UNIVERSIDADE FEDERAL DE JUIZ DE FORA

FACULDADE DE DIREITO

JARDEL FELISBERTO HENRIQUES JÚNIOR

MECANISMOS DE PROTEÇÃO DE DADOS NO AMBIENTE VIRTUAL: uma análise crítica do direito nrasileiro em comparação com o direito estrangeiro

Juiz de Fora

2021

JARDEL FELISBERTO HENRIQUES JÚNIOR

MECANISMOS DE PROTEÇÃO DE DADOS NO AMBIENTE VIRTUAL: uma análise crítica do direito nrasileiro em comparação com o direito estrangeiro

Monografia apresentada à Faculdade de Direito da Universidade Federal de Juiz de Fora, como pré-requisito parcial a obtenção do grau de Bacharel em Direito sob orientação do Professor Flávio Henrique Silva Ferreira.

Juiz de Fora

2021

JARDEL FELISBERTO HENRIQUES JÚNIOR

MECANISMOS DE PROTEÇÃO DE DADOS NO AMBIENTE VIRTUAL: uma análise crítica do direito nrasileiro em comparação com o direito estrangeiro

Monografia apresentada à faculdade de Direito da Universidade Federal de Juiz de Fora como pré-requisito parcial a obtenção do grau de Bacharel em Direito, na área de concentração de Direito Privado, submetida à Banca Examinadora composta pelos membros:

Aprovado em: Juiz de Fora, oito de setembro de 2021

BANCA EXAMINADORA

_____

Prof. Dr. Flávio Henrique Silva Ferreira
Universidade Federal de Juiz de Fora

_____

Prof. Dr. Marcus Eduardo de Carvalho Dantas
Universidade Federal de Juiz de Fora

_____

Prof. Dr. Sergio Avila Negri
Universidade Federal de Juiz de Fora

RESUMO

O seguinte trabalho foi feito a partir de um estudo do Regulamento Geral de Proteção de Dados, acerca dos mecanismos para proteção de indivíduo um cada vez mais conectado, para melhor entender em quais aspectos a nossa legislação foi inovadora e em quais pontos ela se demonstrou insuficiente. Promulgada em 2018, a Lei Geral de Proteção de Dados entrou em vigor em 2020, consagrando o entendimento já pacificado pelo STF de que a proteção dos dados pessoais é um direito fundamental, ainda que subsidiário ao direito à privacidade e intimidade. A partir da evolução do conceito de privacidade, utilizando-se como referência os pensamentos de Stefano Rodotà e Eduardo Magrani, buscou-se fazer uma análise crítica da legislação brasileira e de como a norma tutela os direitos fundamentais à privacidade e à autodeterminação informativa.

Palavras-chave: 1. Proteção de Dados 2. LGDP 3. RGDP

ABSTRACT

This article was written by a case study of the General Data Protection Regulation with the purpose of evaluating the current Brazilian legislation. To reach this goal, this article will point out the major differences between the GDPR and the LGPD, using mainly as a reference the works of Stefano Rodotà and Eduardo Magrani. Approved in 2018, the LGPD recognizes the informational self-determination as a human right, albeit in its relation to other privacy rights. The purpose of this article is to demonstrate how online relations can be harmful to these rights, and how to proper protect persons from it.

Keywords: 1. Data protection 2. LGDP 3. RGDP

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica parece ser uma fonte inesgotável de ideias para a produção fictícia. Sejam nos livros, nos filmes, ou no exercício mental de cada um, imaginar o futuro é também imaginar os rumos pelos quais tomarão a ciência, capaz de tornar o que uma vez fora inimaginável em uma realidade. A evolução exponencial, de simples bytes, que eram processados em poucos Quilohertz, armazenados em disquetes de pouca capacidade, para processamento em Giga-hertz. De salvar informações em *hard disk*s, para a possibilidade de salvar informações em nuvem. Com o progresso do Hardware e do software, aliado à internet, surge uma nova realidade, um novo mundo de possibilidades, que vão desde as áreas de entretenimento e lazer até a área profissional, desde *youtubers* à influenciadores digitais. Muitas empresas passam a operar majoritariamente no ambiente virtual, como é o caso dos bancos digitais.

Nesse cenário de interconectividade, informações são transmitidas com extrema facilidade e conveniência. No entanto, esta mesma ferramenta, que nos é tão útil, permitindo o compartilhamento de fotos, ideias e pensamentos com um número indeterminável de pessoas, nos torna tão vulneráveis ao assédio e à exposição injusta. Alguns dos danos causados, infelizmente, são de difícil previsibilidade justamente por decorrerem de desdobramentos de novas tecnologias cujos benefícios trazem consigo diversos potenciais lesivos, alguns ainda não identificados. De televisões smart a escovas de dente com internet, a possibilidade para a coleta de dados pessoais se amplia, assim como a possibilidade de dano à intimidade.

Nessa conjuntura, torna-se necessário averiguar a proteção da privacidade. Prevista na Constituição Federal como direito fundamental, a devida tutela da privacidade perpassa na capacidade do agente em ter controle sobre seus próprios dados pessoais. Tal entendimento, o da autodeterminação informativa, é compreendido como o direito do titular dos dados em controlar suas informações e de determinar a maneira pela qual será construída sua esfera particular (RODOTÀ, 2008). A primeira seção do trabalho tem como objetivo analisar a importância da autodeterminação informativa para devida tutela da privacidade, a partir da evolução histórica do conceito de privacidade.

Num segundo momento, tem-se como objetivo delinear os entornos da sociedade da informação, que tem como a base de dados como novo capital (ZUBOFF, 2019). A partir da análise feita com relação a autodeterminação informativa, pretende-se averiguar o uso da tecnologia na sociedade atual e os impactos desta na proteção à privacidade.

Por fim, serão abordados a legislação acerca do tema, notadamente o Regulamento Geral de Proteção de Dados (RGPD), aprovado em 2016 e implementado em 25 de maio de 2018, e a Lei Geral de Proteção de dados, aprovada em 2018. O GDPR é uma atualização da legislação de 1995 que estava vigente na União Europeia, portanto, não foi uma legislação inteiramente nova, ficando bem completa e servindo de parâmetro para outros países.

