O DIREITO À PRIVACIDADE NA ERA DIGITAL

Rodrigo Almeida Magalhães
Pontifícia Universidade Católica, Minas Gerais
amagalhaes@ig.com.br

Erika Cristina Rodrigues Nardoni Oliveira
Centro Universitário Unihorizontes, Minas Gerais

RESUMO: Vários modelos de negócios são pautados no uso das tecnologias alimentadas por dados. Com isso, cada vez mais surge a necessidade de proteger o indivíduo, sua privacidade e suas informações, uma vez que dados pessoais são obtidos, usados e circulam entre empresas em um contexto desproporcional, sendo impossível para o titular obter o controle do trânsito de suas próprias informações. Nesse sentido, o presente estudo tem por objetivo analisar a Lei 13.709/2018, com o intuito de entender se a prática do uso compartilhado de dados pessoais fere o direito à privacidade do titular. Para melhor apresentação do tema, será mostrada sucintamente a relevância do direito à proteção de dados pessoais e a inserção deste no contexto do direito à privacidade; bem como os aspectos jurídicos do uso compartilhado, com o intuito de demonstrar a vulnerabilidade do titular diante da intensa circulação de informações pessoais e da impossibilidade de proteção dos dados pessoais. O desenvolvimento será realizado através do método científico qualitativo, e os argumentos serão fundamentados por meio de técnica dedutiva.
PALAVRAS-CHAVE: Dados Pessoais. Privacidade. Vulnerabilidade. Tratamento de Dados. Tecnologia.

The Right to Privacy in the Digital Age

ABSTRACT: Several business models are based on the use of data-driven technologies, so there is an increasing need to protect the individual, their privacy and their information as personal data is obtained, used, and circulates between companies in a disproportionate context, making it impossible for the holder to gain control of the transit of their own information. In this sense, the present study aims to analyze the law 13.709 / 2018, in order to understand if the practice of shared use of personal data violates the right of privacy of the holder. For a better presentation of the theme, the relevance of the right to the protection of personal data and its insertion in the context of the right to privacy will be briefly shown; as well as the legal aspects of shared use, in order to demonstrate the vulnerability of the holder against the intense circulation of personal information and the impossibility of protection of personal data. The development will be accomplished through the qualitative scientific method, and the arguments substantiated by deductive technique.
KEYWORDS: Personal Data. Privacy. Vulnerability. Data Processing. Technology.

INTRODUÇÃO

Não há dúvidas de que as tecnologias possibilitam mudanças significativas para os indivíduos inseridos na sociedade da "Era Informacional". Atualmente, o indivíduo precisa ser observado, fornecer suas informações, expor sua rotina e se comunicar rapidamente, para participar

da sociedade como um ser existente – afinal, não estar conectado ou não ter informações retidas em uma base de dados torna-se quase um sinônimo de inexistir.

Ao ligar o GPS, pedir uma pizza, procurar um emprego ou mesmo transitar pelas ruas da cidade, as pessoas produzem informações que são coletadas e armazenadas em equipamentos eletrônicos, permitindo a quem colheu usá-las conforme seus interesses. Isso se torna um problema para os titulares dos dados e para a sociedade quando essas informações são compartilhadas e disponibilizadas a terceiros, o que acaba transformando a vida particular em um grande *reality show*, tornando o indivíduo um objeto em vigilância constante. (RODOTÁ, 2008, p.19)

Empresas e entidades públicas usam dados pessoais a todo momento, seja para o oferecimento de produtos e serviços de acordo com o perfil do cliente ou para elaboração de controles internos, com o interesse de manter o funcionamento das tecnologias que facilitam esses serviços e melhoram o atendimento aos clientes.

Essas práticas só se tornaram possíveis, contudo, devido ao desenvolvimento das tecnologias que facilitam o uso maciço de dados, gerando assim o fenômeno chamado *Big Data* – que nada mais é do que uma grande base contendo dados e informações desconexas, mas que, se aliada a tecnologias inteligentes e à internet, possibilita ao interessado beneficiar esses dados para chegar a um resultado útil aos interesses dele. Assim, dados pessoais se transformam em um elemento, ou melhor dizendo, em matéria-prima, com valor de mercado, podendo ser compartilhados e usados por outros interessados. Afinal "do que adianta uma montanha de dados se não formos capazes de extrair valor?" (AMARAL, 2016 p. 1).

Dados pessoais podem ser usados de muitas formas. Eles circulam entre empresas e são armazenados em locais virtuais fora do alcance de qualquer forma de controle. Nesse contexto, mostra-se a necessidade e a relevância de proteger informações pessoais, pois, além de serem usados desenfreadamente, dados pessoais revelam a identidade do indivíduo e, dependendo da forma como são usados, atingem a privacidade do titular. Isso porque, por meio do uso de informações, é possível desvendar toda a rotina, gostos, particularidades e até mesmo os desejos de uma pessoa, tornando-a, assim, parte vulnerável perante a quem faz uso das suas informações pessoais.

Com isso, as pessoas podem ser manipuladas (a partir de propagandas personalizadas, por exemplo), tendo suas fragilidades mais privadas exploradas de modo a se colocar em risco a liberdade e a democracia.

Assim, o presente estudo tem por objetivo analisar a Lei Geral de Proteção de Dados Pessoais n°13.709/2018 (LGPD), a fim de responder o problema de pesquisa que reside no seguinte questionamento: a prática do uso compartilhado de dados pessoais entre empresas fere o direito à privacidade do titular? Para tanto, será mostrado sucintamente o contexto histórico do direito à proteção de dados pessoais e a tutela da privacidade no ordenamento jurídico brasileiro, os contornos do direito à privacidade, bem como os aspectos jurídicos da lei quanto ao uso compartilhado de dados pessoais, para, então, serem entendidos os riscos para o titular.

Este artigo será organizado, para melhor compreensão, em três tópicos. O primeiro consiste em revelar conceitos e princípios relevantes sobre a matéria. O segundo aborda a dinâmica do uso compartilhado, formas de uso e as relações jurídicas de dados. No terceiro, será demostrada a vulnerabilidade do titular frente à prática do compartilhamento. O desenvolvimento será realizado por meio do método dedutivo; e os argumentos fundamentados, por meio de pesquisa bibliográfica e análise da lei.

Com o objetivo de responder aos questionamentos apresentados, mas sem a pretensão de esgotar a matéria, Rodotá (2008, p. 139) revela que "a circulação das informações ocorrem em

um contexto amplamente despersonalizado, no qual o respeito é sobrepujado por outras lógicas, e pela necessidade da sociedade da informação de obter seu alimento."

Nesse sentido, faz-se necessária a efetiva atenção à LGPD, para que as empresas que fazem uso de dados pessoais possam ir além das regras contratuais e para que seja de fato assegurado o direito à privacidade dos titulares e o respeito aos valores fundamentais existentes no ordenamento jurídico.

