesito, tem-se o "paradoxo da privacidade", uma vez que, apesar da preocupação das pessoas com o destino dos seus dados, elas não se esforçam para mudar a realidade de recorrentes violações à privacidade em ambientes digitais.

Nota-se, portanto, a manifesta vulnerabilidade do titular dos dados pessoais, visto que, ao optar por não consentir, ele pode ser banido do serviço ou produto desejado, o que revela uma excessiva assimetria entre as partes, assim como a ausência de transparência na relação contratual.

---

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

Sob esse aspecto, Laura Mendes[89] menciona que o comportamento contraditório do ser humano é compreensível, pois, para o indivíduo, vale mais a pena consentir, do que ser privado do serviço ou produto almejado.

São diversas as pesquisas que comprovam o desinteresse e a dificuldade de compreensão das pessoas quanto ao tratamento de dados pessoais no mundo digital. Destaca-se o estudo "*mental models*"[90], elaborado pelas pesquisadoras Lorrie Cranor e Aleecia McDonald, das Universidades de Stanford e Carnegie Mellon, com o intuito de entender o comportamento dos usuários no ambiente on-line.

Após o levantamento dos critérios adotados na pesquisa de Cranor e McDonald, constatou-se que os usuários não estão preparados para "autodeterminar os seus dados pessoais" em razão da falta de conhecimento específico, conforme aponta Bioni[91] ao mencionar o referido estudo.

No experimento de Lorrie Cranor e Aleecia McDonald, foi possível concluir que os usuários estão dispostos a pagar valores mais elevados por um nível de segurança maior sobre seus dados pessoais, quando há um conhecimento maior acerca das práticas envolvendo o tratamento de dados pessoais.

Foi possível apurar que os usuários são capazes de tomar melhores decisões, quando as informações potencialmente relevantes para sua tomada de decisão são facilmente exibidas, sem que haja qualquer manipulação na experiência de uso do serviço, que seja capaz de conduzir o indivíduo a tomar uma decisão.

Somente 23% afirmaram que não permitem a coleta dos dados pessoais, enquanto 50% o fazem. Além disso, surpreende-se quanto ao número ínfimo de usuários que deletam *Cookies* (17%) em contrapartida aos que não excluem essa ferramenta durante a navegação (60%). Após questionados sobre os motivos envolvidos na exclusão dos *cookies*, restou apurado que os titulares dos dados não possuem informações suficientes para a tomada de decisão válida em relação ao gerenciamento dos seus dados pessoais.

---

[89] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: TENDÊNCIAS CONTEMPORÂNEAS DE MATERIALIZAÇÃO. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020.

[90] MCDONALD, Aleecia M.; CRANOR, Lorrie Faith The Cost of Reading Privacy Policies ∗I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue http://www.is-journal.org/

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

Nesse sentido, presume-se pelo consentimento viciado, o que, sem dúvidas, impacta de forma crucial no exercício do direito à privacidade e proteção de dados, enquanto construção da esfera pessoal do indivíduo.

Ocorre que, apesar do desconhecimento técnico, verificou-se uma séria preocupação dos entrevistados quanto à segurança dos seus dados, uma vez que 70% deles afirmaram que, ao realizar compras on-line, levam em consideração a possibilidade ou não do compartilhamento de dados pessoais com terceiros, sendo que 64% dos entrevistados julgam como invasiva a vigilância constante sobre os seus hábitos on-line.

Apesar disso, a parte final da pesquisa evidenciou o contrassenso existente entre as reais intenções dos usuários e os seus comportamentos manifestados no ambiente digital. Os resultados apontaram que uma parcela pequena se dispôs a pagar a quantia em prol dos seus dados pessoais, à medida que um número significativo trocaria os seus dados pelo desconto ofertado.

Logo, os levantamentos apontam que, apesar de se preocuparem com a violação de sua privacidade, os indivíduos não empregam mecanismos aptos para exercer os seus direitos de forma efetiva, assim como possuem conhecimento insuficiente sobre a coleta dos seus dados pessoais, o que não só contamina o processo de tomada de decisão, mas também evidencia a vulnerabilidade dos titulares na gestão de seus dados pessoais.

O tratamento de dados com o uso da base legal do consentimento pode ser falho, pois os usuários parecem consentir de maneira inconsciente, sequer refletindo sobre a sua escolha. Inexiste um autogerenciamento de dados e, sim, uma simples disponibilização de dados.

O que se observa, então, é um crescente desinteresse dos indivíduos em compreender os seus direitos e os meios pelos quais podem exercê-los, o que opera na contramão da caracterização do consentimento.

Esse cenário se intensifica na realidade imposta pela lógica do "*take it or leave it*". Isso é, concordar com o tratamento dos dados ou ser privado de usufruir ou ter o produto ou serviço.

Dessa forma, tem-se que o uso do consentimento nas plataformas digitais é meramente aparente.

Ora, caso o indivíduo opte pelo exercício do seu direito à privacidade, sem o aceite dos termos e condições impostos, o que poderá ser verificada é a simples exclusão do ambiente digital, o que demonstra, ainda mais, ser duvidosa a proteção supostamente assegurada ao titular dos dados.

A decisão individual de consentir, nesse cenário, jamais pode ser considerada livre e autônoma ou, pelo menos, originada de uma avaliação dos ônus e dos bônus envolvidos.

Pelo contrário, ela se oriunda de uma imposição, qual seja, a de consentir ou simplesmente não desfrutar de serviço/produto disponível, que, como visto nas pesquisas, sob a perspectiva do indivíduo, pode ser considerada emergencial ou essencial para a vida em sociedade ou acesso à informação na era digital.

Sendo assim, surge a necessidade do consentimento granular, que permite o estabelecimento de limites, de forma fragmentada específica, pelo titular, no que se refere ao trânsito dos seus dados pessoais. Só assim, será possível determinar quais dados serão tratados, garantindo de forma mais efetiva um maior controle sobre os seus dados.

Nesse ponto, é importante ainda que não haja qualquer manipulação em sua experiência de uso do serviço que o conduza a tomar uma ou outra decisão. A título de exemplo, destaca-se a questão dos *Cookies*.

Os *cookies* tratam-se de pequenos fragmentos de dados criados por sites visitados e que são salvos no computador do titular, por meio do navegador. Em termos técnicos, são arquivos de internet que armazenam o que um internauta está visitando na rede.

Cookies são usados principalmente para gerenciamento de navegação de sites, para fins de personalização e, ainda, para rastreamento do internauta ao visitar páginas na web.

Os *cookies*, enquanto arquivos de dados, contêm informações capazes de identificar o visitante, seja para personalizar a página de acordo com o perfil do internauta ou para facilitar o transporte de informações. Por se tratar de informações que criam um perfil do usuário, sendo possível identificá-lo a partir de comportamentos, há o tratamento de dados pessoais e, por isso, aplica-se a LGPD.

Na LGPD, a princípio, não há regras claras e expressas sobre a coleta e armazenamento de dados por meio de *Cookies*. Contudo, já se verifica em outros países soluções para preservar a privacidade dos titulares quando esses utilizam a internet. É o caso da lei de proteção de dados pessoais da União Europeia - GDPR (Regulamento Geral de Proteção de Dados da União Europeia).

