UNIVERSIDADE FEDERAL DE SERGIPE – UFS
PRO-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA – POSGRAP
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

JEFISON DE ANDRADE DAS CHAGAS

AS MUDANÇAS TRAZIDAS PELA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES NA PROTEÇÃO DE DADOS PESSOAIS DOS CONSUMIDORES PELAS EMPRESAS PRIVADAS

SÃO CRISTÓVÃO (SE)
2023

JEFISON DE ANDRADE DAS CHAGAS

AS MUDANÇAS TRAZIDAS PELA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES NA PROTEÇÃO DE DADOS PESSOAIS DOS CONSUMIDORES PELAS EMPRESAS PRIVADAS

Dissertação apresentada ao Programa de Pós-Graduação em Direito, como requisito parcial à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Lucas Gonçalves da Silva.

SÃO CRISTÓVÃO (SE)
2023

JEFISON DE ANDRADE DAS CHAGAS

AS MUDANÇAS TRAZIDAS PELA LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES NA PROTEÇÃO DE DADOS PESSOAIS DOS CONSUMIDORES PELAS EMPRESAS PRIVADAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe, como parte dos requisitos para a obtenção do Título de Mestre em Direito. Esta dissertação foi julgada e aprovada pela comissão abaixo assinada em ___ de _____ de 2023.

São Cristóvão, Sergipe, Brasil

_____
Prof. Dr. Lucas Gonçalves da Silva – Orientador
Universidade Federal de Sergipe – UFS

_____
Prof. Dr. Henrique Ribeiro Cardoso – Membro Interno
Universidade Federal de Sergipe - UFS

_____
Prof. Dr. Liton Lanes Pilau Sobrinho – Membro Externo
Universidade do Vale do Itajaí - UNIVALI

Dedico este trabalho aos meus familiares, aos colegas de curso, aos professores e a todos aqueles que direta ou indiretamente contribuíram para esta conquista.

AGRADECIMENTOS

Primeiramente, antes de tudo, agradeço a Deus pela força e coragem de encarar mais um desafio, tarefa árdua, que requer dedicação e força de vontade para prosseguir, onde posso afirmar com toda certeza que sem esta força e apoio nada, absolutamente nada, seria possível. Gratidão!

Agradeço ao meu orientador, prof. Lucas Gonçalves da Silva, pelo incentivo para o ingresso na academia, por todo apoio, ensinamentos, compreensão, amizade e força durante esses dois anos.

À minha querida profa. Clara Angélica Gonçalves Dias, por todo incentivo e coorientação, que fora de suma importância.

Aos meus pais, Maria José e Jailton, minhas irmãs, Jaqueline, Jéssica e Jamile, e meu irmão Janisson (*in memorian*), que mesmo distantes emanaram as melhores energias. Vocês, sem sombra de dúvidas, são o meu alicerce, minha fonte de inspiração.

Aos colegas do mestrado que me ajudaram nos momentos mais distintos, onde compartilhamos juntos as dificuldades nas preparações e apresentações dos seminários, pelo companheirismo e respeito, onde respeitamos - apesar das controvérsias - as limitações do próximo, independente da posição que estivéssemos, seja na de Relator ou de Revisor. Não podendo esquecer do melhor momento, quando da finalização de cada semestre, com a entrega dos artigos científicos, que nos dava a sensação de dever cumprido, por estarmos avançando mais uma etapa. Obrigado a cada por tudo!

Ao prof. Carlos Augusto Alcântara Machado, que tanto me ensinou, pelo seu jeito peculiar de ser e passar adiante com maestria seus conhecimentos. Obrigado por ter compartilhado saberes, e por nos dá a oportunidade de banharmos da sua fonte de sabedoria.

A todos os demais professores do Programa de Pós-Graduação em Direito, da Universidade Federal de Sergipe, que dispuseram seu tempo para nos instruir, saibam que cada um marcou de certo modo, a minha jornada. Parabéns a todos pela competência, eficiência, ética e comprometimento com o ensino de qualidade.

A André Gentil que ao longo dos semestres tem suportado tamanha impaciência, ansiedade e desesperos. Sem o seu apoio tudo seria mais difícil.

A todos os meus amigos(as), que acompanharam os obstáculos e vibraram comigo desde o ingresso, especialmente a Tarcísio Barreto, meu amigo e sócio, que diariamente foi obrigado a suportar minhas descortesias no escritório. A vocês, meu muito obrigado por terem tornado meus dias mais leves e divertidos.

Por derradeiro, e não menos importante, agradeço a todos que direta e indiretamente torceram e acreditaram no projeto. Tenham certeza que vocês são como combustível, me deram força para seguir adiante.

A todos, meu muito obrigado.

Avante!

LISTA DE SIGLAS E ABREVIATURAS

AC	-	Apelação Cível
ADCT	-	Ato das Disposições Constitucionais Transitórias
ADIN	-	Ação Direta de Inconstitucionalidade
ANADEC	-	Associação Nacional de Defesa da Cidadania e do Consumidor
ANATEL	-	Agência Nacional de Telecomunicações
ANPD	-	Autoridade Nacional de Proteção de Dados
CADH	-	Convenção Americana sobre Direitos Humanos
CC	-	Código Civil
CDC	-	Código de Defesa do Consumidor
CFOAB	-	Conselho Federal da Ordem dos Advogados do Brasil
CP	-	Código Penal
CPF	-	Cadastro de Pessoa Física
CRFB/1988	-	Constituição da República Federativa do Brasil de 1988
CTN	-	Código Tributário Nacional
DF	-	Distrito Federal
DHNET	-	Direitos Humanos na Internet
DPI	-	*Deep Packet Inspection* (Inspeção Profunda de Pacotes de Rede)
DPO	-	*Data Protection Officer* (Encarregado dos Dados)
FCPA	-	*Foreing Corrupt Practices Act* (Lei de Práticas de Corrupção no Exterior)
GPDR	-	*General Protection Data Regulation* (Regulamento Geral sobre a Proteção de Dados
IBGE	-	Instituto Brasileiro de Geografia e Estatística
LAI	-	Lei de Acesso a Informação
LC	-	Lei Complementar
LGPD	-	Lei Geral de Proteção de Dados
LINDB	-	Lei de Introdução as Normas do Direito Brasileiro
MCI	-	Marco Civil da Internet

MP	-	Medida Provisória
NSA	-	*National Security Agency*
ONG	-	Organização Não-Governamental
PEC	-	Proposta de Emenda Constitucional
PL	-	Projeto de Lei
RG	-	Registro Geral
RGPD	-	Regulamento Geral da Proteção de Dados
RIPD	-	Rede Ibero-americana de Proteção de Dados
SMP	-	Serviço Móvel Pessoal
STF	-	Supremo Tribunal Federal
STFC	-	Serviço Telefônico Fixo Comutado
STJ	-	Superior Tribunal de Justiça
TICs	-	Tecnologia da Informação e Comunicação
UE	-	União Europeia

RESUMO

O presente estudo objetiva verificar, com base na doutrina, legislação e jurisprudência se a proteção trazida pela Lei Geral de Proteção de Dados (LGPD) tem sido suficiente para resguardar a proteção de dados dos consumidores nas empresas privadas em tempos de evolução tecnológica. Para tanto, expõe a evolução legislativa da proteção de dados no Brasil, buscando identificar se há harmonia entre a LGPD e o Código de Defesa do Consumidor (CDC) no sistema jurídico brasileiro; analisar a estrutura da LGPD, seus principais conceitos, nomenclaturas, princípios fundamentadores, aspectos positivos, negativos e mecanismos de *compliance*; compreender a LGPD e suas peculiaridades quando aplicadas às empresas privadas, especialmente no que concerne às vulnerabilidades observadas no tratamento de dados dos consumidores; e investiga o posicionamento jurisprudencial a respeito das violações à proteção de dados pessoais antes e após o advento da Lei nº 13.709/2018, bem como os reflexos do consentimento na avaliação da ocorrência de violação de dados pessoais, especialmente os dados pessoais sensíveis. A metodologia empregada nesta dissertação foi a pesquisa teórico-dogmática, já que optou-se pela pesquisa bibliográfica, realizada a partir de uma revisão de literatura em artigos jurídicos e doutrinas; e pela pesquisa documental em legislações e jurisprudência com o propósito de responder ao problema delineado com vistas a encontrar uma solução para mitigar o conflito que se formou em torno da evolução tecnológica e a necessária proteção de dados dos consumidores de empresas privadas. Foi visto que aliando a positivação à conscientização e educação, o direito será capaz - como já vem se esforçando - de responder às novidades propostas pela tecnologia da informação, com a realização do seu valor fundamental: a pessoa humana, sua dignidade e a segurança de seus dados. Concluiu-se por derradeiro que, considerando que o ciberespaço é um ambiente digital, cuja matéria-prima para sua sustentação, e fomento do capitalismo informacional, é o dado pessoal, resta evidente que o seu uso de maneira irrestrita e incondicionada, pode afetar direitos individuais dos consumidores. Assim, encarar a informação como um produto/serviço possibilita o reconhecimento de que ao seu uso devem ser aplicadas as regras de proteção do consumidor, pois esse continua sendo a parte vulnerável na relação de consumo com o fornecedor. Entende-se que cada empresa possui as suas especificidades, a depender dos seus modelos de negócio, do mercado em que atua e do seu relacionamento com os clientes e parceiros e que, em virtude disso, o compartilhamento dos dados e a celebração de contratos podem ganhar diferentes nuances. Todavia, a base, em todos eles, deve consistir na transparência e na responsabilidade, por meio de demonstração de clara e evidente preocupação com a segurança dos dados dos consumidores e adoção de atitudes que possam assegurá-la.

Palavras-chave: Dados pessoais. Lei Geral de Proteção de Dados. Direito à Privacidade. Consentimento.

ABSTRACT

The present study aims to verify, based on doctrine, legislation and jurisprudence, if the protection brought by the General Data Protection Law (LGPD) has been sufficient to safeguard the protection of consumer data in private companies in times of technological evolution. To this end, it exposes the legislative evolution of data protection in Brazil, seeking to identify whether there is harmony between the LGPD and the Consumer Defense Code (CDC) in the Brazilian legal system; analyze the structure of the LGPD, its main concepts, nomenclatures, fundamental principles, positive and negative aspects and compliance mechanisms; understand the LGPD and its peculiarities when applied to private companies, especially with regard to the vulnerabilities observed in the processing of consumer data; and investigates the jurisprudential position regarding violations of personal data protection before and after the enactment of Law 13,709/2018, as well as the consequences of consent in assessing the occurrence of violation of personal data, especially sensitive personal data. The methodology used in this dissertation was the theoretical-dogmatic research, since we opted for bibliographical research, carried out from a literature review on legal articles and doctrines; and by documentary research on legislation and jurisprudence with the purpose of responding to the problem outlined with a view to finding a solution to mitigate the conflict that formed around the technological evolution and necessary protection of consumer data from private companies. It was seen that by combining positivization with awareness and education, the law will be able - as it has been striving - to respond to the novelties proposed by information technology, with the realization of its fundamental value: the human person, his dignity and the security of your data. It was finally concluded that, considering that cyberspace is a digital environment, whose raw material for its support, and promotion of informational capitalism, is personal data, it remains evident that its use in an unrestricted and unconditional way, can affect rights individual consumers. Thus, viewing information as a product/service makes it possible to recognize that consumer protection rules must be applied to its use, as this remains the vulnerable part in the consumption relationship with the supplier. It is understood that each company has its specificities, depending on its business models, the market in which it operates and its relationship with customers and partners and that, as a result, sharing data and signing contracts can gain different nuances. However, the basis, in all of them, must consist of transparency and responsibility, through the demonstration of clear and evident concern with the security of consumer data and the adoption of attitudes that can ensure it.

Keywords: Personal data. General Data Protection Act. Right to Privacy. Consent.

SUMÁRIO

INTRODUÇÃO **10**
1 EVOLUÇÃO LEGISLATIVA DA PROTEÇÃO DE DADOS NO BRASIL **14**
1.1 Os dados pessoais no ciberespaço na sociedade de consumo **14**
1.2 Diplomas legais que têm previsão quanto à proteção de dados **16**
1.3 Harmonia da Lei Geral de Proteção de Dados – LGPD no sistema jurídico brasileiro **20**
1.3.1 Harmonia entre a LGPD e o CDC 25
1.4 Dados Pessoais e Processo de Anonimização à luz da LGPD **29**
2 ESTRUTURA DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD **33**
2.1 Entendendo a estrutura da LGPD **33**
2.2 Principais conceitos e nomenclaturas **35**
2.3 Tratamento dos dados e princípios que fundamentam a LGPD **40**
2.4 Aspectos positivos e negativos da LGPD **48**
2.5 Os mecanismos de *compliance* **55**
3 A LEI GERAL DE PROTEÇÃO DE DADOS APLICADA ÀS EMPRESAS PRIVADAS **64**
3.1 Principais vulnerabilidades **64**
3.2 Dos responsáveis diretos pelo tratamento dos dados pessoais **67**
3.3 Do Direito à Privacidade **71**
3.4 A questão do Consentimento **81**
3.4.1 O Consentimento *versus* o Princípio da Primazia da Realidade 82
3.4.2 O Consentimento à Luz do princípio da boa fé objetiva 85
3.4.3 O necessário equilíbrio entre o legítimo interesse e o consentimento 92
3.5 Jurisprudência pertinente e expectativas com relação à LGPD **95**
CONCLUSÃO **103**
REFERÊNCIAS **109**

INTRODUÇÃO

Vive-se hodiernamente uma época em que se observa grande "exposição midiática". As pessoas não conseguem mais viver desconectadas e diariamente uma quantidade muito grande de informações e dados pessoais são veiculados na internet dando azo a uma série de violações a direitos fundamentais. Essas violações, por sua vez, têm levado à mobilização de esforços para contê-las, a exemplo da Lei Geral de Proteção de Dados (LGPD), sugerindo que se pense sobre até que ponto poder-se-ia considerar razoável limitar a divulgação destas informações na internet ante ao risco de mitigar o avanço tecnológico.

Pesquisas que demonstrem caminhos para compatibilizar estas duas realidades (proteção de dados pessoais *versus* desenvolvimento tecnológico) são relevantes tendo em vista que limitar excessivamente a divulgação de dados pessoais e permitir que o avanço tecnológico continue sem impor a ele nenhum limite e regulamentação parecem não ser razoáveis.

Ante à realidade exposta, a questão que norteou esta pesquisa foi: a proteção trazida pela LGPD tem se mostrado suficiente para resguardar a proteção de dados de consumidores de empresas privadas em tempos de evolução tecnológica?

Neste trilhar, o objetivo geral deste estudo foi verificar, com base na doutrina, legislação e jurisprudência se a proteção trazida pela LGPD tem sido suficiente para resguardar os dados pessoais dos consumidores de empresas privadas em tempos de evolução tecnológica e de crescimento do comércio eletrônico.

Para cumpri-lo, os seguintes objetivos específicos foram delimitados: expor a evolução legislativa da proteção de dados no Brasil, buscando identificar se há harmonia entre a LGPD e o CDC no sistema jurídico brasileiro; analisar a estrutura da LGPD, seus principais conceitos, nomenclaturas, princípios fundamentadores, aspectos positivos, negativos e mecanismos de *compliance*; compreender a LGPD e suas peculiaridades quando aplicadas às empresas privadas, especialmente no que concerne às vulnerabilidades observadas no tratamento de dados dos consumidores; e investiga o posicionamento jurisprudencial a respeito das violações à proteção de dados pessoais antes e após o advento da Lei nº 13.709/2018, bem como os reflexos do consentimento na avaliação da ocorrência de violação de dados pessoais, especialmente os dados pessoais sensíveis.

O interesse pelo tema surgiu, pois, não se pode negar que a Internet, propiciou a aproximação virtual dos indivíduos, alterando substancialmente a forma como as pessoas (naturais e jurídicas) se relacionam. No entanto, pela perspectiva jurídica – notadamente, no que concerne à proteção de dados pessoais em âmbito global, nota-se que a referida evolução das Tecnologias da Informação e Comunicação (TICs), não veio seguida da necessária evolução jurídica que pudesse possibilitar a identificação e responsabilização adequada daquelas empresas, notadamente as envolvidas com o comércio eletrônico, que não conseguem resguardar os dados pessoais de seus consumidores.

O conjunto de direitos fundamentais em um dado momento entrou em conflito. Com o direito à privacidade e à informação não será diferente; eles também entraram em conflito. No entanto, existe toda uma dogmática de interpretação e ponderação desse conflito. Assim, é bom conhecer o que a LGPD não conseguiu trazer para racionalizar esse problema, pois, mesmo a lei não tendo disciplinado algo em específico, existe uma dogmática constitucional, civil e penal que pode, complementarmente, ser empregada.

Entende-se que as novas TICs operaram mudanças significativas nas relações sociais e, assim como já ocorre em outras áreas jurídicas, é preciso que o Direito as examine objetivando assegurar o seu desenvolvimento (especialmente nas relações de consumo) sem que as garantias individuais e coletivas dos cidadãos sejam violadas.

Assim, com esta dissertação busca-se demonstrar que a justificativa de toda evolução econômica só tem razão de ser caso se coadune com os axiomas que melhor expressam o atual sentimento jurídico e que atue na promoção e proteção da pessoa, bem como de seus valores e direitos fundamentais, no qual está incluída, inafastavelmente, a tutela dos dados pessoais. Melhor dizendo, o desenvolvimento tecnológico leva ao desenvolvimento econômico e impõe mudanças diversas, como é o caso do crescimento do *e-commerce*. Mas a evolução pela evolução, sem cautela, sem respeito aos princípios constitucionais e aos direitos da personalidade não tem razão de ser. É preciso que a evolução venha, sem impor violações à privacidade e aos dados pessoais dos consumidores.

O estudo se mostra relevante, pois, seja qual for a forma encontrada para se alcançar a satisfatória regulamentação sobre os impactos que a sociedade da informação proporciona no seio das relações que envolvem os indivíduos, é pacífico que esta é uma tarefa que ainda requer ampla contribuição da doutrina, além de diálogo entre os ordenamentos dos mais

diversos países, a fim de que seja possível se chegar a um ambiente normativo harmônico e capaz de atuar de forma conjunta e eficaz.

Referente à metodologia, nesta dissertação foi empregada a pesquisa teórico-dogmática, já que optou-se pela pesquisa bibliográfica, realizada a partir de uma revisão de literatura em artigos jurídicos e doutrinas; e a pesquisa documental em legislações e jurisprudência com o propósito de responder ao problema delineado com vistas a encontrar uma solução para mitigar o conflito que se formou em torno do direito à proteção de dados dos consumidores de empresas privadas em tempos de evolução tecnológica.

As áreas do conhecimento que esta pesquisa abrange possuem natureza transdisciplinar, perpassando diversas searas da Ciência do Direito, a exemplo do Direito Civil e o Direito Constitucional. No campo do Direito Civil, foi destacado o estudo da Lei n. 13.709/2018, que se refere à proteção de dados pessoais. No que tange à incidência do Direito Constitucional, foi destacado o conflito que aparentemente se impõe entre o direito à informação e o direito à privacidade em tempos de evolução tecnológica. Para tanto, foi realizada uma pesquisa bibliográfica.

Visando ao alcance dos objetivos geral e específicos propostos, esta dissertação encontra-se dividida em três capítulos.

O primeiro capítulo apresentou a evolução legislativa da proteção de dados no Brasil. Inicialmente, discutiu-se sobre os dados pessoais no ciberespaço em uma sociedade de consumo, passando-se na sequência a expor sobre os diplomas legais que trazem previsões sobre a proteção de dados. Ao final, procedeu-se à análise sobre a harmonia da LGPD no sistema jurídico brasileiro e, neste contexto, a harmonia entre a LGPD e o CDC; e, por fim, discutiu-se sobre os dados pessoais e o processo de anonimização à luz da LGPD.

O segundo capítulo apresentou uma análise crítica sobre a estrutura da LGPD. Em um primeiro momento, expôs os principais conceitos e nomenclaturas presentes na Lei; na sequência, analisou como deve ser feito o tratamento dos dados pessoais bem como os princípios que fundamentam a LGPD; e, por fim, expôs os aspectos positivos e negativos da LGPD, demonstrando a importância dos mecanismos de *compliance*.

Por fim, o terceiro capítulo abordou a LGPD aplicada às empresas privadas. Inicialmente, listou as principais vulnerabilidades a que as empresas e titulares dos dados estão expostos. Em seguida, listou a função e a responsabilidade dos responsáveis diretos pelo

tratamento dos dados pessoais; explicou o direito à privacidade ante ao tratamento dado aos dados pessoais antes e após a LGPD; e discutiu a questão do consentimento, contrapondo-o ao princípio da primazia da realidade, tomando por base o princípio da boa fé objetiva e defendendo o necessário equilíbrio entre o legítimo interesse e o consentimento. Por fim, foi apresentada a jurisprudência pertinente e as expectativas com relação à LGPD.

1 EVOLUÇÃO LEGISLATIVA DA PROTEÇÃO DE DADOS NO BRASIL

Este capítulo apresenta a evolução legislativa da proteção de dados no Brasil. Inicia discutindo os dados pessoais no ciberespaço em uma sociedade de consumo, passando, na sequência a expor os diplomas legais que trazem previsões sobre a proteção de dados. Ao final, analisa a harmonia da LGPD no sistema jurídico brasileiro e, neste contexto, a harmonia entre a LGPD e o CDC; e, por fim, discute os dados pessoais e o processo de anonimização à luz da LGPD.

1.1 Os dados pessoais no ciberespaço na sociedade de consumo

Nas três últimas décadas, a sociedade está passando por substanciais transformações na era das TICs, tendo em vista que estas conquistaram um espaço de grande relevância no meio social e, sendo o seu uso, atualmente, essencial no cotidiano societário (TAKANO; SILVA, 2020).

Com a sociedade hodierna submersa no ciberespaço, o acesso e a utilização de dados compreendem um grande e atraente ativo empresarial, repercutindo, consequentemente, no mercado de consumo. Pierre Levy, pesquisador em ciência da informação e da comunicação afirmou que:

> [...] a quantidade bruta de dados disponíveis se multiplica e se acelera. A densidade dos links entre informações aumenta vertiginosamente nos bancos de dados, nos hipertextos e nas redes. Os contatos transversais entre os indivíduos proliferam de forma anárquica. É o transbordamento caótico de informações, a inundação de dados [...] (LÉVY, 1999, p. 13).

Esses dados, por sua vez, são processados. O processamento dos dados permite, por exemplo, a segmentação dos consumidores a partir do refinamento das informações prestadas pelo próprio consumidor. Dessa forma, os dados passam a ser valiosos, uma vez que a identificação de tendências, antes baseada em amostragens, agora baseia-se no tratamento dos dados, aumentando a precisão sobre o padrão de consumo de cada indivíduo, facilitando a captura mental (MIRAGEM, 2019).

Para se ter uma maior compreensão sobre as informações colhidas pelo tratamento de dados, é possível obter localização, a interação do usuário consumidor em redes sociais, bem como seu comportamento de compra:

> O acesso e a utilização dos dados pessoais compreende um dos principais ativos empresariais na sociedade contemporânea e, ao mesmo tempo expressão dos riscos à privacidade frente às novas tecnologias da informação, repercutindo por isso, amplamente, no mercado de consumo e, consequentemente, sobre o direito do consumidor. O desenvolvimento da tecnologia da informação e a capacidade de processamento de imenso volume de dados variados (*Big data*) permite o refinamento das informações de modo a permitir uma série de utilidades, como a segmentação dos consumidores para quem se dirige uma oferta, maior precisão na análise dos riscos de contratação (seleção de risco), formação de bancos de dados com maior exatidão e eficiência do uso das informações coletadas, de modo a tornar a capacidade de acesso a tratamento de dados um dos valores mais relevantes atualmente. Esta nova capacidade de tratamento de dados permite a identificação de tendências, não mais baseadas em amostragens, mas no processamento da universalidade dos dados. Deste modo, aumenta a precisão e as possibilidades de resultados a serem obtidos, permitindo, dentre outros resultados, identificar padrões de consumo, conforme o comportamento de compra dos consumidores, sua localização (e.g. as discutidas técnicas de *geopricing*, pelas quais a determinação do preço de produtos ou serviços se dá conforme o lugar em que esteja o consumidor), a interação em redes sociais, ou a personalização da negociação com consumidores mediante uso de regras pré-determinadas ou de inteligência artificial (MIRAGEM, 2019, p. 2).

Ainda de acordo com Miragem (2019), os fornecedores anseiam cada vez mais pela fidelização dos consumidores a partir do recebimento de informações precisas e individualizadas dos consumidores por meio da segmentação oferecida pelo acesso aos dos dados pessoais, como, por exemplo, a navegação na internet e as reações e interações em espaços virtuais.

As redes sociais, a seu turno, atendem a um interesse comercial centrado nas informações pessoais colhidas dos usuários, a invasão da intimidade dos usuários tornou-se uma ação lucrativa, considerando a eficiência do *marketing* direcionado. Melhor adendo, as redes sociais são capazes de fazer com que os usuários produzam de forma inconsciente os dados que servirão de base para alimentar o seu vício da gratificação imediata do consumo. Assim,

> [...] o problema da internet é ainda mais grave, uma vez que atende a interesses comerciais e baseia-se na utilização de informações colhidas dos próprios usuários (seja ela oriunda de dados prestados pelo cliente quando de

> cadastros necessários para acesso ao sistema ou do histórico de visitações e visualizações de páginas da internet). Neste sentido o usuário, também consumidor dos serviços prestados pelos sites que utiliza, ao que parece, encontra-se sujeito a estas violações, as quais ocorrem constantemente no mundo cibernético. No mesmo diapasão, na internet são encontradas publicidades direcionadas que se utilizam de mecanismos baseados em dados pessoais dos usuários da rede mundial de computadores, de modo a invadirem a sua intimidade desta forma (LUFT; POLLI, 2012, p.140).

Não se desconsidera a capacidade do *marketing* em aguçar desejos inconscientes e projetivos, por meio de técnicas psicológicas, permitindo assim criar valores por meio da propaganda, agora, nesse momento da discussão, é possível dimensionar o risco do acesso aos dados dos consumidores, uma vez que será possível realizar uma maior captura de atenção do próprio consumidor, fomentando o seu desejo de consumir e empurrando-o ao modo de vida ditado pelo consumismo.

Nota-se, pois, que o acesso e tratamento de dados pessoais repercute na esfera econômica, privacidade e liberdade do indivíduo no ciberespaço, bem como nas relações sociais e políticas do homem moderno na sociedade, demandando regulamentação.

Posto isto, a próxima seção aborda os diplomas legais que têm previsão quanto à proteção de dados.

1.2 Diplomas legais que têm previsão quanto à proteção de dados

É importante relembrar que o processo legislativo previsto na Constituição da República Federativa do Brasil de 1988 (CRFB/1988), Lei Maior, compreende a elaboração de emendas, leis complementares, leis ordinárias, leis delegadas, medidas provisórias, decretos legislativos, resoluções, conforme previsto no artigo 59 da CRFB/1988, o qual se encontra assim redigido:

> Art. 59. O processo legislativo compreende a elaboração de: I – emendas à Constituição; II – leis complementares; III – leis ordinárias; IV – leis delegadas; V – medidas provisórias; VI – decretos legislativos; VII – resoluções.
> Parágrafo único. Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis (BRASIL, 1988, s.p.).

A LGPD, Lei nº 13.709/2018 é uma lei ordinária, a qual veio a integrar no dia 18.09.2020, definitivamente, o arcabouço legal de nosso país e desde então, passou a compor o ordenamento jurídico brasileiro.

Relembrando a lição magistral sobre o ordenamento jurídico, Norberto Bobbio (1995) ensina que na verdade, as normas jurídicas nunca existem de forma dissociada de um contexto, mas sempre em outro contexto de normas que guardam relações particulares entre si.

Assim, a LGPD está inserida, enquanto viger, em um contexto de normas e terá particularidades de atração ou repulsão que serão solucionadas caso a caso, em verdadeiras fricções, as quais poderão representar aplicações de princípios, precedentes, ou mesmo novos atos legislativos, num ir e vir que em nosso sentir está correto, justificável porque o Direito é dinâmico, e a Teoria dos Sistemas, justifica essa ordenada.