1. DADOS PESSOAIS NO CONTEXTO DA PRIVACIDADE

Dependendo da forma como é observado o comportamento de alguém – seja por meio da internet ou de alguma espécie de investigação, ou até mesmo através da janela de casa –, é possível obter muitas informações e usá-las de inúmeras maneiras. Michel Foucault[1], quando explica o fenômeno "*Panópticon*", relata que a observação permite a qualquer interessado o saber, ou melhor dizendo, a intromissão, a vigilância, que conduz a uma forma de controle social.

> No Panópticon vai se produzir algo totalmente diferente; não há mais inquérito, mas vigilância, exame. Não se trata de reconstituir um acontecimento, mas de algo, ou antes, de alguém que se deve vigiar sem interrupção e totalmente. Vigilância permanente sobre os indivíduos por alguém que exerce sobre eles um poder - mestre-escola, chefe de oficina, médico, psiquiatra, diretor de prisão - e que, enquanto exerce esse poder, tem a possibilidade tanto de vigiar quanto de constituir, sobre aqueles que vigia, a respeito deles, um saber. (FOUCAULT, 2005, p. 88)

Pelas palavras de Foucault, é possível assimilar que, a partir de informações obtidas sobre um determinado indivíduo, pode-se entender o comportamento dele, influenciá-lo e o controlar, depreciar direitos sem que ele perceba ou que tenha qualquer poder ou domínio sobre suas próprias informações. Com o uso maciço da internet e das tecnologias inteligentes, é difícil saber quem detém o poder da informação, pois, no mundo virtual, apesar de muito acessível, fácil é a observação, dependendo somente da forma com que se realiza o controle das informações obtidas, tornando a garantia à privacidade um desafio para sociedade informacional.

O direito à proteção dos dados pessoais teve sua origem conjuntamente com a evolução do conceito de privacidade, o qual sofreu várias mutações ao longo do tempo. Contudo, o marco histórico registra-se em 1890, com o artigo '*The Right To Privacy*'[2], escrito pelos autores Samuel Warren e Louis Brandeis: juristas norte-americanos que entenderam ser a privacidade um "direito de ser deixado só" ou, melhor dizendo, um direito de ser esquecido, indicando uma obrigação de todos respeitarem a vida privada e a esfera íntima de cada um, incluindo, no seu conteúdo, a intimidade, a honra e as informações pessoais[3].

Antes do '*The Right To Privacy'*, a privacidade era entendida sob o prisma da propriedade, que era um direito inviolável e sagrado, ninguém dela podendo ser privado, protegida contra intromissões arbitrárias do Estado. Assim, na evolução do conceito da privacidade, esta sai de um direito extrínseco ao indivíduo, que é a propriedade[4], passando a ser um direito intrínseco,

---

[1] FOUCAULT, Michael. A verdade e as Formas Jurídicas. 2008. O Panópticon era um edifício, imaginado por Betham, em forma de anel com várias janelas ao redor, e no meio havia um pátio com uma torre no centro onde ficava o vigilante. Foucault entendia essa figura arquitetônica como uma utopia, que poderia ser usada como uma forma de exercer o poder da observação e controle das ações humanas.

[2] WARREN Samuel D. BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review. 1890.

[3] Desta feita, o conceito de privacidade incluía a esfera intima do indivíduo, a necessidade de proteger a imagem e a honra (fotografias, biografias não autorizadas), ampliando a semântica desse direito.

[4] Declaração Universal dos Direitos do Homem e do Cidadão de 1789. Art. 17.º No século XIX as pessoas não estavam preocupadas com suas vidas privadas como hoje, mas sim com a propriedade, por isso o conceito de privacidade estava ligado diretamente ao direito da propriedade.

inerente à esfera íntima e à personalidade – cabendo não só ao Estado, mas a todos, o cuidado da não intromissão na vida privada.

Gradativamente, esse conceito foi se atualizando até ser reconhecido como direito fundamental na Declaração Universal dos Direitos Humanos de 1948 – que garantiu a não intromissão na vida privada, na família, no domicílio e nas correspondências. Anos mais tarde, diversas cartas normativas internacionais[5] foram editadas, estabelecendo o direito à privacidade e ampliando seu sentido, incluindo as informações pessoais e o direito de controle de seus próprios dados (autodeterminação informativa) como valores a serem protegidos pelo direito à privacidade.

Os avanços tecnológicos influenciaram bastante a evolução desse conceito, contribuindo para inserção das informações inerentes ao indivíduo na sua semântica interpretativa, devido à necessidade do uso automatizado de informações e dados para manter o funcionamento dessas tecnologias e os relacionamentos sociais no mundo atual.

> Partindo dessa constatação, pode-se dizer que hoje a sequência quantitativamente mais relevante é "pessoa-informação-circulação- controle", e não mais apenas "pessoa- informação-sigilo", em torno do qual foi construída a noção clássica de privacidade. O titular do direito à privacidade pode exigir formas de "circulação controlada", e não somente interromper o fluxo de informações que lhe digam respeito. (RODOTÁ, 2008, p. 93)

Conforme lecionou o ilustre Stefano Rodotá, hoje a privacidade deve ser considerada de forma ampliativa, passando do segredo e da inviolabilidade estanque ao controle[6], até mesmo pelo motivo de que atualmente há interesse em que as informações pessoais ou determinadas situações da vida privada venham ao conhecimento de determinadas pessoas ou instituições.

> Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade. (DONEDA, 2011, p. 95)

Assim, a proteção dos dados pessoais tem como núcleo valorativo a privacidade no seu maior sentido, incluindo no seu conceito todos os direitos inerentes ao desenvolvimento da personalidade de um indivíduo, desde a esfera íntima indisponível (como a honra) até os elementos que podem ser negociados (como a imagem) e também o controle sobre as informações (autodeterminação informativa), com a necessidade de serem interpretados, de forma sistemática[7], outros direitos como a dignidade, a liberdade e o acesso à informação[8].

1.1. A tutela dos dados pessoais no ordenamento jurídico brasileiro

Para tratar de proteção de dados e privacidade – contando com a Declaração Universal dos Direitos Humanos (DUDH) de 1948 e a Constituição da República Federativa do Brasil de

[5] Convenção Europeia de Direitos Humanos (1953); Carta de Direitos Fundamentais da União Europeia (2000); Tratado sobre o Funcionamento da União Europeia (2007); e outros diplomas internacionais que seguiram o modelo europeu de proteção de dados e privacidade.

[6] . RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro. RJ 2008. Pág. 97-98.