De todo modo, sendo possível identificar uma pessoa a partir de informações da sua navegação pela internet, o entendimento majoritário é que estar-se-á diante da LGPD. Assim, recomenda-se, de forma geral, a observância das regras dispostas na legislação sobre proteção de dados pessoais na utilização de ferramentas web.

Autoridade Nacional de Proteção de Dados emitiu em 13 de maio de 2022 a recomendação OFÍCIO Nº 6/2022/CGTP/ANPD/PR para adequação da prática de coleta de

cookies do Portal Gov.br direcionados à Secretaria de Governo Digital (SGD/ME), considerando o que dispõe a Lei Geral de Proteção de Dados[92].

O Ofício enviado chama atenção para dois pontos relevantes: o banner de primeiro nível e o banner de segundo nível (Política de *Cookies*) que, pelo que se nota, objetivam trazer maiores esclarecimentos sobre a coleta e uso dos *cookies* para o titular ao navegar pela internet.

No caso, o banner de primeiro nível deve ser disponibilizado um botão de fácil visualização, que permite rejeitar todos os *cookies* não necessários pelo usuário, permitindo que o usuário desative a coleta de *cookies*, utilizando-se um consentimento por padrão (*opt-in*).

Já Política de *Cookies* deve conter a identificação das bases legais, finalidades e necessidades do tratamento de dados pessoais envolvidos e, ainda, fazer previsão da classificação dos *cookies* por categoria, do uso de consentimento específico para a coleta de *cookies*, de acordo com as categorias identificadas e, por fim, a possibilidade de rejeição de *cookies* não necessários.

Seguindo a *Guideline* 05/2020 emitida após pesquisa desenvolvida pelo Grupo de Trabalho do artigo 29 (*Article 29 Data Protection Working Party*), a base legal do consentimento envolve atuação direta do titular, momento em que deve se atentar para quais os dados pessoais que serão coletados, as formas de tratamento, a duração do tratamento e se há ou não o compartilhamento dos dados com parceiros comerciais.

Somente dessa forma e, de forma livre, entende ser possível alcançar o consentimento livre, pondo em xeque, conforme ensina de Bruno Bioni, os *"processos de tomada de decisão antes sufocados pela lógica take-it or leave-it"*[93].

De todo modo, conclui-se: o consentimento pode não ser suficiente para garantir a proteção da privacidade, diante da dificuldade de implementar procedimentos capazes de assegurar o poder decisório do titular dos dados pessoais, o que exigirá, sem dúvidas, a adequação das normativas de proteção de dados no que se refere ao avanço tecnológico.

As estratégias regulatórias que vem sendo verificadas, pelo que se nota, segue em um caminho contrário à consideração quanto à vulnerabilidade do titular dos dados pessoais. Mesmo diante de toda complexidade envolvida, parte do pressuposto que o indivíduo é um sujeito racional, livre e capaz de tomar decisões acerca da proteção de seus dados pessoais, o que emerge o protagonismo do consentimento.

---

[92] Disponível em < https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_pr-3368186-oficio.pdf >. Acessado em 20/04/2023

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

Há uma contradição na referida estratégia regulatória. Mas, diante dessa garantia artificial dos qualificadores da base legal do consentimento, considerando, ainda, a incompatibilidade do desenho normativo de proteção de dados pessoais, deve-se pensar em outras ferramentas com o fim de equilibrar a assimetria do mercado informacional e, ainda, trabalhar na conscientização da sociedade, sendo possível, a partir daí, redesenhar a dinâmica do poder.

É um desafio propiciar ao cidadão um melhor controle sobre as suas informações. Necessário se faz uma maior intervenção, seja do ponto de vista normativo, com a instrumentalização de uma arquitetura de sistema capazes de facilitar o processo de tomada de decisão, seja por meio de políticas públicas que, de fato, conscientize o sujeito, desbancando a sua vulnerabilidade.

7. DO TRATAMENTO DE DADOS EM PLATAFORMAS DIGITAIS

7.1.. Ferramentas equalizadoras

A regulamentação de privacidade deve procurar dar aos titulares de dados um cenário em que se permitirá autogerenciamento inequívoco e consciente, visando fornecer a proteção efetiva à privacidade. Isso é, a regulamentação deve empregar estratégias que se concentra em regular a arquitetura que estrutura a forma como as informações são dispostas para e pelo titular.

Bruno Bioni[94] afirma que para diminuição da assimetria encontrada entre titular de dados e plataforma digital, no âmbito da privacidade, pode estar em ferramentas facilitadoras, capazes de garantir o controle genuíno pelo titular dos dados pessoais, tais como propõe as denominadas *Privacy Enhacing Tecnologies*[95].

As PETs, como o uso da criptografia, por exemplo, apresentam-se como importantes soluções que equalizam as assimetrias do mercado informacional, visto que são capazes de munir os indivíduos com um melhor controle de seus dados.

Atualmente, tem ganhado força metodologias de *Privacy by Design* e *Privacy by Default*, criadas pela canadense Ann Cavoukian[96], comissária de informação e privacidade de

---

[94] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls.190.

[95] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls.167

[96] CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009

Ontário (Canadá). Ela cita que os princípios da *Privacy by Design* podem ser aplicados a todos os tipos de informações pessoais, mas devem ser utilizadas com especial vigor para os dados sensíveis, como informações médicas e dados financeiros. A força da privacidade tende a ser proporcional à sensibilidade dos dados.

O conceito de *Privacy by Design* prevê que qualquer projeto de uma empresa que envolva o processamento de dados pessoais deve ser realizado mantendo a proteção e a privacidade dos dados a cada passo, desde a sua concepção. Isso inclui o desenvolvimento de produtos, desenvolvimento de *software*, sistemas de TI e mais. Na prática, deve-se garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida daquele produto ou sistema, a partir da promoção da segurança e da transparência.

Trata-se, nesse sentido, de uma metodologia de boas práticas, com o intuito de guiar e incorporar a proteção, a segurança e a privacidade de dados pessoais em todo ecossistema. Tal incorporação tem como foco uma postura proativa, em vez de reativa, ou seja, há de se adotar premissas capazes de antecipar e prevenir de incidentes de privacidade antes que eles possam ocorrer e não tentar remediar depois de ocorrido.

A incorporação dos princípios de *Privacy by Design* não se limita à disponibilização de políticas e termos, mas ainda, há a necessidade de implantação das medidas que assegurem a proteção de dados na fase de arquitetura dos sistemas e no próprio design da ferramenta tecnológica.

Esse princípio estabelece que o usuário não deverá sofrer qualquer restrição ou limitação de uso das funcionalidades em determinado sistema ou ferramenta, em razão dele ter optado por níveis mais altos de privacidade ou escolhido não fornecer certas informações pessoais.

Além da preocupação com a forma de coleta e armazenamento dos dados pessoais, também é essencial que as organizações estabeleçam a forma de descarte das informações pessoais. Com isso, haverá em todo o processo a assunção de responsabilidade pelas informações que foram confiadas a determinada organização, desde a sua coleta ou recebimento até o cumprimento da finalidade ou encerramento do fundamento legal estabelecido para determinada operação de tratamento de dados pessoais.