Na categorização legislativa no que diz respeito, à iniciativa, à tramitação, ao quórum, a LGPD, integrando o sistema legal infraconstitucional, coexistirá em harmonia com as demais leis. E não poderá violar a Constituição Federal, princípios expressos ou não, diplomas legais, a coisa julgada, o ato jurídico perfeito, o direito adquirido, como previsto no inc. XXXVI, do artigo 5º da CRFB/1988.

O diploma legal brasileiro que disciplina a vigência e como se dará a existência das leis enquanto vigentes é a Lei de Introdução as Normas do Direito Brasileiro – LINDB, e o artigo 2º assim prescreve:

> Art.2º. Não se destinando à vigência temporária, a lei terá vigor até que outra a modifique ou revogue. [...] § 2º A lei nova, que estabeleça disposições gerais ou especiais a par das já existentes, não revoga nem modifica a lei anterior (BRASIL, 1942, s.p.).

Há que se estar atento para que não se criem dificuldades na aceitação e na aplicação da LGPD, porque esta legislação não acabará com o sistema jurídico brasileiro. Mas sim, vem somar-se a ele e traz em seu âmago uma jornada, uma estrutura, uma categorização, direitos fundamentais, definições, princípios, base legais, de direitos a serem protegidos no que se refere aos titulares de dados pessoais.

Pela leitura atenciosa do artigo 64 da LGPD, percebe-se que há também a previsão expressa de que os direitos e os princípios nela contidos não excluirão outros previstos no

ordenamento jurídico brasileiro ou nos tratados internacionais dos quais o Brasil seja Alta Parte Contratante.

É imperativa uma atenção cuidadosa e uma visão mais acurada do sistema jurídico, tanto pelo julgador, como pelo operador do Direito, quanto à integração da Lei nº 13.709/2018 no sistema jurídico brasileiro porque a LGPD não é uma lei isolada, única. Essa deve respeitar institutos, conceitos e definições de outros ramos do Direito, tais como o Código Civil (CC) brasileiro, o Código Tributário Nacional (CTN), o Código Consumerista (CDC), as Instruções e Regulamentos do Banco Central, da Receita Federal, e demais disposições legais existentes.

A CRFB/1988 em seu artigo 1º[1] e artigo 5º, inc. LXXI[2]; o CC, em seu artigo 2º[3]; o CDC, em seu artigo 43[4]; o Decreto nº 7.962/2013 – o Decreto do Comércio Eletrônico; a Lei nº 12.965/2014 - Marco Civil da Internet (MCI), em seu artigo 3º, inc. III[5] e a Lei nº 12.527, de 18.11.2020, a Lei de Acesso a Informação (LAI), em seu artigo 4º[6] são alguns dos

---

1 Art. 1º da CRFB/1988. "A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: I – a soberania; II – a cidadania; III – a dignidade da pessoa humana; IV – os valores sociais do trabalho e da livre iniciativa; V – o pluralismo político. Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição".

2 Art. 5º da CRFB/1988. "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: LXXII – conceder-se-á habeas data: "a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo";

3 Art. 2º do CC. "A personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro".

4 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às in-formações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor

5 Art. 3º da LGPD. "A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] III – proteção dos dados pessoais, na forma da lei";

6 Art. 4º do MCI. "Para os efeitos desta Lei considera-se: I – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; II – documento: unidade de registro de informações, qualquer que seja o suporte ou formato; III – informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua

diplomas legais, que contêm dispositivos que já dispõem sobre os dados pessoais no ordenamento jurídico brasileiro, antes mesmo que entrasse em vigor a LGPD.

As citações de artigos de cada diploma legal, como exemplos, são necessárias para que seja possível contextualizar, relembrar e compreender que a LGPD, apesar de ser um diploma legal de grande importância e possuir implicações que vão desde os direitos fundamentais ao econômico; das relações consumeristas ao empresarial; das relações de trabalho ao penal; entre elas, de colocar o país em um patamar mais elevado no que tange ao respeito aos direitos fundamentais do cidadão, ao desenvolvimento econômico tecnológico, à respeitabilidade merecida no cenário internacional, principalmente o europeu[7], não é uma ilha isolada, e faz parte de um ordenamento jurídico. E na concepção de Andre Ribeiro (2020), por esta lei geral, o mundo verá o ser humano, sob outra ótica, o de uma igualdade maior porque a percepção primeira será do ser humano, da pessoa, e não pelas informações-dados acerca desta.

Na esteira de André Ribeiro (2020), em entrevista concedida a Irene Hernández Velasco, de Madrid para a BBC News Mundo, a filósofa Carissa Véliz (2020 s.p.) fez a seguinte pontuação: “Se somos tratados de acordo com os nossos dados (se somos mulheres ou homens, magros ou gordos, ricos ou pobres) não somos tratados como cidadãos iguais. Privacidade é poder”.

Tem-se assim que o ordenamento jurídico brasileiro, irritado, ganhou uma legislação geral de proteção de dados que traça os princípios, as bases jurídicas, para o setor privado e público para o tratamento de dados, respeitando o seu titular, e ela, deverá dialogar com as outras. Nesses termos, a próxima seção irá se dedicar à harmonia da LGPD no sistema jurídico brasileiro.

---

imprescindibilidade para a segurança da sociedade e do Estado; IV – informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V – tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; VI – disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados; VII – autenticidade: qualidade da informação que tenha sido produzida, ex-pedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema; VIII – integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; IX – primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações”.

7 Europa adota as diretrizes da GPDR (*General Protection Data Regulation*).

1.3 Harmonia da Lei Geral de Proteção de Dados – LGPD no sistema jurídico brasileiro

No Projeto de Lei da Câmara de 53, em 2018, no Senado Federal, os legisladores tiveram uma grande preocupação de acomodação do então projeto, como futura lei de proteção de dados, a integrar o sistema jurídico brasileiro, ao apresentarem um Anexo Complementar de leis e dispositivos que fundamentava o objetivo apresentado pelo projeto de lei, quanto à necessidade de um disciplinamento, um ordenamento jurídico e institucional para o tratamento de dados pessoais, além da proteção dos direitos individuais, de acordo com a CRFB/1988 e demais diplomas legais.

Ultrapassado todos os trâmites e sancionada a LGPD, tem-se que este diploma legal deve estar em harmonia com o sistema jurídico. Isso quer dizer que se na análise de caso concreto, houver um conflito de normas, uma deverá ceder para que a outra seja aplicada a fim de assegurar o núcleo do direito que naquele momento é importante resguardar, proteger, garantir, sem que a norma, naquele caso não aplicada, seja excluída do ordenamento jurídico (ACUNHA, 2014).

Esse afastamento de uma norma para se aplicar outra no caso concreto, para proteger em determinado tempo um núcleo de um direito fundamental ao invés de outro, se dará com fundamento no Princípio da Ponderação dos Bens, atendendo-se à adequação, à necessidade e à proporcionalidade (SILVEIRA, 2020).

Natália Braga Ferreira (2020), sobre o Princípio de Ponderação de Bens, sob a ótica de Alexy (2008), diz que por sua vez, a ponderação real ou em concreto é aquela realizada levando-se em conta as características específicas de um caso concreto. Assim, se as situações hipotéticas não forem capazes de solucionar o conflito, o aplicador encontrará a norma de solução mais adequada utilizando-se de subsídios fornecidos pelos elementos peculiares que compõem a situação que está sendo analisada.

Sobre o princípio da ponderação, também o professor Henrique Cardoso (2009) expõe que este encontra-se fundamentado em duas regras: a primeira delas expõe que a medida de não satisfação de um princípio depende do nível de importância conferido à satisfação do outro princípio colidente. Assim, a ponderação não pode efetivar-se de maneira arbitrária ou sem que tenha havido reflexão sobre o tema.

Referente à segunda regra de ponderação, Cardoso (2009) destaca que esta relaciona-se ao grau de certeza relacionado às apreciações empíricas que referem-se à medida examinada.

De qualquer modo, segundo ainda Natália Braga Ferreira (2020), um ponto resta claro: a ponderação é *conditio sine qua non* para a garantia e preservação dos princípios e valores consubstanciados nas Constituições atuais, que devem atuar como guardiãs supremas de toda e qualquer sociedade que tenha por aspiração ser justa e democrática.

Constata-se assim que é fundamental a aplicação de princípios quando estão em jogo, portanto, dois ou mais valores de igual grandeza. O afastamento de um, na análise do caso concreto, não o inutiliza para o sistema jurídico, ao contrário, o fortalece, preservando-o hígido e dá ao jurisdicionado a segurança jurídica necessária e fundamental, em qualquer estado de direito.

Para manter-se harmônica, no entanto, a LGPD deve corroborar com as demais legislações, tal como ocorre com o CDC. Isto porque a realidade ditada pela sociedade de consumo no ciberespaço coloca em crescimento exponencial os usuários de redes sociais. O regramento legal não alcança a velocidade das transformações das novas tecnologias, assim a saída mais plausível é buscar alternativas dentro dos diplomas legais já existentes visando a proteção dos usuários.

A maior proteção dos usuários está relacionada à exposição de dados pessoais e comportamentais na rede. Nesse sentido, há dois tipos de informações dos usuários diretamente ligadas às publicidades direcionadas, quais sejam: as informações cadastrais e as informações de preferências.

No estudo realizado por Luft e Polli (2012), tem-se as seguintes definições: as informações cadastrais se referem aos dados solicitados ao usuário para utilização do ciberespaço, já as informações de preferências são divididas em associativas e de navegação. As primeiras se referem às características das páginas que os usuários geralmente curtem ou seguem. Já as de navegação se referem ao histórico de busca de navegação do usuário. Todos esses dados criam um perfil de cada usuário, facilitando o direcionamento de propaganda, em outras palavras, o usuário passa a fornecer às prestadoras de serviços dados que facilitam a sua própria captura mental ao consumo:

> Atualmente na internet há duas espécies de informações relevantes que são levadas em conta quando ligadas a publicidades direcionadas: informações cadastrais e informações de preferências. As primeiras – cadastrais - dizem respeito às informações solicitadas e necessárias para que seja finalizada a etapa cadastral do futuro usuário do sistema, ou do espaço do site, bem como aquelas não obrigatórias que são informadas no perfil do usuário. Já as informações de preferências subdividem-se em "associativas" e "de navegação". As associativas são aquelas retiradas das preferências do usuário, ou seja, aquelas ligadas às características das páginas que este cadastra para receber atualizações ou ficar vinculado de alguma forma (conhecidas como "curtir" no *Facebook* ou "seguir" no *Twitter*). Por sua vez, as de navegação são extraídas da forma mais engenhosa pelas prestadoras de serviço, visto que se utilizam dos dados inerentes da navegação do usuário, ou seja, para qual página aquele se dirige a partir do site de relacionamento. A conjugação de todos estes dados cria um perfil com grande riqueza de detalhes e características dos usuários, destinatário final das propagandas direcionadas e exploradas pelas redes sociais (LUFT, POLLI, 2012, p. 138).

Ainda segundo este mesmo estudo, as redes sociais ofertam os dados de seus usuários às empresas, ao passo que essas empresas usam esses dados para divulgar seus produtos e serviços. Assim o acesso a esse ciberespaço embora ganhe a aparência de gratuidade, na verdade exigem uma contraprestação camuflada, uma vez que as empresas patrocinadoras pagam pelos dados que os usuários consumidores oferecem enquanto utilizam as redes sociais. Na verdade, do ponto de vista do *marketing*, as redes sociais nesse aspecto atuam como armadilha ao consumidor:

> As informações obtidas são utilizadas como "moeda de troca" por parte do site de relacionamento. A rede social oferta a informação dos usuários para empresas, com interesse em divulgar seus serviços/produtos. A publicidade é direcionada e gerenciada pelo site com o uso das informações prestadas pelos consumidores, bem como aquelas inerentes de sua cotidiana navegação. Com isto estas empresas conseguem ofertar ao mercado de publicidade um serviço diferenciado e que aufere gigante lucro na internet. As empresas exploradoras desta espécie de sítios eletrônicos, aparentemente gratuitos e de livre "locomoção do usuário", utilizam dados pessoais de navegação (site visitados regularmente e assuntos frequentes) como forma de destacar seus serviços (publicidade direcionada), auferindo lucro não apenas por veicularem propagandas aleatórias em site de relacionamento, mas por tentarem ofertar a determinado usuário os produtos e serviços que mais lhe interesse de acordo com as informações, sejam elas prestadas ou não, autorizadas ou não (LUFT, POLLI, 2012, p. 138).

Melhor explicando, a contraprestação ao uso das redes sociais é realizada pela empresa patrocinadora que utiliza do ciberespaço da rede para veicular sua publicidade. Portanto, as relações nas redes são compostas por três integrantes: de um lado tem-se os

administradores das redes sociais que oferecem o espaço virtual para relacionamentos e comunicações, bem como os patrocinadores que fazem uso da rede para veicular a propaganda de seus produtos e serviços. De outro extremo encontra-se o usuário da rede que, muitas vezes, não sabe que entrega seus dados aos patrocinadores das redes, e acaba fomentando o seu próprio consumo por meio das técnicas de *marketing* e propagandas direcionadas.

Outro ponto importante a ser ressaltado é a falsa perspectiva de gratuidade de uso das redes sociais. Os usuários, muitas vezes desconhecem a dinâmica das redes das quais fazem uso, uma vez que as redes sociais na internet auferem grandes lucros devido à veiculação das propagandas de seus patrocinadores de forma direcionada aos usuários.

Passada a explicação sobre o desequilíbrio e a ausência de transparência na relação entre os usuários e as redes sociais no ciberespaço, inicia-se as ponderações sobre a incidência do CDC nessa relação.

Para se compreender se o usuário se enquadra no conceito de consumidor estampado no artigo 2º da Lei nº 8.078/1991[8], bem como se as redes sociais no ciberespaço podem ser classificadas como fornecedoras segundo o mesmo diploma legal[9], faz-se necessária uma análise aprofundada das conceituações e a aplicação dos parâmetros do CDC à relação de consumo.

Segundo a lição de Filomeno (2010), consumidor é qualquer pessoa, que de maneira isolada ou coletiva, contrate para seu consumo final, um bem ou serviço. Nos dizeres do autor:

> Entendemos que consumidor, abstraídas todas as conotações de ordem filosófica, tão-somente econômica, psicológica ou sociológica, e concentrando-nos basicamente na acepção jurídica, vem a ser qualquer pessoa física que, isolada ou coletivamente, contrate para consumo final, em benefício próprio ou de outrem, a aquisição ou locação de bens, bem como a prestação de serviços. Além disso, há que se equiparar a consumidor a coletividade que, potencialmente, esteja sujeita ou propensa à referida contratação. Caso contrário se deixaria à própria sorte, por exemplo, o

[8] Art. 2° do CDC – "Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Parágrafo único. Equipara-se ao consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo".

[9] Art. 3° do CDC – "Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial. § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista".

> público-alvo de campanhas publicitárias enganosas ou abusivas, ou então sujeito ao consumo de produtos ou serviços perigosos ou nocivos à sua saúde ou segurança (FILOMENO, 2010, p. 23).

Considerando que o usuário se utiliza da prestação de serviços das redes sociais como destinatário final, este é enquadrado na acepção de consumidor de acordo com o artigo 2º do CDC. Enquanto a empresa prestadora de serviço lucra com o consumo direcionado de seus usuários, se enquadrando na acepção de fornecedora do artigo 3º do mesmo diploma legal (LUFT; POLI, 2012).

O § 2º do artigo 3º do CDC[10] estabelece como requisito para caracterização de serviço a remuneração. No que concerne às redes sociais a remuneração é indireta[11], uma vez que as empresas patrocinadoras lucram junto com a empresa que administra as redes sociais a partir do consumo gerado nos usuários. Portanto, o conceito de remuneração é interpretado de forma ampla e a relação de consumo é configurada:

> No caso das Redes Sociais, tem-se a remuneração indireta. Como exemplo, coloca-se em análise a situação em que um empreendedor qualquer, deseja anunciar seu empreendimento aos usuários de uma determinada Rede Social, então, este paga ao fornecedor deste serviço para que se coloque uma certa publicidade, de tamanho e tipo pré-estabelecidos, no ambiente virtual da mesma. Ora, só existe o interesse do empreendedor de veicular sua propaganda no ambiente virtual da Rede Social, se este tiver acessos suficientes para suprir a sua necessidade mínima de visualizações por anúncio, ou mesmo se o público alvo deste empreendedor acessá-la. (SILVEIRA JUNIOR, 2011, s.p.).

---

[10] § 2º do artigo 3º do CDC – "§ 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista".

[11] Destarte, "a compreensão de 'remuneração' pelos serviços prestados, deve abranger também a que se dá de forma indireta, como no caso das redes sociais que se utilizam de informações pessoais para basear sua indústria de publicidade. As normas da Lei 8.078/90 devem ser interpretadas de modo que se retire de seu sistema, maior proteção ao consumidor, a fim de tentar trazer equilíbrio às relações de consumo, sejam elas remuneradas direta ou indiretamente. Como referido nos itens anteriores, o fundamento para responsabilização dos sites de relacionamento é, principalmente, o fato de que os mesmos auferem lucro com as relações de consumo, pois, caso contrário, em não havendo dados pessoais de seus usuários, estes sites não receberiam a remuneração em tal monta como as que auferem atualmente. Do mesmo modo, se não houvesse público que fizesse uso do 'espaço' virtual disponibilizado, nenhum anunciante teria interesse em veicular suas propagandas naquele ambiente" (LUFT; POLLI, 2012, p. 147).

O Superior Tribunal de Justiça (STJ), por meio de parecer técnico da ministra Nancy Andrighi[12], também compreende que se configura uma relação de consumo entre as redes sociais e seus usuários.

Superada a questão da incidência do CDC nas relações entre as plataformas das redes sociais e os usuários, faz-se necessária uma reflexão sobre a legislação pertinente e vigente sobre a proteção do consumidor no que concerne ao tratamento e à proteção conferida aos dados pessoais por ele mesmo fornecidos, bem como a necessidade de harmonia entre a LGPD e o CDC.

1.3.1 Harmonia entre a LGPD e o CDC

Observe-se que não obstante o CDC possa ser utilizado como um parâmetro legal, devido à importância da proteção dos dados, foi necessária a decisão política-jurídica de disciplinar a coleta e tratamento de dados pessoais por meio da Lei nº 13.709/2018, denominada LGPD, que passou a disciplinar a utilização econômica da informação decorrente dos dados pessoais.

Por uma leitura sistemática das expressas determinações legais contidas no art. 2º, inc. VI, art. 18, § 8º, e art. 55-K, § único, todos da LGPD, a proteção de dados está diretamente relacionada à defesa do consumidor, assim como a Autoridade Nacional de Proteção de Dados (ANPD) atua juntamente com os órgãos de defesa do consumidor na proteção dos dados pessoais.

---

[12] Trecho do parecer técnico da ministra Nancy Andrighi: "Parece inegável que a exploração comercial da Internet sujeita as relações jurídicas de consumo daí advindas à Lei nº 8.078/90. [...] Com efeito, as peculiaridades inerentes a essa relação virtual não afastam as bases caracterizadoras de um negócio jurídico clássico: (i) legítima manifestação de vontade das partes; (ii) objeto lícito, possível e determinado ou determinável; (iii) e forma prescrita ou não defesa em lei. [...] Vale notar, por oportuno, que o fato de o serviço prestado pelo provedor ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração", contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. [...] No caso da GOOGLE, é clara a existência do chamado *cross marketing* – ação promocional, entre produtos ou serviços em que um deles, embora não rentável em si, proporciona ganhos decorrentes da venda de outros. Apesar das pesquisas realizadas via GOOGLE SEARCH serem gratuitas, a empresa vende espaços publicitários no site bem como preferências na ordem de listagem dos resultados das buscas. [...] Há, portanto, inegável relação de consumo nos serviços de Internet, ainda que prestados gratuitamente" (BRASIL, 2012, s.p.).

Destarte, o CDC e a LGPD incrementam a tutela da proteção de dados, o que significa dizer que os direitos elencados nos dois diplomas legais devem ser cumulados na interpretação dos direitos dos titulares de dados[13].

As análises pertinentes às relações entre usuários e as redes sociais no ciberespaço devem considerar tanto o CDC, quanto a LGPD.

Para iniciar os breves comentários referentes às legislações, compila-se o entendimento de Espolador (2013) sobre o CDC, mais precisamente, em seu art. 6º, no qual estabelece o dever de informação[14], prevendo como direito do consumidor a informação adequada sobre os serviços, permitindo-lhe a ciência dos prejuízos e benefícios de suas escolhas:

> O dever de informação advém do disposto no art. 6º, incisos II e III do CDC, que prevê como direito básico do consumidor a informação adequada, além da divulgação sobre o uso adequado dos produtos e serviços. [...] Diante do artigo, o dever de informação está relacionado ao acesso dos consumidores a uma informação adequada que lhes permita fazer escolhas seguras, ciente dos prejuízos e benefícios que possa ter (ESPOLADOR, 2013, p. 151-152).

De pronto, portanto, pode-se identificar uma clara violação ao dever de informação nas relações consumeristas com os usuários nas redes sociais, uma vez que o usuário acredita estar fazendo uso de um serviço gratuito quando, na realidade, há contraprestação.

---

[13] Segundo Laura Rodrigues (2021, s.p.): "A edição da Lei Geral de Proteção de Dados incrementa a tutela dos direitos do consumidor prevista no CDC (LGL\1990\40). O regime previsto pela LGPD não exclui aquele definido pelo CDC (LGL\1990\40). A incidência em comum dos arts. 7º do CDC (LGL\1990\40) e 64 da LGPD firmam a conclusão de que os direitos dos titulares dos dados previstos nas respectivas normas devem ser cumulados e compatibilizados pelo intérprete".

[14] Art. 6º do CDC: "São direitos básicos do consumidor: I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos; II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas; VI - a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos; VII - o acesso aos órgãos judiciários e administrativos com vistas à prevenção ou reparação de danos patrimoniais e morais, individuais, coletivos ou difusos, assegurada a proteção Jurídica, administrativa e técnica aos necessitados; VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências; IX - (Vetado); X - a adequada e eficaz prestação dos serviços públicos em geral. Parágrafo único. A informação de que trata o inciso III do *caput* deste artigo deve ser acessível à pessoa com deficiência, observado o disposto em regulamento".

Há de se ponderar também sobre os limites desta contraprestação consentida pelo usuário, sobre a possibilidade da concessão de uso de dados de forma generalizada poder ser condicionante para o uso de redes sociais, sobre os limites entre a autonomia do usuário que consente e a regulação estatal impondo medida de restrição ao poder do controlador dos dados.

Segundo Miragem (2019), a boa-fé elencada tanto no CDC, quanto na LGPD é um ponto de equilíbrio para harmonizar os interesses nessas relações. Veja-se que o artigo 4º, inc. III do CDC[15] estabelece que um dos mais importantes objetivos da política nacional das relações de consumo é a harmonização dos interesses entre fornecedores e consumidores, resguardando a boa-fé e o equilíbrio. No mesmo sentido, o artigo 6º, *caput*, da LGPD, dispõe que o tratamento destinado aos dados pessoais deverá sempre ser feito observando-se a boa-fé.

Nas relações jurídicas a boa-fé é associada aos deveres de cooperação e lealdade, bem como às legítimas expectativas das partes. De acordo com a interpretação do artigo 10, inc. II da LGPD realizada por Miragem (2019), no caso de tratamento de dados pessoais, a tutela da legítima expectativa é do titular dos dados frente ao controlador a partir das circunstâncias em que fora concedido o consentimento.

Para a boa fé no uso dos dados pelo controlador seja avaliada, deve-se ter como parâmetro, qual a finalidade e o tratamento que o titular consentiu para o uso de seus dados, bem como o modo em que foram apresentadas as informações previamente ao consumidor, ora titular dos dados. A tutela da boa-fé abrange tanto a precisão, quanto a transparência das informações prestadas ao consumidor, quanto o respeito por parte do controlador (fornecedor) da finalidade de uso dos dados comunicada no momento do consentimento do titular (consumidor):

---

[15] Art. 4º do CDC – "A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I – reconhecimento da vulnerabilidade do consumidor no mercado de consumo; II – ação governamental no sentido de proteger efetivamente o consumidor: a) por iniciativa direta; b) por incentivos à criação e desenvolvimento de associações representativas; c) pela presença do Estado no mercado de consumo; d) pela garantia dos produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho; III – harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (artigo 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores".

> No caso do tratamento de dados pessoais, a boa-fé fundamenta a tutela das legítimas expectativas do titular dos dados frente ao controlador (art. 10, II, da LGPD), o que se delineia, sempre a partir das circunstâncias concretas em que se deu o consentimento, a finalidade de uso e tratamento dos dados que foi indicada na ocasião e o modo como foram compreendidas as informações prévias oferecidas. A tutela da confiança do consumidor, neste caso, abrange tanto a crença nas informações prestadas quando de que aquele que tenha acesso aos seus dados, por força do consentimento dado, não se comporte de modo contraditório a elas e respeite a vinculação à finalidade de utilização informada originalmente. Neste particular, recorde-se que a proteção dos dados pessoais se justifica pela proteção à privacidade do titular dos dados. Privacidade é conceito objetivo, mas também contextual, uma vez que se vincula à expectativa legítima do titular do direito em ter preservada, sob certas condições, informações a seu respeito da exposição pública. Dos termos do consentimento resulta esta expectativa, de modo que não poderá o fornecedor ou o controlador dos dados, dando uso diverso da finalidade que motivou o consentimento do consumidor, tal qual foi compreendida por ele, defender a utilização a partir de critérios outros que não aquele que caracterizou o efetivo entendimento do titular dos dados (MIRAGEM, 2019, p. 05).

Assim, as relações contratuais entre fornecedores que condicionam o bem ou serviço ao acesso aos dados pessoais acabam sendo norteadas pela autodeterminação informativa, que prioriza a livre e racional escolha do consumidor titular dos dados.

Ainda segundo a análise feita por Miragem (2019), o consentimento informado baseia-se na compreensão do conteúdo e nas implicações da decisão de consentir, ou seja, não basta meramente avisar o consumidor que haverá acesso aos dados pessoais, é preciso esclarecer todas as implicações de seu consentimento.

Nota-se que tanto o dever de informação adequada elencada no CDC apresentada por Espolador (2013), quanto o consentimento informado elencado pela LGPD e apresentado por Miragem (2019) servem como alicerces do equilíbrio contratual.

Por essa concepção de consentimento e informação adequada indaga-se nesse momento se seria necessário dimensionar o risco de captura mental por meio de mensagens publicitárias direcionadas na fase pré-contratual? Seria necessário informar ao consumidor que o acesso aos seus dados irá conferir ao fornecedor maior poder contratual? No caso das redes sociais que condicionam o uso da plataforma ao acesso dos dados do usuário, seria então necessário alertar ao mesmo que as redes sociais são espaços cibernéticos formatados para capturar sua atenção e realizar a venda de produtos e serviços dos patrocinadores? Pode-se obrigar as redes sociais a realizar esclarecimento pré-contratual que depõe contra os serviços que ela mesma oferece?

Para dar continuidade à crítica a ser desenhada nesse capítulo, se faz necessário, ainda, que se atente para a brecha técnica no processo de anonimização de dados pessoais, no qual a LGPD acaba se olvidando da sua possibilidade de conversão.

1.4 Dados Pessoais e Processo de Anonimização à luz da LGPD

Ao versar sobre dados pessoais veiculados no ciberespaço torna-se necessário elucidar também sobre os dados que passam por um processo de anonimização e são desvinculados da identidade de seu titular por meio de supressão, generalização, randomização e pseudoanonimização, processos que visam desvincular os dados de seu titular.

Ocorre que não se pode afirmar que há um processo de anonimização de dados que seja absolutamente isento de reversão, ou seja, não há como assegurar a eficiência da manutenção do anonimato:

> Torna-se cada vez mais recorrente a publicação de estudos que demonstram ser o processo de anonimização algo falível. A representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo- se, com 100% (cem por cento) de eficiência, o anonimato das pessoas, é um mito. Por essa lógica, qualquer dado pessoal anonimizado detém o risco inerente de se transmudar em um dado pessoal. A agregação de diversos "pedaços" de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico (CAPPELLI et al., 2019, p. 191).