[7] MAXIMILIANO, Carlos. 2011. pag. 100. *"Consiste o Processo Sistemático em comparar o dispositivo sujeito a exegese com outros do mesmo repositório ou de leis diversas, mas referentes ao mesmo objeto".*

[8] *"A intimidade nos dá ideia de algo inviolável a inalienável. O respeito nos dá ideia da relação de cada um com todos os demais. A dignidade conjuga esses dois dados, um individual e o outro social e contribui para definir a posição de cada um na sociedade"*. (RODOTÁ, 2008. pag. 234)

1988 (CRFB/88) como principais fontes –, Cots e Oliveira[9] expõem, em uma linha do tempo, as principais normas que abrangem essa matéria, relatando que, no Brasil, esses direitos eram "abordados de forma esporádica em leis esparsas, tratados sob diferentes aspectos". Além desses dois diplomas basilares, o Brasil dispõe também do Código de Defesa do Consumidor, de 1990, do Código Civil, de 2002, do Marco Civil da Internet, de 2014, e de outras leis que abordam a proteção das informações pessoais e a privacidade, de forma aleatória e pontual.

A Constituição Federal de 1988 (CRFB/88) coloca a privacidade e os dados pessoais no rol dos direitos e garantias fundamentais, sendo protegidos pela inviolabilidade e sigilo[10], o que relembra o "direito de ser deixado só". Contudo, acompanhando as mudanças sociais, esse entendimento no Brasil também muda, conforme lecionado por Bittar (2015, p. 173):

> Esse direito vem assumindo paulatinamente maior relevo, com a continua expansão das técnicas de virtualização do comercio, de comunicação, como defesa natural do homem contra as investidas tecnológicas e a ampliação, com a necessidade de locomoção, do círculo relacional do homem, obrigando-o a exposição permanente perante públicos os mais distintos, em seus diferentes trajetos sociais, negociais ou de lazer. É fato que as esferas da intimidade tem-se reduzido com a internet e os novos meios eletrônicos.

O Regulamento Europeu de Proteção de Dados Pessoais, chamado de *General Data Protection Regulation* (GDPR), editado em 2016, é considerado hoje uma norma relevante para a matéria, pois coloca a privacidade como núcleo valorativo desse direito, concentrando-se no indivíduo titular dos dados.

O vigor do GDPR, em 2018, fez com que as casas legislativas brasileiras acelerassem a edição da Lei nº 13.709 (específica para proteção de dados pessoais), que foi sancionada em 14 de agosto de 2018 – intitulada Lei Geral de Proteção de Dados Pessoais (LGPD)[11] – pelo motivo da previsão da aplicação extraterritorial do GPDR e de seu sistema unificado[12], o que abrange não só as empresas europeias, mas todas as demais que colhem e usam dados pessoais de indivíduos europeus, ou seja: todas as empresas que ofertem bens ou serviços à União Europeia devem estar de acordo com o GPDR, pois se submetem às regras europeias, ficando assim impedidas de realizarem transações negociais com empresas de países que não dispõem de leis especificas para a proteção de dados pessoais[13]. Com a publicação da LGPD, o Brasil agora está apto a estabelecer negócios internacionais com países da União Europeia, que envolvam tratamento de dados de cidadãos europeus e brasileiros.

> Pode-se pontuar que a necessidade de leis especificas para a proteção de dados pessoais aumentou com o rápido desenvolvimento e a expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder. (PINHEIRO, 2018, p. 50)

Conforme leciona Patrícia Peck[14], comparando "a LGPD e o GPDR, ambas as legislações tem como objetivo o regramento do tratamento de dados pessoais buscando em si a defesa dos direitos fundamentais das pessoas naturais". Essas legislações definem o que são dados pessoais e outros conceitos relevantes, estabelecendo o consentimento como um dos fundamentos centrais nas relações que envolvam dados pessoais, com previsão de aplicações de medidas de segurança

[9] COTS, M. OLIVIERA, R. 2018. Pág. 33.
[10] Vide. Artigo 5º X e XII da CRBF.
[11] BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei geral de Proteção de dados Pessoais.
[12] Resolução 2016/679, art.3º, da União Europeia -General Data Protection Regulation.
[13] COTS, OLIVIERA. 2018. Pág. 29.
[14] PINHEIRO, 2018, p.38. Proteção de dados pessoais. Comentários a Lei 13.709/2018 (LGPD)

e sanções no caso de descumprimento, prevendo um órgão competente para fiscalizar e zelar pela proteção dos dados pessoais e da privacidade.

1.2. O uso de dados pessoais e a Lei 13.709/2018 – LGPD

Atualmente, vários modelos de negócios são pautados no uso das tecnologias alimentadas por dados. Fazendo uso das palavras do senador Ricardo Ferraço, dados pessoais são "insumo principal da atividade econômica em todos os setores possíveis da sociedade", que alteram os parâmetros do desenvolvimento da economia do país, sendo necessário o Estado acompanhar todas essas mudanças[15].

O uso dos dados pessoais pelas entidades privadas tem crescido em números consideráveis, a contar da popularização da internet no Brasil e do uso maciço das tecnologias pelas empresas. Assim, cada vez mais surge a necessidade de proteger informações pessoais, sendo essencial tratar o assunto de forma isonômica e multidisciplinar, abarcando a livre iniciativa, a livre concorrência e abrangendo os novos modelos de negócios, no sentido de incentivar o desenvolvimento tecnológico e as inovações no mercado[16] sem prejuízo ao direito à privacidade e à proteção de dados pessoais.

Nesse sentido, a LGPD inova, trazendo ferramentas para o titular controlar suas informações, em vez de isolá-lo em uma garantia inviolável e sigilosa para proteger a privacidade[17]. Além disso, a LGPD estabelece parâmetros para que as empresas possam usar as informações pessoais fornecidas pelos titulares e tentar harmonizar os interesses das duas partes (titular e entidade privada), com os direitos envolvidos nas relações jurídicas.

A LGPD concentra-se no uso e na circulação dos dados pessoais, com o intuito de proteger tanto o indivíduo titular dos dados quanto os dados pessoais em circulação, ressaltando a existência de uma sequência lógica a perseguir: a "coleta–uso–compartilhamento". Além disso, é uma lei que estabelece, na maior parte de seu conteúdo, conceitos básicos – entre eles dados pessoais[18], que é entendido como qualquer informação pela qual seja possível identificar, direta ou indiretamente, uma pessoa natural[19] ou que permite identificação indireta, agregando uma informação a outra, por meio de técnicas de cruzamento de dados e lógicas dedutivas. Estabelecendo critérios relacionados à pessoa e obtendo respostas corretas (como a religião que frequenta, para qual time de futebol torce, sua profissão, gênero), é possível identificar uma pessoa, como nas histórias de Sherlock Holmes[20].