De fato, o usuário deve ser o centro das atenções, com um papel ativo no gerenciamento de seus próprios dados. Assim, um dos princípios do *Privacy by Design* é atender aos interesses e às necessidades individuais dos usuários, possibilitando maior poder de controle e gerenciamento de suas próprias informações.

Para isso, inclusive, há de se observar o princípio da transparência, que visa garantir que todas as partes interessadas possam consultar e verificar se a tecnologia envolvida no tratamento

de dados pessoais está funcionando de acordo com as premissas e objetivos estabelecidos e declarados.

Já o *Privacy by Default* significa que, assim que um produto ou serviço for lançado, as configurações mais seguras de privacidade deverão ser aplicadas por padrão, sem interposição manual. Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto ou serviço devem ser coletados e mantidos apenas quando necessários.

Como o princípio do *Privacy by Design*, o *Privacy by Default* trata-se, por excelência, de uma ferramenta de restrição, isso é, que visa a minimização do tratamento de dados. A ideia é de que a plataforma opere de modo mais restrito possível, dando ao usuário a incumbência de liberar acesso à coleta de mais informações, caso julgue necessário. Mais uma vez, se verifica a presença da autodeterminação informativa.

Ocorre que, atualmente, a maioria das grandes empresas de tecnologia fazem justamente o contrário: coletam o máximo de informações possíveis por padrão, mas permitem que o usuário desative a coleta de dados. Caso *Privacy by Default* fosse de fato aplicado, certamente os aplicativos se limitariam ao necessário e permitiriam que o usuário ativasse a coleta de dados extras, caso pretendido para alguma funcionalidade específica.

Os conceitos estão mencionados de forma expressa no artigo 46, § 2º, da LGPD, assim como no artigo 25 do Regulamento Geral de Proteção de Dados da União Europeia (GDPR). No caso, tal previsão, representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente.

Tem-se mecanismos que podem ser capazes de permitir que proteção de dados seja parte integrante do desenvolvimento tecnológico e também da maneira como um produto ou serviço é criado. Todavia, para o uso adequado de tais mecanismos muitas vezes não será suficiente atualizar os processos herdados com um verniz de privacidade, mas pode ser necessário construir novos processos e sistemas ou redesenhar significativamente os existentes, que deverão ser verificados após processo de auditoria.

Dessa forma, tais mecanismos acabam por depender de uma dimensão normativa mais ampla, implicando na necessária interlocução entre tecnologia e direito, em razão do dinamismo da realidade digital. Há de se canalizar esforços, talvez a partir de uma legislação mais prática, para uso efetivo desses instrumentos, que visem facilitar o exercício do direito à privacidade de um modo geral.

Aposta-se muito na autorregulação pelo próprio mercado. Contudo, ainda que as leis recentemente publicadas indiquem, como visto, posturas mais horizontais e transparentes, ainda assim, a tecnologia parece permanecer em sentido contrário.

De outra banda, importando em uma outra ferramenta, a Lei Geral de Proteção de Dados Pessoais dispõe em seu art. 12 acerca do dado anonimizado como aquele que, originariamente, era relativo a uma pessoa, mas que passa por uma desvinculação da pessoa física. Nesse caso, se um dado é anonimizado, não sendo possível a identificação da pessoa física, então a LGPD não se aplicará a ele.

De fato, a anonimização de dados pode se apresentar como uma saída mais segura e transparente acerca do uso de informações de pessoas, sendo considerados essenciais para o crescimento da inteligência artificial, da internet das coisas, do aprendizado das máquinas, da análise de comportamentos, entre outros.

Aliás, sempre que possível, recomenda-se que uma organização, pública ou privada, realize a anonimização de dados pessoais, pois isso aperfeiçoa a segurança da informação na organização e gera, assim, mais confiança em seus serviços e para seus públicos.

De todo modo, vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos, se reconstrua o caminho de identificação de quem era o titular do dado. Se, de alguma forma, a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD.

Na verdade, o processo de anonimização pleno, ainda que a partir do uso de criptografia, é bastante complexo, uma vez que a reidentificação dos indivíduos pode ser realizada facilmente por meio do cruzamento das informações disponíveis com outras bases de dados.

7.2. Comportamento de usuários e a importância da conscientização

Contudo, mesmo diante de mecanismos previstos na legislação e na doutrina estrangeira recepcionados pela norma nacional, o dilema entre comportamento e proteção dos dados permanece, principalmente por depender do próprio comportamento de usuários ao disponibilizarem informações, gerenciar senhas, acessos em plataformas e dispositivos.

Soma-se a isso o fato de que, diante capitalismo de vigilância presente, não se verifica o interesse crescente no uso de tais processos de criptografia por redes digitais. E nesse aspecto, mais uma vez, a transparência necessária e o esclarecimento do titular quanto ao funcionamento das plataformas, frente ao capitalismo de vigilância, permanecem limitados.

Repita-se, há riscos nem sempre previsíveis e deveres acessórios que, no geral, não estarão previstos de forma expressa e compreensível para os usuários das plataformas e aplicativos.

Desse modo, a ausência de clareza acaba por desmantelar a ideia de autogerenciamento informativo, que pode ser proposital e, consequentemente, lesivo aos interesses coletivos de pessoas que não dispõe de instrumentos básicos para que possam exercer plenamente o controle e a proteção da vida privada e da dignidade da pessoa humana.

A cultura de vigilância normaliza as condutas abusivas dessa nova política econômica, dificultando a conscientização das pessoas quanto aos abusos praticados, principalmente quanto à extração e análise dos seus dados sem consentimento e sem observar a devida transparência, o que acarreta severas violações aos direitos fundamentais.

Nesse sentido, se alcança a conclusão de ser necessário que se busque a promoção da proteção de dados em âmbito cultural e informacional.

Isso é, não se descarta o dever de informação consagrado não só pelo art. 9º da LGPD e, ainda, previsto no Código de Defesa do Consumidor. Também não se permite desconsiderar outras concretizações do dever de cooperação consistente na facilitação da tutela dos direitos das pessoas, como se prevê no Capítulo III da LGPD, mas é de suma importância ir além.

A noção de privacidade das pessoas merece atenção. Acerca da proteção de dados, entende Stefano Rodotà que "*a proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isto a cada momento não é verbosidade, pois toda mudança que afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar.*"[97]

Mesmo com vários episódios envolvendo o uso indevido de dados, como o caso do *Facebook vs Cambridge Analytics*, por exemplo, ainda falta muita conscientização sobre o assunto para que os usuários se atentem mais com o uso de plataformas e aplicativos digitais.

Já se vive em uma sociedade datificada, que a todo momento são coletados dados pessoais, com inferências sobre as diferentes áreas da vida das pessoas. Nesse sentido, utilizar aplicativos e plataformas que estimulam ainda mais a cessão de dados, inclusive imagens, não parece ser uma escolha sensata.

---

[97] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 21.

Verifica-se amplamente no nosso cotidiano, discurso pronto que naturaliza e individualiza os danos gerados pela invasão de privacidade, como o “não tenho nada a esconder” ou “nossos dados já estão na internet mesmo”.

Ocorre que é preciso conscientizar sobre a importância da redução de danos e participação nas discussões públicas para que esse engajamento civil se torne pressão pública que culmine em medidas efetivas acerca do tratamento de dados pessoais LGPD.