Em razão justamente do processo de reversão de anonimização dos dados que o conceito de dados pessoais pode seguir uma orientação expansionista ou reducionista. O que significa dizer que no conceito expansionista, dados pessoais são aqueles capazes de tornar a pessoa identificável, já o conceito reducionista conceitua os dados pessoais como aqueles de identificação direta de seu titular.

Em conformidade ao estabelecido pelo artigo 12 da LGPD[16], não se consideram os dados anonimizados como dados pessoais, exceto se houver reversão do processo de anonimização.

---

[16] Art. 12 da LGPD - "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente

Na mesma linha o artigo 5º, incs. I e III da LGPD[17] conceituam dados pessoais e anonimização para fins da referida lei, estabelecendo ora o conceito expansionista de dado pessoal, ora o conceito reducionista de dado pessoal.

No primeiro inciso do artigo 5º da referida lei, tem-se que o dado pessoal é a informação relacionada a uma pessoa natural de forma direta (reducionista), ou de forma a ser identificável o titular do dado (expansionista). Nos incs. III e XI do mesmo artigo, a LGPD trata sobre o processo de anonimização considerando-o infalível, em outras palavras, a Lei acaba por desconsiderar a possibilidade real de fácil conversão do processo de anonimização dos dados.

Por exemplo, pela leitura do artigo 16, inc. IV[18] da mesma lei, entende-se que deve-se eliminar os dados após o fim de seu tratamento, no entanto se estiverem anonimizados podem ser usados pelo controlador.

---

meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais".

[17] Art. 5º da LGPD – "Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado";

[18] Art. 16 da LGPD. "Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: [...] IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados".

Veja-se que a LGPD ao se olvidar da falibilidade do processo anonimização confere uma brecha legal ao tratamento dos dados pessoais, isso porque o controlador pode usar os dados anonimizados, ciente da possibilidade de conversão.

Embora o inc. I, do artigo 5º adote o conceito tanto reducionista, quanto expansionista dos dados pessoais, pela leitura sistemática da LGPD, o conceito de dados pessoais é o reducionista, uma vez que os dados identificáveis pela reversão do processo de anonimização não são considerados dados pessoais.

Assim, tanto pela dinâmica lucrativa principalmente das redes sociais no ciberespaço, quanto pela falibilidade do processo de anonimização, pode-se concluir que os termos de consentimento que materializam a relação de consumo no ciberespaço não devem ser regidos pelo prisma liberal, no qual se sobrepõe a autonomia do usuário em consentir o livre acesso de seus dados. Segundo Oliva e Viégas (2019), é evidente que pela fragilidade social, psicológica e jurídica do consumidor no ciberespaço, há a necessidade da regulação estatal impondo limites ao poder do fornecedor e das plataformas digitais de entretenimento, em razão da incapacidade do homem em compreender a dinâmica na qual está inserido para dar de fato um consentimento livre e consciente.

Deve-se ponderar sobre todo impacto inconsciente do homem consumidor cada vez mais submerso na lógica de uma cultura materialista, e de uma sociedade classificada pelas posses e poder de consumo, que se utiliza do *marketing* aliado a recursos psicológicos para alcançar o inconsciente do homem e empurrá-lo cada vez mais ao consumo. Esse incentivo, no entendimento de Tepedino e Teffé (2019) ocorre de maneira sutil e, muitas vezes, o próprio homem não percebe que consome para exteriorizar o seu sucesso, ou a sua autorrealização, de tanto que a sua mentalidade já está adstrita à sociedade de consumo. O homem moderno encontra-se escravizado pelos desejos e valores criados no meio em que está inserido.

A vulnerabilidade aqui ganha novos contornos a partir do ciberespaço, em que eleva substancialmente o risco de roubo de dados do consumidor, principalmente nas redes sociais em que o acesso aos dados dos usuários permite o direcionamento do *marketing* e do *telemarketing*. Isto porque em tempos de comércio eletrônico, as redes tornam-se uma vitrine sobre a capacidade de consumir, além de conferir maior vantagem contratual ao fornecedor pelo acesso as preferências pessoais de cada consumidor (SCHULMAN, 2021).

Os abusos decorrentes do *telemarketing*, especialmente as ligações excessivas oferecendo produtos e serviços, ensejam indenizações irrisórias e, consequentemente, não obstam a continuidade da prática[19].

Segundo Oliva e Viégas (2019), a falibilidade do processo de anonimização, bem como a própria estrutura das redes sociais mercantiliza a privacidade de forma tão atraente e viciante que o usuário é colocado numa posição social e política de exponencial destrutibilidade.

Importante esclarecer aqui que o objetivo da presente crítica não é negar o avanço tecnológico que já faz parte da vida do homem e tendência em fazer cada vez mais parte do dia a dia da humanidade, muito menos negar ao homem a necessidade de consumir, principalmente, a bens e serviços essenciais. O objetivo é atentar para o caminho pernicioso que a falta de cuidado quanto à sociedade de consumo aliada ao *marketing* agressivo no ciberespaço pode levar a humanidade e as relações de poder existentes no meio social. A provocação aqui delineada é um chamado para o resgate de uma postura republicana a fim de proteger o homem de uma espécie de "escravidão moderna".

[19] Como exemplo cita-se a sentença da Juíza Rita de Cássia de Cerqueira Lima Rocha no Processo 0701636-08.2021.8.07.0016 em que uma empresa de telemarketing, com base no art. 6°, inc. VI, do CDC, foi condenada a pagar a um consumidor uma indenização de R$ 1.500,00 (Hum mil e quinhentos reais) em razão de ligações reiteradas, que causaram ao autor da ação incômodo e perturbação (CONSULTOR JURÍDICO, 2021).

2 ESTRUTURA DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Este capítulo apresenta uma análise crítica sobre a estrutura da LGPD. Inicialmente, expõe os principais conceitos e nomenclaturas presentes na Lei; analisa como deve ser feito o tratamento dos dados pessoais bem como os princípios que fundamentam a LGPD; e, por fim, expõe os aspectos positivos e negativos da LGPD, demonstrando a importância dos mecanismos de *compliance*.

2.1 Entendendo a estrutura da LGPD

O Projeto de Lei do Deputado Federal Milton Monti recebeu o número 4.060/2012 na Câmara dos Deputados e apresentou a necessidade de se ordenar juridicamente o tratamento de dados. Na Justificativa[20] de apresentação da lei se lê que o projeto tem por objetivo "dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas, de acordo com a CRFB/1988" (BRASIL, 2012, s.p.).

Quando o Projeto 53 da Câmara dos Deputados, em 2018, foi aprovado pelo Senado Federal gerou a Lei nº 13.709 de 14.08.2018, a qual foi sancionada com vetos pelo Presidente da República à época, Sr. Michel Temer.

Com *vacatio legis* determinada em seu texto, e com idas e vindas quanto à vigência, à estrutura da ANPD, à Políticas e Diretrizes, neste cenário todo, no dia 18.09.2020, entrou em vigor a LGPD, ficando para agosto de 2021, no que diz respeito às penalidades, conforme o disposto em seu artigo 65[21].

A LGPD é uma lei geral que veio, em meu sentir, restabelecer o direito fundamental da pessoa humana, a sua privacidade e ao mesmo tempo alavancar, com a proteção nela contida, a economia, o desenvolvimento tecnológico, o respeito às regras, à moralidade, à

---

[20] Justificativa ao Projeto de Lei do Deputado Federal: Milton Monti que recebeu o nº 4060/2012 na Câmara dos Deputados (BRASIL, 2012). Disponível em: https://www.camara.leg.br/proposicoes Web/ prop_mos trarintegra?codteor=1001750&filename=PL+4060/2012. Acesso em: 13 Julho 2022.

[21] Art. 65 da LGPD. Esta Lei entra em vigor: I – dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

personalidade. Define os dados pessoais e os dados pessoais sensíveis, conceitua atores, prevê responsabilizações, infrações, e aplicações de multa para o infrator.

Não tem esta dissertação a pretensão de entrar na discussão acadêmica de institutos, conceitos, teorias, e estudo de artigos por artigos ou mesmo apontar o direito comparado. A proposta deste texto é mostrar além da acomodação, que esta lei indubitavelmente terá no ordenamento jurídico brasileiro, apontar que outras fontes falarão com esta lei. Pretende-se também expor, descortinar, a estrutura legal, ou seja, a sua coluna dorsal. E, ainda, fazer uma pequena referência a dois dispositivos: um que trata dos princípios, artigo 5º, e o outro, da base legal, artigo 7º, porque poderão representar a causa de pedir e a fundamentação jurídica de pedidos extrajudiciais ou judiciais.

Para alcançar o objetivo primeiro, como se observa, a LGPD é dividida em dez (10) capítulos, a saber:

1) O Capítulo I é o das "Disposições Preliminares" e as disposições preliminares são tratadas no artigo 1º ao artigo 6º.

2) O Capítulo II refere-se ao "Tratamento de Dados Pessoais" o qual vai do artigo 7º ao artigo 16. Este capítulo possui quatro importantes seções quais sejam: (i) os "Requisitos Para o Tratamento de Dados Pessoais"; (ii) o "Tratamento Dos Dados Pessoais Sensíveis"; (iii) o "Tratamento de Dados Pessoais de Crianças e de Adolescentes"; e por último, mas não menos importante, (iv) o "Término de Tratamento de Dados".

3) Por sua vez o Capítulo III trata "Dos Direitos do Titular", direitos estes dispostos nos artigos 17 ao 22.

4) No Capítulo IV encontra-se o "Tratamento de Dados Pessoais Pelo Poder Público", o tratamento está previsto no artigo 23 ao artigo 32. Este capítulo possui duas seções importantes, sendo a primeira: "Das Regras", e, a segunda: "Da Responsabilidade".

5) O Capítulo V trata "Da transferência Internacional de Dados" e esta é tratada nos artigos 33 ao 36.

6) No Capítulo VI se encontra a previsão acerca "Dos Agentes de Tratamento de Dados Pessoais", artigos 37 a 45. Possui três seções, a saber: (i) "Do Controlador e do Operador"; (ii) "Do Encarregado pelo Tratamento de Dados Pessoais"; (iii) "Da Responsabilidade e do Ressarcimento de Danos".

7) O Capítulo VII trata da “Da Segurança e Das Boas Práticas”, nos artigos 46 ao 51. Este Possui duas Seções: (i) “Da Segurança e do Sigilo de Dados”; e, (ii) “Das Boas Práticas e da Governança”.

8) Por sua vez, o Capítulo VII tem nos dispositivos 52 ao 54, as disposições acerca “Da Fiscalização”. Possui uma única seção, qual seja a “das Sanções Administrativas”.

9) No Capítulo IX, nos artigos 55 ao 59, se tem a disposições acerca “Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade”. Tem este capítulo duas seções: (i) “Da Autoridade Nacional de Proteção de Dados (ANPD); e, (ii) “Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade”.

10) Por último e não menos importante, o Capítulo X o qual trata “Das Disposições Finais e Transitórias”, nos artigos 60 ao 65.

É importante também trazer uma breve análise sobre os principais conceitos e nomenclaturas presentes na LGPD.

2.2 Principais conceitos e nomenclaturas

Inicialmente importa definir informação, conhecimento e dado. A informação é o recebimento de um conhecimento o qual não se detinha, não se era portador. Este conhecimento recebido, comunicado, o qual não se tinha, uma vez, ordenado, organizado, tratado, passa a ter um significado, e será compreendido dentro de um contexto em virtude de dados nele contido.

O dado contido na informação, sem o conhecimento, sem a comunicação, sem tratamento, sem organização, sem ordenação é, mal comparando, uma pedra carvão e não um diamante. Conhecida a informação e tratados os dados nela contidos, se estes dados servirem para identificar uma pessoa diretamente ou torná-la identificável, passam a ter valor, e esse valor, para o titular dos dados, que afinal é o seu proprietário, foi definido como o centro nevrálgico de proteção da LGPD.

Para o legislador foi importante especificar, definir, eleger atores, prever infrações, prever a ANPD e o Conselho Nacional, porque nesse período da evolução humana, um dos

principais ativos hoje do mundo, é a informação devido ao desenvolvimento tecnológico. E o conhecimento processado, organizado, torna a informação valiosa, ou seja: o acesso aos dados pessoais significa conquista de mercado. Assim, os dados pessoais equivalem a uma matéria-prima de consumo para a venda de primeira grandeza. Neste contexto evolucionário, o sistema jurídico viu, por irritação, a necessidade de regular as relações, com intuito de continuidade, sem disrupção, mas preservando o que é o núcleo desta matéria-prima: os dados pessoais e os seus titulares.

João Ferreira do Amaral ao escrever sobre a economia da informação, afirma que:

> [...] o que faz a empresa ganhar dinheiro não é receber a informação em si própria. É transformar essa informação em conhecimento que depois é aplicado. Falta-nos por isso introduzir a questão da transformação da informação em conhecimento (AMARAL, 2009, p. 116).

Por seu turno Bruno Bioni (2019, p. 2-3) entende que "a informação deve ser, assim, convertida em conhecimento, a fim de torná-la produtiva e estratégica para a atividade empresarial".

No magistério de Biriti (2021), a informação é o conhecimento. O dado, por seu turno, é o estado primitivo da informação, pois, é algo que apenas por si nada acresce ao conhecimento.

Nessa esteira, como já adiantado, tem-se que os dados pessoais são as informações conhecidas, tratadas, organizadas, e por isso a necessidade de seu tratamento visando à proteção de direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural que é o ponto central do artigo 1º da LGPD, não importando os meios em que se encontram tais dados, tais como: arquivos, meios digitais, *cookies, pendrives*.

Outros conceitos importantes para este trabalho são os de meio e mídia digital. Tem-se que meio digital é qualquer mídia que utiliza um computador ou equipamento digital, e tem como suporte a Internet, a comunicação *on-line* ou *off-line*, produções gráficas, videogames, conteúdos audiovisuais. Já mídia digital é qualquer comunicação realizada pela Internet (GIONÉDIS; VIANA, 2021).

É importante também trazer aqui o conceito de internet, que é uma rede remota de domínio internacional que serve a uma ampla área geográfica e torna possível a transferência

de arquivos e dados, juntamente com outras funções, a exemplo da função de correio eletrônico (*email*) para milhões de usuários em todo o mundo: *net*, rede, *web* (LEONARDI, 2012).

A internet derrubou todas as fronteiras e distâncias e permitiu a ampla e instantânea comunicação entre as pessoas, independentemente do país em que se encontram. Encurtando as distâncias, houve expansão das negociações, viabilizando às empresas maiores lucros. No entanto, a internet também expõe seus usuários a vulnerabilidades. A vulnerabilidade pode ser definida como uma fragilidade, uma inconsistência, uma falha, existente no sistema, a qual permite reduzir a inteireza da informação, por ataque interno ou externo, que explorará essa fragilidade (SOMBRA, 2019).

Todos esses vocábulos e definições serão muito úteis ao operador do Direito e ao aplicador da Lei quando houver um pedido, feito pelo titular acerca dos seus dados pessoais, pois a coleta, o armazenamento e o descarte desses dados devem atender às exigências da LGPD, a forma prescrita na lei, aí incluindo os meios digitais, como está estampado no artigo 1º[22] deste diploma legal.

O legislador infraconstitucional, além de dispor sobre o tratamento, previu no artigo 2º[23] da LGPD um a um os fundamentos pelos quais se dará a proteção de dados pessoais. Na realidade, assenta o porquê, de os dados pessoais necessitarem de proteção, quais sejam: o respeito à privacidade, como direito fundamental, a autodeterminação informativa (porque cabe ao titular dos dados o poder sobre suas próprias informações), a liberdade de expressão, a inviolabilidade de sua imagem, intimidade, e o livre desenvolvimento da personalidade humana, direito este fundamental.

Em seu artigo 3º, a LGPD prevê que, independente na operação de tratamento, a realização desta por pessoa natural ou pessoa jurídica de direito público ou privado, não importa o meio (aqui quer significar, o digital), o país de sua sede ou o país onde estejam

---

[22] Art. 1º da LGPD. "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".

[23] Art. 2º da LGPD. "A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

localizados os dados, a lei se aplicará sem exceção, não se aplicando somente nas hipóteses previstas no diploma legal.

No artigo 4º há a previsão das exceções de aplicação da lei quanto ao tratamento de dados pessoais e a definição de dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, anonimização, consentimento, bloqueio, eliminação, transferência, uso compartilhado de dados, relatório de impacto à proteção de dados pessoais, órgãos de pesquisa, autoridade nacional, encontra-se no artigo 5º[24] da LGPD.

Pela leitura do artigo verifica-se que o legislador optou pelo conceito expansionista[25] pelo qual será considerado dado pessoal toda e qualquer informação que possibilitar a identificação de uma pessoa, ou um prolongamento dela, de forma imediata, de forma direta. Mas se assim não ocorrer e se puder fazer o liame entre o dado, e este levar de forma indireta, mediata, indeterminada, a uma pessoa identificável, será também considerado dado pessoal para os efeitos da lei geral.

O dado pessoal sensível vem expresso no inc. II[26] do artigo 5º da LGPD e, como o próprio nome diz, é todo o dado que pelo seu conteúdo de intimidade, pode trazer como consequência o preconceito e a exclusão.

Monteiro (2007) afirma que os dados pessoais sensíveis são os que estão relacionados à esfera de privacidade. Exemplifica citando a origem racial, a saúde, crenças religiosas, orientação sexual, registros policiais, dentre outros. Os não sensíveis são aqueles que pertencem ao domínio público. Portanto, qualquer pessoa pode se apropriar deles. Como exemplos, citam-se: o nome, o estado civil, profissão, etc. Afirma-se que a difusão ou o uso indevido de dados pessoais não sensíveis dificilmente poderão implicar em violações à vida privada.

Ocorre que em razão de diversos fatores sociais atuais, cujo mais determinante é o avanço tecnológico, especialmente o uso da Internet como forma de comunicar e de obter

---

[24] Art. 5º da LGPD. "Para os fins desta Lei considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável";

[25] Em contrapartida ao conceito expansionista há o conceito reducionista pelo qual só será considerado dado pessoal se a informação identificar direta, imediata, determinada pessoa.

[26] Inc. II do art. 5º da LGPD – "II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural";

informações, por intermédio da "mineração de dados"[27], a utilização de determinados dados considerados não sensíveis por terceiros, a exemplo do domicílio e profissão, sem o conhecimento do titular, em determinadas circunstâncias pode causar danos à pessoa. Nessas condições, o fator determinante é a intenção desses terceiros na utilização desses dados, sem que o indivíduo saiba qual o propósito dessa "mineração".

Portanto, dados pessoais "são quaisquer informações relacionadas com a pessoa titular que, a depender da associação de um determinado dado com outro, forma um conjunto de informações que podem ser utilizadas para os mais diversos fins [...]" (BRASIL, 2018, s.p.). A Lei nº 12.965/2014 traz algumas definições essenciais para esse cenário, no entanto, não prevê uma definição para dados pessoais. O conceito previsto na LGPD foi simplória, definiu como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018, s.p).

Dito isto, depreende-se que os dados pessoais podem ser os mais variados. Essa divisão dicotômica trabalhada na doutrina não atende à complexidade das circunstâncias atuais, e limita a análise de casos concretos, especialmente os mais complexos. Por isso, "mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos da personalidade de alguém, podendo levar a práticas discriminatórias" (DONEDA, 2006, p. 162).

Portanto, os dados pessoais, da forma como o sistema europeu os definiu, podem ser: uma imagem, uma conversa gravada, uma filmagem, hábitos de consumo pessoal, registrados por meio de Internet ou administradora de cartão de crédito, dentre outras informações. Vê-se que as possibilidades são várias, devido a tudo estar interligado tecnologicamente nos dias atuais, num maior ou menor grau. Assim, simples dados cadastrais quando cruzados e comparados com outros de outro sistema, mediante a mineração de dados, podem detalhar quase muitos os aspectos da vida de uma pessoa.

Diante desse panorama, a Lei nº 13.709/2018 deveria prever uma definição mais ampla do que são dados pessoais, como ocorre na legislação interna dos países europeus que legislaram primeiramente sobre a matéria, tendo em vista o caráter geral da LGPD

---

[27] O processo de minerar dados visa descobrir conexões escondidas e prever tendências futuras (...) o termo "mineração" só foi cunhado nos anos 1990, mas sua base compreende três disciplinas científicas interligadas: a estatística (o estudo numérico das relações entre dados), a inteligência artificial (inteligência exibida por softwares e/ou má-quinas, que se assemelha à humana) e a *machine learning* (algoritmos que podem aprender com dados para realizar previsões) (MÈLO, 2019, p. 116).

(RODOTÁ, 2008). Outra razão para se trazer essa definição mais ampla é que o Brasil faz parte da Rede Ibero-americana de Proteção de Dados – RIPD e o interesse primordial das instituições que atualmente constituem esta Rede é promover o desenvolvimento do direito fundamental à proteção de dados pessoais, a fim de conseguir obter adequação ao sistema europeu de proteção desses dados.

Referente à anonimização dos dados, a previsão encontra-se no inc. III[28] do artigo 5º, sendo, pois, o processo pelo qual o dado pessoal passou para torná-lo anônimo, tornando-o não vinculável ao titular do dado, assim, não será possível, via de regra, ligá-lo a uma pessoa. É um termo que será muito utilizado na cultura de proteção de dados. Exemplo de anonimização é a criptografia.

2.3 Tratamento dos dados e princípios que fundamentam a LGPD

Na forma da LGPD as atividades relacionadas ao tratamento de dados pessoais devem fundar-se na boa-fé (art. 6º, LGPD) e em outros princípios que serão melhor descritos a seguir.

O princípio da boa-fé é destacado como um princípio fundamental aplicável a todos os ramos do Direito, máxime na área obrigacional. Sua principal função é estabelecer um padrão de conduta ético a ser seguido pelas partes, em todas as relações jurídicas, nas dimensões: boa-fé objetiva e a boa-fé subjetiva. A boa-fé-subjetiva é de difícil perquirição, porque incrustrada na reserva mental do indivíduo, antes prevista vetusto diploma civilista (CC/1916), deu lugar a boa-fé objetiva haurida da conduta externada pelo agente nas relações obrigacionais (art. 422, CC; art. 4º, inc. III do CDC), incluída a boa-fé administrativa, própria das relações entre a Administração Pública e os particulares (art. 2º, inc. IV da Lei 9.784/1999).

Nesse passo, na aplicação, interpretação e execução da LGPD deve ser observada a boa-fé objetiva na operação de tratamento de dados pessoais, o que majora os deveres anexos de agir com: cuidado, respeito, lealdade, honestidade, probidade, colaboração ou cooperação, razoabilidade, equidade, boa razão e, ainda, em conformidade com a confiança depositada que

[28] Inc. III do art. 5º da LGPD – "III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

atrai o dever de informar a outra parte acerca do conteúdo de determinado negócio (PINHEIRO, 2020).

O princípio do consentimento informado, por seu turno, é um desdobramento do princípio da boa-fé objetiva. A Lei nº 13.709/2018 traz a figura do consentimento livre, espontâneo, específico, informado e qualificado. O artigo 5º, inc. XII entende o consentimento como "a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018, s.p.).

O consentimento deverá estar relacionado às finalidades determinadas: (i) não há valia no consentimento genérico (*blanket consent*), pois serão nulas (art. 8º, § 4º, LGPD); (ii) deve ser requerido novo consentimento cada vez que o uso dos dados passar por atualização, preservando o livre acesso, a qualidade dos dados e a transparência; (iii) em caso de alteração de informação, deve o controlador informar ao titular dos dados, com destaque específico ao conteúdo das alterações, podendo o titular, naqueles casos em que for obrigatório o seu consentimento, revogá-lo caso não concorde com a mudança (art. 8º, § 6º; 9º, I, II, III, V da LGPD).

O princípio da informação além de ser um princípio constitucional (art. 5º, incs. IV, XXII e XXIV da CRFB/1988) é também um princípio do CDC. No Direito do Consumidor, o dever de informação e de transparência inauguram novas regras de conduta no mercado, ao inverter a ultrapassada ideia do *caveat emptor*, segundo a qual cabia ao consumidor, pessoalmente, buscar por informações referentes ao produto ou serviços, para a regra oposta do *caveat vendictor*, pois, é dever do fornecedor informar ao consumidor sobre todos os aspectos relevantes sobre o produto nos termos do artigo 6º, inc. III, artigos 8º, 9º e 31, todos do CDC.

Na LGPD, a obrigação legal de informação tem amplo espectro, abrange qualquer situação na qual o titular de dados pessoais manifeste seu interesse, relacionados com os direitos de personalidade e autodeterminação. Ainda, se aplica o *caveat personal data holder*, em que há o dever de informação permanentemente e de forma adequada, ao titular e de seus representantes legais, de todos os aspectos relevantes acerca do tratamento dos seus dados pessoais (BRAMANTE; DE MARTINO; ALVES, 2021).

É o direito à informação que assegurar ao titular dos dados pessoais um consentimento informado, qualificada e consciente, ou uma vontade qualificada. O poder de escolha e

tomada de decisão do titular de dados pessoais depende, em grande parte, da informação que lhe é transmitida, a partir da qual haverá a formação da opinião, do poder de decisão livre e da emissão do consentimento informado. A falta da informação acarreta um vício no consentimento, representa falha na operação de tratamento de dados e agregados aos elementos dano e o nexo causal gera o dever de indenizar por danos materiais e morais. O dever de informação será efetivamente cumprido quando esta for revestida da necessária especificidade, individualidade e clareza, sendo insuficiente a informação genérica. Da mesma forma que é impossível validar a informação genérica (*generic information*), não há valia no consentimento genérico (*blanket consent*), que necessita ser informado, específico, claro e individualizado (BRAMANTE; DE MARTINO; ALVES, 2021).

O artigo 6º, inc. I, dispõe sobre o princípio da finalidade específica definindo-o como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018, s.p.).

Neste caso, ganha importância a teoria dos fins determinantes para aferição do legítimo interesse e da adequação no tratamento de dados.

Os princípios da finalidade, adequação e necessidade formam um tripé que dá origem ao legítimo interesse. Cumpre destacar que a interpretação desses princípios deve ser feita levando-se em conta direitos específicos do titular, a saber: "liberdade, privacidade, intimidade, inviolabilidade da honra e da imagem" (BRASIL, 1988, s.p.), encravados como cláusulas pétreas no artigo 5º, *caput*, e incs. V e X da CRFB/1988. A finalidade há que ser específica, sendo vedado o tratamento de dados com fins genéricos. Aliada a esta vedação, a finalidade, ainda, deve corresponder aos propósitos legítimos, específicos e comunicados ao seu titular, sem que exista possibilidade de tratamento posterior de maneira incompatível com as aludidas finalidades.

O princípio adequação ou idoneidade diz respeito à compatibilidade do tratamento com as finalidades comunicadas ao titular, em conformidade com o contexto em que é feito o tratamento (art. 6º, inc. II da LGPD). Ainda, relaciona-se com a necessidade ou exigibilidade, sendo um mandado de otimização que comanda: na tipologia e procedimentalização da operação dos dados pessoais a serem tratados devem ser eleitas aquelas compatíveis, correlacionadas e relevantes com a finalidade e a necessidade informada. O tratamento de

dados deverá guardar relação com a destinação que possui, vedadas a contradição e a incompatibilidade com a atividade-fim (MULHOLLAND, 2020).

A título de exemplificação, configura-se tratamento de dados inadequado, a captação dados de saúde e do convênio médico do titular, com o pretexto de concessão de desconto no *e-commerce* de produtos farmacêuticos, pois o dado coletado perfilha tipologia incompatível com a finalidade.

O princípio da necessidade ou da minimização, ou da intervenção mínima da privacidade, ou da vedação do excesso comanda a restrição do tratamento ao mínimo necessário para que suas finalidades sejam realizadas, abrangendo os dados pertinentes, proporcionais e que não se mostrem excessivos no que concerne às finalidades do tratamento de dados, consoante inteligência do artigo 6º, inc. III da LGPD e, por esta razão, atrai os princípios da proporcionalidade e da razoabilidade.