Citando a legislação brasileira podemos identificar traços do regulamento europeu, como por exemplo no detalhamento sobre a transferência internacional de dados, nas definições utilizadas pelo legislador, na especificação dos dados sensíveis, na premissa sobre a necessidade de autorização dos proprietários dos dados para que sejam usados, na clareza e objetividade na comunicação e possibilidade de portabilidade e exportação dos dados, dentre outros. Tal estudo será de suma importância para a análise crítica da legislação brasileira, permitindo-se concluir quanto à eficácia das normas na proteção do direito fundamental a privacidade e autodeterminação informativa.

2 A PRIVACIDADE E OS DIREITOS DE PERSONALIDADE

As fronteiras do que é propriamente público e do que é propriamente privado, longe de terem limites atemporais, variam conforme a sociedade, assim como o conceito de privacidade. Por parte da história da humanidade, o ato de estar só e de esconder intenções e pensamentos era malvisto, principalmente em sociedades marcadas pela primazia da coesão social. A própria etimologia da palavra privacidade, derivada do latim, significava privados de exercer cargos públicos; em outras palavras, privados de uma completa e apropriada sociabilidade. Noutras sociedades, faltavam-se condições sociais para efetiva concretização da privacidade (SPACKS, 2003).

Exemplo disso pode ser observado na Inglaterra do século XVIII. A privacidade era um privilégio, ainda que limitado, da esfera do senhor, único a possuir aposentos, enquanto os serviçais, por falta de espaço físico, dividiam seus quartos com desconhecidos ou colegas de profissão (HOWARD et al., 1732). À época, a maior parte dos adultos convivia com um desconhecido ou mais, sendo tal coabitação uma necessidade social. A título exemplificativo, o bairro de Bethnal Green, em Londres, contava com uma população de 15 mil habitantes, tendo-se, portanto, mais de oito pessoas por casa, a maioria serviçais que transitavam regularmente entre moradias, não havendo estabilidade nem poder de escolha para decidirem com quais pessoas conviveriam. Soma-se ao cenário a questão estrutural: a ausência de fechaduras, a falta de camas para todos os habitantes, as paredes cuja construção não providenciava nenhum isolamento sonoro, dentre outros aspectos da Inglaterra de 1732 que, juntos, faziam da privacidade uma exceção (BAKER, 1998).

O problema da falta de moradia persiste na modernidade, estimando-se que cerca de um bilhão e meio de pessoas não tenham condições de moradias adequadas (ONU, 2020). Tendo em vista que a moradia, espaço da vida intima por excelência, ainda não é um direito assegurado a todos, conclui-se que a garantia ao direito à privacidade também é precária.

Não obstante, a moradia inviolável é apenas uma das condições para proteção da privacidade, considerando que o advento da sociedade da informação trouxe consigo novas problemáticas para a proteção desse direito. Antes de abordar propriamente o objeto do presente trabalho, a proteção de dados, entende-se necessário retomar a dinâmica histórica propulsora da criação do direito à privacidade.

A efetivação da privacidade, enquanto direito, ocorre no século XX, período

em que diferentes países reconhecem a importância da tutela jurídica à privacidade. A Organização das Nações Unidas (1948), em seu artigo 12, reconhece o direito à privacidade nos seguintes termos: "Ninguém se sujeitará a arbitrária interferência em sua privacidade, sua família, sua casa, suas correspondências, nem sofrerá ataques a sua honra e a sua reputação". Todos devem estar legalmente protegidos contra tais ataques ou interferências à sua privacidade[1].

Nos Estados Unidos, o primeiro caso a reconhecer a existência desse direito foi o de Griswold v Connecticut (ESTADOS UNIDOS, 1965), Tinha como pauta a proibição feita pelo estado de Connecticut, vedando o uso de qualquer droga, serviço médico ou outro instrumento cuja finalidade fosse anticonceptiva, sendo que, Griswold, médico, foi multado por ofertar serviços anticonceptivos. Quando o caso foi analisado pela Suprema Corte americana, entendeu-se que a norma era inconstitucional pois violava a quarta emenda da Constituição Americana, entendendo-se, a partir de então, a privacidade como garantia constitucional.

Tal entendimento é reforçado por outros escritos da época. Reconhecido o direito à privacidade, passou-se abranger a proteção aos escritos pessoais que, embora não gozem de proteção literária, são considerados como parte da intimidade de alguém e, por essa razão, dignos de tutela jurídica. Passou a ser vedado tirar fotos de pessoas que, embora estejam em espaços públicos, não consentiram em ter suas fotos tiradas. Consolidou-se, dessa maneira, o "direito de ser deixado só" [2] (WESTIN, 1967).

Já no Brasil, o direito à privacidade foi mencionado explicitamente pela primeira vez com o advento do Marco Civil da internet, Lei 12.965, de 23 de abril de 2014. No entanto, ele já era um direito efetivado, ainda que indiretamente, como podemos ver na Constituição Política do Império do Brasil, elaborada por um Conselho de Estado e outorgada pelo Imperador D. Pedro I, em 25.03.1824:

> Art. 179. A inviolabilidade dos Direitos Civis, e Políticos dos Cidadãos Brazileiros, que tem por base a lide, a segurança individual, e a propriedade, é garantida pela Constituição do Imperio, pela maneira seguinte. […] VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar. […] XXVII. O Segredo das Cartas é inviolavel. A Administração do Correio fica rigorosamente responsavel por qualquer infracção deste Artigo.

Embora haja diversas acepções de privacidade, em seu cerne, trata-se de um di-

---

[1] No original: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Tradução livre.

[2] No original: "right to be left alone". Tradução livre.

reito *erga omnis*, ou seja, oponível a qualquer um que o viole, em prol de resguardar a intimidade da pessoa. Noutras palavras, é a proteção do espaço íntimo, a residência, bem como os escritos pessoais, correspondências, cujas informações são destinadas às pessoas específicas, devendo ser resguardados para a devida tutela da intimidade. A Constituição Federal Brasileira de 1988 prevê:

> Art. 5. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes. [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação;

Trata-se, portanto, de uma garantia constitucional que protege a intimidade e garante a prerrogativa indenizatória daquele que foi lesado. O Código Civil de 2002, na mesma esteira:

> Art. 11. Com exceção dos casos previstos em lei, os direitos de personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária. [...] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Por essa normativa, o direito à privacidade, além de um direito fundamental previsto na Constituição Federal, configura-se como um dos Direitos de Personalidade e, por essa razão, tem tutela jurídica como tal. Notadamente, sua proteção *erga omnis*, sua irrenunciabilidade, sua indisponibilidade, sua intransmissibilidade, dentre outras.