Mesmo que haja a observância efetiva do princípio da transparência e, ainda, o uso de ferramentas facilitadoras à privacidade, complexidade tecnológica permanece e, se faz mister, ir além. A tecnologia impõe situações imprevisíveis e, a todo momento e de forma veloz, surgem ferramentas disruptivas e novidades que poderão impedir o conhecimento inequívoco por parte do indivíduo acerca da escolha do tratamento de seus dados ou não.

Seja a partir do uso da própria tecnologia ou não, há de se fazer uma análise dos riscos envolvidos, análise essa de cunho pessoal frente às funcionalidades apresentadas nas plataformas e, dessa forma, o que se apresenta fundamental é, sem dúvidas, o conhecimento do direito à privacidade e a consciência enquanto titular desse direito.

A escola é a instituição onde o aluno aprende as primeiras lições que ficarão marcadas para o resto de sua vida. Deste modo, é importante destacar a importância de se abordar temas juridicamente relevantes, ao passo em que esse cidadão, com o passar do tempo, compreenderá os seus direitos e deveres na sociedade.

Verifica-se a importância de se formar cidadãos conscientes, responsáveis e seguros de seus direitos e deveres, além de abordar uma perspectiva básica a fim de lapidá-lo enquanto sujeito questionador e formador de sua própria esfera social. Esse sujeito busca informações, elabora propostas junto aos órgãos e instituições, propõe soluções, questiona abusos, entre outros. Em suma, é exalta o papel democrático do cidadão.

Para além do dever de informação e do princípio da transparência, a base da privacidade está, justamente na educação básica, pois é dela que decorre os primeiros questionamentos e a consciência do ser.

O indivíduo será lapidado desde a infância e, já na fase adulta, terá todo um repertório básico, porém suficiente para exercer os seus direitos na sociedade e, em especial, ao utilizar plataformas digitais.

Portanto, ensinar os direitos e garantias relacionados à importância da gestão dos dados para construção da personalidade nas escolas pode ser vista como uma solução. Deve-se mudar a perspectiva e adotar um olhar de justiça e de inclusão social. Muitas pessoas não têm acesso

à informação jurídica e acabam deixando de exercer diversos direitos que lhe são inerentes, segundo à Constituição Federal.

Como na Alegoria de Platão[98], o processo de saída da caverna da ilusão do mundo sensível para o mundo inteligível corresponde a todo um processo pedagógico e de aprendizado.

O Mito da Caverna é uma metáfora em que Platão[99] levanta a importância da educação na criação de um novo cidadão, com o qual será possível construir um mundo com melhores escolhas e, é claro, para o ato de sair da caverna, tem-se como fundamental, no contexto da tecnologia, condutas mais transparentes e horizontais pelas plataformas.

E, nesse processo, o primeiro passo é o reconhecimento da natureza incompleta deste mundo de ilusões, ou para um viés atual, na complexidade tecnológica. No contexto das suas limitações iniciais, os prisioneiros têm uma forma de olhar para o mundo e, pelo menos para eles, essa forma de ver a realidade fazia sentido. Mas pouco a pouco, e na medida em que são libertados e levados a ver o mundo fora da caverna, com mais luz, vão percebendo uma nova forma de ver o Mundo. Tornam-se então seres mais conscientes do mundo que os rodeia.

De sorte, o Mito de Platão trata-se de uma boa exemplificação de como podemos nos libertar da condição de escuridão da tecnologia, ou melhor, da Caixa Preta, que aprisiona o usuário e, por meio da transparência e do conhecimento, atingir novas formas de conhecimento. E, nesse caso, a Alegoria da Caverna traz uma teoria do conhecimento e da educação.

A Alegoria da Caverna é uma metáfora da condição humana perante o mundo, no que diz respeito à importância do conhecimento e à educação como forma de superação da ignorância, isso é, a passagem gradativa do senso comum enquanto visão de mundo e explicação da realidade para o conhecimento filosófico, que é racional, sistemático e organizado, que busca as respostas para as grandes questões que afligem a condição humana.

A valer, a LGPD representou um grande avanço por buscar garantir maior equilíbrio dos interesses envolvidos, porque há o temor produzido pela complexidade tecnológica, tão pouco se tem como avaliar os riscos advindos do que se fará com os dados coletados, uma vez que podem ser usados de forma lícita, mas também de forma ilícita.

Todavia, a LGPD inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais.

---

[98] PLATÃO.A República. Tradução de Leonel Vallandro.Rio de Janeiro: Nova Fronteira, 2011.
[99] PLATÃO.A República. Tradução de Leonel Vallandro.Rio de Janeiro: Nova Fronteira, 2011.

Em geral, o titular de dados ao utilizar dispositivos conectados não tem meios de conhecer todas as informações geradas por suas interações com a plataforma, nem de obter a certeza de que seus dados estão em segurança, tendo em vista a complexidade técnica envolvida na referida tecnologia.

Toda essa complexidade tecnológica limita a compreensão dos usuários acerca dos riscos associados ao tratamento de dados pelos dispositivos. Ocorre que, mesmo diante de certa incerteza acerca da complexidade envolvida na tecnóloga, verifica-se a disponibilização crescente de dados pessoais por usuários diante das funcionalidades dispostas nas redes digitais.

Tal cenário resulta no dilema entre comportamento e a efetiva proteção da privacidade e proteção de dados, impasse considerado tema problema do presente trabalho.

A título de exemplo, no final do ano de 2022, o aplicativo de *smartphone* lenas AI[100] se tornou um tópico popular nas mídias sociais em razão da funcionalidade de gerar avatares estilizados de Inteligência Artificial com base em *selfies* que os usuários carregam na plataforma. Apesar de não ser novidade aplicativos que editam *selfies* de pessoas, sem dúvida, a primeira vez que a geração de avatar de difusão latente personalizada atingiu um público de massa.

O Lensa foi lançado em 2018, criado pela Prisma Labs, como um aplicativo de assinatura paga focado na edição de fotos com inteligência artificial. No final de novembro de 2022, o aplicativo cresceu em popularidade graças ao seu novo recurso "*Magic Avatar*", que é um gerador de imagens ultrarrealistas com base em inteligência artificial (IA) a partir de comandos de texto e imagens fornecidos pelos usuários.

As polêmicas sobre o Lensa estão em uma série de fatores – inclusive acerca dos direitos autorais envolvidos – mas, principalmente, na quantidade de informações que o aplicativo acaba coletando sobre os seus usuários e tratando com o uso de inteligência artificial.

O principal ponto de fricção é o armazenamento das fotos tiradas pelos usuários para aplicação do efeito. O Lensa possui uma tecnologia de reconhecimento facial, mas para obter os avatares, é necessário escolher 50 fotos, com várias expressões, para que se replique o Avatar o mais parecido possível com um rosto real.

Sobre o uso das referidas imagens, que envolve o reconhecimento facial, com a captura de dados biométrios, o aplicativo dispõe de uma Política de Privacidade[101], inclusive robusta, quando comparado com a de outros aplicativos do mesmo seguimento.