O princípio da proporcionalidade, é oriundo do direito alemão (*civil law*) e decorre diretamente do princípio da legalidade e da pauta de valores demarcados no Estado de Direito, com evidente ligação ao princípio da constitucionalidade, segundo o qual: (i) os direitos fundamentais encravados na CRFB/1988 regem todo ordenamento jurídico (ii) e servem de limites aos poderes constituídos (iii) instrumental axiológico para promover a contenção da arbitrariedade no exercício dos direitos e da instrumental axiológico para promover a contenção da arbitrariedade no exercício dos direitos e da autonomia privada. O princípio da razoabilidade trata-se de noção jurídica do razoável, enquanto *standard*, oriundo do *common law* no direito inglês. Deste modo, os elementos ou subprincípios da proporcionalidade são: adequação ou idoneidade; conformidade; necessidade ou exigibilidade; e, por fim, o princípio da proporcionalidade em sentido estrito (OLIVEIRA, 2006).

O princípio da necessidade, também conhecido como princípio da exigibilidade, da indispensabilidade, da suficiência, da vedação do excesso, decorre da necessidade na operação de dados pessoais, que apenas deve ocorrer: (i) quando for de extrema necessidade a proteção do legítimo interesse e a proteção do interesse público; (ii) quando for o menos invasivo possível na esfera privada do indivíduo; (iii) quando for a melhor possibilidade viável para a obtenção de certos fins; (iv) quando apresentar menor custo ou gravame ao indivíduo (MULHOLLAND, 2020).

Com efeito, em meio à existência de diversos meios idôneos, ordena-se à preferência aquele que se mostra menos gravoso ao exercício dos direitos fundamentais. Caso exista

somente uma medida adequada, é importante que seja apurada a existência de outra alternativa diferente, mas igualmente apropriada e eficaz, além de menos danosa ao direito fundamental em análise.

Trata-se do sopesamento dos bens jurídicos tutelados pelos princípios constitucionais que se confrontam: de um lado a livre-iniciativa e a autonomia privada ou, a determinação legal no tratamento dos dados pessoais; de outro os direitos de personalidade. Assim, como expõe Mulholland (2020), é autorizada uma medida restritiva do direito fundamental para a obtenção de uma dada finalidade perseguida e autorizada na lei. Ainda, trata-se de indagar se a medida é capaz, favorável, adequada e apropriada para chegar ao fim perseguido. Assim da relação medida-fim surge o princípio da conformidade, da adequação, à consecução de um fim suficiente ao que se visa concretizar.

Em suma, a expressão necessidade significa essencialidade, diz respeito a minimização de dados e das responsabilidades. Assim, a operação de dados pessoais deve ser restritiva ao mínimo essencial e necessário, para a realização das finalidades pretendidas, vedada o excesso. O operador de dados deve fazer uma ponderação entre o que é conveniente e o que é realmente essencial para o seu negócio jurídico. Cumpre lembrar que quanto mais dados pessoais forem tratados, maior será a responsabilidade pelos incidentes, invasão, vazamentos, etc. Equivale dizer, que a maximização de dados acarreta por igual o aumento da responsabilidade. Significa que é recomendável um *compliance*, um levantamento e uma varredura dos dados pessoais armazenados e de suas naturezas, bem como uma revisão na estrutura de armazenamento e de segurança da informação, a fim de que esta se mostre adequada à magnitude da operação (TEIXEIRA, 2020).

O livre acesso refere-se a garantir, aos titulares, consulta simples e gratuita a respeito da forma, duração do tratamento e sobre a integralidade de seus dados pessoais (art. 6º, inc. IV, LGPD). Este princípio decorre do princípio da transparência e eleva o direito à informação, a comunicação e a consulta sobre o tratamento dos dados pessoais e, que sejam de fácil acesso e compreensão, formulados em uma linguagem clara, simples e objetiva. O livre acesso às informações e aos dados deve ficar à disposição do titular de forma física, mediante requisição do titular; por meio eletrônico e ou de visualização sempre que for adequado. O formato de acesso pode ser por meio de declaração clara e completa, sendo indicada a origem dos dados, a ausência de registro, os critérios empregados e o fim do tratamento, resguardados os segredos comerciais e industriais. O formato da entrega será

simplificado e imediato, o que torna possível a sua posterior utilização, inclusive em outras operações de tratamento de dados. Para tanto, o diploma legal estabelece que as respostas precisam ser encaminhadas em um prazo máximo de 15 dias a partir da data em que o titular procedeu ao requerimento (art. 19 da LGPD). Para operacionalizar o direito as empresas devem possuir um departamento ou pessoa encarregada, responsável em receber o requerimento e dar a resposta, ciente importância e das consequências advindas da lesão do direito (BRASIL, 2010).

O princípio da qualidade, no que diz respeito ao tratamento de dados pessoais deve ser o objetivo fixo de qualquer gestor de dados, porque encerra também o dever de adaptação, melhoria contínua e, principalmente, o dever de segurança (FLUMIGNAN; FLUMIGNAN, 2020). Esse princípio atende a um duplo desiderato: oferecer segurança e evitar riscos aos seus titulares de discriminação, invasão da privacidade; é, pois, condição importante para o firmamento de uma empresa no mercado competitivo.

A qualidade conecta-se com os princípios da transparência e do livre acesso, porque garante ao titular conhecer:

> [...] a exatidão, clareza, relevância e atualização dos seus dados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento. Ainda, oferece ao titular dos dados o direito de correção de dados incompletos, inexatos ou desatualizados; o direito de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e; sobre a possibilidade de não fornecer consentimento e sobre as consequências negativas (PONTES, 2018, s.p.).

Todos os processos pertencentes a uma determinada empresa interagem entre si e podem afetar os resultados obtidos em todo o sistema da organização. Por esta razão devem ser identificados e gerenciados. Um dado pessoal coletado de forma inadequada, ou mantido desatualizado, pode acarretar uma sequência de impactos negativos e incidentes em relação ao titular, cliente, fornecedores e parceiros. Pode acarretar também punições e as indenizações cabíveis.

Esse princípio é previsto no CDC e dispõe que o consumidor tem o direito fundamental à proteção de sua vida e saúde. Desta forma, o fornecedor não está autorizado a colocar no mercado determinados produtos ou serviços que sejam potencialmente arriscados ao consumidor. Os riscos devem ser advertidos com clareza, inclusive, agregando orientações

seguras sobre a melhor forma de minimizá-los (art. 6º, inc. I; art. 8º; art. 10 e art. 12, § 1º, do CDC).

O princípio da transparência (*right to be informed*) traz aos titulares a garantia de informações explícitas, precisas e acessíveis a respeito da coleta, tratamento e uso dos seus dados pessoais, incluindo os seus propósitos, os períodos de retenção e a operação de compartilhamento com terceiros, pelos agentes de tratamento, resguardados os segredos comerciais e industriais (art. 6º, inc. VI da LGPD). Logo, *a contrario sensu*, é vedada a conduta de operação e compartilhamento de dados pessoais de forma oculta, subliminar ou sub-reptícia.

O princípio da segurança diz respeito ao emprego de medidas técnicas e administrativas visando proteger os dados pessoais contra acessos não autorizados e eventos acidentais ou ilícitos que gerem destruição, perda, modificação, comunicação ou difusão. O cerne da lei é a proteção dos dados pessoais contra invasão, acessos indevidos ou não autorizados, para evitar o resultado chamado privacidade hackeada. A prevenção refere-se à adoção de medidas que previnam os danos decorrentes do inadequado tratamento de dados pessoais (art. 6º, inc. VIII da LGPD), reforçando o entendimento de Melo e Dias (2014) que fazem alusão à refundamentação da responsabilidade civil através do princípio da prevenção.

Destarte, na observância dos princípios da prevenção, da precaução e da segurança, a novidade da LGPD é utilização do código trinário lícito/ilícito/abuso de direito na consideração de que existem atividades empresariais, que por si só, apresentam potencial ou efetivo risco de lesão a integridade material e moral das pessoas. Ainda há condutas, embora lícitas, podem ou não produzir um resultado ilícito (invasão da privacidade) e ou um dano (material e moral). O cerne da lei é deslocado da conduta para o resultado (BRAMANTE; DE MARTINO; ALVES, 2021).

Já o princípio da prevenção comanda a adoção de medidas que previnam a ocorrência de danos decorrentes do inadequado tratamento de dados pessoais e não se confunde com precaução. Este princípio visa impedir o risco de perigo in concreto; retrata o dever de diligência, é um dos desdobramentos da responsabilidade civil e um dos pilares da segurança, e apresenta as seguintes características: (i) visa inibir o dano potencial e vem fundamentado em uma certeza científica de que certa atividade poderá causar danos; (ii) a decisão de prevenção se localiza no presente, independentemente da efetividade das consequências futuras; (iii) impõe as necessárias medidas efetivas prévias para elidir ou minimizar os riscos

da operação que possam ocorrer; (iv) indica a necessidade de estratégias antecipadas, para lidar com as consequências danosas de certas atividades de risco, passíveis de serem evitadas ou, ao menos, de terem seus efeitos mitigados por decisões (BRAMANTE; DE MARTINO; ALVES, 2021).

Existe diferença entre prevenção e precaução no binômio: incerteza/certeza em relação às consequências de uma atividade econômica. Assim a LGPD oferece estratégias no sistema jurídico e na sociedade para que os riscos sejam tratados de forma a elidir, prevenir e ou mitigar eventuais incidentes danosos. O princípio da precaução objetiva conter o risco de perigo *in abstrato* e, para esse desiderato, indica estratégias para lidar com as incertezas decorrentes da impossibilidade de prever as consequências de determinada atividade desempenhada pelo homem.

Na modernidade, a prevenção e a precaução trazem um problema novo para o sistema jurídico: a utilização do código binário lícito/ilícito sobre condutas já definidas como lícitas, mas que podem ou não desencadear um resultado ilícito (dano), embora sem ter a certeza de que esse resultado realmente será produzido. Agregue-se que, as condutas embora lícitas podem causar danos. Por isso, o sistema jurídico insere a precaução e prevenção para evitar resultados lesivos, e equipara ao ilícito a conduta de abuso do direito como ato ilícito (ROSA, 2021).

A lei veda que os dados pessoais sejam tratados para fins discriminatórios (princípio da não-discriminação) ou para finalidades ilícitas ou abusivas (art. 6º, inc. X, LGPD). Ainda, traz regras específicas para o tratamento dos dados pessoais sensíveis, a exemplo dos que guardam relação com origem racial ou étnica, crença religiosa, convicção política, filiação a algum sindicato ou a organizações religiosas, filosóficas ou políticas, dado sobre a saúde, sexualidade, dado genético ou biométrico (ROSA, 2021).

O último dos princípios, o princípio da responsabilização e da prestação de contas requer que o agente demonstre que está fazendo uso de medidas eficazes e aptas a comprovar se as normas protetivas de dados pessoais têm se mostrado eficazes e, inclusive, do quão eficazes são estas medidas (art. 6º, inc. X, LGPD). E de rigor o cumprimento integral da lei, e as empresas devem ter provas de todas as medidas adotadas, e que demonstram a boa-fé e as diligências encetadas.

Todos esses vocábulos e definições serão muito úteis ao operador do Direito e ao aplicador da Lei quando houver um pedido, feito pelo titular acerca dos seus dados pessoais,

pois a coleta, o armazenamento e o descarte desses dados devem atender às exigências da LGPD, a forma prescrita na lei, aí incluindo os meios digitais, como está estampado no artigo 1º[29] deste diploma legal.

O legislador infraconstitucional, além de dispor sobre o tratamento, previu um a um os fundamentos pelos quais se dará a proteção de dados pessoais. Na realidade, assenta no artigo 2º[30] o porquê, de os dados pessoais necessitarem de proteção, quais sejam: o respeito à privacidade, como direito fundamental, a autodeterminação informativa (porque cabe ao titular dos dados o poder sobre suas informações), a liberdade de expressão, a inviolabilidade de sua imagem, intimidade, e o livre desenvolvimento da personalidade humana, direito este fundamental.

2.4 Aspectos positivos e negativos da LGPD

A dinâmica de atividade e desenvolvimento da cultura digital contemporânea se desenvolve em uma via de mão dupla, ao mesmo tempo em que oferece a conectividade contínua ao usuário, este obrigatoriamente permite a coleta e armazenamento de seus dados individuais.

Em outras palavras, para que o consumidor mantenha seu acesso individualizado ao serviço, ele próprio consente para com o seu monitoramento contínuo. Assim, mediado pelas tecnologias digitais, o usuário passa a facilitar o seu próprio controle em troca de ter o seu espaço na vitrine das redes sociais e às comodidades dos serviços que fazem uso de seus dados.

Em posse do conhecimento do perfil de cada segmento através do compartilhamento de dados, as empresas exploram as informações individuais para levar os usuários a consumirem pelo desejo de inserção e projeção social (GRANERO; COUTO, 2013).

---

[29] Art. 1º da LGPD. “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”.

[30] Art. 2º da LGPD. “A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais”.

Em uma sociedade onde a competitividade e o estresse encaminham os sujeitos à constituição de um corpo social alicerçado na ansiedade, o compartilhamento de dados personalíssimos é um grande risco, terreno rico para manipulação de dados, algoritmos e fraudes.

No que concerne à manipulação de algoritmos que direcionam o comportamento do consumidor, é importante que exista limites, no entanto, no Brasil, atualmente não há uma legislação específica para o setor de inteligência artificial que obrigue as empresas a informarem sobre o funcionamento de seus algoritmos (MEDEIROS, 2022).

A título de exemplo, a empresa britânica de publicidade na internet, Phorm, através de um recurso chamado *Deep Packet Inspection* – DPI (Inspeção Profunda de Pacotes de Rede) obtém informações de seus usuários que permite analisar o tráfego virtual do mesmo justamente para direcionar sua publicidade.

Pela lógica privada a DPI possibilita o fornecimento de um serviço direcionado e mais qualificado ao usuário consumidor. No entanto, conforme o Observatório Brasileiro de Políticas Digitais, a DPI traz o risco de invasão de privacidade e monitoramento excessivo dos usuários. Tal recurso nas mãos de governos ditatoriais pode significar risco à democracia e risco à liberdade (BOFF; FORTES, 2014).

Em conjunto com todo esse acesso de dados é possível a elaboração de um *marketing* agressivo e segmentado a cada consumidor no ciberespaço que é chamado de usuário. Dessa forma, não se pode olvidar que o poder de consumo passa a ser régua ainda mais hierarquizante nas mídias sociais, que vivem da exposição do consumo. Assim, o consumidor orienta o seu consumo pela mídia, pois o consumo passa a desempenhar um papel de mediador dos valores e hierarquias no corpo social, fomentando ainda mais, pelas redes, a desigualdade social, marcada pela inacessibilidade de experimentar o que é veiculado pela mídia e pelas redes:

> Numa sociedade sinóptica de viciados em comprar/assistir, os pobres não podem desviar os olhos; não há mais para onde olhar. Quanto maior a liberdade na tela e quanto mais sedutoras as tentações que emanam das vitrines, e mais profundo o sentido da realidade empobrecida, tanto mais irresistível se torna o desejo de experimentar, ainda que por um momento fugaz, o êxtase da escolha. Quanto mais escolha parecem ter os ricos, tanto mais a vida sem escolhas parece insuportável para todos (BAUMAN, 2001, p. 114).

Com a intensificação da interação pelas redes sociais, a exemplo do *facebook, instagram, youtube* e *google*, acaba-se criando uma dinâmica da cultura digital que é marcada pelo consumo e pelo *marketing* ainda mais incisivo. Isso porque para o consumidor poder acessar as redes sociais, ele precisa consentir com o seu monitoramento contínuo e com o uso de seus dados:

> A dinâmica de funcionamento da cultura digital capitalista contemporânea está fortemente ligada à busca do prazer e, por outro o consumidor, para ter acesso individualizado um serviço ou bem, passa a participar de uma rede na qual seus dados serão coletados e armazenados. A facilitação do acesso ao prazer garantida pela conectividade contínua implica também, sob esse ponto de vista, numa facilitação do controle a partir de um monitoramento contínuo. Esta relação entre busca do prazer e aceitação do controle se dá, em boa medida, através da mediação de tecnologias digitais (RODRIGUES, 2018, p. 199).

O ciberespaço trouxe muitas facilidades à rotina diária de trabalho, no entanto, sem a regulamentação necessária o espaço virtual proporciona terreno fértil à captura do inconsciente do homem, e, consequentemente, não só ao estímulo muito mais forte ao consumo, mas à fragilidade diante da dificuldade em compreender a dinâmica da rede no qual se encontra como usuário[31]. Esta fragilidade pode favorecer o aumento da criminalidade, especialmente o cometimento de delitos virtuais, uma vez que há dificuldade na identificação dos agentes, na determinação de competência de jurisdição, aliado a isso, as transações são realizadas em velocidade muito maior por meio de contratos de adesão e com baixos custos e lucros imediatos[32].

---

[31] Nesse sentido, o ciberespaço acaba por abalar os alicerces do Direito Privado, uma vez que a autonomia sofre alterações em seus aspectos objetivo, subjetivo e formal. Do aspecto objetivo devem-se abranger novos bens jurídicos como os dados existenciais e pessoais que circulam pela rede com finalidade comercial, ou seja, há um repasse de informações personalíssimas de usuários ou terceiros. Sob o aspecto subjetivo novos interesses devem ser tutelados, uma vez que o potencial lesivo da informática no que tange à intimidade de seus usuários é muito amplo e multifacetado. No que concerne à forma, o aparato registral constituído pela legislação vigente torna-se insuficiente para atender os negócios jurídicos realizados no ciberespaço. As relações negociais de consumo celebradas via aplicativos/sites acaba por exigir uma autenticação formal inteiramente nova, com a finalidade de proteção não somente do patrimônio como se encontra no aparato legislativo atual, mas de proteção também a valores existenciais, como identidade pessoal, intimidade, honra, privacidade e direito à informação. Segundo Martins (2014), os negócios efetuados no ciberespaço desafiam os fundamentos da teoria contratual, estabelecendo a necessidade de definição normativa protetiva ao usuário: Esse cenário de transformação torna-se ainda mais complexo quando se têm em mente os negócios celebrados pela Internet, já que, neste caso, todos os fundamentos da teoria contratual são desafiados a darem resposta às demandas de segurança indispensáveis ao sucesso das transações. Estas, em volume gigantesco, mobilizam usuários em todo o mundo, exigindo a definição urgente da normativa aplicável para a proteção de quem contrata serviços ou adquire produtos no ciberespaço.

[32] Para se destacar o potencial lesivo dos delitos virtuais e sua ocorrência crescente destaca-se que dados levantados pela Central Nacional de Denúncias de Crimes Cibernéticos da Organização Não-Governamental (ONG) *Safernet* Brasil, dados estes que são reportados voluntariamente a entidade por usuários quando

> Ainda sobre a vulnerabilidade no ciberespaço pelo uso de dados personalíssimos, pode-se identificar a ineficiência de políticas de privacidade, fomentando até mesmo fraudes: As vítimas por sua vez, são vulneráveis, [...] pois acreditam estar seguras, por conta da política de privacidade que a maioria das páginas e sites diz praticar. O que não é verdade, tais políticas não são infalíveis, mostram-se ineficazes diante de inúmeros crimes praticados se beneficiando das mesmas. Todos os usuários, [...] independente do nível social, cultural e de escolaridade estão passíveis de sofrer algum tipo de crime virtual. Quanto maior o nível de exposição de informações pessoais, maior o risco de sofrer algum golpe. Uma reportagem publicada no site JusBrasil mostra que as mulheres são a maioria entre as vítimas de crimes contra a honra, em uma faixa etária de 25 a 45 anos, e a maioria com formação superior. Em pesquisa feita pelo jornal O Dia, foi demonstrado que entre os adolescentes de 11 a 17 anos, os crimes contra a honra aparecem em destaque. [...] De maneira geral, crianças e jovens são as principais vítimas de crimes cibernéticos (DESLANDES; ARANTES, 2017, p. 177).

O estudo indica que a vulnerabilidade é ainda mais acentuada no ciberespaço, e a permissão de coleta de dados é um risco que os consumidores usuários, sem a devida informação, pagam para continuar tendo acesso às redes sociais que ditam a interação pela mentalidade do consumo e o consumidor, usuário de aplicativos no ciberespaço, apresenta uma vulnerabilidade ainda mais sensível que o consumidor tradicional, isso porque o primeiro é incapaz tecnicamente de entender a rede no qual está submerso, não se olvidando às dificuldades atinentes ao idioma, usos contratuais alienígenas, da lei aplicável e da incerteza quanto ao local de contratação (DESLANDES; ARANTES, 2017).

Esta conjuntura fragiliza sobremaneira não só a posição contratual do consumidor, como também influencia o seu processo de tomada de decisão, já que o compartilhamento de seus dados personalíssimos é capaz de fomentar a sua própria manipulação. Dessa forma, usuários submetem-se às cláusulas abusivas para buscar visibilidade e acesso na era de aparências ditadas pelo triunfo das redes sociais.

Por esta razão entende-se que uma das principais vantagens da LGPD é a garantia do fortalecimento da segurança dos dados. Diversas obrigações que devem ser observadas pelos agentes de tratamento são listadas na LGPD, a começar pelos procedimentos que devem ser cumpridos até a existência de mecanismos empregados na prevenção e no controle de danos.

---

encontram conteúdos criminosos, em 2014 os crimes cibernéticos aumentaram 8,29%. Crimes como os de apropriação de conteúdo, como, por exemplo, de fotos íntimas, cresceram 119,8%. Nas denúncias recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos no Brasil mostram que em 2016 foram encontradas 593 páginas relacionadas com o crime de racismo, 284 páginas com pornografia infantil, 246 páginas de apologia a crimes contra a vida, 83 páginas de xenofobia, 82 páginas de homofobia, 71 páginas com relação a tráfico de pessoas, 31 páginas com intolerância religiosa, 19 páginas referentes a maus tratos contra animais (DESLANDES; ARANTES, 2017, p. 176).

Os agentes ficam sujeitos a sanções caso cometam infrações. Referidas sanções vão desde as advertências, multas e suspensão até a proibição das atividades de tratamento de dados a depender da gravidade do caso. Referente à responsabilidade civil pelos danos causados, esta legislação cumulou a possibilidade de responsabilização do responsável pelo tratamento dos dados com subcontratantes e a responsabilidade solidária com direito de regresso sobre os demais agentes.

Como já visto, dentre os princípios da LGPD, destacam-se: o da finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, todos eles contidos no artigo 6° do aludido diploma legal. Denota-se a consolidação e organização do sistema de proteção de dados em formação no Brasil através da cristalização de tais princípios na LGPD de forma a fortalecer a coerência da lei e unidade do sistema com destaque para a identificação de seus preceitos ao longo de seus dispositivos.

Nesse contexto, é imperativo destacar a reflexão de Rodotá (2008) ao indagar sobre o real benefício do surgimento de legislações rígidas abordando a proteção de dados. A percepção do autor vislumbra que a rigidez de ordenamentos jurídicos e legislações, com possível abandono do protagonismo de cláusulas gerais e princípios, os tornam obsoletos rapidamente, posto que, na sociedade da informação, as mudanças são constantes e frenéticas. A adaptabilidade dos princípios com novas interpretações e mutações solidifica a proteção ao direito.

Destaca-se como ponto negativo da LGPD em relação à responsabilização civil o fato de o ônus da prova referente ao preenchimento dos três requisitos necessários para responsabilizar os responsáveis pelos danos - ilicitude, dano e nexo causal -, ser de iniciativa daqueles que forem lesados, consoante exposto no artigo 82.

Compreende-se que o correto seria atribuir a responsabilidade objetiva à pessoa física ou jurídica que detiver os dados de terceiros, tendo em vista que esta atribuição poderia servir para elevar o comprometimento com o tratamento adequado de dados, com a ressalva de que sempre deve existir a possibilidade de o ônus da prova ser invertido.

Um segundo ponto negativo digno de relevo é que a massificação das relações sociais e econômicas torna cada vez mais propícia a utilização e análise de perfis de redes sociais para seleção de candidatos a vagas de emprego.

Schreiber (2014) aponta que entidades públicas e privadas se valem com certa frequência de padronizações com o objetivo de avaliar os indivíduos. Nesse contexto, os dados pessoais fornecidos de forma irrefletida ou obtidos involuntariamente são utilizados para construir os perfis dos candidatos. A partir desses dados verifica-se se cada indivíduo enquadra-se nas exigências e características que o gestor das informações entende ser relevantes. Trata-se do chamado *data mining*, expressão utilizada para designar a atividade de extrair padrões de determinados conjuntos de dados, relegando os candidatos a certos perfis comportamentais.

Exemplo a ser citado é que, apesar de o artigo 373-A, inc. II[33] da CLT vedar recusa de emprego em virtude de estado de gravidez, salvo quando a natureza da atividade a ser exercida seja notoriamente incompatível com gestação, uma vez que a Lei nº 9.029/1995 proíbe a exigência de atestados de gravidez, esterilização e quaisquer outras práticas discriminatórias em exames admissionais, as redes sociais tornaram-se aliadas nessa busca de dados acerca do planejamento familiar feminino.

Tal fato veio a facilitar novamente a discriminação velada por parte de contratantes que somente vislumbram diminuição de custos, eliminando tais candidatas imediatamente, pois não desejam funcionárias ausentes do trabalho no período da licença-maternidade. Qualquer ato de tratamento de dados com vistas ao impedimento de acesso da mulher ao mercado de trabalho em virtude de seu planejamento familiar ou da maternidade, sem justificativa plausível, deve ser considerado discriminatório, sendo cabível pagamento de indenização, uma vez que tal proteção advém de artigos constitucionais como o valor social do trabalho, artigo 1°, inc. IV[34]; o objetivo de erradicar quaisquer formas de discriminação, artigo 3°, inc. IV[35] e a proteção à maternidade, artigo 10, inc. II, alínea b[36] do Ato das

---

[33] Artigo 373-A da CLT– "Ressalvadas as disposições legais destinadas a corrigir as distorções que afetam o acesso da mulher ao mercado de trabalho e certas especificidades estabelecidas nos acordos trabalhistas, é vedado: [...] II - recusar emprego, promoção ou motivar a dispensa do trabalho em razão de sexo, idade, cor, situação familiar ou estado de gravidez, salvo quando a natureza da atividade seja notória e publicamente incompatível".

[34] Artigo 1º do Ato das Disposições Constitucionais Transitórias - "A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...] IV - os valores sociais do trabalho e da livre iniciativa".

[35] Artigo 3º do Ato das Disposições Constitucionais Transitórias - "Constituem objetivos fundamentais da República Federativa do Brasil: [...] IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação".

[36] Artigo 10 do Ato das Disposições Constitucionais Transitórias – "Até que seja promulgada a lei complementar a que se refere o art. 7º, I, da Constituição: [...] II – fica vedada a dispensa arbitrária ou sem justa causa: b) da empregada gestante, desde a confirmação da gravidez até cinco meses após o parto".

Disposições Constitucionais Transitórias – ADCT por extensão. No entanto, fazer prova desta discriminação neste caso é muito difícil, já que a empresa não assumirá que a contratação da mulher não ocorreu em razão de sua gravidez.

A discriminação estética também está em voga com a massificação das redes sociais. Empresas e contratantes têm a possibilidade de conhecerem visualmente o candidato à vaga de trabalho, baseando-se além do currículo profissional dos trabalhadores. Constante também é a vigilância de condutas dos trabalhadores por meio das redes sociais pelas empresas, que verificam se há consonância com o perfil estabelecido pela empresa em relação a opiniões políticas e sindicais, opções religiosas, preferências sexuais, costumes (MACHADO, 2019). Caso não haja sintonia, os trabalhadores podem ser censurados ou, até mesmo, despedidos, apesar dos dispositivos constitucionais que preveem liberdade de pensamento, liberdade de associação sindical, liberdade de crença, convicção filosófica ou política, conforme artigo 5º, incs. IV, VI, VIII, XVII[37] e artigo 8º, *caput*[38].