Dentre as características supracitadas, deve-se atenção especial à indisponibilidade e à irrenunciabilidade. Não há consenso doutrinário de como deverão ser tratadas a indisponibilidade e a irrenunciabilidade dos direitos de personalidade, sendo consenso pela doutrina majoritária que tais características não seriam absolutas. Autores como Gonçalves (2012), entendem que tal limitação é feita a partir de um núcleo fundamental dos direitos de personalidade, sendo esse núcleo irrenunciável. Outros autores, como Silva (2014), entendem que a irrenunciabilidade não poderá ser a partir de critérios objetivos pré-concebidos de terceiros. Ao dissertar sobre o direito de personalidade sobre o próprio corpo, diz:

> A proteção aos chamados direitos de personalidade corresponde à proteção da chamada *identidade pessoal* em suas mais diversas manifestações, seja a liberdade religiosa e/ou sexual, seja o reconhecimento de um direito subjetivo sobre o próprio corpo, uma das formas de concretização espaço-temporal dessa identidade que não se pode pré-determinar, constitui-se de maneira autônoma e se caracteriza pela mutabilidade.

Por esse prisma, o da pessoa enquanto agente autônomo, com uma identidade pautada pela intersubjetividade e individualidade, sendo um processo dinâmico, aderir a uma percepção estática acerca dos direitos de personalidade, articulando a proteção à pessoa a partir de paradigmas teórico-dogmáticos típicos de relações patrimoniais seria incoerente com a própria ideia dos direitos de personalidade (SILVA, 2014). Deve-se, portanto, buscar por uma abordagem adequada frente à temática dos direitos de personalidade. Nesse sentido, afirma Agamben (2000):

> O paradoxo da soberania consiste no fato de que o soberano está, ao mesmo tempo, dentro e fora da ordem jurídica. Se o soberano o é por uma norma que reconhece a prerrogativa de se autoproclamar um estado de exceção e, portanto, capaz de suspender a própria validade da norma, então o soberano está fora do ordenamento jurídico e, de qualquer forma, pertencente a esse, já que cabe ao mesmo decidir se a constituição da norma deverá ser suspendida, faculdade que lhe é reconhecida pela própria norma[3].

Tal compreensão acerca dos direitos de personalidade se faz necessária, pois traz a tão necessária subjetividade para o debate, viés adequado para a efetiva tutela dos direitos de personalidade. Afinal, uma total indisponibilidade quanto aos direitos de personalidade seria sinônimo de uma subjugação da pessoa perante o Estado, incapaz de exercer sua autonomia. Uma noção de indisponibilidade a partir de critérios objetivos que não originem da própria pessoa a faz refém da sociedade e dos bons costumes. A pessoa, para ter sua tutela de direitos de personalidade resguardada, deverá ter suas noções de vida boa ou ideais considerados, os chamados *hiperbens*, entendidos como a avaliação individual acerca do que é melhor ou pior para si, fundamental na criação da identidade pessoal (TAYLOR, 1997).

Quanto a como lidar com os limites do exercício dos direitos de personalidade, no caso do direito ao corpo, Silva (2014) propõe os seguintes critérios.

> Sob o prisma dessa concepção, os atos de disposição acerca do próprio corpo devem ser analisados quanto ao seu enquadramento na norma em três hipóteses distintas, quais sejam: i) o ato de disposição não transcende os limites de exercício do poder soberano da pessoa; ii) o ato de disposição transcende os limites de exercício do poder soberano da pessoa e invade a esfera de soberania pessoal de outra; iii) o ato de disposição transcende os limites de exercício do poder soberano da pessoa, inserindo-se, ainda que mediante autorização, na esfera de soberania de outro e produz consequências relevantes na esfera pública relacional.

---

[3] No original: “The paradox of sovereignty consists in the fact the sovereign is, at the same time, outside and inside the juridical order. If the sovereign is truly the one to whom the juridical order grants the power of proclaiming a state of exception and, therefore, of suspending the order's own validity, then "the sovereign stands outside the juridical order and, nevertheless, belongs to it, since it is up to him to decide if the constitution is to be suspended in toto" (Schmitt, Politische Theologie, p. 13).” Tradução livre.

Utilizando desses mesmos parâmetros aplicados ao direito à privacidade, entende-se a pessoa como soberana para publicar informações sobre si ou para ter a sua privacidade resguardada, conforme sua autonomia, desde que a exposição atinja somente a privacidade do agente que se expõe ou outorga sua exposição. No caso da ação cuja consequência alcance a privacidade de mais de um agente, deve-se ter o consentimento de todas as partes envolvidas.

Observando-se como aplicar tal acepção na prática, utiliza-se como exemplo o caso da atriz Maitê Proença. Após a atriz ter tirado fotos com o seu consentimento para uma revista especifica, foi surpreendida com as fotos expostas em jornais. Indignada por ter suas fotos usadas num contexto adverso do que permitiu, buscou tutela jurídica.

> Recurso Especial. Direito Processual Civil e Direito Civil. Publicação não autorizada de foto integrante de ensaio fotográfico contratado com revista especializada. Dano moral. Configuração. - É possível a concretização do dano moral independentemente da conotação média de moral, posto que a honra subjetiva tem termômetro próprio inerente a cada indivíduo. É o decoro, é o sentimento de autoestima, de avaliação própria que possuem valoração individual, não se podendo negar esta dor de acordo com sentimentos alheios. - Tem o condão de violar o decoro, a exibição de imagem nua em publicação diversa daquela com quem se contratou, acarretando alcance também diverso, quando a vontade da pessoa que teve sua imagem exposta era a de exibí-la em ensaio fotográfico publicado em revista especializada, destinada a público seleto. - A publicação desautorizada de imagem exclusivamente destinada a certa revista, em veículo diverso do pretendido, atinge a honorabilidade da pessoa exposta, na medida em que experimenta o vexame de descumprir contrato em que se obrigou à exclusividade das fotos. - A publicação de imagem sem a exclusividade necessária ou em produto jornalístico que não é próprio para o contexto, acarreta a depreciação da imagem e, em razão de tal depreciação, a proprietária da imagem experimenta dor e sofrimento. (STJ - REsp: 270730 RJ 2000/0078399-4, Relator: Ministro CARLOS ALBERTO MENEZES DIREITO, Data de Julgamento: 19/12/2000, T3 - TERCEIRA TURMA, Data de Publicação: DJ 07.05.2001 p. 139LEXSTJ vol. 144 p. 191RDTJRJ vol. 53 p. 55)

Percebe-se que, mesmo as fotos tendo sido tiradas com o consentimento da atriz, elas foram tiradas para um proposito específico. Não ocorreria, somente pela outorga da atriz em ter suas fotos tiradas, uma renúncia ao direito à privacidade.