A lei ainda traz outras categorias especiais de informações pessoais, como os dados sensíveis, que são aquelas informações relacionadas a opiniões políticas, religião, raça, dados sobre saúde e informações biométricas. Outra categoria de dados posta na lei são os dados anonimizados, que resumidamente são dados pessoais que passaram pela técnica da anonimização e perderam o elemento que possibilita a identificação, direta ou indireta, de uma pessoa. A dificuldade

[15] Parecer da comissão de assuntos econômicos. Relator, Sen. Ricardo Ferraço. Publicado em 30/05/2018. Disponível em: http://portaldaprivacidade.com.br/wp-content/uploads/2018/05/Doc-SF180511498853-Entrega-FINAL-Ricardo-Ferra%C3%A7o-03.05.18.pdf. Acesso em: 01 maio 2019.

[16] Vide Artigo 219 CRBF

[17] COTS & OLIVEIRA. 2018. Pag. 63.

[18] Artigo 5º I. informação relacionada a pessoa natural identificada ou identificável.

[19] GAGLIANO. FILHO, 2015. Pg. 129. "A pessoa natural para o direito é portanto o ser humano enquanto sujeito/destinatário de direitos e obrigações".

[20] Sherlock Holmes, personagem da literatura Britânica, famoso por desvendar crimes e identificar criminosos através do uso de técnicas cientificas e lógicas dedutivas (cruzamento das informações), criado pelo escritor Sir Arthur Conan Doyle (1859-1930). História disponível também na plataforma Netflix, como série da dramaturgia.

que existe quanto ao uso de dados anonimizados é comprovar que as técnicas de anonimização e segurança de informação foram adotadas, tendo em vista que a LGPD não incide sobre dados anonimizados, a menos que sejam comprovadas falhas graves no processo de anonimização[21].

Um assunto central, de relevante importância para a compressão desse artigo, é o conceito de tratamento de dados pessoais, entendido pela LGPD[22] como sendo todas as operações realizadas com dados pessoais. Em outras palavras, tratamento de dados pode ser entendido como todas as formas de uso de informações pessoais, incluindo nesse conceito todo o processo, desde a coleta, armazenamento, compartilhamento e outras operações até o momento do término do tratamento. Até a mera visualização é considerada tratamento de dados pessoais.

> [...] tendo em vista a clareza do inciso X desse artigo, é que o rol descrito é exemplificativo e não exaustivo. [...] as hipóteses não são cumulativas, ou seja, uma única atividade da lista já se inclui no conceito de tratamento, por mais simples que ela seja. Armazenar dados sem utiliza-los, por exemplo, já é considerado tratamento de dados pessoais (COTS; OLIVEIRA, 2018, p. 94)

Assim, a lei autoriza o uso de dados pessoais pelas empresas e entidades públicas, mas limita esse uso, estabelecendo garantias específicas para os titulares, como o direito de ter acesso livre e facilitado aos dados tratados, direito de saber quais dados estão sendo tratados, garantia de que a coleta e tratamento sejam realizados sob o mínimo de dados necessário e, se possível, com o emprego das técnicas de anonimização, bem como o direito de retificação e de portabilidade, entre outros constantes nos artigos 17 a 22 da LGPD.

A lei também pontua parâmetros para o uso dos dados, começando com a exigência da observação do princípio da boa-fé e de outros dez princípios específicos[23], constantes no artigo 6º, bem como as dez hipóteses que legitimam o uso dos dados, como: a) o cumprimento de uma obrigação legal, b) execução de políticas públicas; c) estudo por órgãos de pesquisa; d) execução de contratos ou diligências contratuais, e) exercício regular de direitos; f) proteção da vida; g) tutela da saúde; h) interesses legítimos do controlador ou de terceiros que tiverem acesso aos dados pessoais; e, por último e não menos importante, i) o consentimento.

Esse consentimento deverá ser: a) livre (o titular tem a liberdade de escolher que tipo de dado será fornecido); b) informado (disponível para o titular todas as informações sobre o tratamento, como nas políticas de privacidade); c) inequívoco (não precisa de ser expresso, bastando demostrar que o titular tomou conhecimento acerca do tratamento de seus dados) e d) específico (as empresas não poderão compartilhar os dados pessoais sem que o titular dê o consentimento especificamente para essa forma de tratamento de dados[24]). O consentimento poderá ser coletado por qualquer meio, desde que sejam apresentadas as finalidades, devendo ser disponível ao titular das informações a possibilidade de revogar o consentimento a qualquer momento[25], sendo vedado o tratamento sob qualquer forma de vício de consentimento.

---

[21] Vide Art. 5º, II – conceito de dados sensíveis. Vide Art. 5º, XI – e Artigo. 12. Dispõe sobre dados anonimizados.

[22] Vide Art. 5º - X. conceito de tratamento de dados pessoais.

[23] Vide Art. 6º. I – finalidade; II – adequação; III – necessidade, IV - livre acesso; V - qualidade dos dados; VI – transparência; VII – segurança; VIII – prevenção; IX - não discriminação; X - responsabilização e prestação de contas.

[24] "*É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento*". Recurso Especial Nº 1.348.532 – SP - 10/10/2017- STJ. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/526809457/recurso-especial-resp-1348532-sp-2012-0210805-4/inteiro-teor-526809464. Acesso em: 22 mar. 2019.

[25] Vide art. 8º hipóteses do uso de dados sem o consentimento do titular.

É importante frisar que qualquer forma de tratamento de dados pessoais precisa ser pautada em uma dessas nove hipóteses somadas ao consentimento, para que o uso desses dados seja justificado e considerado legítimo.

Embora a LGPD seja uma lei que ampara os direitos e deveres para a proteção dos dados pessoais no Brasil, existem posicionamentos resistentes – e alguns merecem destaque. Esses posicionamentos chegaram a ser debatidos na Comissão de Assuntos Econômicos do Senado Federal, para aprovação do Projeto de Lei da Câmara nº 53, de 2018, que deu origem à Lei 13.709/2018.

Uma das críticas aponta falhas na redação da lei, por conter uma alta carga de conceitos e termos advindos da legislação europeia, mostrando que, futuramente, será necessário interpretá-los por meios de outros mecanismos normativos – encargo que a lei atribui à Agencia Nacional de Proteção de Dados: um órgão ligado à Presidência da República. Outras críticas indicaram a necessidade de amparar, na lei, os dados das pessoas jurídicas, visto que incorrem nos mesmos riscos e incidentes que podem ocorrer com os dados das pessoas físicas. Também foi apontada a dificuldade de as empresas colocarem em prática todas as regras prevista na lei.

Certo é que não há experiências suficientes que indicam o caminho a ser trilhado por empresas, sociedade e governo, a fim de chegarem ao nível de garantia desses direitos, como é desejado pela lei, ou seja, ainda não existe, no Brasil, jurisprudências robustas (casos de reiterados registros de incidentes envolvendo o uso de dados pessoais por entidades privadas) para indicar como essas questões se apresentam. Entretanto, são pontos que indicam a tradição de se preocupar em redigir leis somente depois de existir problemas a serem solucionados, termos em que justificam a inovação da lei.