Outra lacuna identificada é a de que a LGPD baseia-se na livre iniciativa, no desenvolvimento econômico e tecnológico do país, em consonância com a dignidade e o exercício da cidadania. O artigo 1° da aludida legislação objetiva garantir a proteção da liberdade e da privacidade como direitos fundamentais, bem como do livre desenvolvimento da pessoa natural. Porém, como bem afirma Frazão (2019), não só a privacidade é colocada em risco pela economia movida pelos dados, mas também a própria individualidade e a autonomia, devendo ser resgatada a dignidade dos titulares de dados bem como o cumprimento de direitos que guardam relação com a autodeterminação informativa serem os objetivos primordiais da LGPD.

Do exposto depreende-se, que se por um lado, a LGPD significou avanço e maior proteção às pessoas, por outro, também abriu margens para a ocorrência de eventos discriminatórios de natureza diversa. Por esta razão, mecanismos de *compliance* se fazem necessários, conforme será abordado na próxima seção.

---

[37] Artigo 5º da CRFB/1988 - "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: IV - é livre a manifestação do pensamento, sendo vedado o anonimato; VI – é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias; VIII - ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei; XVII - é plena a liberdade de associação para fins lícitos, vedada a de caráter paramilitar".

[38] Artigo 8º da CRFB/1988 - "É livre a associação profissional ou sindical, observado o seguinte".

2.5 Os mecanismos de *compliance*

A origem da palavra *compliance* encontra-se no verbo da língua inglesa "*to comply*", "*to comply with*" cuja tradução literal significa "cumprir com", "estar em conformidade com", "obedecer", dentre outros sinônimos semelhantes (BARBIERI, 2019).

O surgimento do *compliance* ocorreu a partir dos primórdios do séc. XX com a fundação do Banco Central dos Estados Unidos com o propósito de ser um ambiente financeiro dotado de maior segurança, estável e adequado às leis. Após, na década de 1970, foi criada a Lei Anticorrupção, a *Foreing Corrupt Practices Act* (FCPA), a qual estabeleceu penas mais rígidas para organizações americanas envolvidas em corrupção no exterior (FRAZÃO, 2019).

Diante dos escândalos de corrupção que nos últimos tempos envolveram empresas privadas e governos, diversas empresas deram início, de forma espontânea, à adoção de práticas e técnicas de *compliance*, obtendo bons resultados.

No Brasil, o *compliance* tem sido incorporado ao ordenamento jurídico desde a década de 1990 sendo interpretado pela legislação brasileira como o conjunto de disciplinas e práticas que devem ser seguidas, dentro e fora do ambiente corporativo, para estar em conformidade com as leis e atendendo aos padrões éticos, não se restringindo somente à prevenção da corrupção, mas estar em conformidade também com os regulamentos internos e externos de determinada empresa ou instituição, sendo esta pública ou privada. Assim, a expressão "estar em *compliance*" significa agir em conformidade com o determinado ou o permitido em lei, regulamentos internos, normas de condutas e a ética (BARBIERI, 2019).

Com efeito, dentre os diplomas legais que abordaram o *compliance* nos últimos anos, podem-se citar: o Decreto nº 678, de 06.11.1992 – Convenção Americana sobre Direitos Humanos – CADH (Pacto de São José da Costa Rica), que determina o cumprimento da CADH, de 22.11.1969; a Lei nº 9.605/1998 – Lei de Crimes Ambientais e Política Nacional de Resíduos Sólidos, a qual dispõe sobre as sanções penais e administrativas que derivam de condutas e atividades que podem lesar o meio ambiente; a LC nº 105/2001, que trata sobre o sigilo das operações de instituições financeiras e outros reguladores, que dispõem sobre procedimentos destinados ao controle da origem dos recursos que são aplicados em operações que envolvem comércio exterior e combate à interposição de pessoas valendo-se de

subterfúgios fraudulentos. Ainda, importante citar que o *compliance* vem mencionado no Decreto nº 4.923, de 18.12.2003, que traz disposições sobre o Conselho de Transparência Pública e Combate à Corrupção.

Contudo, foi com a entrada em vigor da Lei Anticorrupção – Lei nº 12.846/2013, regulamentada pelo Decreto nº 8.420/2015, que os programas de *compliance* ganharam destaque e importância para as empresas brasileiras.

Por fim e não menos importante, anote-se a referência ao *compliance* na Lei nº 12.846/2013 – Lei da Empresa Limpa, que dispõe sobre a possibilidade de responsabilização na esfera administrativa e na civil de pessoas jurídicas em razão da prática de atos que lesam a administração pública, seja em âmbito nacional ou internacional; na Lei nº 12.965/2014 – MCI, que lista princípios, garantias, direitos e deveres relacionados ao uso da rede mundial de computadores no Brasil; e no Decreto nº 9.468/2018, que conforme já citado dispõe sobre o Conselho de Transparência Pública e Combate à Corrupção.

Esse arcabouço legislativo visa regulamentar e implementar o objetivo principal do *compliance*, que é evitar que empresas pratiquem condutas antiéticas ou de corrupção, mas não é só isso, objetiva evitar a prática de quaisquer tipos de infração e desvio de finalidade, tais como fraudes, irregularidades e atos ilícitos em geral que possam, inclusive, comprometer todo o funcionamento da empresa, minimizando assim os riscos do empreendimento e garantindo maior segurança a todos os envolvidos no negócio, sejam seus administradores, representantes, funcionários e até mesmo fornecedores e prestadores de serviços (BARBIERI, 2019).

A função do *compliance* é impedir ou ao menos minimizar os riscos de práticas de condutas que não estejam em conformidade com os preceitos da empresa ou em conformidade com a lei, através do monitoramento das atividades de seus colaboradores, a fim de obstar o cometimento de atitudes ou comportamentos irregulares (FRAZÃO, 2019).

Para melhor elucidar a aplicação do *compliance* em termos práticos, Berrius e Wolf (2021) destacam algumas das principais ações que devem ser adotadas pelas empresas/organizações:

a) Elaborar um código de conduta/ética e políticas da empresa, o qual deverá ter uma linguagem clara e ser de conhecimento e domínio de todos os funcionários e colaboradores da empresa.

b) Criar um canal de comunicação prático e de simples acesso para que os funcionários, colaboradores e clientes possam relatar eventuais ocorrências que estejam em desacordo com os preceitos da empresa, respeitando, sempre que possível, o direito ao sigilo do denunciante.

c) Criar um programa e um comitê de *compliance*, o qual será responsável por nortear as ações da empresa e apurar eventuais falhas e ocorrências de práticas em desconformidade com os objetivos da empresa. Ainda, será esse o setor responsável pela aplicação das eventuais sanções cabíveis e por buscar soluções ao problema, bem como por intermediar a comunicação da empresa com as autoridades competentes.

d) Promover treinamentos e orientações aos funcionários e colaboradores de forma contínua. Essa é uma prática que deverá ser rotineira nas empresas e escritórios, pois é através desses treinamentos que será conferida a devida orientação aos colaboradores, a fim de impedir a prática de ações em desacordo com a ética, com o determinado em lei ou até mesmo em conflito com o regimento interno da empresa, deixando os colaboradores cientes das possíveis consequências de suas atitudes e das sanções cabíveis para os casos de descumprimento.

e) Agir sempre com integridade e transparência. Empresas, corporações e escritórios deverão criar um canal destinado ao controle e divulgação das informações contábeis e financeiras, principalmente para pessoas jurídicas que participam de contratos com o setor público.

As práticas de *compliance* são importantes justamente para prevenir ou ao menos minimizar as consequências advindas de eventuais atitudes cometidas por qualquer pessoa envolvida na atividade empresarial, seja pela diretoria, gestão, funcionários, colaboradores e até mesmo de fornecedores e prestadores de serviço que estejam em desacordo com as legislações ou em incompatibilidade com as políticas internas da empresa (HOFFMANN-RIEM, 2021).

Cada vez mais a sociedade exige que as empresas se comportem dentro da ética e com transparência, esperando entre outras tantas ações, que não estejam envolvidas em escândalos de corrupção, que respeitem o direito à privacidade e que demonstrem preocupação com a questão ambiental, adotando práticas sustentáveis.

Para tanto, cabe à empresa a eleição de equipe multidisciplinar para atuar de forma permanente e que seja capaz de avaliar e identificar os riscos das mais variadas naturezas e não limitados a jurídicos, socioambientais, cibernéticos, a que possa estar sujeita a empresa no cumprimento de seu objeto social. Essa equipe agirá na tomada de decisões para atitudes específicas em áreas de alto risco ou mais sensíveis, conforme a necessidade da empresa no momento, bem como será responsável ainda pelas adequações e treinamentos das equipes, funcionários e colaboradores periodicamente para que todos estejam sempre atualizados e cientes da maneira como devem se comportar dentro do ambiente de trabalho e até mesmo fora dele (ZANATTA, 2021).

Para além do *compliance*, essas boas práticas esperadas na atividade empresarial e que decorrem dos textos legais mencionados, receberam em 2018, um aditivo relacionado diretamente à Proteção do Indivíduo, mediante a edição da Lei nº 13.709/2018, chamada de LGPD, a qual dispõe sobre a proteção de dados pessoais e foi pensada diante da necessidade de melhorar a regulamentação e estabelecer princípios claros e expressos acerca do tratamento de dados pessoais.

De maneira geral, a LGPD tem o propósito de proteger o cidadão do uso abusivo e indiscriminado de seus dados, sabendo-se que as empresas privadas e demais organizações só terão o direito de solicitar os dados que de fato são necessários para que se atinja a finalidade proposta, observando-se as bases legais previstas e os princípios aplicáveis (COTS; OLIVEIRA, 2021).

Assim, a LGPD estabelece uma diversidade de regras, tanto para as empresas privadas, quanto para as instituições governamentais, com o objetivo de autorizar que o cidadão possa ter um maior controle sobre o tratamento que é destinado às suas informações pessoais.

Alguns dados ainda são tratados de maneira especial pela lei e seu uso será autorizado de uma forma ainda mais restrita. Referidos dados recebem a classificação de “dados pessoais sensíveis”, pelo fato de se referirem a questões mais subjetivas da pessoa natural, como é o caso de sua origem racial ou étnica, convicções religiosas, posicionamento na política, dados relacionados à saúde ou à sexualidade, dados genéticos ou biométricos, na forma do conceito legal antes referido (HOFFMANN-RIEM, 2021).

No geral, a LGPD é bastante direta e específica em suas definições e aplicações, cabendo às empresas e aos titulares dos dados a sua adequação às obrigações existentes e à

realidade de seu negócio, de modo a compatibilizar o tratamento inerente e adequado a cada operação, desde o início da coleta dos dados até a fase final de eliminação destes. O maior desafio neste momento é se lograr uma adequada conscientização e criação de uma cultura de proteção de dados e de privacidade, ainda muito incipiente na sociedade brasileira e praticamente inexistente na grande maioria das empresas nacionais (COTS; OLIVEIRA, 2021).

É de se reconhecer que o elemento pessoal é a figura que gera maior dificuldade de adaptação, já que está extremamente arraigada no inconsciente coletivo, a falta de preocupação com as informações pessoais, que são via de regra, amplamente fornecidas, divulgadas e negligentemente tratadas na maioria das relações comerciais. Essa conscientização se faz necessária, a formação desse direito comunitário é imprescindível para que a necessidade da proteção dos dados pessoais se embrenhe no inconsciente coletivo (DONEDA, 2006).

As empresas em geral, não possuem a cultura de guarda, tratamento, arquivamento e limitação de acesso a documentos e informações. Em muitos casos, ficam eles armazenados em locais inadequados, sem segurança, sem proteção, possibilitando o livre acesso e conhecimento. Essas são situações que deverão ser obrigatoriamente alteradas nas rotinas internas das empresas, nas quais é absolutamente necessário que a direção da companhia esteja altamente comprometida, de modo a se lograr disseminar essa cultura em todos os setores da empresa (ZANATTA, 2021).

À vista da edição e vigência da LGPD, caberá a todos, titulares e operadores, pessoas físicas e empresários, uma mudança cultural drástica, com vistas à efetiva proteção de dados e da privacidade dos titulares. Isto porque, ao estabelecer qual é o objeto do tratamento de dados pessoais, a LGPD, é bastante abrangente e no inc. X, do artigo 5º da LGPD, uma diversa gama de operações em relação aos dados é citada, a exemplo da coleta, recepção, utilização, reprodução, distribuição, armazenamento, eliminação, controle da informação, dentre outras.

Assim, todo o caminho do dado junto à corporação será importante e legalmente protegido, desde a sua recepção e coleta, até a sua eliminação e isto demandará de todas as empresas, a elaboração de projetos e programas de conformidade, de modo a estruturar e prever o mapeamento dos dados, a análise dos riscos inerentes a cada atividade, a

implementação das medidas necessárias à adequação, tratamento e salvaguarda, assim como a gestão das comunicações e treinamento de seus colaboradores.

Justamente nesse processo e na adequação do tratamento a ser atribuído aos dados pessoais surge o estreito relacionamento da LGPD com o *compliance*. Isto porque, a Proteção de Dados e o *compliance* deverão andar juntos com vistas à implementação de um programa efetivo de gestão de proteção de dados, com a efetiva observância às regras de tratamento de proteção de dados dentro das corporações (COTS; OLIVEIRA, 2021).

Dessa forma, se por um lado é função do *compliance* fazer com que as empresas atuem em conformidade com as leis, regulamentos e melhores práticas de governança corporativa, a LGPD, por outro lado, busca essa observância em relação à governança dos dados pessoais e que será alvo das operações realizadas pelas empresas.

Cabe ao *compliance* fazer o gerenciamento do risco corporativo, realizando o tratamento interno das demandas de modo a alinhar a estratégia do negócio, com as melhores práticas e controles internos, de modo a minimizar riscos, atuando em conformidade com os ditames legais e os princípios de governança (CHAVES, 2020).

A LGPD não se afasta dessa orientação, na medida em que busca, da mesma sorte, mapear as rotinas e realizar o tratamento dos dados pessoais, observadas as bases legais e princípios para o melhor e mais adequado tratamento, de modo também que os riscos sejam minimizados e as salvaguardas estabelecidas, formulando procedimentos de segurança e nos termos do artigo 50,

> [...] regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018, s.p.).

Ainda em correlação, caberá às empresas e corporações estabelecer além das políticas de governança já vinculadas ao *compliance*, também políticas de privacidade, essas atinentes à LGPD e voltadas especificamente para o chamado *assessment* de dados.

Desse modo, além das empresas necessitarem estruturar a sua área de *compliance*, a fim de atuar à luz da governança corporativa, também deverão alinhar as suas rotinas e

tratamento de dados aos ditames da lei especial destinada à proteção dos dados pessoais. São dois desafios que deverão andar juntos na gestão empresarial. Contudo, um cuidado deverá estar na mente do *board*, da direção da empresa, quanto a essas gestões, de modo a não cumular tais funções na mesma pessoa, no mesmo gestor. Veja-se que para as atividades do *compliance* é necessário que a corporação designe um responsável, uma pessoa a quem seja atribuída a coordenação das atividades relacionadas à gestão da governança, usualmente denominado de *Head of Compliance, Chief Compliance Officer* ou Chefe do *Compliance* (FEIGELSON; SIQUEIRA, 2019).

Especialmente desde a Lei Anticorrupção, de 2013, empresas cada vez mais têm tido o cuidado de nomear um gestor responsável por fazer a coordenação e gerenciamento das atividades de *compliance* da companhia. E embora, normalmente se associe a figura desse gestor à profissão de advogado, uma vez que lhe cabe a criação, desenvolvimento e disseminação de programa de *compliance* e do código de conduta a este inerente e a ser seguido pela companhia, essa função pode ser exercida por qualquer outro profissional, desde que tenha conhecimento de finanças, de legislação e especialmente, do negócio onde deverá ser implementado o programa (CHAVES, 2020).

Na mesma esteira, a LGPD destinou uma seção inteira (Seção II, do Capítulo VI) para a figura do encarregado pelo tratamento de dados pessoais, para o qual tem se adotado a denominação mediante o uso do termo em inglês *Data Protection Officer* (DPO), que é basicamente a pessoa que fará a gestão interna acerca dos requisitos de conformidade, treinamento de pessoal, tratamento de informações e auditorias, bem como o relacionamento com mercado e com a ANPD.

A LGPD não exige formação profissional determinada para o DPO, assim como não exige que o mesmo seja pessoa física ou funcionário da companhia, de modo que até que a ANPD regulamente tais normas, não há exigência ou vedação inclusive, a que o cargo de DPO seja exercido por pessoa ou empresa terceirizada para tal função.

Note-se que o mesmo silêncio e ausência de regulamentação específica se aplicam à possibilidade ou eventual vedação da empresa nomear a mesma pessoa como seu Diretor, *Head* de *Compliance* e DPO. Levando-se em conta que a LGPD se aplicará da mesma forma para todas as atividades de prestação de serviços e fornecimento de produtos, independentemente de seu tamanho. A questão ganha relevância notadamente em empresas de menor porte, nas quais não haja a possibilidade de se fazer a indicação em pessoas distintas e

a mesma pessoa necessite cumular as funções e exercer todas as atividades inerentes a esses cargos.

É muito provável que a ANPD venha a estabelecer normativas que regulamentem a necessidade ou dispensa da indicação de DPO, isso porque, a princípio, a LGPD não trata de tal situação. O § 3º, do artigo 41, prevê apenas que a ANPD "poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados" (BRASIL, 2018, s.p.). Tal regulamentação dependerá, portanto, da atuação da Autoridade Nacional.

Contudo, se considerar-se que a LGPD, sofreu relevante influência da GDPR, é muito provável que a ANPD igualmente se inspire e balize naquele regulamento e nas orientações emanadas de Autoridades Europeias, por ocasião da regulamentação das disposições da lei nacional, que ainda demandam tal complemento, como é o caso dessas definições, atribuições e condições de atuação do DPO (COTS; OLIVEIRA, 2021).

Em sendo essa a linha a ser seguida e caso efetivamente se verifique a possível influência do direito europeu na atividade da ANPD, é importante noticiar decisão proferida pela Autoridade Belga, em abril de 2020, no processo AH-2019-001313, que poderá servir de precedente para a ANPD na regulamentação da matéria atinente à figura do DPO (CHAVES, 2020).

Nessa decisão, a Autoridade Nacional da Bélgica decidiu não ser possível o mesmo gestor cumular as funções de *Head of Compliance* e DPO, condenando empresa, do ramo de telecomunicações, ao pagamento de 50.000 EUR. O fundamento da referida decisão informa que as rotinas do gestor de *compliance* incluem uma avaliação constante do tratamento de dados pessoais, de modo que não haveria a necessária isenção na supervisão dessas atividades atinentes à responsabilidade do DPO, por ambos se tratarem da mesma pessoa. Essa cumulação de cargos denotaria uma negligência da empresa e justificou a imposição da multa (CHAVES, 2020).

A decisão belga chama a atenção para uma circunstância que nem ao menos era vedada pela GDPR, haja vista que esse regulamento permite a cumulação das funções do DPO com outros cargos, desde que não haja conflito de interesses. É um precedente significativo, para um país como o Brasil, em que a lei sequer prevê a possibilidade dessa cumulação de funções, embora também não a proíba expressamente.

Como dito, o silêncio da lei deverá ser regulamentado pela ANPD, neste e em outros pontos, mas o precedente é um importante alerta para as empresas nacionais e/ou que atuam em território nacional e que ainda estão em processo de implantação de seus programas de conformidade, políticas de governança e políticas de privacidade, para que se evite essa cumulação de funções, nos cargos de Diretor, *Head of Compliance* e DPO, a qual embora não proibida, pode não ser vista com bons olhos na prática, conforme se depreende do precedente da Autoridade Nacional Belga (COTS; OLIVEIRA, 2021).

Desse modo, se a empresa já possui Programa de Governança e *Compliance*, este deverá se adequar à LGPD e se não o possui, deverá realizar a implementação dos dois programas: de Governança e *Compliance* e de Governança e Privacidade de Dados.

Dito isso, para além da conscientização das equipes internas, desde a alta direção, passando por todos os departamentos e colaboradores, a companhia deverá mapear todas as rotinas e o caminho que os dados coletados fazem desde a recepção até sua eliminação, realizando testes de segurança, para avaliar pontos e aspectos deficitários e inseguros, de modo a promover a necessária adequação e mitigar os riscos da atividade.

Ademais, a empresa deverá fazer uma avaliação precisa e objetiva acerca de quais dados são efetivamente relevantes para a atividade e que realmente merecem tratamento, de modo a limitar a sua coleta e tratamento ao mínimo de dados possível, fazendo essa gestão da forma sigilosa, reservada e segura, apenas pelo período de tempo suficiente e necessário ao tratamento, com ferramentas adequadas e procedimentos claros e transparentes; e assim, reduzir eventuais riscos envolvidos.

3 A LEI GERAL DE PROTEÇÃO DE DADOS APLICADA ÀS EMPRESAS PRIVADAS

Este capítulo aborda a LGPD aplicada às empresas privadas. Para tanto, lista as principais vulnerabilidades a que as empresas e titulares dos dados estão expostos; lista a função e a responsabilidade dos responsáveis diretos pelo tratamento dos dados pessoais; explica o direito à privacidade ante ao tratamento dado aos dados pessoais antes e após a LGPD; discute a questão do consentimento, contrapondo-o ao princípio da primazia da realidade, tomando por base o princípio da boa fé objetiva e defendendo o necessário equilíbrio entre o legítimo interesse e o consentimento. Por fim, foi apresentada a jurisprudência pertinente e as expectativas com relação à LGPD.

3.1 Principais vulnerabilidades

O pilar da manutenção da sociedade de consumo reside na transformação do paradigma social, no qual os bens que o indivíduo consome são os ressignificadores de sua vida. Nesses termos,

> O capitalismo não entregou os bens às pessoas; as pessoas foram crescentemente entregues aos bens; o que quer dizer que o próprio caráter e sensibilidade das pessoas foi reelaborado, reformulado, de forma tal que elas se agrupam aproximadamente com as mercadorias, experiências e sensações, cuja venda é o que dá forma e significado a suas vidas (SEABROOK, 1988, p.183).

A sociedade de consumo estrutura o seu corpo social pela hierarquia do ato de consumir, o cidadão constrói a sua identidade no seu consumo, as relações de poder se baseiam na capacidade de consumir e este consumo tem se dado cada vez com maior frequência, pela internet. Para que a negociação seja concluída, são preenchidos formulários com os dados pessoais deste consumidor, que muitas vezes são utilizados com outros propósitos que não o de simplesmente identificar aquele indivíduo para fins de cobrança e entrega de um produto ou serviço. O mesmo se observa nas redes sociais, em que um grande número de dados pessoais, inclusive dados pessoais sensíveis, é disponibilizado.

Diante desse contexto, são muitos os países que já promulgaram suas legislações relacionadas à proteção de dados com o objetivo de garantir o direito à proteção de dados de seus cidadãos, notadamente no continente europeu. Atualmente, a normatização válida para a UE é o RGPD, que passou a viger em maio de 2018, apenas refinando e atualizando a Diretiva de Proteção de Dados Pessoais 95/46/CE, que foi revogada.

Até o ano de 2018, em relação à proteção de dados, o Brasil não contava com uma legislação específica, havendo, portanto, somente dispositivos gerais que eram interpretados de forma a assegurar a proteção de dados de titular (COLAÇO; MENEZES, 2019). Dentre eles, citam-se o artigo 5°, incs. X e LXXII, que versam respectivamente acerca da intimidade, vida privada, honra e imagem das pessoas e a respeito do remédio constitucional o qual denomina-se de *habeas data* que tem a finalidade de assegurar ao impetrante conhecimento de quais dados pessoais encontram-se à disposição de órgãos públicos e ratificá-los se assim desejar.

Ademais, a LAI, Lei nº 12.527/2011 foi a primeira legislação a tratar acerca do tratamento de dados e da internet. Na sequência, cita-se o Decreto nº 7.962/2013 (Decreto do Comércio Eletrônico), que regulamenta o CDC para dispor sobre normas de aquisição de produtos e serviços com segurança pela rede mundial de computadores, a exemplo da apresentação de um resumo sobre o teor do contrato antes que a contratação seja efetivada, contendo aquelas informações imprescindíveis para que o consumidor tome a sua decisão e deixando em destaque os direitos e deveres do cliente e da loja; e o MCI, Lei nº 12.965, que foi promulgada no ano de 2014, estabelecendo princípios, garantias, direitos e deveres que permitem que se faça uso da internet no país. No entanto, a proteção trazida pelo MCI não se mostrava suficiente, especialmente porque esta legislação se limitou à proteção dos dados pessoais, ao prever a tutela apenas para usuários da Internet, quando esta proteção deveria ser para qualquer pessoa (PILAU SOBRINHO; PIAIA, 2015).

O MCI se limitou a proteção dos dados pessoais, quando previu a tutela somente para usuários da Internet. Tal tutela de direitos não deve ser somente do usuário, mas de qualquer pessoa.

No entanto, apesar dos muitos avanços que advêm de ambas as legislações, tendo em vista que ainda persistia a insuficiência normativa, em 2018, tomando-se por base as diretrizes europeias sobre a regulamentação de proteção de dados, o Brasil publicou a sua LGPD, Lei nº 13.709, que modifica o MCI e trata especificamente da proteção de dados.

Trata-se de temática de grande importância. Inclusive, no Brasil, tramita no Congresso Nacional a PEC nº 17/2019, que objetiva incluir a proteção de dados disponibilizados em meios digitais no rol de garantias individuais da CRFB/1988. Nos dias 06 e 07 de maio de 2020 o Supremo Tribunal Federal (STF) proferiu uma decisão histórica que reconheceu a proteção de dados como um direito autônomo a partir do julgamento em plenário que referendou a Medida Cautelar nas ADINs nº 6.387, 6.388, 6.389, 6.393, 6.390 e suspendeu a aplicabilidade da MP nº 954/2018, que compelia as operadoras de telefonia a entregarem ao IBGE o número do celular e o endereço de seus consumidores de telefonia móvel.

Importa mencionar também o Projeto de Lei (PL) nº 1515/2022, de iniciativa do deputado do Partido Liberal, o Coronel Armando, que dispõe sobre a aplicação da LGPD para fins de segurança e defesa nacional, segurança pública e para fins de investigação e repressão de infrações penais. Este PL está fundamentado em três pilares: "proteção dos direitos fundamentais de segurança, liberdade e de privacidade; eficiência da atuação dos órgãos responsáveis; e intercâmbio de dados pessoais entre autoridades competentes" (BRASIL, 2022, s.p.). Caberá à ANPD, que atualmente está incumbida da aplicação da LGPD, supervisionar também a proteção dos dados pessoais nos casos previstos no Projeto.

Apesar das medidas citadas acima, o direito à proteção de dados já deveria ser visto como um direito fundamental com fundamento no artigo 5°, § 1° da CRFB/1988 que prevê que as normas definidoras de direitos e garantias fundamentais têm aplicação imediata, sendo o rol de direitos e garantias fundamentais meramente exemplificativos. Por esta razão, a atribuição de novo direito fundamental à proteção de dados pode provir da ampliação hermenêutica do texto constitucional por estar implícito em outros dispositivos já salvaguardados.

Denota-se que a utilização de dados pessoais coletados, principalmente por instrumentos tecnológicos, apresenta riscos aos seus proprietários, uma vez que possibilita sua utilização de forma indevida por parte de terceiros, pessoas físicas ou jurídicas. A dispersão de dados, principalmente com o avanço da tecnologia, dificulta o controle acerca das informações proferidas por tais tratamentos.

3.2 Dos responsáveis diretos pelo tratamento dos dados pessoais

São responsáveis pelo tratamento dos dados pessoais: o controlador, o operador e o encarregado pela proteção dos dados.

O Controlador geralmente é o dono do negócio, da empresa, das sociedades, das ONGs, etc., e poderá ser um dos sujeitos passivos, em ações, procedimentos, se houver coleta, armazenamento, fluxo, descarte, em desacordo com a lei. Por sua vez, o Operador é a pessoa que realizará em nome do Controlador o tratamento de dados e o encarregado pela proteção de dados é como a lei nomina o que as consultorias e a *General Data Protection Regulation* (GDPR), denominam de *Data Protection Officer* (DPO). Segundo Bioni (2019), as atribuições de um DPO, ou encarregado, são de três ordens: deve verificar se a LGPD está implantada, é e possui um importante papel na solução de conflitos que poderá surgir entre as partes: controlador, titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD. Deverá, pois, cuidar e registrar a sua atuação, porquanto irá responder caso extrapole as suas funções ou caso se omita, tal como ocorre com um verdadeiro administrador de uma atividade empresária.