---

[100] https://apps.apple.com/br/app/lensa-editor-de-fotos/id1436732536

[101] https://lensa-ai.com/privacy

Contudo, a referida política de privacidade só está disponível em inglês e, analisando pelo prisma da Lei Geral de Proteção de Dados, ele não cumpre as normas impostas, afinal, de acordo com o art. 3º da LGPD, a política de privacidade, obrigatoriamente, deve ser divulgada na língua portuguesa, mesmo que o aplicativo seja estrangeiro.

Ainda assim, há brechas de interpretações problemáticas que podem ser impostas ao usuário.

É disposto que as fotos enviadas à plataforma só serão usadas para produção dos avatares e, depois, seriam removidas da nuvem da empresa em até 24h.

Na sequência, ao fazer a leitura da Política e dos Termos de Uso[102] do aplicativo é evidenciada a concessão de uma licença perpétua, revogável, não exclusiva, isenta de *royalties*, mundial, totalmente paga, transferível e sub-licenciável para usar, reproduzir, modificar, adaptar, traduzir, criar trabalhos derivados e transferir conteúdo do usuário, sem qualquer compensação e sempre sujeito ao consentimento explícito adicional para tal uso quando exigido pela lei aplicável.

De forma direta, apesar da suposta proteção das fotos com limite de 24 horas, havia a cessão de todas as ilustrações – realistas – criadas por meio de leitura facial no aplicativo para que a empresa use do jeito que quiser, mantendo armazenadas nos servidores da empresa disponibilizados pela *Google Cloud Platform* (Ireland e USA) e *Amazon Web Services* (USA). Dessa forma, não há a compra de um serviço, mas a doação da propriedade intelectual atrelada a imagem, que é um dado pessoal, para a empresa monetizar sem qualquer compensação.

Ainda que se trate de ilustrações, uma vez ser possível identificar o titular em razão da leitura facial gerada pelo aplicativo, sem dúvidas, para além do direito autoral, tem-se a aplicabilidade da LGPD. De fato, fotos e vídeos, podem envolver dados pessoais (identificação de uma pessoa natural), até sensíveis, sendo o seu tratamento regulado pela LGPD.

Para além disso, o avatar é reflexo da pessoa no mundo virtual, sendo categorizado como extensão da personalidade jurídica de seu titular[103]. Por isso, há a aplicação da LGPD.

Ora, não restam dúvidas de que as relações comerciais e institucionais firmadas no âmbito virtual por meio do avatar, são feitas em nome de seu criador, utilizando-se de dados pessoais, sendo o avatar apenas um meio. É dizer, o avatar é uma forma gráfica que representa o indivíduo nos mundos virtuais, ou seja, uma extensão de seu "eu", sua personalidade e caráter

---

[102] https://lensa-ai.com/terms

[103] PExt na SUSPENSÃO EM INCIDENTE DE RESOLUÇÃO DE DEMANDAS REPETITIVAS Nº 79 – SP.2021/0206612-0. MINISTRO PRESIDENTE DA COMISSÃO GESTORA DE PRECEDENTES.Publicação no DJe/STJ nº 3289 de 14/12/2021

acrescentados pelos próprios desejos representados no ciberespaço ou em uma plataforma virtual.

E não é só isso. A Política de Privacidade dispunha acerca da existência do compartilhamento de dados pessoais, bem como outras informações coletadas (incluindo, entre outros, informações de *cookies*, identificadores de dispositivos e dados de uso) com empresas que legalmente fazem parte do mesmo grupo de empresas das quais a Prisma Labs faz parte.

Detalham que compartilham dados pessoais e outras informações coletadas com organizações terceirizadas, como contratados e prestadores de serviços para apoiar os seus negócios e também podem compartilhar "certos dados pessoais", bem como outras informações coletadas com parceiros de publicidade terceirizados.

Nesse ponto, questiona-se: realmente o consentimento que é dado inicialmente está adequado e pode ser usado como respaldo para o compartilhamento de tantos dados e para tantas empresas não identificadas?

Ao analisar uma nova ferramenta virando *"trend"*, viralizando entre as pessoas sem a preocupação do que ocorre com dados pessoais e fotos, é no mínimo muito preocupante, pois, não há consciência de que os dados fornecidos de forma gratuita ou onerosa e, por vontade própria, se tornaram o produto mais valioso a ser utilizado no universo da engenharia social.

É preciso, cada vez mais, divulgar os conceitos, a aplicação e os motivos pelos quais a Lei Geral de Proteção de Dados faz parte do ordenamento jurídico brasileiro e como ela deve ser utilizada.

É necessário usar os meios de comunicação e as redes sociais para conscientizar a população que dados pessoais não podem ser fornecidos de forma ampla, irrestrita e inadequada.

Essa não foi a única polêmica envolvida no sucesso do Lensa que esbarra em direitos fundamentais da pessoa humana. Há o viés da inteligência artificial, que de acordo com usuários e outros especialistas, estaria afinando os traços de pessoas negras nas imagens produzidas pelo recurso.

A inteligência artificial consiste em um ramo da ciência e da informática que tem como objetivo a criação de máquinas inteligentes, se propondo a desenvolver máquinas que tenham a habilidade de pensar e agir como seres humanos. Embora a tecnologia seja recente, os primeiros estudos surgiram em 1956, quando o termo "Inteligência artificial" foi criado por John McCarthy, professor de matemática do *Dartmouth College.*

A Inteligência Artificial é composta por códigos e dados, sendo que os primeiros são responsáveis pela leitura e pela interpretação dos segundos. Assim, devido à capacidade de

aprender, a IA precisa ser constantemente alimentada por dados para que possa continuar em evolução, assim como uma pessoa.

Hoje, estão no conceito de inteligência artificial, também, sistemas que consigam abstrair, criar, deduzir e até mesmo aprender ideias. Atualmente, o objetivo desse tipo de tecnologia é, simplesmente, de facilitar tarefas do dia a dia do homem, modernizar os processos industriais e obter avanços em pesquisas científicas com a utilização de um "cérebro" artificial mais avançado e eficiente.

As tecnologias de *Big Data* e da Inteligência Artificial (IA) passaram a ser, no contexto da Quarta Revolução Industrial, utilizadas de forma combinada, permitindo a análise por meio de algoritmos de padrões de interesses com base em um banco de dados previamente consolidado pelo programador do código fonte.

Nesse contexto, basicamente, a tecnologia de *Big Data* passa a ser principal fonte para a Inteligência Artificial. Isso, pois a tecnologia de *Big Data* reúne uma imensa quantidade de dados digitais disponíveis na rede que, quando exposta, permite a criação de modelos que analisam e antecipam o comportamento e a dinâmica de sistemas e interações complexas.

Ocorre que, em razão da ausência de autonomia plena da tecnologia, tais padrões têm se revelado enviesados e capazes de produzir uma nova espécie de dano, chamada discriminação algorítmica

Tal como os homens que programaram a IA, os algoritmos não são perfeitos e acabam por reproduzir os preconceitos e vieses do próprio ser humano[104]. Ao estabelecer uma codificação para a execução das tarefas, os computadores podem esquecer ou desconsiderar condições específicas que, em razão de uma análise de dados enraizada, poderá gerar atos de discriminação.