Sem entrar no mérito do debate da privacidade de figuras públicas, percebe-se, pelo que até então foi exposto, a necessidade de entender a privacidade não somente numa dimensão negativa, de estar só sem interferência do Estado ou de terceiros, mas também numa dimensão positiva como prerrogativa do agente de ter autodeterminação informativa; de ter o controle sobre suas próprias informações e de construir a sua própria esfera particular (RODOTÀ. 2008). Por essa conceituação aqui exposta, resguarda-se a autonomia, colocando-a no eixo central da proteção a privacidade, protegendo a pessoa *per si* e garantindo a soberania dela em atuar com consonância com sua identidade pessoal.

3 O AMBIENTE VIRTUAL E OS DADOS PESSOAIS

Atrelado ao direito à privacidade está o direito à proteção de dados pessoais. Entende-se como dados pessoais como qualquer informação que permita identificar uma pessoa específica, seja essa informação suficiente, como é o caso do CPF e endereço de residência ou que, com informações adicionais, permita-se identificar a pessoa. A informação só deixara de ser pessoal caso seja possível desvincular a informação do indivíduo, de forma irreversível (UNIÃO EUROPEIA, 2016).

Como já exposto anteriormente, as primeiras acepções ao direito de privacidade estavam limitadas a não interferência, seja por parte do Estado, seja por agentes privados, na vida intima do individuo No entanto, tal acepção não é suficiente numa sociedade da informação, tópico que será dissertado nesta seção.

Com o surgimento da internet e do ambiente virtual, notava-se uma dissociação entre o real e o virtual, no qual se haveria uma "realidade virtual", alheia a um suposto mundo real que existe fora da realidade sintética, como entidades apartadas. Atualmente, se entende a extensa maneira como ambos ambientes, o virtual e o não virtual, se dialogam, razão pela qual é preferível descrever o meio virtual como ambiente virtual, sem criar uma associação errada entre virtual e irreal (BLASCOVICH, 2002). A definição de virtual, nas últimas décadas, também se amplia para incluir o tudo aquilo cuja existência dependa de *software* computacional, como é o caso da sala de aula e bibliotecas virtuais (OXFORD, 2021) O meio virtual, portanto, também inclui o ambiente onde são armazenados dados.

Tal evolução conceitual ocorre, em parte, pois as fronteiras do virtual se ampliam a cada dia. Tal constatação pode ser demonstrada com o advento da Internet das Coisas, tendo como definição a maneira como "computadores. sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de *hiperconectividade*" (MAGRINI, 2018. P. 20). Na atualidade, além da comunicação de dados entre pessoas por intermédio de um aparelho eletrônico, existem diversos equipamentos que comunicam entre si pela internet, enviando e receber dados automaticamente.

O *smartwatch*, por exemplo, é capaz de executar diversos aplicativos, com funcionalidades como acompanhamento de batimento cardíaco, de atividades físicas e de monitoramento de sono. Através da internet, o relógio envia dados pessoais automaticamente, sendo essencial para as funcionalidades do relógio. Em contrapartida, a empresa detentora desses dados pessoais, na ausência de qualquer legislação que a proíba, poderia vender os da-

dos pessoais para empresas que ofertem planos de saúde, para empresas que ofertam produtos esportivos ou qualquer outra empresa que tenha interesse em obter dados pessoais. Além do *smartwatch*, temos como exemplos de objetos inteligentes o *smartphone*, a *smart* TV, aparelhos eletrodomésticos como geladeira, máquina de lavar, dentre outros.

Logo, a própria residência, considerada o lugar privativo por excelência, pode ser considerada inteligente, tendo fechaduras, lâmpadas, tomadas e interruptores comandados remotamente através do envio de dados. Assim como os *smartwatch,* para funcionar adequadamente, esses equipamentos coletam dados do usuário. O termostato *Nest,* exemplo dado por Zuboff (2019), aprende a se autoprogramar baseado na atividade dentro de casa, nas condições meteorológicas atuais e outros fatores, ajustando o aquecimento e resfriamento baseado nos hábitos de seus moradores:

> O termostato, conectado a internet, obtém e entrega as informações ao servidor da Google. Cada termostato vem com uma política de privacidade, um termo de prestação de serviço e um termo de uso. Esses revelam práticas opressivas em relação à privacidade e a segurança das informações sensíveis que são compartilhadas com outros aparelhos *smart,* com funcionários e com outras empresas para análises preditivas de vendas para outras empresas que não foram especificadas. Há pouca responsabilidade da empresa em si quanto à informação coletada e nenhuma quanto ao uso que outras empresas farão desses dados. [4]

Nesse sentido, a sociedade da informação é, conforme Wertheim (2000), um novo paradigma econômico. A base de dados é para o autor um novo marco na sociedade pós-industrial. Para Zuboff (2019), tratar-se-ia de uma "terceira modernidade", marcada pelo capitalismo de vigilância; exploram-se os anseios humanos da modernidade sob o argumento de que a privacidade é o preço a ser pago para o acesso em abundância de bens digitais. Nesse sentido, a autora afirma que "uma nova forma de poder econômico surge, sendo que cada clique, pesquisa, curtidas é tida como ativo para que empresas rastreiem e monetizem uma transformação ocorrida em menos de uma década desde o lançamento do *iPod*" [5].