No que concerne à possibilidade de responsabilização civil cumulada à responsabilidade administrativa, importa, em um primeiro momento, deixar claro que os agentes responsáveis pelo tratamento de dados pessoais (controlador e operador) devem manter registro das operações de tratamento de dados pessoais que por eles forem realizadas, especialmente quando fundamentado no legítimo interesse, consoante previsão do artigo 37 da LGPD.

A ANPD poderá determinar ao controlador que redija relatório de impacto à proteção de dados pessoais, descrevendo os tipos de dados coletados, consoante previsão do § único do artigo 39 da LGPD e englobando, inclusive, dados sensíveis relacionados às suas operações de tratamento de dados.

Assim, o operador de dados deverá proceder ao tratamento em conformidade com as instruções fornecidas pelo controlador, que deverá verificar que suas próprias instruções e as normas sobre a matéria estão sendo observadas (BRAMANTE; DE MARTINO; ALVES, 2021).

O controlador deverá indicar encarregado pelo tratamento de dados pessoais. Este último, por sua vez, é responsável pela execução das atividades previstas no artigo 41, § 2º da LGPD[39].

O artigo 42, § 1º da LGPD prevê que o controlador ou o operador que, devido ao tratamento de dados pessoais, causar danos de natureza patrimonial ou moral a outrem, violando a novel legislação de proteção de dados pessoais, ficará obrigado a repará-lo, sendo a responsabilidade do operador uma responsabilidade solidária com aquelas atribuídas aos controladores.

Importa consignar que há muitos debates sobre a natureza da responsabilidade civil na LGPD. Os artigos 46 a 54 da novel legislação expõem as condutas que devem ser seguidas pelos agentes de tratamento de dados visando à segurança, sigilo, boas práticas no que concerne ao tratamento dados e governança. Há discussões a respeito das diferentes regulações insertas nos artigos 42 e 44 da LGPD e a doutrina se divide entre a responsabilidade civil objetiva e a subjetiva.

Alguns entendem que a LGPD adota a teoria subjetiva da responsabilidade civil, fundada na conduta culposa ou dolosa do agente de tratamento, máxime na culpa por omissão. O artigo 42 da LGPD lista as condutas que devem ser observadas, quais sejam: (i) não fornecer a segurança que o titular de dados dele pode esperar; (i) deixar de observar a legislação. De modo que, a simples omissão no que concerne à adoção de medidas de segurança para tratar adequadamente os dados, bem como o descumprimento das obrigações impostas na lei, independente de causar efetivo dano, ensancha a responsabilidade pelas multas. E havendo dano, surge a responsabilidade de reparação do dano material e moral (COTS; OLIVEIRA, 2021).

O artigo 44, em seu § único, embora use a expressão "tratamento irregular" traz o "dever qualificado de indenizar" os danos decorrentes dos incidentes, da efetiva "violação da segurança dos dados", diante da omissão na adoção das medidas de segurança previstas no artigo 46 da LGPD. Destarte, no que tange a Segurança e Boas Práticas há diretriz no sentido de "medidas aptas" a proteger os dados pessoais contra acessos não autorizados e "situações

[39] Art. 41 da LGPD. [...] § 2º [...]: "I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II – receber comunicações da autoridade nacional e adotar providências; III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares".

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (BRASIL, 2018, s.p.).

A Lei 13.709/2018, no inc. III do artigo 43 da LGPD dispõe que ainda que presente o dano, há excludentes da responsabilidade, se não houver violação dos dispositivos previstos na legislação de proteção de dados, o que serve de reforço para o caráter subjetivo da responsabilidade.

Outra teoria professa que o artigo 42 da LGPD, traz o dever de indenizar "em razão do exercício de atividade de tratamento de dados pessoais" (BRASIL, 2018, s.p.). Toda vez que a lei impõe deveres de conduta de precaução e de prevenção significa que a atividade é de risco, compatível com a responsabilidade civil objetiva, prevista no artigo 927 do CC/2002 e por esta razão, a lei traz os principais fundamentos para a mitigação dos riscos de dano.

Moraes e Queiroz (2019) esclarecem que a LGPD adotou a teoria ativa ou proativa da responsabilidade civil, inscrita no artigo 6º, inc. X, em que prevalece o dever de precaução e de prevenção. Já a obrigação de indenizar surge como uma medida excepcional. Isto porque,

> [...] a proteção da intimidade por vias da mera não interferência na esfera individual cede espaço à tutela positiva e proativa, isto é, que garanta ao titular o conhecimento pleno das formas de tratamento, finalidade e destino de seus dados. [...] a coleta e o tratamento de dados pessoais devem ser precedida de medidas rigorosas e eficazes de proteção, especialmente em relação aos dados sensíveis, núcleo duro da dignidade humana (MORAES; QUEIROZ, 2019, p. 121).

Caitlin Mulholland (2020), também vê as notas características da responsabilidade objetiva nos deveres ativos de prestação de contas, transparência, comunicação de todas as medidas de segurança que deverão ser adotadas para evitar o dano ocasionado pelo agente de tratamento de dados.

Mendes e Doneda (2018), tomando por base o artigo 6º, inc. III e o artigo 44 da LGPD entendem que o tratamento de dados encerra riscos intrínsecos e potencialidade de danos hauridos:

> (i) do próprio conceito de tratamento irregular de dados, que comanda o modo como o tratamento é realizado, o resultado e os riscos razoavelmente esperados pelo tratamento e as técnicas de tratamento de dados disponíveis à época em que este foi realizado, dentre outras circunstâncias; (ii) motivo pelo qual o art. 6, III, LGPD encerra o princípio da finalidade, necessidade, minimização do risco, responsabilidade e prestação de contas, entre outros

> como “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”: (iii) outras notas características são: o uso deste termo legal “mecanismos de mitigação do risco”; os deveres da gestão dos riscos relacionados à atividade desenvolvida, haurida da conduta “deixar de observar a legislação”; a “proteção da legítima expectativa”, ou seja, não oferecer a segurança que o titular dele pode esperar (MENDES; DONEDA, 2018, p. 470-471).

Sumariando as diversas doutrinas no tema proteção de dados pessoais, haurem-se as várias modalidades de responsabilidade, objetiva e subjetiva.

A responsabilidade será subjetiva, artigos 186 e 187 do CC/2002 nas hipóteses: do terceiro não preposto dos agentes de tratamento de dados; do terceiro preposto dos agentes de tratamento, inclusive o encarregado pelo tratamento de dados; do controlador dos dados pessoais pelos danos causados ao titular, com inversão do ônus da prova, presumindo-se a culpa (MEIRELES, 2020).

A responsabilidade será objetiva pelo tratamento de dados: na relação de consumo, regida pelo CDC (§ único do art. 927 do CC); nas relações com as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos (art. 37, § 6º, CRFB/1988); nas atividades de tratamento de dados “que realmente possa enquadrar como atividade de risco” a exemplo de dados financeiros, bancários e aqueles acessíveis pela internet (MEIRELES, 2020, p. 75-76).

Por fim, como esclarecem Miziara, Pessoa e Millicone (2020), a responsabilidade será objetiva e/ou subjetiva se o operador de tratamento, por ato próprio ou a mando do proponente (controlador), responde de forma subjetiva pelos seus atos, mas com inversão do ônus da prova, com responsabilidade solidária e objetiva do controlador, já que aquele é preposto.

Assim, não restam dúvidas que é possível cumular a responsabilidade administrativa e civil em razão do tratamento inadequado dos dados pessoais de consumidores do comércio eletrônico podendo a responsabilidade pelos danos causados recair solidariamente sobre o controlador e o operador, havendo, ainda, em favor daquele que reparar o dano causado, a previsão de regressar contra os demais responsáveis, de acordo com a participação destes no incidente.

3.3 Do Direito à Privacidade

Em sentido lato, a liberdade é descrita como um pilar valorativo da humanidade, sendo uma pré-condição para que se desenvolva a noção da cidadania. A necessidade de ser livre é natural do homem (SILVA; SIQUEIRA, 2020), assim como também é a necessidade de se expressar.

A liberdade de expressão tem uma conotação negativa, de não interferência do Estado ou da sociedade quanto à livre manifestação de opiniões ou ideias, salvo nos casos de abuso, como é o caso do discurso do ódio (SILVA; SANTOS, 2018).

O abuso no direito à informação se dá quando a informação veiculada não é de interesse público e traz prejuízos à vida de uma pessoa por violar-lhe a intimidade e a honra (SARMENTO, 2009).

Importa ressaltar que a liberdade de expressão precisa ser vista também em sua conotação positiva, ou seja, no livre acesso das pessoas aos meios de expressão, com o objetivo de garantir a todos a possibilidade do seu exercício e a melhor qualidade do debate público (SARMENTO, 2007). Assim, pode-se aferir que a proteção constitucional para a liberdade de expressão, relaciona-se à sua feição negativa, ao mesmo tempo em que a proteção da liberdade de comunicação social, que por sua vez consubstancia-se na liberdade de imprensa, encontra-se inserida nesse aspecto positivo do direito de informar (SILVA; CERQUEIRA, 2015).

Nesse contexto, incluído na liberdade de expressão, está o direito à informação, o qual se subdivide em três aspectos: o direito de informar, de se informar e o direito de ser informado (PASQUALINI, 2009).

O direito de informar consubstancia-se na faculdade de veicular informações irrestritas a terceiros, sendo prevista na Constituição na sua forma individual e na comunicação social, realizada pela mídia. Segundo Nunes Junior (2011), na comunicação social (mídia) o direito de informar é exercido pelos detentores da mídia televisiva, escrita, radiofônica e virtual (Internet). Já o direito de se informar refere-se à faculdade de conseguir informações sem óbices impostos pelo Estado ou pela sociedade. Por fim, o direito de ser informado é referente à liberdade para receber informações plenas, reais e contínuas, sem impedimentos, além de obter proteção constitucional.

Para Nunes Junior (2011), esses três níveis do direito de informação apresentam elevado grau de interdependência. Nesse sentido, discute-se a interdependência desses três níveis tendo em vista que só é possível extrair, por exemplo, de um ordenamento jurídico, o direito de ser informado, se este mesmo ordenamento atribuir a alguém a obrigação/dever de prestar estas informações; o mesmo se pode afirmar referente ao direito de informar, que, revestido positivamente, só poderá ter espaço se o ordenamento direcionar a alguém a obrigação de fornecer meios para que as informações possam ser veiculadas, como ocorre, com o direito de resposta. No entanto, acredita-se que como os meios de comunicação e informação podem produzir informações inverídicas, o correto seria ouvir a outra parte antes de divulgar a informação.

Segundo Franco (1999, p.26), "a liberdade de manifestação do pensamento está consagrada entre os direitos fundamentais do homem, sendo atualmente um dos instrumentos basilares de uma sociedade democrática". Ela teve sua primeira positivação na "Declaração dos Direitos do Bom Povo de Virgínia", de 12.06.1776, dos Estados Unidos da América, cujo artigo 14 dispunha que a liberdade de imprensa é um robusto baluarte da liberdade estatal e só pode ser limitada pelos governantes despóticos[40].

A Revolução Francesa também contemplou a positivação da liberdade de imprensa na Declaração dos Direitos do Homem, de 1793 (artigo VII), bem como ela se faz atualmente garantida no artigo 19 da Declaração dos Direitos da Humanidade, de 1948 e em outros tratados internacionais, a exemplo da Carta de Direitos Fundamentais da União Europeia (UE), publicada em 2000, ratificada pelo Tratado de Lisboa de 2007 (Constituição Europeia), e a Convenção Americana sobre Direitos Humanos – Pacto San de José da Costa Rica, de 1969 (artigo 13).

Gamiz (2012) entende que a liberdade de informação esbarra em um direito à informação que não se destina a uma pessoa, mas sim à coletividade, porque engloba o direito de as pessoas serem bem informadas. Neste contexto, é importante explicar também a liberdade de expressão.

---

[40] DHNET – Direitos Humanos na Internet. Declaração dos Direitos do Homem e do Cidadão; Declaração dos Direitos do Bom Povo de Virgínia; Declaração Universal dos Direitos do Homem, das Nações Unidas; Convenção Europeia dos Direitos do Homem (1950); Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica); Carta de Direitos Fundamentais da União Europeia, de 2000; Declaração de Princípios sobre Liberdade de Expressão da Comissão Inter-Americana para os Direitos Humanos, de 2000. Disponível em: http://www.dhnet.org.br/direitos/ anthist. Acesso em: 14 Julho 2022.

Segundo Moraes (2016), a liberdade de expressão traz em seu bojo uma dimensão que se relaciona com as manifestações da individualidade de cada indivíduo, através de palavras, produções artísticas e até mesmo da forma como cada um se apresenta pessoalmente. Possui uma dimensão que se relaciona à cidadania e seu exercício, à faculdade de comunicar opiniões, ideias, tecer críticas e empreender debates que contribuam para desenvolver a sociedade plural e democraticamente. Assim entende-se que o simples fato das pessoas se sentirem ofendidas não quer dizer que ocorreu abuso ou discurso de ódio. Exemplo disso são os recentes acontecimentos protagonizados pelo STF.

Recorde-se que o ministro Alexandre de Moraes, em março de 2019, abriu inquérito no STF para investigar críticas à Suprema Corte. O mesmo também determinou diversas ordens de busca e apreensão para pessoas não beneficiadas por foro por prerrogativa de função. Ademais, em janeiro de 2020, intimou para depor no referido inquérito o jornalista Allan dos Santos sem ao menos possibilitá-lo de conhecer os autos do inquérito, o que contraria sua jurisprudência e, inclusive, a súmula vinculante nº14, do próprio STF.

A liberdade, nas duas dimensões, ao ser expressa, pode gerar desconfortos a pessoas que podem se sentirem ofendidas, humilhadas, prejudicadas, caluniadas, difamadas, dentre outras possibilidades. No entanto, como expõe Novais (2010), em uma democracia não é possível suprimir indistintamente o direito à liberdade de expressão, incluindo as manifestações que atuem representando as minorias, que incentivem debates ou que objetivem alterar o estado atual das coisas.

O alcance, bem como o desenvolvimento de outros direitos, dependem do direito à liberdade de expressão, que torna possível enfrentamentos e mudanças. Referidos debates trazem inquietudes e, não raro, divergências.

As ordens jurídicas democráticas precisam assegurar o exercício da liberdade de expressão, de maneira que seja possível aceitar a diferença de ideias e modos de vida, tolerância, diálogo e irrestrito respeito às diferenças (SILVA; COSTA, 2020). No entanto, referidos ordenamentos às vezes necessitam restringir o abuso desse direito com vistas a resguardar a democracia, e, complementarmente, tutelar a humanidade, guarnecer os direitos personalíssimos e a dignidade. Porém, para que isto seja efetivamente implementado no seio social, é preciso que as pessoas entendam verdadeiramente que uma abstratividade por si só não basta para ofender o outro.

Por fim, não obstante o direito à informação ser de grande relevância, entende-se que este não pode invadir o direito à privacidade. Sobre o direito à privacidade, será melhor detalhado a seguir.

Preliminarmente, uma questão que dificulta o entendimento da privacidade consiste no fato de que o instituto envolve diversos aspectos, ou dispõe de vários âmbitos de proteção: "honra", "imagem", "intimidade","vida privada" (GAMIZ, 2012). Tal consideração mostra que o consenso referente a conceitos pelos doutrinadores também em relação à privacidade é extremamente difícil. Em razão dessa complexidade, quando um direito é violado, nem sempre ocorre, necessariamente, a violação dos demais.

Com isso, a dificuldade em conceituar "privacidade" e "intimidade" advém da própria extensão e do próprio conteúdo desses direitos. Normalmente, é exposta por meio de interesses que se caracterizam por objetivos diversos. Nesse aspecto, a privacidade tem por objetivo proteger o homem contra: 1. Uma diversidade de invasões que possam influenciar em sua vida particular, familiar e doméstica; 2. A comunicação de acontecimentos importantes e embaraçosos afetos à sua intimidade; e 3. A transmissão de informações enviadas ou recebidas decorrente de segredo profissional. Entretanto, existem inúmeros obstáculos para a referida conceituação, conforme retrata Silva:

> São inúmeras as dificuldades que o tema suscita. A primeira delas é precisar a extensão e o conteúdo desse direito, cujo interesse subjacente é de caráter eminentemente subjetivo, por isso mesmo variável de pessoa para pessoa; os valores sociais são diferentes e mutáveis no tempo e no espaço; o sentimento que constitui o seu núcleo oscila no âmbito de cada pessoa. Essa dificuldade ainda mais se evidencia nas tentativas dos autores em formular uma definição do direito à intimidade. Torna-se mais difícil ainda quando se tem que estabelecer em que medida ou em que situações o interesse de preservação da intimidade deve ser sacrificado em prol de um outro interesse juridicamente protegido, quando os dois se colocam em posição de absoluto antagonismo (SILVA, 2003, p.4-5).

Fora esses aspectos, um ponto que contribui para dificultar o consenso no entendimento da questão provém do fato de que as legislações ou convenções internacionais não precisam seu conceito. Exemplo disso é visto na CRFB/1988, que identifica em quais situações o referido direito não pode sofrer violações, porém, em momento algum, estabelece qualquer conceito sobre o tema.

Além desses fatores, outra questão que torna essa tarefa árdua advém do pluralismo social: os valores entre as diferentes comunidades não são homogêneos ou iguais. Em adição

às condições sociais, os aspectos materiais afetam significativamente o entendimento do direito à intimidade.

Para Sarlet, Marinoni e Mitidiero (2014), por exemplo, a densidade da população, o grau de interação, as condições de residência, a divisão do trabalho, a natureza da família e outras relações sociais devem ser considerados como fatores determinantes na definição do referido direito.

Nessa mesma linha de pensamento, Doneda (2006) destaca que a definição de privacidade não é um problema puramente dogmático, visto que se encontra estreitamente relacionada aos valores e projeções humanas em cada sociedade e, no âmbito de cada um dos muitos grupos, esta tarefa possui forte conteúdo social e também ideológico. Desta forma, há uma multiplicidade de opiniões arroladas acerca do tema.

É, também, necessário buscar um mínimo conteúdo que seja comum para o entendimento do direito à privacidade. Todavia, Leal (2015) pontua que não se pode, a princípio, definir, em toda a sua plenitude, a intimidade e a vida privada posto que seus contornos inequívocos só podem ser mensurados, considerando suas especificidades e o contexto em que ocorreu o caso concreto.

A situação em pauta conduz à noção de que a privacidade é um problema que precisa ser solucionado pelo meio jurídico, principalmente agora, com o avanço tecnológico e, em especial, com a proliferação do acesso à internet, tendo em vista que, como demonstrado por Silva e Cury (2020) o problema torna-se ainda mais evidente quando as informações coletadas por empresas públicas ou privadas são utilizadas para a prática de atos ilícitos ou como forma de controle social valendo-se da manipulação de algoritmos de inteligência artificial que traçam um perfil dos usuários na rede mundial de consumidores e passa a tentar influenciar e direcionar suas escolhas.

Com base na dignidade da pessoa humana, Silva e Melo (2019) sustentam que a privacidade, no passado concebida como um direito que o indivíduo possuía de resguardar-se contra as interferências de terceiros, com a massificação dos dados passou a ser concebida "como um direito à autodeterminação informativa".

Isto porque o entendimento que atualmente se tem sobre os contornos da privacidade foi modificado ao longo dos tempos, "tendo havido uma mudança de perspectiva para a tutela da dignidade humana, bem como uma adequação às novas exigências de proteção da esfera

privada em um mundo moderno, diante de recentes tecnologias de informação" (SILVA; MELO, 2019, p. 373).

É importante também distinguir privacidade de direito à privacidade. Sobre essa dicotomia, nas várias consultas bibliográficas realizadas na doutrina brasileira, não se vislumbrou – de forma clara e objetiva – a preocupação dos estudiosos pátrios com o tema. Entretanto, na doutrina norte-americana, Solove, Rotenberg e Schwartz (2006), por meio de sua obra *Privacy Information and Technology*, tratam do assunto como preliminar para a defesa do entendimento do referido direito numa visão pragmática. Nesse sentido, o direito da privacidade diz respeito às medidas pelas quais ela deve ser legalmente protegida. Então, por essa linha de raciocínio, entende-se como tal, no Direito brasileiro, o constante dos incs. X, XI e XII do artigo 5º da CRFB/1988. Em contrapartida, "privacidade" engloba todo o conceito que não esteja inserido em documento legal, vislumbrado, consequentemente, como um valor que deve ser compreendido.

Contribui, outrossim, para a complexidade do entendimento da privacidade – dificultando a elaboração de uma definição fechada sobre o tema – a possibilidade de renúncia, ainda que temporária, do direito à privacidade, o que decorre do fato de ele mesmo integrar o direito da personalidade e apresentar a característica, entre outras, de não ser absoluto.

No espaço virtual, isso ocorre normalmente quando um indivíduo se associa a uma rede social na Internet – trata-se de uma teia de conexão de um grupo de pessoas que se comunicam entre si, podendo ou não ter uma relação estreita de amizade. Nesse contexto, as pessoas costumam preencher perfis em que normalmente constam números de telefone, endereços eletrônicos e outros dados pessoais que podem ser disponibilizados somente para um grupo fechado de indivíduos ou ser inteiramente acessíveis ao público em geral (SILVA; MELO, 2019).

Nesse novo contexto, quando o internauta disponibiliza informações *online*, ele não está somente renunciando à sua privacidade: muitas vezes, restringe igualmente a privacidade de seus pais, de amigos e de outras pessoas sem que eles tenham sequer conhecimento sobre isso. O problema, então, é que muitas informações disponibilizadas na Internet são preservadas para sempre – até pelo fato de alguém copiá-las e mantê-las a seu bel-prazer na rede.

Canotilho e Machado (2015), em pesquisa sobre a privacidade, destacam que as expressões “intimidade” e “vida privada” carecem de interpretações consoante o contexto variável e possível de mudanças no tempo e no espaço. Assim sendo, o conceito de privacidade poderá obter maior ou menor elasticidade, dependendo da evolução da mentalidade da época, da identidade dos indivíduos envolvidos, de sua função social e estilo de vida dos interessados. Assim, quando uma pessoa decide tornar público seu comportamento (geralmente protegido pelo direito à privacidade), ela não renuncia totalmente ao referido direito, apenas passa a exercê-lo conforme suas preferências. Assim, a privacidade não pode ser analisada de forma generalizada e única para todos: necessita avaliação conforme o caso concreto.

Feitos estes necessários esclarecimentos sobre o direito à privacidade, passa-se à análise deste direito na sociedade da informação. Isto porque na atualidade, a importância da Internet requer a adequação de inúmeros conceitos ao seu ambiente, entre os quais a privacidade.

Fortes (2016, p.183) estabelece quatro direitos-base a título de direitos de privacidade na Internet (originalmente, *Internet Privacy Rights*): “o direito de navegar pela Internet [sic] com privacidade; o direito de monitorar quem monitora; o direito de deletar os dados pessoais; o direito a uma identidade online”.

Os conceitos de privacidade e de proteção de dados pessoais na Internet possuem muitos aspectos, resultado das várias possibilidades de uso desse instrumento, o que cria um desafio legal para a correta tutela dos interesses dos indivíduos.

Tendo em vista que o direito à privacidade é corolário do princípio da dignidade humana e um direito fundamental de primeira dimensão, sua tutela adequada é indispensável em um Estado democrático de direito. Nesse sentido, o ciberespaço tem enorme potencial para a participação política e atividades comunitárias. Longhi (2017) salienta que a privacidade na Internet é um pressuposto de um sistema democrático deliberativo por dois grandes motivos.

O primeiro diz respeito à guarida dos dados pessoais como forma de evitar hierarquizações e discriminações fundamentadas somente em informações pessoais. O segundo, a restrição da autonomia privada do indivíduo frente ao abuso de poderes públicos e privados quando detentores de informações pessoais.

Mas estes não são os únicos problemas jurídicos em torno da proteção da privacidade dos cidadãos em um sistema democrático. O primeiro deles é o da definição de sua abrangência. Isto porque, há, no ocidente, dois grandes sistemas que se dedicam à guarnecer a privacidade: liberdade e dignidade. O da liberdade, oriundo dos países da *common law*, tutela a privacidade como uma espécie de liberdade pública abrangente, que justifica a não intervenção de terceiros na esfera de decisão do indivíduo. Já a privacidade como dignidade é característica dos países de tradição jurídica continental, limitando-se à proteção da intimidade e vida privada dos indivíduos (DONEDA, 2006).

Restringindo-se às TICs, leciona Rodotà (2008) que o direito à privacidade hoje ganha novos contornos, dando margem à existência de um direito autônomo dele decorrente, a proteção dos dados pessoais. Embora ambas façam alusão à proteção da dignidade humana, os dados pessoais tutelam um bem jurídico distinto da intimidade. Enquanto um cuida do "corpo físico" o outro cuida do "corpo eletrônico". Ou seja, os dados, quando analisados e disponibilizados em conjunto, possibilitam que se construam perfis a serviço tanto do mercado como do Estado. Algo que põe em risco todos os outros direitos e garantias fundamentais.

E o tema da proteção dos dados pessoais se depara com novos desafios diuturnamente. Exemplificativamente, a questão do *big data*, o problema do direito ao esquecimento, o "consentimento" do cidadão no que tange à disponibilização de informações relevantes em sites de redes sociais, cujos provedores "praticamente sabem o que pensamos" (FERGUSON, 2015, s.p).

Assim, o avanço tecnológico, além de trazer diversos benefícios para a sociedade, também trouxe algumas pertinentes preocupações. Cada dia mais o acesso a dados pessoais contendo informações sensíveis do indivíduo não depende do acesso ao seu *smartphone* ou dispositivo pessoal, mas pode ser realizado através do consentimento de provedores, ou seja, "terceiros" nesta relação (no direito norte-americano conhecido por *third-party providers*), o que na prática representa um controle cada vez menor de seus dados pessoais (FERGUSON, 2015).

Desta maneira, episódios como o escândalo de espionagem[41] praticado pela *National Security Agency* (NSA) norte-americana em todo o mundo, são apenas uma amostra do ambiente de vigilância constante a que se está submetido hoje, no entanto, não entende-se que esta vigilância esteja a serviço do direito à informação, mas sim que, neste caso, devido aos excessos observados, há clara violação do direito à privacidade.

Nas relações de consumo firmadas *online* o consumidor é colocado em uma posição ainda mais vulnerável. A vulnerabilidade que envolve os seus dados, as suas informações pessoais. Informações essas que fazem parte das novas relações de consumo, dentro de uma nova sociedade informacional.

É direito do consumidor saber qual o destino dos seus dados e de todas as informações que ele é obrigado a fornecer para poder efetivar a relação. Também, é direito do consumidor proibir a negociação dos seus dados e exigir que eles sejam colocados em segurança (BIONI, 2019).

Em contrapartida, é obrigação do fornecedor assegurar que os dados e todas as informações colhidas não sejam utilizadas de forma que não foram expressamente autorizadas pelo consumidor de forma consciente, bem como garantir a segurança dos seus sistemas de forma que não sofram ataques de cibercriminosos.

Com a finalidade de assegurar essa proteção, a LGPD regulamentou o tratamento dos dados pessoais, vez que tem o "objetivo de proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018, s.p.). Visando o alcance desse fim, em seu art. 7ª estabelece que os dados somente podem ser utilizados, principalmente, mediante o fornecimento do consentimento do titular.

Sobre a coleta dos dados e o consentimento do seu titular, o art. 8º da LGPD especifica que deve a manifestação de vontade ser feita na forma escrita ou por outro meio que demonstre a sua realização. E sendo por escrito, deverá constar como cláusula contratual destacada.