Isso é, embora os principais elementos tecnológicos por trás da ascensão dessa nova economia com a 4ª Revolução Tecnológica sejam fenômenos completamente novos, seu impacto no âmbito empresarial pode ser caracterizado como a continuação lógica e extrapolação de tendências de longa data.

Essa quarta onda de automação, em razão da dependência na análise de bancos de dados já consolidados, exige uma reformulação fundamental dos elementos-chave do aparato tradicional do direito, que considere questões sociais.

---

[104] Disponível em: O Direito do Trabalho dos Flintstones aos Jetsons - JOTA.pdf

Portanto, no mundo de IA que começamos a experimentar, todo o aparato tecnológico apenas reforça uma condição humana. Ser Humano e Tecnologia existem em uma realidade muito semelhante: a do capitalismo que gera empregos e riqueza, mas, ao mesmo tempo, impõe a submissão do homem pela tecnologia.

O uso de IA, como o Lensa, pode ser problemático quando se fornecem à máquina amostras desprovidas de um satisfatório nível de consistência e representatividade, o que faz com que certos grupos sejam erroneamente excluídos, configurando-se uma sub ou uma super-representação.

Como não temos ainda uma legislação que trate especificamente de Inteligência Artificial no Brasil, nada impede que este recurso possa ser usado indevidamente para fins discriminatórios e/ou para criação e associação de perfil de consumo indesejado.

A União Europeia fez frente em questões regulatórias. Para além da proteção de dados (*General Data Protection Regulation*), o próximo alvo se tornou a Inteligência Artificial (IA).

Inclusive, a União Europeia, por meio do Grupo Europeu de Ética em Ciência e Novas Tecnologias (*European Group on Ethics in Science and New Technologies*), já elaborou a Declaração sobre Inteligência Artificial, Robótica e Sistemas Autônomos (*Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*)[105], na qual se propõe um conjunto de princípios básicos e pré-requisitos democráticos, com base nos valores fundamentais, nos tratados da UE e na Carta dos Direitos Fundamentais da União Europeia.

A legislação pátria, que inaugurou o debate de forma expressa a partir do Marco Civil de Internet, parece ter bebido dessa fonte com a publicação da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, em 2018 (LGPD), que regula as atividades de tratamento de dados pessoais, trazendo como um de seus princípios a não discriminação.

A partir do art. 20 da LGPD, que disciplina o direito do titular dos dados pessoais à revisão das decisões tomadas unicamente com base em tratamento automatizado (direito à explicação), pode-se visualizar a proteção dos dados pessoais como o início da regulação do uso da inteligência artificial.

A regra do art. 20 da LGPD revela-se tímida na medida em que restringe o direito à explicação às decisões inteiramente automatizadas. Mas, adotando princípios semelhantes à Declaração sobre Inteligência Artificial, Robótica e Sistemas Autônomos, ainda que

[105] European Commission, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies, Statement on artificial intelligence, robotics and 'autonomous' systems : Brussels, 9 March 2018, Publications Office, 2018, https://data.europa.eu/doi/10.2777/531856

sistematizados de modos distintos, a lei brasileira trilha o mesmo caminho para efetivar a proteção da pessoa humana, diante do crescente uso da IA.

8. CONCLUSÃO

O presente trabalho propôs um debate acerca da esfera de proteção de dados pessoais e da privacidade possível no acesso a redes digitais, considerando o comportamento de usuários e a busca por funcionalidades dispostas na referida estrutura tecnológica.

Assim, a discussão se concentrou na problemática em cima do autogerenciamento pelos próprios titulares do tratamento de dados pessoais em plataformas digitais em face da arquitetura tecnológica envolvida.

A valer, para além da privacidade, a desinformação do usuário ao concordar com o tratamento de dados pessoais impulsiona, ainda, a modulação do comportamento humano, de forma a enfraquecer a autonomia humana, considerando a construção de perfis preditivos que permitem antecipar e dirigir comportamentos.

A sociedade ainda pouco atua frente aos riscos aos processos democráticos, desconsiderando que uso sistemático de dados pessoais dispostos livremente no meio digital, uma vez interações com funcionalidades das plataformas digitais, pode interferir no Estado Democrático de Direito.

Para fins de proteção de dados e responsabilização, é possível dizer que a estratégia regulatória, que consiste na promoção da transparência e da segurança da informação[106], está sujeita, no contexto das plataformas digitais, a diversas limitações, considerando compartilhamento de dados, a racionalidade limitada dos próprios usuários e os altos custos de transação associados à formulação de um consentimento informado, livre, inequívoco e específico.

Se verifica, assim, a existência de um paradoxo[107] quando analisamos problemas de privacidade nas plataformas digitais. Esse paradoxo resulta na análise do descasamento entre os comportamentos dos usuários em ambientes digitais e as suas preferências em relação à sua privacidade que, no geral, são acompanhadas do devido conhecimento acerca da tecnologia envolvida.

106 Artigos 7º e 8º da Lei Geral de Proteção de Dados

107 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar,2ª edição de 2019.

O problema se agrava, ainda mais, quando se tem os dados pessoais categorizados como sensíveis em razão de considerado potencial lesivo[108] no que tange, em especial, ao princípio da discriminação e da liberdade de autodeterminação informativa.

Buscou-se, então, sedimentar que a regulamentação de privacidade não deve procurar dar aos titulares de dados mais autogerenciamento de privacidade, visto que não fornecerá a proteção efetiva à privacidade, mas sim maior amplitude acerca dos riscos envolvidos no tratamento de dados pessoais e transparência acerca da tecnologia. A regulamentação deve propor o emprego de estratégias viáveis, considerando a arquitetura tecnológica que estrutura a forma como as informações são usadas, mantidas, compartilhadas e transferidas em meio digital.

Tendo como pano de fundo os princípios da segurança e da transparência previstos no art. 6º, incisos VI e VII, da LGPD, é possível fazer a avaliação ainda são impostos mecanismos para as plataformas e aplicativos digitais, visando a proteção de dados, verifica-se a necessidade da construção da cultura da privacidade na sociedade civil.

Tem-se como exemplos a serem utilizados as metodologias de *Privacy by Design* e *Privacy by Default,* criadas pela canadense Ann Cavoukian[109], comissária de informação e privacidade de Ontário (Canadá). Ela cita que os princípios da *"Privacy by Design"* podem ser aplicados a todos os tipos de informações pessoais, mas devem ser aplicados com especial vigor para os dados sensíveis, como informações médicas e dados financeiros. A força da privacidade tende a ser proporcional à sensibilidade dos dados.

O conceito de *Privacy by Design* prevê que qualquer projeto de uma empresa que envolva o processamento de dados pessoais deve ser realizado mantendo a proteção e a privacidade dos dados a cada passo, desde a sua concepção. Isso inclui o desenvolvimento de produtos, desenvolvimento de *software*, sistemas de TI e mais. Na prática, deve-se garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida daquele produto ou sistema, a partir da promoção da segurança e da transparência.

Já o *Privacy by Default* implica em configurações mais seguras de privacidade aplicadas por padrão, sem interposição manual. Além disso, impera-se o princípio da necessidade: todos os dados pessoais fornecidos pelo usuário devem ser coletados e mantidos apenas quando necessário para fornecer o produto ou serviço.

---

[108] MULHOLLAND, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista De Direitos E Garantias Fundamentais, 19(3), 159-180. https://doi.org/10.18759/rdgf.v19i3.1603.