Portanto, seja através de sensores ou do comportamento do usuário, acumulam-se informações e, quanto maior a quantidade, mais dados é produzida, estruturados e analisa-

---

[4] No original: "Wi-Fi–enabled and networked, the thermostat's intricate, personalized data stores are uploaded to Google's servers. Each thermostat comes with a "privacy policy," a "terms-of-service agreement," and an "end-user licensing agreement." These reveal oppressive privacy and security consequences in which sensitive household and personal information are shared with other smart devices, unnamed personnel, and third parties for the purposes of predictive analyses and sales to other unspecified parties. Nest takes little responsibility for the security of the information it collects and none for how the other companies in its ecosystem will put those data to use." Tradução livre.

[5] No original: "A new breed of economic power swiftly filled the void in which every casual search, like, and click was claimed as an asset to be tracked, parsed, and monetized by some company, all within a decade of the iPod's debut." Tradução livre. Página 55.

dos. Dessa forma, obtêm-se grandes volumes de dados, também chamados de *big data*[6], que permitem revelar padrões e tendências nas interações e nos comportamentos humanos (MAGRINI, 2018). Pode-se entender *big data* como os "(...) trabalhos em grande escala que não podem ser feitos em escala menor, para extrair novas ideias e criar novas formas de valor de maneira que alterem os mercados, as organizações, a relação entre cidadãos e governos, etc. (SCHOBERGER; CUKIER, 2013)". A partir da acumulação de dados, possibilita-se reunir e analisar as informações de forma barata e rápida.

O uso de *cookies* é uma dessas ferramentas para coleta de dados. Hormozi (2005) define *cookies* como "um pequeno arquivo de texto que é salvo no *hardrive* pelo servidor de internet" [7]. Sua funcionalidade permite ao domínio virtual guardar informações e preferências do usuário para visitações futuras, bem como disponibilizar essas informações com outros *sites.* Ademais, mesmo que um sítio virtual não tenha *cookies,* é possível seu uso por terceiros, através das propagandas tão comuns aos *sites* de hoje em dia. Um exemplo comum é visitar um sítio eletrônico sobre determinado assunto e, logo após, começar a receber propagandas ou informações sobre o mesmo tema. Com o uso de *cookies* é possível determinar o interesse do usuário, permitindo propagandas personalizadas para aquela pessoa.

Por se tratar de conhecimento técnico da área da informática, ainda que o usuário escolha por ter controle sobre os *cookies* de seu próprio navegador, não seria estranho que o usuário se veja incapaz de lidar com as técnicas de armazenamento de *cookies,* estando desta forma exposto (ABBAS; OLIVEIRA, 2018).

Mesmo sem o uso de *cookies*, Zuboff (2019) demonstra outras formas que as empresas usam para coleta e análise de dados. A *IBM*, por exemplo, tem uma inteligência artificial que, a partir de e-mails, publicações e fotos, determina as necessidades do consumidor em doze dimensões, sendo elas excitação, harmonia, curiosidade, ideais, intimidade, liberdade de expressão, amor, praticidade, estabilidade, desafio e estrutura. A partir dessas informações, a inteligência artificial identifica valores que influenciam a tomada de decisões em cinco dimensões: conservadorismo, hedonismo, autoaprimoramento, novas experiências ou ajudar os outros. Com base nesses dados é possível, em tese, prever como a pessoa reage frente a diferentes situações, seja para auxiliar na resolução de conflitos, para delimitar as predileções dos clientes, para divulgação de propagandas de forma discriminada, dentre outros.

Os riscos da extensiva coleta de dados se tornou evidente após o paradigmático

---

[6] Megadata, em português.

[7] No original: "A cookie is a small text file that is saved on a user's hard drive by a Web server." Tradução livre.

caso da empresa *Cambridge Analytica*, que utilizou um aplicativo de *Facebook* para coletar dados, violando os termos de uso da plataforma, que proíbe o compartilhamento de informações com terceiros.

Sejam por objetos *smart* ou pelo uso da internet, o comportamento humano está sobre constante vigilância. Razão pela qual se faz imperioso uma normativa para proteção da privacidade.

4 LEGISLAÇÃO

Expostos os conceitos pertinentes à privacidade e a proteção de dados, prossegue-se ao estudo da legislação acerca do tema.

Neste tópico, haverá duas subdivisões: uma para a legislação europeia e uma para a legislação nacional. Pretende-se ressaltar os artigos previstos na RGPD que sejam mais relevantes para, logo em seguida, expor como são tratados os dados pessoais na legislação brasileira de maneira crítica.

4.1 LEGISLAÇÃO EUROPEIA

O Regulamento Geral de Proteção de Dados (RGPD), aprovado em 2016, foi implementado em 25 de maio de 2018 e tem com o objetivo harmonizar as normas que regulam o processamento de dados pessoais dentro da União Europeia no que se refere à proteção de dados. Apesar de cada país da União Europeia possuir legislação e jurisprudência própria, cada lei federal deverá se respaldar na RGPD, de forma a obter uma aplicação mais coerente e homogénea das regras e da defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

Tal entendimento é expresso no item 10 do artigo 1° da RGPD:

> (10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

No que se refere à proteção de dados, influi-se que, para o direito europeu, trata-se de um direito fundamental e autônomo, sem necessidade de correlação ao direito à privacidade. Tal proteção aos dados pessoais corresponde com o que foi proposto por Rodotà e a acepção do direito a autodeterminação informativa, conforme diz a RGPD.

> (1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Quanto à aplicação normativa, excluem-se da aplicação dessa norma atividades domésticas ou de cunho pessoal, bem como pessoas já falecidas, conforme previsto nos artigos 2° e 3° da RGPD. Aplica-se as disposições da RGPD para todas as empresas estabelecidas na União Europeia que tratem dados pessoais e para empresas que, embora estejam fora da União Europeia, ofereçam bens ou serviços a cidadãos europeus, conforme previsto nos itens 24 e 25 do título normativo. Por se tratar de proteção de dados pessoais, excluem-se de proteção jurídica os dados dos quais foram completamente anomizados, assim como as informações de pessoas jurídicas.

> 26) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.

Como pode ser observado, a norma difere dados pseudonimizados de dados anonimizados. Tal distinção é relevante, considerando que os dados que ainda permitam a identificação do indivíduo sejam equiparados a dados pessoais. Yoseph (2015) sugere três questionamentos que devem ser respondidos negativamente para confirmar a anomização: "(...) (1) É possível, através dos dados pseudomizados, destacar um indivíduo? (2) Seria possível relacionar a informação com outras de forma a encontrar um indivíduo? (3) É possível in-

ferir informações de um indivíduo?" [8]. Embora o autor afirme que pseudonimização apenas seja uma forma de anonimização, devido tal tratamento jurídico diferenciado é importante ressaltar a diferença entre ambos os termos. Para alcançar a anonimização é necessário, portanto, apagar todos os registros que tornariam a informação identificável a uma pessoa específica.