A grande questão é que apesar de a LGPD ser um marco na regulação e na proteção efetiva dos dados de natureza pessoal, ela não é uma lei voltada para as relações de consumo,

---

[41] Ressalte-se que as pessoas envolvidas neste caso estão no Brasil e se envolveram em casos de violações de aplicativo telefônico de autoridades em território brasileiro e encontraram abrigo no STF. Destaque-se também que um dos países que é acusado de fazer espionagem por diversos outros é a China.

deixando alguns pontos em aberto. Boff, Fortes e Freitas (2018) colocam que dois pontos importantes são:

1. quando se consome algo, principalmente pela internet, muitas condições são impostas ao consumidor, como regras de uso da página, forma de coleta de dados e o próprio uso deles, exigindo a aceitação. O consumidor aceita/concorda com o que está ali colocado sem nem saber o que está aceitando.

2. a aceitação/concordância com o uso dos dados é colocado de tal forma para o consumidor que ou ele aceita/concorda ou não consome.

Esse contrato que está sendo firmado é claramente um contrato de adesão nos termos do art. 54 do CDC, pois o consumidor não tem a possibilidade de discutir as cláusulas que lhe são impostas.

Os contratos por adesão são oferecidos ao público em um modelo normalmente uniforme, impresso, faltando somente que sejam inseridos os dados que se referem à identificação do contratante, do objeto contratado e do preço. Desta forma, aqueles que desejarem firmar contrato com a empresa que faz uso desta modalidade de contrato para adquirirem algum produto ou serviço já irão receber relação contratual pronta e não poderão discutir e nem negociar as cláusulas contratuais.

Desta forma, o elemento essencial do contrato por adesão é a ausência de um debate prévio das cláusulas contratuais, isto é, a sua predisposição unilateral, restando à parte contratante a mera alternativa de aceitar ou rejeitar o contrato, que não pode ser modificado de maneira relevante (PILAU SOBRINHO; MIGUEL, 2013). Ao se tratar de espécie contratual utilizada principalmente em relações de consumo, ressalta-se que o consentimento do consumidor-contratante se manifesta apenas aderindo ao conteúdo estabelecido pelo fornecedor de bens ou serviços. Nesses termos, entende-se que o seu consentimento resta fragilizado nestes casos.

Finda esta seção, postula-se que a violação ao direito à privacidade se dá sem o consentimento da vítima, no entanto, há algumas situações que envolvem o consentimento e que demandam maior atenção. Sendo assim, a próxima seção irá se dedicar à análise do consentimento contrapondo-o ao princípio da primazia da realidade.

3.4 A questão do Consentimento

Entende-se por consentimento "a manifestação livre, informada e inequívoca através da qual o titular expressa sua concordância com o tratamento de seus dados pessoais para finalidades determinadas" (GIARLLARIELLI, 2021, s.p.), não sendo assentidas as autorizações genéricas e vedando-se o tratamento em caso de permissão obtida mediante o vício de consentimento.

Por "livre" compreenda-se a liberdade do titular que não pode ser forçado a consentir com o tratamento de seus dados. Por "informada" compreenda-se a transparência da informação referente a o que especificamente o titular está consentindo a fim de que ele possa tomar sua decisão de maneira consciente. Por derradeiro, entende-se por inequívoca a manifestação por parte do titular na qual não exista nenhuma dúvida sobre a verdadeira aceitação não apenas das condições, mas, também, das repercussões decorrentes do tratamento de seus dados (TEPEDINO; TEFFÉ, 2019).

A regra geral que prevê a obrigatoriedade do consentimento seja para o acesso ou para a divulgação de dados é destaque da LGPD, sendo dispensado apenas em casos em que se faz necessário o cumprimento de ordem judicial, proteção aos direitos humanos, e estudos científicos relevantes à sociedade, casos em que o interesse público deve ser priorizado com relação ao interesse privado. Com o crescimento exponencial dos crimes cibernéticos, em 2012, para tal temática foi promulgada a Lei nº 12.373, dando-se destaque à inclusão do crime de invasão de dispositivo informático, tipificado no artigo 154-A do Código Penal (CP)[42], que reforça a preocupação do legislador com a proteção de dados pessoais.

Nesta seção, o consentimento será analisado à luz do princípio da primazia da realidade, da boa-fé objetiva e do equilíbrio do legítimo interesse. Inicia-se contrapondo o consentimento ao princípio da primazia da realidade.

---

[42] Artigo 154-A – "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa".

3.4.1 O Consentimento *versus* o Princípio da Primazia da Realidade

Segundo o professor Clodomiro Bannwart (2013), o primeiro filósofo a trazer contornos do conceito de vontade foi Santo Agostinho por meio de sua obra "O Livre Arbítrio". Neste livro, encontra-se uma estrutura de pensamento, no qual o mal deixa de ser algo próprio, externo ao homem, para ser compreendido dentro do homem, como forma de realizar escolhas que o distanciam cada vez mais da verdade. Ao versar sobre escolhas, Agostinho trabalha com a autonomia do homem que possui discernimento sobre o que está a escolher:

> Agostinho coloca o problema, a saber, porque o homem, mesmo conhecendo a verdade (Deus) – por meio da razão – opta por escolher outros bens inferiores – por intermédio da vontade – distanciando-se da possibilidade de alcançar felicidade no encontro com Deus? Essa estrutura teórica da pergunta, ainda que simplificada aqui, demonstra que a vontade é uma faculdade cindida nela própria de querer e não querer e, ademais, que as escolhas efetuadas dependem do conhecimento, dependem da razão, enfim do discernimento em relação aquilo que se está escolhendo. Num primeiro momento, é possível ver uma parcial daquilo que o Direito entende por agente capaz. Só faz sentido delegar ao agente a capacidade de escolha se ele for capaz, no sentido de dispor de autonomia (auto-nomos), ou seja, capacidade de dar a si próprio o sentido do seu ato. Somente aquele que é autônomo é capaz de responder pelas consequências do seu ato, enfim, é passível de ser imputado (BANNWART JÚNIOR, 2013, p. 49).

A partir dessa estrutura de pensamento é que foi possível retirar do externo a causa do mal, para implicar no homem a responsabilidade de suas escolhas. Ainda incurso na conceituação jusfilosófica de autonomia da vontade, traz à luz o conceito trazido pela filosofia Kantiana, na qual a autonomia da vontade trata-se de prerrogativa da vontade do homem. Sendo este último livre para determinar-se pela vontade, no entanto, essa vontade só é válida se passível de universalização (KANT, 1997).

Partindo-se da conceituação de autonomia pode-se depreender sua relação ao poder de se autodeterminar por meio de escolhas verdadeiramente conscientes. O homem que carece de conhecimento sobre o que está a eleger para si, não se autodetermina, apenas é motivado a fazer escolhas.

Por esta razão, ao se falar de autonomia da vontade é preciso abordar também o outro lado da moeda, a vulnerabilidade. Uma vez que muitos sujeitos vulneráveis no plano fático são considerados formalmente capazes. Importante observar que se a capacidade de decidir do

consumidor é precarizada e a sua capacidade negocial é previa e limitada, embora formalmente capaz está factualmente submetido a condições sociais, culturais e econômicas que dificultam o exercício de sua autonomia.

Destaca Claudia Lima Marques (2011, p. 323), que o princípio da vulnerabilidade é inafastável e serve para que a norma seja bem aplicada: "é noção instrumental que guia e ilumina a aplicação destas normas protetivas e reequilibradas, à procura do fundamento da igualdade e da justiça equitativa."

Segundo Guimarães e Novaes (2009), a mitigação da autonomia e da vulnerabilidade são fenômenos que podem ou não estar associados, uma vez que a autonomia é individual e a vulnerabilidade pressupõe desigualdade entre grupos:

> A redução da autonomia e a vulnerabilidade são fenômenos que podem estar ou não associados. A autonomia é um conceito ético e individual, enquanto que a vulnerabilidade pressupõe o estabelecimento de relações desiguais entre indivíduos ou grupos. Ela se manifesta quando as relações estabelecidas entre indivíduos ou entre um grupo minoritário e outro nacional envolvente, além de diferentes, são desiguais (GUIMARÃES; NOVAES, 2009, p. 2).

Veja-se que os fatores que contribuem para a vulnerabilidade de um grupo são os mesmos que impedem uma escolha livre e individual. Segundo as autoras citadas supra, a vulnerabilidade[43] é consequência de uma relação de desigualdade no âmbito social, político, cultural e econômico (GUIMARÃES; NOVAES, 2009). A eliminação das vulnerabilidades necessita da superação das privações suportadas por determinados segmentos populacionais no âmbito de suas desigualdades.

Dentro da discussão ainda se faz preciso realizar a diferenciação de autonomia privada e liberdade contratual, no qual a primeira incorpora uma variedade de formas de expressão, enquanto a segunda se refere especificamente às obrigações pactuadas:

---

[43] Segundo exposto no Jornal Estado de Minas (2016, s.p.), "VULNERABILIDADE TÉCNICA nada mais é que o desconhecimento técnico sobre o objeto (produto ou serviço) da relação de consumo; VULNERABILIDADE JURÍDICA é a falta de conhecimento jurídico que permita ao consumidor entender as consequências jurídicas daquilo a que se obriga e se desvencilhar das abusividades do mercado; VULNERABILIDADE FÁTICA (ou socioeconômica) advém da relação de superioridade, do poder que o fornecedor tem no mercado de consumo em relação ao consumidor; VULNERABILIDADE INFORMACIONAL advém da ausência, insuficiência ou complexidade da informação prestada que não permite compreensão pelo consumidor (ESTADO DE MINAS. Vulnerabilidade no CDC. **Jornal Estado de Minas**, 03/10/2016. Disponível em: https://www.em.com.br/app/noticia/direito-ejustica/2016/10/03/interna_direito_e_justica,828595/vulne rabilidade-no-cdc.shtml. Acesso em: 15 Julho 2022).

> Autonomia privada e liberdade contratual não são sinônimas. Embora a autonomia privada imbrique a liberdade contratual, possui uma acepção muito mais ampla, posto que incorpora todas as formas de expressão da liberdade individual ou coletiva, não se limitando aos contratos, ao passo que a liberdade contratual é direcionada apenas às obrigações firmadas por meio de contratos. Autonomia privada pode se manifestar em negócios jurídicos patrimoniais e extrapatrimoniais (NANNI, 2001, p. 199-200).

Segundo Amaral e Ferreira (2014), a busca por paridade nas relações negociais consumeristas acaba por destacar a desigualdade material e justifica a intervenção estatal nesse tipo de negócio jurídico.

No artigo 7º da LGPD estão previstos os fundamentos legais que justificam o tratamento de dados pessoais. Observados os princípios e a correta a base legal que serve para justificar o tratamento do dado pessoal, o gatilho de excludente de responsabilidade a título de indenização, estará ativado, em razão de faltar o nexo de causalidade capaz de justificar a indenização.

Apesar de o consentimento constar no inc. I, do artigo 7º, da LGPD, como primeira base legal para a coleta, armazenamento, do dado pessoal, alguns doutrinadores, entendem que essa não será a base primeira a excluir a responsabilidade do usuário. E esta base legal deverá ficar muito clara para o titular do dado, e aqui em meu entendimento, prevalecerá o Princípio da Primazia da Realidade, previsto no artigo 112[44] combinado com o artigo 113[45], ambos do CC/2002.

Importante aqui ainda destacar que o titular dos dados deverá saber, com clareza de um homem médio, o motivo pelo qual está dando o consentimento para o tratamento de seus dados pessoais.

Reputa-se necessário lembrar que as outras bases legais constante no artigo 7º, poderão ser utilizadas com melhor fundamento legal, do que o próprio consentimento ou além deste. E em uma eventual prestação de contas, a base escolhida que não seja o consentimento, poderá representar para a Autoridade Nacional, ou para o Poder Judiciário, uma base legal mais correta para o armazenamento do dado, justificando assim a finalidade de seu tratamento.

---

[44] Art. 112 do CC. “Nas declarações de vontade se atenderá mais à intenção nelas consubstanciada do que ao sentido literal da linguagem”.

[45] Art. 113 do CC. “Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração”.

3.4.2 O Consentimento à Luz do princípio da boa fé objetiva

Considerando que o comportamento humano é volátil, tal qual a manifestação de sua identidade no ciberespaço, observa-se que a forma de manifestação de vontade pode ter como mola propulsora, inúmeras condições. A análise dos elementos substancial e formal do consentimento não é suficiente para verificar se a coleta do mesmo para o tratamento dos dados pessoais possui a eficácia jurídica necessária para surtir os efeitos esperados.

A análise contextual do consentimento, partindo da privacidade contextual, é um instrumento que pode trazer elementos para a análise da eficácia jurídica do instituto em comento. A teoria da privacidade contextual tem como fundamento a premissa de que o fluxo informacional deve ser apropriado de acordo com suas respectivas esferas sociais (NISSEMBAUM, 2010).

O titular dos dados, deste modo, detém legítimas expectativas da forma como os mesmos fluirão, isto é, de quais seriam seus verdadeiros desígnios. Não obstante, ao analisar a legítima expectativa do titular dos dados, busca-se verificar se haveria o consentimento para o fluxo de informações, e de que forma – o que remete, novamente, à autodeterminação informativa. Este seria o consentimento contextual, o qual não é delimitado por uma finalidade específica, mas sim a um leque de ações que podem ser realizadas durante o uso daqueles dados pessoais, sempre com fundamento na legítima expectativa do titular (BIONI, 2019).

A ideia do consentimento contextual já era estudada quando da análise dos contratos relacionais, os quais preveem cláusulas destinadas a regrar a disciplina de questões futuras, bem como pactuar o dever de negociar o contrato em caso de mudanças no cenário, desde que expressamente previstas no instrumento (MARTINS-COSTA, 2018). Sendo assim, percebe-se que nestes contratos relacionais se faz impossível prever o futuro da relação contratual, sendo que a continuidade desta relação deixa para o futuro a completude obrigacional e adimplemento.

Assim, seria impossível nestes tipos de contrato existir um consentimento expresso com relação a todos os seus termos, eis que os elementos contextuais não estão integralmente definidos. Os contratantes, então, necessitam manifestar um grau de confiança em um nível mais elevado (MARQUES, 2011).

Com base em uma analogia aos contratos relacionais, é possível perceber que o consentimento contextual segue a mesma lógica, haja vista a impossibilidade do titular dos dados, no ato de consentir, não saber, naquele momento, o caminho do fluxo informacional a ser traçado com base em seus dados pessoais – que pode se alongar no tempo. No magistério de Bioni:

> É só pensar que tal fluxo informacional progride e evolui com a própria inovação e novas funcionalidades que são oferecidas por tais plataformas. Todos esses elementos são ajustados com o desenrolar das relações, havendo uma dinamicidade que inviabiliza cravar, pelo menos de forma rígida, todas as variantes desse continuum. [...] Consente-se, por isso, acerca da relação que protrairá no tempo e, com ela, as variantes de tratamentos dos dados pessoais que devem estar adequadas ao contexto da relação (BIONI, 2019, p. 245).

Apenas em razão dos elementos legais trazidos na legislação a respeito do consentimento (substanciais), bem como da inviabilidade técnica de se aferir a eficácia jurídica do consentimento (forma), imprescindível a análise de outros institutos jurídicos para tentar se alcançar uma solução. Assim, ante a analogia realizada com os contratos relacionais, para se chegar à ideia de consentimento contextual, devemos analisar a legítima expectativa do titular de dados ao optar, ou não, por consentir com o tratamento. Segundo Lisboa (2012), a legítima expectativa do titular de dados, ao consentir, engloba dois elementos: a confiança e a boa-fé objetiva. Apesar de haver uma aparente semelhança entre os termos, está-se diante de institutos diferentes. A autora explica que:

> Boa-fé e confiança não se confundem, se complementam. Boa-fé não se tutela, boa-fé se espera. Boa-fé se revela na conduta pessoal. O que se tutela é a pessoa. O direito tem por finalidade proteger pessoas. Quando se afirma a proteção da confiança, o mais apropriado é dizer "do confiante". Por isso, repito, agora de forma mais completa: boa-fé não se tutela, boa-fé se presume e se espera. O que se tutela é a pessoa que se espera a conduta de boa-fé, porque nela se depositou sua confiança (LISBOA, 2012, p. 151).

A confiança, deste modo, é como se fosse a aceitação e a internalização de uma conduta correta e adequada (LISBOA, 2012); a forma de exercício da autodeterminação no contrato leva a que o destinatário da declaração, se aceitar a proposta, passe a confiar no cumprimento da obrigação.

No tocante ao consentimento e o ulterior fluxo informacional, observa-se que o titular dos dados pessoais confia que o caminho da informação não será desviado em detrimento de

seus interesses. No entanto, como bem expõe Martins-Costa (2018), esta não é uma prática que ocorre com frequência no ciberespaço, eis que apesar da confiança do titular dos dados, por vezes estes são utilizados para finalidades diversas, com inúmeros contornos no fluxo informacional, sendo inviável se aferir a eficácia jurídica do consentimento com fundamento na *fides*.

A boa-fé, por sua vez, é um modelo jurídico que deve propiciar o direcionamento de comportamentos no tráfico negocial (MARTINS-COSTA, 2018). Igualmente, verifica-se que o instituto da boa-fé objetiva seria um mecanismo eficaz na atualidade, para se interpretar o consentimento com o intuito de se aferir sua eficácia jurídica, aliado à interpretação substantiva e formal.

Além do princípio da confiança e da boa-fé objetiva, impende mencionar, também, o princípio da autonomia privada e da autorresponsabilidade, eis que interligados, apesar de suas diferenças conceituais.

A autonomia privada constitui o fundamento da ação jurídico-privada além de traduzir uma fonte de poder normativo, por meio do qual se forma e são criados negócios jurídicos. O exercício da autonomia privada se dá, também, como meio de proteção das expectativas geradas por atos dos particulares; é a aptidão a dar-se regras em uma ordem social juridicamente conformada, ou seja, em uma ordem de relações jurídicas, em que particulares estabelecem normas, mas, também, assumem responsabilidades por seus atos, nos limites do ordenamento jurídico (MARTINS-COSTA, 2018).

Neste cenário, a problemática se instaura em verificar qual dos polos deve prevalecer, motivo pelo qual, mais uma vez, deve se analisar o contexto da arquitetura de determinada relação. O exercício da autonomia privada, deste modo, está intimamente ligado ao princípio da confiança, outrora mencionado, que busca a proteção das expectativas legítimas, na medida em que toda declaração negocial (exercício da autonomia privada), implica que o destinatário da declaração, ao aceitar a proposta, ganhe o direito a confiar no cumprimento da prestação (VAINZOF, 2018).

A autorresponsabilidade significa que todo agir, toda conduta ativa do indivíduo, implica em uma autovinculação, uma exigência de fidelidade à pretensão que lhe é inerente (MARTINS-COSTA, 2018).

Em se tratando de tratamento de dados pessoais com fundamento na base legal do consentimento, constata-se que a boa-fé seria o princípio mais apropriado, eis que apesar da confiança, a autonomia privada e a autorresponsabilidade objetivam a tutela de um modelo jurídico, de um padrão de conduta esperado, independente da posição da parte contrária da relação negocial (como ocorre na confiança, na autonomia privada e na autorresponsabilidade). No caso de tratamento de dados pessoais com base no consentimento, a conduta a ser interpretada, e que se busca verificar a eficácia jurídica, é a do titular do dado pessoal, apenas, motivo pelo qual a boa-fé se mostra o veículo mais adequado nesta situação específica.

A LGPD, em seu artigo 6º, dispõe de maneira genérica, que o tratamento de dados pessoais deve observar a boa-fé, bem como os demais princípios descritos no rol do dispositivo mencionado. A boa-fé objetiva surge como este critério para direcionar comportamentos durante uma tratativa negocial, a qual deve ser regida por regras de conduta entre as partes, de maneira a evitar injustos danos. Segundo Martins-Costa (2018, p. 43), "o agir segundo a boa-fé objetiva concretiza as exigências de probidade, correção e comportamento leal hábeis a viabilizar um adequado tráfico negocial".

Assim sendo, a boa-fé como uma norma de interpretação serve como o ponto de convergência entre a confiança e o consentimento; o consentimento, sendo a maior expressão da autonomia privada, e a confiança, com sua capacidade subjetiva, impossível de ser comprovada, devem ser analisados de acordo com a boa-fé (PEREIRA, 2018). No ciberespaço, em que as relações são massificadas, bem como em razão da inviabilidade de se analisar o real motivo pelo qual o titular dos dados consentiu com o tratamento, a boa-fé é um dos instrumentos que possibilitaria tal análise, com o fito de apurar a eficácia jurídica da manifestação volitiva.

Como salientado anteriormente, apesar da possibilidade de interpretação do consentimento com relação à forma e ao conteúdo, a boa-fé seria necessária para aclaração do sentido da expressão volitiva, a qual possui valência integrativa, completando o conteúdo da manifestação de vontade. Deste modo, tem-se alguns contextos em que a boa-fé atua, com relação aos deveres anexos, que são os pilares do referido princípio: deveres de previdência, dever de segurança, dever de cuidar, dever de avisar e de esclarecer, dever de informar, dever de prestar contas, dever de colaborar e cooperar, dever de proteger e cuidar e dever de guardar

sigilo sobre atos dos quais se teve conhecimento em razão de determinada relação (MARTINS-COSTA, 2018).

Deste modo, quando da necessidade de análise do consentimento, em especial nas relações do ciberespaço, evidente que as partes devem agir de acordo com determinados padrões, de maneira a verificar a sua eficácia jurídica; os deveres anexos trazidos pela boa-fé pautam tais condutas, principalmente aquelas envolvendo o consentimento no ciberespaço, por se tratar de relações, normalmente em desequilíbrio no mundo digital, em que usuários (titulares de dados) estão em posição hipervulnerável.

Ainda, de maneira a sedimentar a boa-fé como interpretação do consentimento nas relações do ciberespaço, importante mencionar, também, que o instituto possui três funções, que nos ajudam a viabilizar sua aplicabilidade, quais sejam: função hermenêutica, função integrativa e função corretora (MARTINS-COSTA, 2018).

A função hermenêutica da boa-fé busca uma conjugação de padrões para averiguar como o comportamento é individualizado, naquela determinada situação; interpreta-se a manifestação da vontade. Ao invocar a boa-fé para interpretar o consentimento, se busca a necessidade de dar uma resposta adequada a problemas concretos e singulares (MARTINS-COSTA, 2018); desta feita, considerando a análise contextual do consentimento, o qual é expressado de acordo com os interesses do próprio indivíduo, baseado na cultura, experiências, lugar, tempo, etc., a função hermenêutica da boa-fé segue na mesma direção, posto que estuda estes padrões de comportamento de maneira a verificar sua eficácia jurídica casuisticamente.

A função integrativa da boa-fé é aquela utilizada para sanar uma lacuna, algo que está incompleto. A integração visa suprir uma lacuna, que deve ser preenchida para alcançar eventual normalidade de uma operação, bem como a utilidade visada pelas partes. A boa-fé autoriza detectar quais os deveres que são necessários para verificar a eficácia de determinado negócio, e que ali não foram inseridos, de maneira a proteger os envolvidos bem como os bens jurídicos protegidos. As lacunas nem sempre aparecem no momento da concretização de determinada relação, elas podem surgir futuramente, em razão de imprevidências (MARTINS-COSTA, 2018), tendo em vista que é impossível cogitar a ocorrência de todas as situações, ainda mais em se tratando de comportamento humano e de relações travadas no ciberespaço.

A última função da boa-fé é a corretora; considerando que a boa-fé possui como objetivo o direcionamento de condutas em determinada relação, a sua principal função é corrigir comportamentos no exercício de direitos, faculdades, pretensões, ações, exceções e ônus. A função corretora da boa-fé se desdobra em duas vertentes: a de auxiliar a corrigir o exercício jurídico, direcionando-o e ajustando-o aos padrões de licitude e a correção do próprio conteúdo da relação negocial. Neste sentido, a função corretora do exercício jurídico visa impedir o exercício manifestamente desleal, incoerente, imoderado ou regular de direitos subjetivos, possuindo um caráter dinâmico eis que abrange todas as fases da relação obrigacional (MARTINS-COSTA, 2018).

Ainda, com relação à interpretação do consentimento nas relações travadas no ciberespaço, em especial no tocante ao tratamento dos dados pessoais, poderíamos cogitar a questão da dinâmica das referidas relações no transcorrer de sua existência, bem como do caminho do fluxo informacional, situações estas que podem gerar outros direitos e deveres que não os expressos na relação de subsunção observada entre a situação fática e a hipótese legal (LISBOA, 2012).

Há uma evidente e intensa ligação entre a boa-fé e a confiança, em que um dever de coerência é por elas compartilhado, no sentido de manter a palavra dada ou o comportamento manifestado (MARTINS-COSTA, 2018). De igual forma, analisando o consentimento no âmbito das relações no ciberespaço, bem como suas características, em especial a autodeterminação in-formativa e a finalidade específica, ambas as partes da relação devem, em razão da boa-fé, agir de maneira proba.

Desta maneira, se apesar de o consentimento ter preenchido requisitos substanciais e formais, em razão da inviabilidade de aferir a sua eficácia jurídica, por se desconhecer o sentimento íntimo do indivíduo, ou em razão das limitações em que o mesmo é fornecido, bem como as condições que o mesmo foi manifestado (lugar, ambiente, tempo etc.), é inevitável a aplicação do princípio da boa-fé objetiva para a interpretação da manifestação de vontade. Portanto, tem-se que o consentimento, apesar da aparente facilidade de interpretação, demanda uma análise mais aprofundada, eis que, quando expresso na amplitude das relações do ciberespaço, pode não refletir verdadeiramente a exata intenção do titular dos dados.

O comportamento humano, como já salientado, é pautado por assimetrias sociais derivadas de poderes fáticos (econômicos, informativos, estratégicos), o que leva à proposição de novos modelos dogmáticos, em especial no âmbito do ciberespaço. A teoria do contato

social, deste modo, sustenta que fontes de obrigações podem ser reconduzidas a atos existenciais (atos-fatos), que são produzidas a partir de condutas socialmente típicas (COUTO E SILVA, 1988). Considerando que o consentimento é fortemente influenciado por fatores sociais (além de culturais e históricos), evidente a sua inexatidão, motivo pelo qual sua interpretação também demanda a aplicação de um princípio que permita a análise de suas condições de maneira particular, em conformidade com seu contexto, qual seja, o da boa-fé objetiva.

O contato social seria, dessa forma, uma fonte geral e comum a todas as espécies de relações, capaz de acomodar numa mesma estrutura de sistematização os fatos jurídicos nascidos da autonomia privada e da confiança legítima. Assim sendo, o consentimento, por possuir este caráter geral, influenciado por diversas condições, deve ser analisado a partir de sua substância conteudística, i.e., de seu contexto, para se aferir a sua eficácia jurídica, ainda mais quando manifestado no ciberespaço. Os atos existenciais são espécies que integram o contato social, e se referem a necessidades básicas do indivíduo (alimentação, vestuário, água etc.) (MARTINS-COSTA, 2018), e são manifestados nas condutas socialmente típicas. Nesses termos,

> De fato, a proposição de um tratamento dogmático particularizado para esses atos se insere na temática mais vasta das consequências da tipicidade social que impõe, concomitantemente com a emergência do fenômeno da massificação social e das novas tecnólogas da informação, a necessidade de reconhecer como dotados de juridicidade outros elementos de fixação no mundo social além da lei e da vontade (MARTINS-COSTA, 2018, p. 268).

Ainda neste sentido, tem-se que a sociedade moderna se caracteriza por incessante e progressiva padronização, em que se estabeleceram tipos sociais, que resultam em práticas continuadas, de costumes; os atos sociais, por consequência, são providências típicas da sociedade massificada, necessárias para que o cidadão subsista de forma digna, de acordo com os padrões sociais vigentes em cada época (PEREIRA, 2018).

O consentimento, portanto, pode ser um ato social na medida em que o indivíduo, no ciberespaço, consente com o tratamento de seus dados por um impulso social, visando uma identidade ou pertencimento em determinado grupo.

Considerando a assimetria das relações no ciberespaço, em especial no tocante ao consentimento, haja vista a inviabilidade de se verificar sua eficácia jurídica com base apenas em elementos substanciais e técnicos, evidente a necessidade de um instituto jurídico que

permita sua interpretação, atenta às legítimas expectativas do titular de dados; este instrumento é a boa-fé objetiva.