[109] CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009

Os conceitos estão mencionados de forma expressa no artigo 46, § 2º, da LGPD, assim como no artigo 25 do Regulamento Geral de Proteção de Dados da União Europeia (GDPR). No caso, tal previsão, representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente.

Ademais, a Lei Geral de Proteção de Dados Pessoais dispõe em seu art. 12 acerca do dado anonimizado como aquele que, originariamente, era relativo a uma pessoa, mas que passa por uma desvinculação da pessoa física. Nesse caso, se um dado é anonimizado, não sendo possível a identificação da pessoa física, então a LGPD não se aplicará a ele.

De fato, os dados anonimizados podem se apresentar como uma saída mais segura e transparente acerca do uso de informações de pessoas, sendo considerados essenciais para o crescimento da inteligência artificial, da internet das coisas, do aprendizado das máquinas, da análise de comportamentos, entre outros.

Aliás, sempre que possível, recomenda-se que uma organização, pública ou privada, realize a anonimização de dados pessoais, pois isso aperfeiçoa a segurança da informação na organização e gera, assim, mais confiança em seus serviços e para seus públicos.

De todo modo, vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos, se reconstrua o caminho de identificação de quem era o titular do dado. Se, de alguma forma, a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD.

Na verdade, o processo de anonimização pleno, ainda que a partir do uso de criptografia, é bastante complexo, uma vez que a reidentificação dos indivíduos pode ser realizada facilmente por meio do cruzamento das informações disponíveis com outras bases de dados.

De todo modo, o dilema entre comportamento e proteção dos dados permanece, principalmente por depender do próprio comportamento de usuários ao disponibilizarem informações, gerenciar senhas, acessos em plataformas e dispositivos.

Não se descarta, desse modo, a necessária conscientização da sociedade, com papel de destaque, no cenário pátrio, da Autoridade Nacional de Proteção de Dados e Procons. É de suma importância que cada indivíduo tenha consciência da importância do exercício do direito individual da privacidade e, ainda, da proteção de seus dados.

O titular de dados ao utilizar plataformas digitais não tem meios de conhecer todas as informações geradas por suas interações com a plataforma, nem de obter a certeza de que seus dados estão em segurança, tendo em vista a complexidade técnica envolvida na referida tecnologia. Toda essa complexidade limita a compreensão dos usuários acerca dos riscos

associados ao tratamento de dados pelas plataformas, o que envolve compartilhamento de dados.

Necessário o impulso pela Autoridade Nacional de Proteção de Dados da adoção de práticas educacionais capazes de impulsionar o indivíduo à realização de ações em relação ao meio digital, no intuito de garantir a privacidade e reduzir a ingerência das plataformas no cotidiano humano. Um exemplo é a alteração das configurações para evitar a coleta de dados dos dispositivos, como o da *Apple* ou a simples desativação de serviços ou opções de segurança nas plataformas digitais, buscando impedir, ainda que parcialmente, a captura de dados.

Como no Mito da Carvena de Platão, é preciso que homem saia da caverna da desinformação[110], para encontrar uma realidade muito mais ampla e complexa acerca do tratamento de dados pessoais evolvidos, para que a tomada de decisão seja mais eficaz, consciente e congruente com as interações pretendidas nas plataformas digitais. Não se contraria aos benefícios do perfilamento, mas necessário que o titular de dados consiga, de fato, controlar o uso de suas informações para tal.

No estágio atual, com legislações ainda recentes e com a jurisprudência ainda em construção, pode ser que homem perceba certo incômodo frente à complexidade tecnológica envolvida. Após a prevalência da cultura da privacidade de dados, o homem conseguirá enxergar e percebe que a realidade criada a partir de suas próprias interações e a totalidade do mundo digital será mais transparente e horizontal.

É essencial a conscientização para a efetiva gestão pelo próprio titular dos riscos envolvidos no tratamento de dados em plataformas digitais, considerando as dificuldades impostas pela tecnologia, inclusive para fins de responsabilização dos agentes de tratamento.

Deve-se buscar meios de se alcançar um denominador comum entre o desenvolvimento tecnológico e as regras de proteção de dados pessoais, o que, na atualidade, concentra-se na necessidade de uma mudança cultural acerca da privacidade, seguindo o caminho educacional e de conscientização a ser impulsionado pelos próprios agentes públicos.

[110] PLATÃO.A República. Tradução de Leonel Vallandro.Rio de Janeiro: Nova Fronteira, 2011.

REFERÊNCIAS

AGOSTINELLI, Joice. **A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE ONLINE**. ETIC 2018 – Encontro de Iniciação Científica, ISSN 21-8498.

BIONI, Bruno**. Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes**. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

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

BUCAR, Daniel; VIOLA, Mario. **Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.

CAVOUKIAN, Ann. **Privacy by Design: The 7 Foundational Principles**. August, 2009

CHAVES, Natália Cristina; COLOMBI, Henry (Orgs.) **Direito e Tecnologia: novos modelos e tendências [recurso eletrônico]** / Natália Cristina Chaves; Henry Colombi (Orgs.) -- Porto Alegre, RS: Editora Fi, 2021

DE LIMA, Cíntia Rosa Pereira; MACIEL; Renata Mota. **Direito e Internet IV: Sistema de Proteção de Dados Pessoais** (De acordo com a Lei n.º 13.709, de 14 de agosto de 2018 e a Lei n.º 13.853 de 08 de julho de 2019, que converteu a lei Medida Provisória n.º 869, de 27 de dezembro de 2018) São Paulo: Editora Quartier Latin, 2019.

DE LUCCA, Newton. **A disciplina Normativa que Faltava**. In: DE LUCCA, Newton; FILHO, Adalberto Simão; DE LIMA, Cíntia Rosa Pereira; MACIEL; Renata Mota Direito e Internet IV: Sistema de Proteção de Dados Pessoais (De acordo com a Lei n.º 13.709, de 14 de agosto de 2018 e a Lei n.º 13.853 de 08 de julho de 2019, que converteu a lei Medida Provisória n.º 869, de 27 de dezembro de 2018) São Paulo: Editora Quartier Latin, 2019.

DENARDIS, Laura, and Mark Raymond. "**The Internet of Things as a Global Policy Frontier."** U.C. Davis Law Review, vol. 51, no. 2, December 2017, p. 475-498. HeinOnline.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2ª edição de 2019.

FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti. **Adaptive learning e educação digital: o uso da tecnologia na construção do saber e na promoção da cidadania**. Revista de Estudos Jurídicos UNESP, Franca, a.23, n.37, p. 487-514, 2019

FEKETE, Elizabeth. **Segredo de empresa**. Enciclopédia Jurídica da PUC-SP, São Paulo, 2018. Disponível em: https://enciclopediajuridica.pucsp.br/ verbete/248/edicao-1/segredo-de-empresa. Acesso em: 10 nov. 2020.

FILHO, Adalberto Simão; SCHWARTZ**. Big em tempos de internet das coisas**. In: Direito, Tecnologia e Inovação. V.1. Coordenação de Leonardo Parentoni. Belo Horizonte: D´Plácido, 2019.