A pseudonimização é, na RGPD, uma das medidas de proteção das quais ajudará os responsáveis pelo tratamento dos dados e seus subcontratantes em garantir a segurança dos dados, sendo vedada a reversão não autorizada da pseudonimização, conforme expresso no item 85. Não se trata, portanto, de uma forma de afastar a aplicabilidade da RGPD, diferente do que ocorre com os dados anonimizados.

Para que os dados sejam coletados, é necessário que haja uma das hipóteses previstas na lei, em seu artigo 6°. Sempre que o tratamento dos dados for realizado fundado no consentimento da parte, o indivíduo deverá dar o consentimento expresso para uma finalidade específica e legítima. Caso o usuário se recuse, não poderá tal recusa implicar na impossibilidade do uso do serviço.

> (32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.

O consentimento, portanto, deverá ser informado e é restrito a finalidades específicas, sendo vedado o uso dos dados para motivo diverso. Ademais, é necessário clareza dos termos, conforme expresso nos itens 39 e 43 do artigo 1°. Tampouco será considerado um consentimento válido, quando houver manifesto desequilíbrio entre o titular dos dados e o responsável do tratamento, de forma que não se possa presumir que o consentimento tenha se dado livremente. Nos moldes do item 43 do artigo 1°, isso poderá ser constatado pela inequidade de uma situação fática, ou se a execução do contrato depender do consentimento apesar de

---

[8] No original: "(...) (1) Is it still possible to single out an individual, (2) is it still possible to link records relating to an individual, and (3) can information regarding an individual be inferred?". Tradução livre, página 6.

desnecessário para sua execução.

A RPGD Também trata do direito de corrigir as informações prestadas, prevendo a prerrogativa do usuário de alterar os dados para que estejam em consonância com a verdade. No caso da empresa, qualquer alteração nos dados deverá ser encaminhada ao usuário, de forma que somente com o consentimento dele poderão ser alterados. Trata-se do direito à retificação, previsto no artigo 6° da RGPD. Caso, porventura, não se queira mais que os dados sejam tratados, o usuário poderá, com a mesma facilidade que foi oferecido, remover o consentimento, de forma a ter seus dados pessoais apagados, sendo tratado, pela RGPD, como o direito de ser esquecido.

Ainda que não haja manifestação da parte que prestou os dados, esses deverão ser apagados caso a finalidade pretendida esteja cumprida ou caso os dados deixaram de cumprir a finalidade consentida entre as partes. Tal previsão se encontra no artigo 17 e no item 65 do artigo 1°.

> (65) Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento. Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto. No entanto, o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Como se pode notar, a legislação possui certas particularidades quando o fundamento jurídico do tratamento dos dados for diferente daquele fundado no consentimento. Enquanto fundado no consentimento, a mera remoção deste é o suficiente para ter os dados removidos. No entanto, desde que a razão para coleta dos dados seja fundada no interesse público, os dados poderão ser retidos.

Outra particularidade dos dados coletados com fundamento diverso do consentimento é a mutabilidade entre finalidades.

> (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais

> os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior deverá ser considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, deverão ser consideradas tratamento lícito compatível. O fundamento jurídico previsto no direito da União ou dos Estados-Membros para o tratamento dos dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior. A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação 4.5.2016 PT Jornal Oficial da União Europeia L 119/9 com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

Ademais, quando as razões para coleta de dados forem para efeitos de investigação científica e forem usados para uma finalidade cuja identificação no momento da coleta dos dados for de impossível delimitação, os titulares dos dados poderão consentir para determinados domínios de investigação ou partes de projetos de investigação, conforme previsto no item 33 da RGPD.

Certos dados são, a priori, intratáveis. A RGPD elenca, em seu artigo 9°, restrições quanto ao tratamento de dados genéticos, de dados biométricos que permitam identificar uma pessoa específica, ou dados relativos à saúde, quanto à origem racial ou étnica, às opiniões políticas, às convicções religiosas ou filosóficas, à filiação sindical, à orientação sexual e à vida sexual de uma pessoa. Tais dados, denomidados pela RGPD como dados sensíveis, só poderão ser tratados em hipóteses específicas. Isso pois os dados pessoais sensíveis possuem dilatado potencial lesivo, razão pela qual merecem tutela diferenciada (KORKMAZ; NEGRI, 2019)

> (51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais

> não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.

Tal preocupação com o tratamento de dados sensíveis surge pela possibilidade discriminatória de se, porventura, tais dados forem utilizados para o proposito de *profiling*, definido pela RGPD, em seu artigo 4°, item quatro, como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar desses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular", podendo ser estes a sua situação econômica, a de sua saúde, o seu desempenho profissional, interesses, fiabilidade, comportamento, dentre outros. Salvo a exceção do artigo 22, item 2, quando a decisão automatizada for necessária por virtude do contrato, com concordância explicita da parte, ou por virtude de lei, o *profiling* automatizado é vedado pela RGPD.

> (71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança.

Gonzales (2019) afirma que a vagueza e subjetividade ao se permitir o *profiling* apenas com base no consentimento e legítimo interesse no responsável pelos dados. Apesar do *profiling* ter benefícios, eles também criam riscos, principalmente quando usados sem consentimento da parte, razão pela qual a RGPD coíbe tal prática e torna necessário o consentimento explícito, bem como permite a revisão dessas informações por um agente humano. Tais medidas, embora incipientes para proteção do indivíduo contra danos ocasionados por *profiling*, representam um importante passo na proteção do indivíduo contra ser discriminado por um sistema automatizado.

Outra preocupação da RGPD é quanto aos dados de menores de idade. A RGPD, em seu item 38 do artigo 1° e no artigo 8° estabelece que, por estarem menos cientes dos riscos inerentes ao tratamento de dados pessoais, deverá ser exigido o consentimento dos responsáveis parentais. Só não se exige no caso de serviços preventivos ou de aconselhamento para crianças.