Esgotados os conceitos relevantes da LGPD, passa-se para a próxima etapa deste artigo, que se concentra em mostrar o compartilhamento como uma das modalidades de tratamento de dados pessoais previstas na lei e a situação do titular dos dados diante dessa prática. Pelo motivo da complexidade e importância do assunto, o tema terá delimitação específica, considerando somente os dados pessoais comuns compartilhados entre entidades privadas.

2. O USO COMPARTILHADO DE DADOS PESSOAIS

O uso compartilhado de dados pessoais é entendido pela LGPD[26] como sendo toda forma de comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais, por órgãos e entidades públicas, no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

A LGPD, como relatado no tópico anterior, é uma lei com alta carga de conceitos; porém, ela não especificou o significado de cada forma de compartilhamento. Entretanto, considerando o compartilhamento entre entes privados, pode-se extrair do conceito posto na lei que o uso compartilhado consiste em variadas formas de circulação e acesso a dados pessoais, armazenados em banco de dados, que ocorrem entre as empresas. Na verdade, é uma das formas em que

[26] Vide artigo 5º inciso XVI-

a LGPD aborda o tema da mercantilização de dados pessoais, mas sem usar diretamente a expressão, na tentativa de alcançar as várias possibilidades que envolvam troca e acesso de dados pessoais[27].

Para entender melhor essa prática, agora regulamentada pela LGPD[28], toma-se como exemplo os aplicativos de músicas para celular. Para que uma pessoa possa ter acesso à plataforma, é preciso fornecer dados pessoais como nome e número no Cadastro de Pessoas Físicas (CPF). Entretanto, para ter acesso ao conteúdo e aos serviços *premium* oferecidos por aqueles aplicativos, é preciso fornecer também *e-mail*, idade, dados bancários, o que permite traçar um perfil individual. Aqui, verifica-se uma relação jurídica que envolve uso de dados pessoais mediante manifestação livre da vontade e do consentimento inequívoco do titular (tendo em vista que o usuário precisou realizar um cadastro fornecendo suas informações).

Ainda no mesmo exemplo, em alguns casos, não é preciso fazer um cadastro, basta vincular o aplicativo de música a uma rede social (exemplo: Spotify vinculado ao Facebook, o famoso "entre com o Facebook"). Além disso, é preciso concordar com as "políticas de Privacidade", chamadas usualmente de "li e concordo" (o que normalmente ninguém lê ou mesmo concorda de fato, mas seleciona simplesmente para ter acesso rápido), sendo isso o suficiente pra ter acesso ao serviço do aplicativo em questão. Aqui se mostra a prática do uso compartilhado dos dados pessoais: a partir do momento em que o titular permite à rede social ser sua base de acesso ao aplicativo; na verdade, ele está autorizando o aplicativo a usar dados pessoais já fornecidos para a rede social. Note que existe, nessa relação, um trânsito de informações entre as duas empresas, ou seja: o titular consente que as empresas façam uso, de forma compartilhada, de seus dados pessoais. Assim, uma empresa tem acesso ao banco de dados com informações pessoais da outra.

Essas relações jurídicas se apresentam de forma simples e encantadora devido à facilidade de acesso ao serviço. Contudo, é necessário ressaltar a complexidade quanto ao uso e à circulação dos dados pessoais. É possível identificar, no exemplo citado, que uma pessoa ocupa, ao mesmo tempo, a qualidade de titular dos dados e de consumidor. Ainda é possível verificar a relação entre as duas empresas, que consiste na reciprocidade das plataformas digitais e no compartilhamento de dados tratados por elas – somando-se a isso, também, que a relação jurídica se estabelece entre três pessoas, uma pessoa física e duas pessoas jurídicas (em alguns casos, pode envolver muitas outras empresas), e que essas pessoas jurídicas podem ser empresas multinacionais, ou seja, dados de pessoas brasileiras podem ser armazenados e usados em outro país, com leis diferentes.[29]

Muitos não fazem ideia de quantos direitos estão envolvidos nisso, nem da importância dos dados pessoais. Só no exemplo citado, poderão incidir regras consumeristas, contratuais, de proteção de dados, constitucionais e normas de reciprocidade com outros países.

---

[27] Parecer legislativo: relator Ricardo Ferraço: EMENDA Nº…– Cae (Substitutivo) Projeto de Lei do Senado Nº 330, de 2013. Artigo 3º, V -Comunicação: ato de revelar dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma; X -Difusão: ato de revelar dados pessoais a um ou mais sujeitos indeterminados diversos do seu titular, sob qualquer forma; XI -Interconexão: transferência de dados pessoais de um banco de dados a outro, mantido ou não pelo mesmo proprietário;

[28] A LGPD é a primeira lei federal brasileira que prevê o uso compartilhado de dados pessoais entre entes privados de forma abrangente a todos os setores privados. Antes era previsto somente em leis direcionada a setores privados específicos como o de crédito, e entre a administração pública. Vide Decreto nº 8777/2016, Lei de acesso a informação 12.527/2011

[29] Transferência internacional de dados pessoais como forma de uso compartilhado no artigo 5º, entretanto tem um capítulo inteiro reservado a esse assunto na LGPD. Vide capitulo V art. 33.

Atualmente, as informações pessoais são fornecidas (ou mesmo geradas) principalmente por meios eletrônicos, pelos quais são coletadas, armazenadas e usadas por empresas, que extraem o valor delas conforme seus interesses e compartilham essas informações com outras empresas, para que estas também possam extrair valor, e assim sucessivamente.

> Hoje é possível saber quais as preferências do usuário por meio de sites que acessa, ou mesmo das palavras que digitam em mecanismos de buscas, por exemplo, criando-se verdadeiros perfis acerca do cruzamento dos dados de conexão. A remuneração hoje não é mais calculada por meio do número de acessos aos websites, mas sim pelo número de cliques em determinado link (*cots per click*). Assim se calculam os preços dos contratos de publicidade por intermédio de estimativa de consumidores em potencial, especificados pelas informações que disponibilizam sobre si mesmos revelando preferencias, opções religiosas, sexuais, a cidade em que vivem etc. (MARTINS, 2016, p.54)

Com isso, as informações pessoais estão em um constante trânsito, com circulação desordenada, sendo difícil conhecer seu caminho e impor regras. Contudo, para as empresas, é uma facilidade para obtenção de resultados e lucros.

Existem notícias de incidentes com dados pessoais, em que uma empresa teve acesso ao banco de dados de outra empresa, como foi o caso da empresa Cambridge Analítica (especializada em análise de dados), que teve acesso a dados tratados pelo Facebook e foi acusada de traçar perfis e manipular informações de cidadãos americanos, com o intuito de influenciar nas eleições dos Estados Unidos.