FOITZIK, Piotr. **Publicly available data under the GDPR: Main considerations**. Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/>. Último acesso em 02/09/2020.

FRAZÃO, Ana**. Data-driven economy e seus impactos sobre os direitos de personalidade**. Jota, [s. l.], 17 jul. 2018. Disponível em: https://www. jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/ data-driven-economy-e-seus-impactos-sobre-os-direitos-depersonalidade-18072018. Acesso em: 15 nov. 2020.

FRAZÃO, Ana. **Nova LGPD: as demais hipóteses de tratamento de dados pessoais.** Jota. 19.09.2018. Disponível em [https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018]. Acesso em: 27/08/2021.

FURBINO, Meire; SAMPAIO, José Adércio Leite; MENDIETA, David. CAPITALISMO DE VIGILÂNCIA E A AMEAÇA AOS DIREITOS FUNDAMENTAIS DA PRIVACIDADE E DA LIBERDADE DE EXPRESSÃO. Revista Jurídica Unicuritiba. Curitiba.V.01, n.63, p.89-113, Janeiro-Março. 2021.

HERNANDES, Raphael**. Leitura de 'termos e condições' de serviço na internet exige 4,5 horas**. Folha de São Paulo, São Paulo, 24 dez 2017. Disponível em: https://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-condicoes-deservicos-na-internet-exige-45-horas.shtml#:~:text=Paulo%20no%20Twitter-,Leitura%20de%20'termos%20e%20condi%C3%A7%C3%B5es'%20de%20servi%C3%A7os%20na,internet%20exige%204%2C5%20horas. Acesso em: 19 dez 2022.

HSING, Chen Wen. Coleta de dados pessoais e paradoxo da privacidade: um estudo entre usuário de aplicativos móveis. São Paulo, 2016.

IAB Europe. **A Guide to the Post Third-Party Cookie Era**., 2020.

JURCYS, Paul;DONEWALD, Chris; GLOBOCNIK, Jure; LAMPINEN, Markus. MY DATA, MY TERMS: **A PROPOSAL FOR PERSONAL DATA USE LICENSES**. Harvard Journal of Law & Technology Volume 33, Digest Spring 2020.

KONDER, Carlos Nelson. **O tratamento de dados sensíveis à luz da Lei 13.709/2018**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019

LEONARDI, Marcel. **Fundamentos de Direito Digital.** Revista dos Tribunais, 3ª triagem, 2019.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LÓPEZ, Santiago Ramírez. Informing Consent: Giving Control Back to the Data Subject from a Behavioral Economics Perspective, (2018) JIPITEC 35.

MENDES, Laura Schertel; DONEDA, Danilo. **"Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil"**. Revista de Direito do Consumidor, v. 120, p. 555, 2018.

MULHOLLAND, C. S. (2018**). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados** (Lei 13.709/18). Revista De Direitos E Garantias Fundamentais, 19(3), 159-180. https://doi.org/10.18759/rdgf.v19i3.1603.

OECD. *Guidelines* on the Protection of Privacy and Transborder Flows of Personal Data, 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OLIVEIRA, Nairobi Spiecker; GOMES, Moises Alexandre; LOPES, Ronaldo; Nobre, Jéferson C. **Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). Curso Superior de Tecnologia em Segurança da Informação**. Universidade do Vale do Rio dos Sinos (UNISINOS): São Leopoldo/RS, 2018.

PARENTONI, Leonardo.**Proteção de Dados Pessoais no Brasil**. In: DE LUCCA, Newton; FILHO, Adalberto Simão; DE LIMA, Cíntia Rosa Pereira; MACIEL; Renata Mota Direito e Internet IV: Sistema de Proteção de Dados Pessoais (De acordo com a Lei n.º 13.709, de 14 de agosto de 2018 e a Lei n.º 13.853 de 08 de julho de 2019, que converteu a lei Medida Provisória n.º 869, de 27 de dezembro de 2018) São Paulo: Editora Quartier Latin, 2019.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Harvard University Press: Cambridge, Massachusetts London, England, 2015

PFEIFFER, Roberto. **A Saga da ANPD**. In: DE LUCCA, Newton; FILHO, Adalberto Simão; RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. A Proteção de Dados Pessoais na Internet no Brasil: Análise de decisões proferidas pelo Supremo tribunal Federal. In: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936 Acesso em 30 de junho de 2022.

REQUIÃO, Maurício. **A natureza jurídica do consentimento para o tratamento de dados pessoais**. In: Proteção de dados pessoais: novas perspectivas. Salvador: EDUFBA, 2022.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODOTÁ, Stefano. **Tecnologie e diritti**. Bologna: 1l Mulino, 1995

ROVER, Aires José (org). **DADOS E INFORMAÇÕES NA INTERNET: É LEGÍTIMO O USO DE ROBÔS PARA FORMAÇÃO DE BASE DE DADOS DE CLIENTES?** Direito e Informática. SP: Manole, 2003, p. 27-40.

SANTOS, Lino **CYBERSPACE REGULATION: CESURISTS AND TRADITIONALISTS.** JANUS.NET, e-journal of International Relations, vol. 6, núm. 1, mayo-octubre, 2015, pp. 86-99

SCHAWAB, K. A. **Quarta Revolução Industrial.** São Paulo: Edipro, 2017, p. 11.

SOLOVE, Daniel J. **The Myth of the Privacy Paradox**. 2020.

SOLOVE, Daniel J**..Understanding Privacy. Harvard University Press**. Cambridge Massachusettes, 2008.

SOLOVE, Daniel J**. Privacy Self-Management and the Consent Dilemma**. Harvard Law Review, v. 126, pp. 1880-1903, 2013.

TAMÒ-LARRIEUX, A. (2018). **Privacy Protection in an Internet of Things Environment. In: Designing for Privacy and its Legal Framework. Law, Governance and Technology Series.** vol 40. Springer, Cham. https://doi.org/10.1007/978-3-319-98624-1_4

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>. Último acesso em 27/08/2022.

TRACHTMAN, Joel P. **Cybersecurity versus Trade in Internet of Things Products.** Manchester Journal of International Economic Law, vol. 16, no. 3, December 2019, p. 301-340. HeinOnline.

VELIZ, Carissa. **Privacdade é o poder: por que e como você deveria retomar o controle de seus dados**. Tradução Samuel Oliveira – 1 ed. São Paulo: Editora Contracorrente, 2021.

VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR)**. A Practical Guide. Springer, 2017.

WACHTER, Sandra. **Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR**. Computer Law & Security Review, 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

WESTIN,Alan F.**Privacy And Freedom**, 25 Wash. & Lee L. Rev. 166 (1968).

COSTA JÚNIOR, Paulo José da. **O direito de estar só: tutela penal da intimidade.** São Paulo: Revista dos Tribunais.Acesso em: 21 abr. 2023. 2007

LOPES, José Reinaldo de Lima. **O direito na história: lições introdutórias**. 4 ed. São Paulo: Atlas, 2012

ZUBOFF, Shoshana. **A era do capitalismo de vigilância. A luta por um futuro humano na nova fronteira do poder.** Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

ZUBOFF, Shoshana. **Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação**. In: BRUNO, Fernanda et al. Tecnopolíticas da Vigilância: perspectivas da margem. São Paulo: Boitempo, 2018.