Para fins de responsabilização, a RGPD não é precisa quanto à aplicação da responsabilidade objetiva ou subjetiva. Tende-se a compreender que se trataria de uma semi-objetiva responsabilidade, já que, embora haja direito de reparação quando o titular sofre danos, o item 2 prevê como matéria de defesa o cumprimento do standard de conduta estabelecido pela lei, numa análise casuística de negligência (RICCIO, 2019). Noutras palavras, embora seja requerido do titular apenas a comprovação do dano sofrido, o controlador poderá demonstrar ter adotado todas as medidas, previstas no artigo 40, para evitar o dano causado como matéria de defesa.

> Artigo 82.° (...) 2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.

Como se trata de uma regulação harmonizadora, e não unificadora, para a União Europeia, cabe ressaltar que os entornos adquiridos a respeito da Proteção de Dados variarão conforme o país. Os valores indenizatórios levarão tanto em conta a gravidade do dano quanto às ações tomadas pelo responsável dos dados em evitar a ocorrência do dano e sua mitigação após constatá-lo.

4.2 LEGISLAÇÃO BRASILEIRA

A Lei Geral de Proteção dos Dados, aprovada em 2018, prevê em seu artigo 1°:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Embora não tenha sido tratado a autodeterminação informativa como um direito autônomo, a tutela dada a autodeterminação informativa é de direito fundamental, como extensão ao direito à privacidade e do livre desenvolvimento da personalidade da pessoa natural.

Quanto a aplicação da lei, ela é mais ampla do que o que foi previsto na RGPD. Enquanto na RPGD é necessário constatar o objetivo da empresa em prestar serviços destinados aos cidadãos europeus, a lei brasileira afirma, em seu Art. 3°, inciso III, uma hipótese de aplicação da lei mais ampla, bastando que os dados coletados sejam de indivíduos localizados no território brasileiro no momento da coleta.

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

O consentimento, para LGPD, foi tratado de forma menos específica, quando comparado à RPGD. Enquanto no Regulamento Europeu se faz menção explicíta de como deverá ser feito um consentimento válido, vedando o uso de opções pré-validadas, de omissão por parte do titular dos dados, e da impossibilidade de se tornar um serviço inutilizável em caso de desacordar de ceder dados pessoais que não sejam absolutamente necessários para prestação do serviço, o artigo 8° da LGPD determina apenas que o consentimento deverá ser informado, de manifestação livre e inequívoca.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os 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. § 6º Em caso de alte-

> ração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Considerando que se trata uma manifestação livre e informada, infere-se que as opções pré-marcadas e omissivas também não devem ser consideradas como consentimento válido para LGPD. Isso pois, conforme afirma Sunstein (2003), um dos obstáculos para o liberalismo em sua acepção tradicional é que, ainda que seja facultado ao agente a escolha, nota-se uma tendência, seja por desconhecimento ou por preferências mal-formadas, à se optar pelas opções padronizadas.

Tal conceituação de racionalidade, denominada racionalidade liminada, foi introduzida por Herbert Simon (1995) e se opõe a visão do *homo economicus* entendido como "o homem que se presume ter conhecimento de todos os aspectos relevantes, dos quais, mesmo que incompletos, são claros e extensos. Presume-se ter uma organizada lista de preferências, e uma capacidade de calcular a melhor rota de ação de acordo com suas preferências". Ao se constatar que a visão do *homus economicus* é idealistica, torna-se necessário adequar ao paradigma e reconhecer que, para fins práticos, agentes racionais frequentemente tomam decisões contrárias ao seu interesse.

Com base no exposto, percebe-se que os conceitos de *privacy by design* e *privacy by default* têm um papel fundamental na proteção da autodeterminação informativa. De acordo com Tamo-Larrieux (2018), a privacidade deve ser considerada desde o início da criação de um sistema tecnológico, de forma que seja parte integral do sistema, evitando consertar após que o sistema está pronto e se torna demasidamente caro e tarde para consertá-lô. Cavoukian (2010) sugere 7 princípios que devem ser seguidos, sendo a privacidade padronizada um deles. Entende-se como a privacidade por padrão como todas as opções que garantem a privacidades como pré-estabelecidas, sendo facultado ao titular dos dados ceder dados. Considerando que a legislação considera o consentimento como uma manifestação livre e informada, tais conceitos devem ser levados em consideração para fins de determinar se um consentimento é válido e se um controlador cumpriu com a devida diligência para proteger a autodeterminação informativa do titular dos dados.

Como afirmado previamente, dados sensíveis possuem dilatado potencial lesivo, justificando tutela diferenciada. Ambas legislações apontam a origem étnica, as convicções políticas, filosóficas e religiosas assim como as informações pessoais referentes a sexualidade, saúde e biometria. No entanto, os dados pessoais referentes a condenações criminais, diferente da RGPD, não constam no rol de dados sensíveis na LGPD. Essas informações tem

nítida potencialidade de gerar situações discriminatórias, havendo possibilidade de ensejar um impedimento para que indivíduos reiniciem sua vida após serem condenados judicialmente (KORKMAZ; NEGRI, 2019).

O artigo 11 da LGPD prevê: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas". Tem-se como diferença a remoção da possibilidade de se arguir interesses legítimos do controlador como fundamento para o tratamento dos dados pessoais sensíveis, bem como o fundamento jurídico de tratamento desses dados para a proteção de crédito. Logo, enquanto a RGPD estabelece como regra geral que os dados sensíveis são intratáveis, a LGPD faz o contrário, criando uma ampla hipótese de utilização dos dados sensíveis.

O parágrafo 3° do artigo 11 prevê a possibilidade de vedação ou de regulamentação por parte da autoridade nacional, previsto no quanto o compartilhamento de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica. O que significa que, na ausência de pronunciamento da ANPD, dados sensíveis poderão ser compartilhados para obter vantagem econômica, desde que tal finalidade seja prevista e consentida pelo titular do dados. Somente os dados pessoais relativos à saúde, previstos no parágrafo 4° do mesmo artigo, tem como regra a vedação de serem compartilhados para a obtenção de vantagem econômica.

Ademais, a LGPD carece de proibição no que tange o *profiling.* Não há menção à utilização automática de tratamento de dados que ocasione na criação de um perfil do usuário, possibilitando que esse perfil seja usado discriminatoriamente em desfavor do titular dos dados. Tampouco há previsão de um direito subjetivo de obter revisão humana de dados gerados automaticamente.