Note-se que, nesse caso, houve compartilhamento de informação entre Facebook e Cambridge[30], ou seja: ocorreu o acesso ao banco de dados de uma empresa por outra, mas não houve consentimento dos usuários para as duas empresas. Esse é um dos exemplos clássicos que podem ser encontrados em quase todos os jornais e artigos sobre o assunto de proteção de dados, pois mostra claramente a dificuldade de uma pessoa controlar suas informações, ainda que a lei disponibilize ferramentas para isso. Assim, a posição do indivíduo diante da mercantilização e manipulação dos dados pessoais se mostra consideravelmente desproporcional[31].

Ainda que a LGPD imponha a regra do consentimento específico do titular (requisito basilar para o compartilhamento), o respeito ao princípio da boa-fé e a outros valores em que as relações jurídicas de uso de dados pessoais devem observar, estes apresentam-se de forma frágil, podendo ser ignorados e violados, sem que o titular perceba.

3. A VULNERABILIDADE E OS RISCOS À PRIVACIDADE

A dificuldade de controle diante da intensa circulação de informações pessoais entre as empresas fragiliza as barreiras da privacidade, permitindo que esta seja invadida, visto que, no uso compartilhado, uma única empresa é capaz de deter muitos tipos de informações sobre muitas pessoas, sem precisar do fornecimento direto do titular.

Nesse sentido, se uma empresa tem acesso ao banco de dados da farmácia, do supermercado, do aplicativo de música, do aplicativo de GPS, da faculdade e da academia que uma pessoa ou um grupo de pessoas frequentam normalmente, por meio de cruzamento de dados e de tecnologias inteligentes, é possível identificar cada uma dessas pessoas e saber muitas coisas da vida

[30] https://www1.folha.uol.com.br/mundo/2018/05/consultoria-pivo-de-polemica-sobre-privacidade-no-facebook-vai-fechar-diz-jornal.shtml- Depois do incidente tanto a Cambridge Analíticas quanto a Facebook perderam muita credibilidade no mundo dos negócios.

[31] Fala-se em mercantilização pois dados pessoais são como componentes, parte dos elementos contidos em um bancos de dados. Banco de dados também entendido como produto eletrônico que pode ser comercializado.

privada delas (como preferências, intimidades, relacionamentos etc.) e assim controlá-las, por meio da manipulação dos dados a distância. Isso relembra o fenômeno *Panópticon* citado no primeiro tópico deste artigo, no qual as pessoas são vigiadas em tempo integral, mas não têm a possibilidade de descobrir quem é o vigilante.

Como se pode notar atualmente, se uma pessoa realizar uma pesquisa na internet sobre determinado objeto, logo aparecem propagandas daquilo que se pesquisou na caixa de *e-mail* pessoal, ou, no canto das páginas dos *sites* que ela visitar, estará lá uma propaganda oferecendo aquele produto e outras opções com as cores que a pessoa mais gosta – e ainda com frete grátis, indicando a região onde mora[32]. A questão é: onde conseguiram tantas informações? Endereço de *e-mail*, cores preferidas e região onde mora? Essas questões são difíceis de saber, pois é inviável controlar a intensa circulação das informações de caráter pessoal, quantas pessoas ou entidades tiveram acesso a elas ou mesmo refazer o caminho percorrido pela informação pessoal.

A lei estabelece que a Agencia Nacional de Proteção de Dados (ANPD) pode exigir das empresas um relatório de impacto[33], com descrição detalhada de todo tratamento de informações pessoais contidas nos bancos de dados, como um mecanismo de fiscalização; uma espécie de boletim de ocorrência, indicando também a criação de novos cargos e setores[34]; e a adoção de técnicas e normas de segurança da informação que essas empresas deverão instalar como medidas de proteção dos dados tratados – o que se torna oneroso tanto para as empresas quanto para os titulares que precisam ter a segurança. Contudo, mesmo com muitos esforços, percebe-se que é complicado refazer, ou mesmo demostrar, todo o caminho percorrido pelos dados durante a prática do compartilhamento, para obter o controle da informação.

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados podendo escapar a ele próprio o grau de periculosidade do uso desses dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições é totalmente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser um álibi de um poder público desejoso de esquivar-se de novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória, dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente, poderá sair com perdedor. (RODOTÀ, 2008, p. 37)

É o poder de saber tanta informação sobre as pessoas que faz com que a privacidade seja diminuída, a ponto de deixar o indivíduo titular dos dados de mãos atadas, fornecendo informação e desfrutando dos produtos e serviços oferecidos, visto que é oneroso e inviável para o titular controlar suas informações.

É nesse sentido que o uso compartilhado fere o direito de privacidade, pois uma pessoa não é capaz de controlar o trânsito de suas próprias informações ou de exercer seu direito de ser deixado só, ou mesmo escolher aquilo que está disposto a revelar, tendo a necessidade de se expor a todo momento (algumas vezes por impulso; outras vezes, sem escolha), para participar de uma sociedade movida e alimentada por informação, deixando rastros que são registrados por quem tem interesse na informação pessoal.

---

[32] SILVA, Hannah Ferreira e. A Nulidade das Cláusulas de Compartilhamento de Dados Pessoais nos Contratos de Adesão sob a Perspectivada Proteção Constitucional e Consumerista. 2018 Pag.46.

[33] Vide artigo 5º XVII - relatório de impacto à proteção de dados pessoais: documento emitido pelas empresas contendo a descrição de todos os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Ver também artigo 38.

[34] Vide artigo 5º VI, VII, VIII. Agentes de tratamento e encarregados, responsáveis pelo tratamento de dados pessoais.

No entanto, a simples justificativa da dificuldade de controle sob as informações que circulam não é suficiente para alegar que o uso compartilhado fere o direito de privacidade, tendo em vista que a lei disponibiliza mecanismos de controle e regras de tratamento de dados, mas a legalidade pura e simples não emana a justa posição do indivíduo. É a soma de vários fatores que ocorrem na prática do compartilhamento que fragiliza os valores fundamentais que formam as barreiras da privacidade, tornando vulnerável o titular.

O fato de o indivíduo ser observado por meio da análise de dados pessoais, somado à dificuldade de controle e à necessidade dele de expor suas informações, *versus* a capacidade das tecnologias informacionais inteligentes e a facilidade de obtenção de informações pessoais que uma empresa pode possuir transforma o indivíduo numa espécie de objeto e coloca os interesses mercadológicos numa posição hierarquicamente acima da privacidade.

A lógica se inverte: as instituições têm o controle das informações que querem usar, sabem muito sobre a vida privada de uma pessoa ou de várias pessoas, e os indivíduos usam suas informações e as fornecem como se fossem uma moeda de troca, passando a ser meros fornecedores.