5 CONSIDERAÇÕES FINAIS

Na sociedade da informação e de constante fluxo de dados, é necessário regular as relações no ambiente virtual para garantir a proteção da pessoa. A privacidade, portanto, adquire novos contornos com o passar do tempo, deixando de ser apenas uma prerrogativa do cidadão frente ao Estado, para se tornar uma prerrogativa da pessoa frente aos outros agentes privados.

No paradigma da autodeterminação informativa, o indivíduo deverá ter controle de seus dados pessoais. Para que isso ocorra de maneira efetiva, é necessário o estabelecimento de rigorosos padrões de conduta por parte das empresas que manejam os dados pessoais.

Nessa esteira, ambas a RGPD e LGPD propõem, de maneira semelhante, os critérios para proteção dos dados pessoais. Nota-se, no entanto, que a legislação brasileira é precária no que tange a proteção contra a criação de perfis automatizados e proteção dos dados sensíveis, aumentando a importância da Agência Nacional de Proteção de Dados em preencher essas lacunas normativas.

Por ser uma legislação que entrou em vigor recentemente, não há julgados suficientes para saber com exatidão como será a jurisprudência acerca do tema. A partir do princípio da não-discriminação previsto tanto na Constituição quanto na LGPD, preza-se que seja aplicado para proteção das pessoas contra eventuais ingestões praticadas pelos responsáveis dos dados, cujo tratamento automatizado pode resultar em tratamento discriminatório para com o titular dos dados. De certo, a ação judicial só ocorre quando o dano já foi ocorrido, razão pela qual a atuação da ANPD em prevenir lesões ao direito à autodeterminação informativa e à privacidade é fundamental.

REFERÊNCIAS

BENTHAL GREEN. **Settlement and Building to 1836, in A History of the County of Middlesex**: Volume 11, Stepney, Bethnal Green, ed. T F T Baker (London, 1998), pp. 91-95. British History Online. Disponível em: http://www.british-history.ac.uk/vch/middx/vol11/pp91-95. Accesso em 24 de fevereiro de 2021.

BLASCOVICHT, Jim; SCHROEDER, Ralph. **The social life of Avatars**. Chapter: Social Influence within Immersive Virtual Environments. Springer Verlag-London Ltd, 2002. 127-144.

BRASIL. **Constituição de 1824**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm. Acesso em: 10 de maio de 2021.

BRASIL. **Constituição de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 de maio de 2021.

BRASIL. **Lei N°10.406 que institui o Código Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 de maio de 2021.

BRASIL. **Lei N°12.965 que institui o Marco Civil da Internet**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 de maio de 2021.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**, Volume 1: Parte Geral, Livro Digital, 10. ed. São Paulo/SP: Saraiva, 2012.

GONZALES, Gil Elena; DE HERT, Paul. **Understanding the legal provisions that allow processing and profilling of personal data-an analysis of GDPR provisions and principles**. ERA Forum, 2019. 597-621.

HERBERT, A. Simon. **A Behavioral Model of Rational Choice**. The MIT Press. Disponível em: http://www.jstor.org/stable/1884852. Acesso em: 10 de julho de 2021.

HITCHCOCK, Tim; SHOEMAKER, Robert; EMSLEY, Clive; HOWARD, Sharon; MCLAUGHLING, Jamie, et al., **The Old Bailey Proceedings Online**, 1674-1913. Disponível em: www.oldbaileyonline.org. Acesso em 24 de março de 2021.

HORMOZI, Amir M. **Cookies and Privacy**: Information Systems Security. Disponível em: http://dx.doi.org/10.1201/1086/44954.13.6.20050101/86221.8. Acesso em 25 de fevereiro de 2021.

KORKMAZ, Maria Regina Rigolon; NEGRI, Sérgio Ávila. **A normatividade dos dados sensíveis na lei geral de proteção de dados**: ampliação conceitual e proteção da pessoa humana. Revista de Direito Governança e Novas Tecnologias. 2019.

MAGRANI, Eduardo. **A internet das Coisas**. FGV editora. 1ª Edição. 2018 Rio de Janeiro, Brasil.

MAYER-SCHÖNBERGER, Victor; CUKIER; Kenneth. **BIG DATA**: como extrair volume, variedade e valor. Tradução: Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013. p. 6.

OLIVEIRA, J. V; SILVA, L. A. **É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede**. R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/8419. Acesso em: 24 de março de 2021.

Organização das Nações Unidas. **First-ever United Nations Resolution on Homelessness**. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf. Acesso em: 24 de fevereiro de 2021.

Oxford Dictionary. **Definition of virtual adjective from the Oxford Advanced Learner's Dictionary**. Disponível em: https://www.oxfordlearnersdictionaries.com/us/definition/english/virtual?q=virtual. Acesso em 24 de abril de 2021

RODOTÀ, Stefanò. A **vida na sociedade da vigilância:** a privacidade hoje. Maria Celina Bodin de Moraes (org.). Rio de Janeiro: Renovar, 2008.

RODOTÁ, Stefanò. **Il mondo nella rete Quali i diritti, quali i vincoli**. Roma: Laterza, 2014.

SUNSTEIN, Charles; THALER, Richard. **Libertarian Paternalism is not an Oxymoron**. Chicago Law Review. Disponível em: http://www.law.uchicago.edu/Lawecon/index.html. Acesso em 5 de julho de 2021.

SILVA, Denis Franco. **Livre uso do corpo e direitos de personalidade**. Revista Pensar. 2014. 56-70.

SPACKS, Patricia Meyer. Privacy: **Concealing the Eighteenth-Century**. Chicago Press, 2003.

TAMÒ-LARRIEUX, Aurelia. **Designing for Privacy and its Legal Framework**. Gewerbestrasse: Springer Nature Switzerland, 2018.

TAYLOR, Charles. **Sources of the Self**: The Making of the Modern Identity. Havard University Press. 1ª Edição. Março de 1992.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**: General Regulation Data Protection (Regulamento Geral sobre a Proteção de Dados). Bruxelas, ps://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 21 de junho de 2021.

WESTIN, Alan. **Privacy and Freedom**. New York: Ig Publishing, 1967.

ZUBOFF, Shoshana. **The age of surveillance capitalism**. New York: Public affairs, 2019.