Entretanto, não há balança nivelada, visto que o titular fornece seus dados e permanece na confiança de que as instituições irão usá-los de forma idônea[35], em um espaço virtualizado com uma imensa dificuldade de controle, apesar de muito acessível. O que na realidade se verifica é uma vulnerabilidade do titular, que:

> [...] ao contrário do que podemos ver nas relações de consumo, nas quais a vulnerabilidade pode até ser quase nula, como poderia ser o caso de consumidores com maior expertise técnica, ou poder econômico superior ao do fornecedor, ao falarmos de tratamento de dados isso não é assim, pois o mesmo pode ser dá, inclusive sem o consentimento do titular, ou seja dificilmente uma pessoa natural, deixaria de se encontrar na posição de fragilidade, pois os dados , por serem na grande maioria dos casos intangíveis, não permitem ao titular certeza jurídica de seu tratamento. (COTS; OLIVEIRA, 2018, p. 60)

Assim como no direito do consumidor encontra-se a figura da inversão do ônus da prova como instrumento da proteção ao consumidor (parte mais frágil na relação de consumo), na Lei de proteção de dados também é previsto esse instrumento. Entretanto, a diferença se concentra no fato de que, para os titulares dos dados, inexiste a condição de expertise, ou seja, a vulnerabilidade precisa ser presumidamente considerada, sem precisar de uma avaliação prévia da condição de ser parte mais frágil e se eximir do ônus, visto que, na possibilidade de contratação de serviço ou compra de produtos, a troca legitima é feita pela moeda e não por dados – e as empresas, querendo ou não, ao permitirem a outras empresas o acesso aos dados, ainda que informalmente, lucram com as transações de dados[36].

Verifica-se, no entanto, uma dupla vulnerabilidade: a primeira, no sentido de exposição dos dados; a outra, no sentido de que o titular nada ganha com o uso compartilhado – por isso essa vulnerabilidade precisa ser considerada de plano.

Assim, é necessário que sejam efetivados todos os mecanismos de proteção à privacidade e aos dados dos titulares, pois existem interesses em via de mão dupla, na qual o mercado tem a

[35] As relações jurídicas de tratamento de dados pessoais devem ser pautadas no princípio da boa-fé. Artigo 6º LGPD

[36] Art. 42. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. Assim a LGPD prevê a inversão do ônus da prova, mas ainda sem a possibilidade de considerar de plano a vulnerabilidade do titular.

necessidade de se alimentar de informações e os indivíduos têm a necessidade de expor seus dados de forma controlada.

Entretanto, só a legalidade não basta: tem que haver o mútuo respeito aos direitos envolvidos nas relações jurídicas de dados, tanto dos titulares quanto das empresas. Assim, as entidades privadas precisam ir além das regras contratuais e da cultura do "passa e repassa" de dados pessoais, com a tendência de incorporar os valores fundamentais como mecanismos de proteção e controle dos dados, no sentido de elevar a privacidade ao verdadeiro *status* de direito fundamental.

CONSIDERAÇÕES FINAIS

As inovações do mercado, aliadas às tecnologias informacionais, revelam o valor dos dados pessoais e mostram a fragilidade da privacidade do indivíduo em um cenário no qual dados pessoais ingressam no mundo das mercadorias.

O cenário apresentado utilizou o fenômeno "*Panópticon*" para demonstrar como os indivíduos são observados e como as informações são colhidas na era informacional. Mostrou também os mecanismos de proteção da privacidade e dos dados pessoais, bem como as formas de uso das informações pessoais previstas na LGPD, usando como enfoque o compartilhamento de dados pessoais para demonstrar que o direito de privacidade se encontra sobrepujado pelos interesses econômicos. Isso revela a vulnerabilidade do titular nas relações jurídicas que envolvem uso de dados pessoais, devido à dificuldade do exercício do direito à privacidade.

Faz-se necessário os titulares dos dados atentarem para a cultura da valorização das informações pessoais no mundo dos negócios, tendo em vista que o fornecimento dos dados muitas vezes acontecem de forma instantânea, bem como o consentimento, este pela pressa e necessidade dos titulares de acesso rápido ao que se pretende.

Nesse sentido, inúmeras são as razões pelas quais os titulares dos dados não se atentam para suas informações pessoais, principalmente quando se trata do ambiente digital – no qual não se pode ver a olho nu, ou em tempo real, o que realmente acontece com os dados. Uma dessas razões pode orbitar o fato de que a sociedade ainda não tem a experiência necessária ou, melhor, que não houve ainda um despertar social sobre o valor das informações na era digital. Na verdade, nem as autoridades políticas, nem o judiciário, nem os próprios cientistas de dados estão preparados para a avalanche de problemas que o uso e o compartilhamento desenfreado de informações pessoais podem gerar.

No cenário histórico mundial, em que se verifica a formação de nações sob um pano de fundo de lutas por direitos e revoluções, é possível verificar que a cultura e os costumes ensinados de geração em geração são os de que os documentos e as informações pessoais comprovam que o indivíduo está de acordo com os deveres de cidadão, mostrando assim que esse indivíduo pode desfrutar dos direitos e garantias, dos insumos e dos bens de seu país. Essa ideia não é aceitável em ambientes virtuais, e um dos motivos é a inexistência de fronteiras neles. Entretanto, essa cultura está sofrendo muitas alterações, pois envolve questões políticas e abre um diálogo que desperta o interesse de entidades públicas e privadas, das ciências tecnológicas e do direito, da sociedade e dos governos, o que traz à tona uma nova discursão – que, devido à sua alta complexidade, merece um estudo aprofundado, à parte.

Não se trata de escolher valores, mas é necessário realizar balanceamentos entre os interesses envoltos nas relações de uso de dados e os direitos relacionados ao intenso trânsito de informações pessoais, no sentido de traçar limites que permitam ao titular controlar e exercer o

direito à privacidade e, às empresas, usar informações pessoais sem inverter a lógica proposta na lei e sem que o ônus do controle dos dados se transforme em tormenta para o titular.

REFERÊNCIAS

ALVIM, José Eduardo Carreira. **Processo de Habeas Data.** Curitiba/PR: Juruá, 2013.

AMARAL, Fernando. **Introdução a ciências de dados. Mineração de dados e big data**. Rio de Janeiro: Alta Books, 2016.

BITAR, Carlos Alberto. **Os Direitos da Personalidade**. 8. ed. São Paulo: Saraiva, 2015.

BRASIL. **Constituição Federal** (1988). Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 08 mar. 2019.

BRASIL**. Lei Federal nº 13.709 de 14 de agosto de 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 08 mar. 2019.

BRASIL. **Lei. Nº 10.406, de 10 de Janeiro de 2002. Código Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 08 mar. 2019.

BRASIL. **Lei Nº 8.078, de 11 de Setembro De 1990.** Código de defesa do consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 08 mar. 2019.

BRASIL. **Lei Nº 12.965, de 23 de Abril de 2014**. Marco Civil Da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 mar. 2019.

BRASIL. **Decreto legislativo n° 8789, de 29 de junho de 2016.** Compartilhamento de base de dados na administração pública. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8789.htm. Acesso em: 09 mar. 2019.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial Nº 1.348.532**. Rel. Min. Luis Felipe Salomão. São Paulo: 2017. Disponível em: http://www.stj.jus.br/docs_internet/informativos/PDF/Inf0616.pdf. Acesso em: 22 mar. 2019.

COPETTI, Rafael; MIRANDA, Marcel Andreata De.*et al.* **Autodeterminação Informativa e Proteção de Dados: Uma Análise Crítica da Jurisprudência Brasileira. Direito, governança e novas tecnologias**. Florianópolis: CONPEDI, 2015. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/j6023guzncw4in57.pdf Acesso em: 04 mar. 2019.

COTS, Marcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada.** São Paulo: Thomson Reuters Brasil, 2018.

CUEVA**.** Ricardo Villas Boas. **A Insuficiente Proteção de Dados Pessoais no Brasil**. Rio de Janeiro: Revista Justiça e Cidadania, nov. 2016. Disponível em: https://www.editorajc.com.br/wp-content/uploads/2016/12/RJC-195_.pdf. Acesso em: 13 out. 2018.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. Teoria Geral do Direito Civil. vol. 1, 35 ed. São Paulo: Saraiva, 2018.

DONEDA, Danilo. **A Proteção Dos Dados Pessoais como um Direito Fundamental.** Rio de janeiro. Revista Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 06 mar. 2019.

DONEDA, Danilo Cesar Maganhoto. *et al*. **Considerações iniciais sobre inteligência artificial, ética e autonomia Pessoal.** Revista de Ciências Jurídicas - Pensar. Fortaleza, v. 23, n. 4. out./dez. 2018. Disponível em: https://periodicos.unifor.br/rpen/article/view/8257/pdf. Acesso em: 04 mar. 2019.

DONEDA**,** Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Escola Nacional de Defesa do Consumidor. Caderno de investigações Cientificas. Brasília: 2010. Disponível em: https://www.defesadoconsumidor.gov.br/images/manuais/vol_2_protecao_de_dados_pessoais.pdf. Acesso em: 03 mar. 2019.

FERNANDES**,** Bernardo Gonçalves. **Curso de Direito Constitucional**. 9. ed. Salvador/Bahia: JusPodvun, 2017.

FOUCAULT. Michel. **A Verdade e as Formas Jurídicas**. Rio de Janeiro, Nau: 2005. E-book

FONTES**,** Jose Igor Alves. **Dados Pessoais Digitais e seu Tratamento No Ordenamento Jurídico Brasileiro.** Trabalho de Conclusão de Curso (Graduação em direito) -UFRN. Natal/RN: Biblioteca Setorial CCS, 2018. Disponível em: https://monografias.ufrn.br/jspui/bitstream/123456789/7356/1/Dados%20Pessoais_Fontes_2018.pdf. Acesso em: 05 mar. 2019.

GHISI, Silvano. Responsabilidade Civil em Matéria de Proteção a Dados Pessoais no Ordenamento Jurídico Brasileiro. **Revista Jurídica**. Pato Branco/ PR, v. 2, n. 3, p. 273-288, set. 2018. Disponível em: http://revistajuridica.fadep.br/index.php/revistajuridica/article/view/80. Acesso em: 05 mar. 2019.

MACHADO, Ronny Max. FUJITA, Jorge Shiguemitsu. **Os impactos da sociedade da informação no direito à Privacidade da pessoa natural e da pessoa jurídica**. RTJ/ STF. São Paulo/SP: 2018. Disponível em: https://periodicos.uninove.br/index.php?journal=thesisjuris&page=article&op=view&path%5B%5D=11270. Acesso em: 05 mar. 2019.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet:** uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (raduação em Direito) -UNB. Brasília/DF. 2017. Disponível em: http://bdm.unb.br/bitstream/10483/18883/1/2017_LuizaFernandesMalheiro.pdf. Acesso em: 13 out. 2018.

MARTINS, Guilherme Magalhães. **Contratos Eletrônicos de Consumo**. 3 ed. Campos Elísios/SP: Atlas, 2016.

MAXIMILIANO, Carlos. "**Hermenêutica e Aplicação do Direito**". 20 ed. Rio de Janeiro: Forense, 2011.

MAZZA, Alexandre**. Manual de Direito Administrativo.** 7. ed. São Paulo: Saraiva Jur, 2017.

MORASSUTTI, Bruno Schmitt. **Considerações sobre bancos de dados e o comércio de informações**. Direito e Justiça. Rio Grande do Sul: Pucrs, 2015. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/fadir/article/viewFile/21428/13325. Acesso dia 04 mar. 2019.

FERRAÇO, Ricardo. **Parecer da comissão de assuntos econômicos**. Publicado em 30/05/2018. Senado Federal. 2018. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7751914&ts=1594012451916&disposition=inline. Acesso em: 01 maio 2019.

PINHEIRO**,** Patrícia Peck. **Direito Digital**. 2° ed.. São Paulo: Saraiva, 2008.

PINHEIRO**,** Patrícia Peck. **Proteção de dados pessoais. Comentários à lei 13.709/2018 (LGPD)**. São Paulo: Saraiva Jur, 2018.

RODOTÁ**,** Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Org. Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SANTANA, Héctor Valverde**.** VIANA, Rafael Souza. **O compartilhamento de dados e informações pessoais de consumidores: o abuso dos fornecedores e as propostas apresentadas no PLS 181/2014.** Brasília: Rev. Bras. Polít. Públicas, v. 7, n 1, 2017. Disponível em: https://search.proquest.com/openview/8bbe20db1f77dfc3cf4e374451bf3162/1?pq-origsite=gscholar&cbl=2031897. Acesso em: 05 mar. 2019.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais uma Teoria Geral dos Direitos Fundamentais na Perspectiva Constitucional.** 11. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2012.

SILVA, Hannah Ferreira e. **A Nulidade das Cláusulas de Compartilhamento de Dados Pessoais nos Contratos de Adesão sob a Perspectiva da Proteção Constitucional e Consumerista.** Trabalho de Conclusão de Curso (Graduação em Direito) -UFPB, Santa Rita/Paraíba, 2018. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/11495/1/HFS14062018.pdf. Acesso em: 05 mar. 2019.

SILVA, Alexandre Ribeiro. **A proteção de dados no Brasil:** A tutela do direito à privacidade na sociedade da informação. Dissertação de Mestrado em Direito, Faculdade de Direito - UFJF, Juiz de Fora/MG. 2017. Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/5374. Acesso em: 04 mar. 2019.

SCHEREIBER, Anderson. **Direitos da Personalidade**. 2. ed. -São Paulo: Atlas, 2013. E-book.

VIEIRA, Tatiana Malta. **Direito a privacidade da sociedade da informação**. Dissertação de Mestrado em Direito – Faculdade de Direito, UnB, Brasília. 2007. Disponível em: http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf. Acesso dia 03 nov. 2019.

Submetido em: 10 set. 2019.

Aceito em: 23 out. 2020.