Portanto, considerando a hipersubjetividade do consentimento no tocante ao tratamento de dados pessoais, em especial nas relações massificadas do ciberespaço, evidente que apenas condições relativas à forma de sua expressão ou algum outro meio técnico para tentativa de sua validade, são insuficientes para averiguar a eficácia jurídica do instituto. O real motivo pelo qual o consentimento foi ou não dado, nunca será motivo de conhecimento e comprovação pelo interessado, ou por terceiros, razão pela qual sua interpretação com base no princípio da boa-fé objetiva é uma das possíveis soluções para tentativa de resolver a questão na atualidade.

3.4.3 O necessário equilíbrio entre o legítimo interesse e o consentimento

De acordo com o já exposto anteriormente, observa-se que o protagonista do consentimento é o próprio titular dos dados pessoais, o qual exerce tal manifestação de vontade com base na autodeterminação informativa. Além do consentimento, que possui um artigo específico na LGPD, com os seus requisitos e disposições, apenas outra base legal trazida pela legislação teve o mesmo tratamento formal, qual seja, o legítimo interesse, tratado de maneira específica no art. 10, da LGPD.

O consentimento já foi tratado nas seções anteriores, tal qual a dificuldade de sua interpretação em razão do caráter subjetivo e volátil do instituto. Deste modo, de maneira a traçar um paralelo entre o consentimento e o legítimo interesse, é importante tecer alguns comentários a respeito desta outra base legal também empregada no tratamento de dados pessoais.

O legítimo interesse é uma situação subjetiva, uma faculdade ligada à uma provável pretensão de um sujeito de direito privado face à um interesse social. A LGPD não trouxe um conceito específico do que seria o legítimo interesse do controlador ou de terceiro, muito pelo contrário, eis que pela leitura do artigo 10 da LGPD, foi possível concluir pela demasiada abrangência do termo. Deste modo, levando-se em conta que o legítimo interesse é um conceito indeterminado, alguns mecanismos são necessários para tentar obter equilíbrio na relação envolvendo os titulares de dados e os agentes reguladores responsáveis pelo

tratamento (WALDMAN; FUJITA, 2020). Assim, o legítimo interesse é uma proposição jurídica abstrata, não possuindo uma definição imutável, eis que sua conceituação dependerá de uma interpretação da realidade para a qual existe um consenso razoável (WALDMAN, 2001).

O legítimo interesse, tal qual o consentimento, deve ser interpretado de acordo com os princípios trazidos pela LGPD, em especial o da finalidade, transparência, necessidade e adequação. Além dos princípios, o legítimo interesse também deve ser concreto e claro (VAINZOF, 2018), sendo necessária uma ponderação de modo a atingir um equilíbrio entre os interesses em jogo e os direitos fundamentais do titular dos dados pessoais (WALDMAN; FUJITA, 2020).

Destaque-se, complementarmente, que o legítimo interesse, em razão de sua flexibilidade e subjetividade, conquistou o status de uma nova "carta coringa regulatória" (BIONI, 2019, p. 249), que viabiliza uma grande possibilidade para o uso de dados.

O Grupo de Trabalho do Artigo 29 (*Working Party* 29) formulou uma opinião sobre o legítimo interesse, a qual foi, ulteriormente, incorporada no GDPR, nas consideradas 47 a 50; o Grupo de Trabalho, deste modo, estabeleceu critérios para aplicação do legítimo interesse, o qual deveria a) trazer previsibilidade e segurança jurídica quando da aplicação desta base legal; b) evitar que o legítimo interesse passasse a ser uma "porta aberta" para driblar os direitos e princípios inerentes à diretiva, especialmente com relação às demais bases legais para o tratamento dos dados (BIONI, 2019).

O artigo 29 também menciona que a verificação do legítimo interesse deve ser realizada sob quatro aspectos, os quais também foram adotados pela LGPD brasileira: i) verificação da legitimidade interesse (art. 10, *caput* e inc. I, da LGPD); ii) necessidade do tratamento de dados (art. 10, §1º, da LGPD); iii) balanceamento entre impactos sobre o titular de dados e as legítimas expectativas (art. 10, inc. II, da LGPD) e iv) resguardar a transparência e assegurar a minimização dos riscos ao titular dos dados (art. 10, §§2º e 3º da LGPD).

Com relação ao primeiro aspecto relativo à análise do legítimo interesse, há de se verificar se o mesmo é lícito; é dizer, considerando os limites do que é lícito, há de se verificar se o controlador auferirá alguma vantagem com o tratamento daqueles dados (WALDMAN; RUIZ, 2020), ou se seu interesse está claramente articulado (ZANFIR-FORTUNA, 2018).

O segundo aspecto prega que o tratamento com base no legítimo interesse deve atender uma finalidade específica pretendida (arts. 6º e 10º, §1º da LGPD), em que deve se levar em consideração a possibilidade de atingir o mesmo resultado por meio do tratamento de uma quantidade menor de dados (art. 6º, inc. III, da LGPD – princípio da necessidade), ou se o mesmo poderia ser realizado com suporte em outra base legal (WALDMAN; RUIZ, 2020).

O terceiro ponto a ser observado para o tratamento com base no legítimo interesse é o equilíbrio entre os impactos do titular dos dados e suas legítimas expectativas (art. 10, inc. II, da LGPD). O último aspecto a ser verificado é a adoção de medidas para salvaguardar a transparência do tratamento dos dados, bem como a possibilidade da ANPD, solicitar um relatório de impacto à proteção dos dados pessoais.

Desta maneira, pode-se verificar que existem mecanismos que limitam a atuação do controlador ao optar pelo uso do legítimo interesse como fundamento legal para tratar os dados pessoais; no entanto, mesmo em razão das citadas limitações, novamente o comportamento humano pode surpreender. O legítimo interesse, tal como o consentimento, é uma base legal que possui natureza subjetiva, eis que depende de uma interpretação de determinada situação por parte do indivíduo (controlador ou titular do dado). Nos dizeres de Bioni:

> O fio condutor de toda essa avaliação é "balancear" os direitos em jogo. De um lado, do titular dos dados, e de outro lado, de quem faz uso das suas informações. Tão importante quanto aferir se há algum interesse legítimo é verificar se as legítimas expectativas e os direitos e liberdades fundamentais do cidadão serão respeitadas (BIONI, 2019, p. 252).

Assim, se eventualmente o titular dos dados pessoais consente com o tratamento, para uma finalidade específica, na contramão deste procedimento encontramos o controlador ou terceiro (como mencionado no texto legal), o qual pode, também, realizar o tratamento daqueles dados para outra finalidade com base no legítimo interesse, desde que haja especificação e preencha os aspectos anteriormente mencionados, de maneira a legitimar sua opção.

Evidente que o controlador, que atua em nome de alguma plataforma ou aplicativo, está em situação de maior vantagem face ao indivíduo que navega e consome no ciberespaço; além disso, apesar do teste de balanceamento para verificar o legítimo interesse, é notório que existem inúmeras outras justificativas emanadas da criatividade humana para aplicação desta

base legal, motivo pelo qual imperioso um cuidado maior nestes casos (inclusive no relatório de impacto à proteção de dados pessoais).

Deste modo, considerando que tanto o consentimento quanto o legítimo interesse possuem critérios subjetivos para sua utilização, imperiosa a observação dos direitos fundamentais do titular dos dados pessoais, protagonista da proteção legislativa e detentor da matéria-prima do capitalismo informacional. O tratamento de dados pessoais com base no legítimo interesse, não pode ir de encontro à direitos fundamentais, haja vista a posição do controlador em face do sujeito, bem como das características das relações travadas no ciberespaço, devendo se analisar o contexto do consentimento para justificar o interesse legítimo.

Finalizando esta pesquisa, busca-se demonstrar como a jurisprudência tem se posicionado em ações que têm como fundamento a LGPD e quais as expectativas que é possível ter com relação à novel legislação.

3.5 Jurisprudência pertinente e expectativas com relação à LGPD

Mesmo antes da entrada em vigor da LGPD, o Poder Judiciário já tem posicionamentos acerca de tratamento dos dados pessoais. O STF diante de dados obtidos ao arrepio da garantia da inviolabilidade, da intimidade das pessoas, assim julgou na Ação Penal 307/1994, fls. 2104, sendo Ministro Relator Dr. Ilmar Galvão.

Quanto à divulgação indevida de dados pessoais, o STJ reconheceu a existência de dano moral ainda no contexto de ausência da Lei nº 13.709/2018 – LGPD, como se observa no acórdão a seguir:

> AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. PROCESSUAL CIVIL (CPC/1973). INDENIZAÇÃO. DANO MORAL. ILEGITIMIDADE PASSIVA E INTERESSE DE AGIR AFASTADAS. DADOS PESSOAIS DA AUTORA DIVULGADOS PELO BANCO RECORRENTE. DANO MORAL. OCORRÊNCIA. VALOR ARBITRADO COM RAZOABILIDADE. REVISÃO DO ENTENDIMENTO PROFERIDO PELO TRIBUNAL DE ORIGEM QUANTO AOS TEMAS. IMPOSSIBILIDADE. PRETENSÃO RECURSAL QUE ESBARRA NO ÓBICE DA SÚMULA 7/STJ. AUSÊNCIA DE FUNDAMENTOS QUE JUSTIFIQUEM A ALTERAÇÃO DA DECISÃO AGRAVADA. AGRAVO

INTERNO MANIFESTAMENTE INADIMISSÍVEL. AGRAVO DESPROVIDO[46].

Constata-se que, embora não houvesse uma legislação específica sobre a proteção de dados pessoais na época, o Poder Judiciário acabava recorrendo aos diplomas legais genéricos com o objetivo de tutelar os direitos dos cidadãos e isto é importante, pois, como já afirmado na introdução desta pesquisa, mesmo com a LGPD e tendo esta legislação deixado de disciplinar algo em específico, há que se buscar respaldo na dogmática constitucional, civil e penal que pode e deve ser empregada para solucionar conflitos que eventualmente possam surgir.

Dentre os aplicativos de celular mais utilizados pelos cidadãos, evidenciam-se aqueles que autorizam a comunicação entre as pessoas. Embora não haja legislação que salvaguarde as informações privadas dos cidadãos, o STJ – em sede de recurso ordinário em *habeas corpus*[47] – foi instado a se manifestar sobre a privacidade das mensagens contidas no aplicativo *WhatsApp*.

Do exposto, verifica-se que o STJ assegurou o direito à privacidade e à proteção dos dados pessoais dos aplicativos de celular que operam também com trocas instantâneas de mensagens.

---

[46] "AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. PROCESSUAL CIVIL (CPC/1973). INDENIZAÇÃO. DANO MORAL. ILEGITIMIDADE PASSIVA E INTERESSE DE AGIR AFASTADAS. DADOS PESSOAIS DA AUTORA DIVULGA-DOS PELO BANCO RECORRENTE. DANO MORAL. OCORRÊNCIA. VALOR ARBITRADO COM RAZOABILIDADE. REVISÃO DO ENTENDIMENTO PROFERIDO PELO TRIBUNAL DE ORIGEM QUANTO AOS TEMAS. IMPOSSIBILIDADE. PRETENSÃO RECURSAL QUE ESBARRA NO ÓBICE DA SÚMULA 7/STJ. AUSÊNCIA DE FUNDAMENTOS QUE JUSTIFIQUEM A ALTERAÇÃO DA DECISÃO AGRAVADA. AGRAVO INTERNO MANIFESTAMENTE INADIMISSÍVEL. AGRAVO DESPROVIDO" (BRASIL. Superior Tribunal de Justiça. *Agravo Interno no Agravo em Recurso Especial 704.886/São Paulo*. Agravante: Banco Safra S/A. Agravada: Adriana Bittar de Santis Suplicy. Rel. Min. Paulo de Tarso Sanseverino. Brasília/DF, 7.03.2017).

[47] "2. A Lei 12.965/2014, conhecida como Marco Civil da Internet, em seu art. 7º, assegura aos usuários os direitos para o uso da Internet no Brasil, entre eles, o da inviolabilidade da intimidade e da vida privada, do sigilo do fluxo de suas comunicações pela Internet, bem como de suas comunicações privadas armazenadas. [...] 4. Com o avanço tecnológico, o aparelho celular deixou de ser apenas um instrumento de comunicação interpessoal. Hoje, é possível ter acesso a diversas funções, entre elas, a verificação de mensagens escritas ou audível, de correspondência eletrônica, e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional. 5. Por se encontrar em situação similar às conversas mantidas por e-mail, cujo acesso é exigido prévia ordem judicial, a obtenção de conversas mantidas pelo programa whatsapp[sic], sem a devida autorização judicial, revela-se ilegal" (BRASIL. Superior Tribunal de Justiça. *Recurso Ordinário em Habeas Corpus 75.055/Distrito Federal*. Recorrente: Thiago Costa Vieira Paes Landim. Recorrido: Ministério Público do Distrito Federal e Territórios. Rel. Min. Ribeiro Dantas. Brasília/DF, 21.03.2017).

Complementarmente, em sede de Recurso Especial[48], o Tribunal entendeu que é proibido o compartilhamento dos dados pessoais, como se constata da leitura dos trechos da ementa do acórdão citado em nota[49].

Percebe-se que o acórdão compara a situação de inexistência de diploma legal direcionado à proteção de dados pessoais no Brasil, com o Regulamento Geral da Proteção de Dados (RGPD) da UE que à época já dispunha sobre esta questão.

Questão relevante é a localização dos arquivos de dados, eis que o tratamento deles pode funcionar de acordo com a lei do território em que se encontra, e não do país do titular dos dados.

O derradeiro julgamento[50] do STJ versa sobre a prescindibilidade da cooperação internacional, quando a empresa possui sede no Brasil – mesmo que o tratamento de dados pessoais aconteça no exterior.

---

[48] BRASIL. Superior Tribunal de Justiça. *Recurso Especial 1.348.532/São Paulo*. Recorrente: HSBC Bank Brasil S.A. – Banco Múltiplo. Recorrida: Associação Nacional de Defesa da Cidadania e do Consumidor – ANADEC. Rel. Min. Luís Felipe Salomão. Brasília/DF, 10.10.2017).

[49] RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. [...] 3. 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. 4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança. 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição. 7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão. [...] (BRASIL. Superior Tribunal de Justiça. *REsp 1.348.532-SP*. Rel. Min. Luis Felipe Salomão, por unanimidade. Julgado em 10/10/2017).

[50] RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. QUEBRA DE SIGILO TELEMÁTICO. DESCUMPRIMENTO DE ORDEM JUDICIAL. ALEGAÇÕES DE AUSÊNCIA DE INDÍCIOS DE AUTORIA DELITIVA E DE VIOLAÇÃO A DIREITO DE TERCEIRO. NÃO CABIMENTO. APLICAÇÃO DE MULTA DIÁRIA. EMPRESA SITUADA NO PAÍS. SUBMISSÃO À LEGISLAÇÃO NACIONAL. MARCO CIVIL DA INTERNET. INCIDÊNCIA. [...] 3. Conforme jurisprudência do Superior Tribunal de Justiça "por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo" (RMS 55.109/PR, Rel. Min. REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 07/11/2017, DJe 17/11/2017) 4. Observe-se, ainda, que não há qualquer ilegalidade no fato de o delito investigado ser anterior à vigência do Marco Civil da Internet. Isto porque a Lei 12.965/2014 diz respeito tão somente à imposição de astreintes aos descumpridores de decisão judicial, sendo inequívoco nos autos que a decisão judicial que determinou a

A decisão entendeu que é dispensável a cooperação internacional para requerer dados pessoais constantes em bases estrangeiras, uma vez que a legislação brasileira regula a situação.

A Ministra Rosa Weber em recente decisão na Medida Cautelar na Ação Direta de Inconstitucionalidade (ADIN) 6.387/DF, em que é Relatora, e Requerente, o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), deferiu a suspensão do inteiro teor da MP nº. 954/2020, que dispõe sobre o compartilhamento de dados pelas empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação IBGE, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19), sobre a qual dispõe a Lei nº 13.979/2020.

Destaque-se somente parte do acórdão deferindo a suspensão da MP nº 954/2020, cujo inteiro teor encontra-se disponível no site do STF onde se ressalta ainda mais a necessidade do respeito aos direitos fundamentais, a finalidade e a adequação no tratamento dos dados pessoais[51].

---

quebra de sigilo telemático permanece hígida. Com efeito, a data dos fatos delituosos é relevante para se aferir apenas a incidência da norma penal incriminadora, haja vista o princípio da anterioridade penal, sendo certo que o inquérito policial investiga condutas que se encontram tipificadas no art. 10 da Lei 9.296/1996 (Lei de interceptação) e art. 153, § 1º-A, do CP e não na Lei 12.965/2014". [...] (BRASIL. Superior Tribunal de Justiça. *Recurso em Mandado de Segurança 55.019/Distrito Federal*. Recorrente: Yahoo! do Brasil Internet Ltda. Recorridos: Distrito Federal e Ministério Público Federal. Rel. Min. Joel Ilan Paciornik. Brasília/DF, 12.12.2017).

[51] [...] A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal". 15. O art. 2º da MP n. 954/2020 impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação IBGE, da relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas. Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade. Sua manipulação e tratamento, assim, hão de observar os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da LGPD, como fundamentos específicos da disciplina da proteção de dados pessoais. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. 16. Cumpre, pois, equacionar se a MP n. 954/2020 exorbitou dos limites traçados pela Constituição ao dispor sobre a disponibilização dos dados pessoais de todos os consumidores dos serviços STFC e SMP, pelos respectivos operadores, a entidade integrante da Administração indireta. 17. Observo que o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas não presenciais no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem

Também, a Sexta Turma do STJ, tendo por relatora a Ministra Laurita Vaz, anulou uma prova obtida pelo *WhatsApp Web* sem o conhecimento e consentimento do proprietário do celular[52].

---

como serão efetivamente utilizados. Já o art. 1º, § único, da MP nº 954/2020 apenas dispõe que o ato normativo terá aplicação durante a situação de emergência de saúde pública decorrente da COVID-19. Ainda que se possa associar que a estatística a ser produzida tenha relação com a pandemia invocada como justificativa da edição da MP, tal ilação não se extrai de seu texto. Nessa ordem de ideias, não emerge da MP nº 954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade. E tal dever competia ao Poder Executivo ao editá-la. Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 não oferece condições para avaliação da sua adequação e necessidade. Desatende, assim, a garantia do devido processo legal, em sua dimensão substantiva. 18. De outra parte, o art. 3º, I e II, da MP nº 954/2020 dispõe que os dados compartilhados "terão caráter sigiloso" e "serão utilizados exclusivamente para a finalidade prevista no § 1º do art. 2º", e o art. 3º, § 1º, veda ao IBGE compartilhar os dados disponibilizados com outros entes, públicos ou privados. Nada obstante, a MP nº 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, ou no seu tratamento. Limita-se a delegar a ato do Presidente da Fundação IBGE o procedimento para compartilhamento dos dados, sem oferecer proteção suficiente aos relevantes direitos fundamentais em jogo. Enfatizo: ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando for o caso, o anonimato dos dados compartilhados, a MP nº 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros. Essas considerações são corroboradas pela manifestação trazida aos autos pela Agência Nacional de Telecomunicações – ANATEL, que destacou necessária "a observância de extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações". E recomendou a adoção de medidas visando a adequar a medida à garantia dos princípios estabelecidos na Constituição Federal, na Lei Geral das Telecomunicações e na Lei LGPD, de modo a assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações, mediante: [...] 22. Presente, à luz do exposto, o *fumus boni juris*, tenho por satisfeito igualmente o *periculum in mora*, uma vez que a determinação do imediato compartilhamento de dados leva à eficácia plena do ato normativo questionado. Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. [...] 24. Nesse contexto, e a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, defiro a medida cautelar requerida, ad referendum do Plenário desta Suprema Corte, para suspender a eficácia da MP nº 954/2020, determinando, em consequência, que o IBGE se abstenha de requerer a disponibilização dos dados objeto da referida MP e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia. 25. Por fim, considerando que as ADINs nºs 6388, 6389, 6390 e 6393, a mim distribuídas por prevenção, igualmente impugnam a validade da MP n. 954/2020, determino a tramitação conjunta dos feitos, com a reprodução desta decisão nos autos respectivos. À Secretaria Judiciária. Publique-se" (BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6390 – Distrito Federal 0090595-58.2020.1.00.0000*, Relator: Ministra Rosa Weber. Data de Julgamento: 17/04/2020).

[52] Segue parte de julgamento transcrito do site do STJ: "Cumpre assinalar, portanto, que o caso dos autos difere da situação, com legalidade amplamente reconhecida pelo Superior Tribunal de Justiça, em que, a exemplo de conversas mantidas por e-mail, ocorre autorização judicial para a obtenção, sem espelhamento, de conversas já registradas no aplicativo *WhatsApp*, com o propósito de periciar seu conteúdo", afirmou a relatora. "Ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para apreensão de aparelho telefônico, o espelhamento via QR Code depende da abordagem do indivíduo ou do vasculhamento de sua residência, com apreensão de seu apare-lho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da autoridade policial, à realização da medida constritiva, ou mesmo, porventura – embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto –, acompanhada de afirmação falsa de que nada foi feito", afirmou a relatora (JUSBRASIL, 2018).

Ao dar provimento ao recurso em *habeas corpus*, declarar nula a decisão judicial e determinar a soltura dos investigados, a ministra ainda considerou a presença de algumas ilegalidades, como: a ausência de fato novo que pudesse justificar a medida; e a inexistência na decisão, de indícios razoáveis da autoria ou participação, aptos a fundamentar a limitação do direito de privacidade.

A LGPD é relativamente nova e são poucos os julgados posteriores à legislação. Ainda não é possível afirmar incisivamente, com base na pequena construção jurisprudencial posterior a esta legislação, se com o advento da nova lei observa-se maior proteção à privacidade. Veja-se, neste sentido, um acórdão que se refere ao vazamento de dados de um consumidor:

> APELAÇÃO CÍVEL - AÇÃO ANULATÓRIA DE CONTRATO E INDENIZAÇÃO POR DANOS MORAIS - CONTRATAÇÃO DE EMPRÉSTIMOS - CAIXA ELETRÔNICO - CULPA EXCLUSIVA DA VÍTIMA - NÃO CONFIGURADA - DEFEITO NA PRESTAÇÃO DO SERVIÇO BANCÁRIO - VAZAMENTO DE DADOS PESSOAIS - DANOS MORAIS CARACTERIZADOS - QUANTUM INDENIZATÓRIO – ADEQUAÇÃO DEVIDA - SENTENÇA REFORMADA EM PARTE. [...] Reveste-se de ilicitude a hipótese em que a instituição financeira permite ou não cuida para impedir o vazamento dos dados pessoais de seus clientes oportunizando, assim, a atuação ilícita de terceiros fraudadores (MINAS GERAIS, 2019, s.p.).

Observe-se que este julgado se posicionou favorável ao consumidor e contrário à instituição bancária que deixou vazar dados pessoais de um cliente, o que oportunizou que este fosse vítima de uma fraude.

Do exposto é possível constatar que apesar de não ter havido tempo para a construção de uma construção jurisprudencial baseada nesta nova lei, a perspectiva social leva a crer que posicionamento jurisprudencial dominante, com o advento da Lei nº 13.709/2018 deverá se esforçar para que o direito à privacidade seja assegurado, sem, porém, obstar o desenvolvimento das Tecnologias da Informação e Comunicação (TICs).

Inclusive, a construção jurisprudencial do STJ já rumava neste sentido mesmo antes da LGPD, no entanto, é necessário que se atente às contradições, pois, a priori, o sistema brasileiro coaduna com a teoria de que juízos de valor são protegidos pela liberdade de expressão, ou seja, asseguram-se as manifestações de opiniões subjetivas, que, ainda que possam criticar ou ofender, integram um Estado pluralista e democrático. Não obstante, por vezes, a prática se vale de restrições severa da liberdade de expressão, como é o caso no qual

se envolveu a artista Mônica Iozzi, que foi condenada pela Segunda Vara Cível de Brasília, ao pagamento de uma indenização de R$ 30.000 (trinta mil reais). A artista publicou em uma rede social uma foto do Ministro do STF, Gilmar Mendes, com a legenda "Cúmplice? Gilmar Mendes concedeu *Habeas Corpus* para Roger Abdelmassih, depois de sua condenação a 278 anos de prisão por 58 estupros". O juiz do caso, concluiu que Mônica "abusou do seu direito de liberdade de expressão, por imputar ao ministro a cumplicidade do crime de estupro, tornando questionável o seu caráter e imparcialidade na condição de julgador" (GLOBO.COM, 2016, s.p.).

A incógnita fica também sobre as decisões do STF, que como já citado neste trabalho, em 2019 não se mostrou afeto às críticas à atuação da Suprema Corte. Em outro momento, quando as pessoas se envolveram em vazamentos de supostas conversas de autoridades hackeadas, ou seja, roubadas sem a autorização das mesmas em um claro caso de violação à privacidade, o mesmo não fez nenhum juízo crítico da situação. Inclusive, um dos ministros do STF estava no meio dos telefones hackeados, mas suas supostas conversas não foram divulgadas.

Por fim, importa citar um caso que ocorreu recentemente envolvendo a empresa holandesa C&A, que opera também no Brasil. Referida empresa, quinze dias após o presidente sancionar a LGPD protagonizou um maciço vazamento de dados de seus clientes, dados estes obtidos junto aos mesmos nas diversas lojas distribuídas no Brasil, quando os clientes são abordados por vendedores e induzidos a fazer um cartão de crédito da loja. Esta é uma prática, aliás, bastante comum em lojas âncoras, como é o caso também das Lojas Pernambucanas, Renner, Riachuelo, dentre outras.

Referente à C&A, denúncias foram realizadas acusando a empresa de fazer uso de informações coletadas de pessoas que se candidataram às vagas de emprego para que fossem emitidos cartões não solicitados. No dia 30 de agosto de 2018, foram vazados os endereços eletrônicos de clientes e funcionários da empresa, supostamente com o intuito de retaliar a denúncia. À época, um perfil do Twitter assumiu a autoria do feito.

Segundo expõe o site Flipside (2018), não se sabe a época em que o sistema foi invadido, no entanto vários registros do sistema de vendas de cartão da empresa foram divulgados. O grupo que assumiu a autoria do feito afirmou que teve acesso a aproximadamente 36 mil dados cadastrais, incluindo nome, Cadastro de Pessoa Física (CPF) e Registro Geral (RG).

Neste caso, por exemplo, se a LGPD já estivesse em vigor à época destes ataques, todos os usuários atingidos pelo incidente deveriam ser notificados pela empresa, o que desencadearia uma quebra de confiança e mácula na imagem da empresa junto aos clientes. Ademais, se ficasse comprovado que o vazamento ocorreu em razão de negligência (a exemplo de desatualização do sistema ou uso de senhas fracas), são previstas sanções pela legislação que podem ir, de acordo com a gravidade do incidente, desde as advertências até as multas que podem chegar a até 50 milhões de reais ou 2% do faturamento anual da empresa.

Não obstante a C&A ser uma empresa holandesa, a lei aplicada a este caso é a brasileira, exceto se existirem vítimas cuja nacionalidade seja a européia. Neste último caso, a lei aplicada seria a GDPR e as multas teriam o dobro do valor previsto na legislação do Brasil.

Assim, o que se percebe é que o caso concreto é que ditará a sanção que será aplicada. Decerto que aparecerão situações que irão suscitar dúvidas e questionamentos, mas a construção doutrinária, jurisprudencial e até mesmo legislativa se incumbirá de tratar destas lacunas à medida que estas forem surgindo.

CONCLUSÃO

O privado e o público são âmbitos paradoxais, porém de estreita relação e em prováveis situações de conflito. A relação entre esses dois âmbitos na Era da Informação mudou significativamente, no sentido de tornar público algumas situações que ocorriam no âmbito privado.

As instituições públicas e privadas do mundo contemporâneo têm oferecido, por intermédio da TIC, utilidades para as mais diversas necessidades humanas, com destaque para aquelas relacionadas com a informação, comunicação, consumo e os serviços públicos em geral.

As TICs estão a cada dia se tornando necessárias para as mais diversas atividades humanas, devido à maneira como as instituições públicas e privadas, bem como a sociedade, estão se estruturando, seja em função das políticas públicas implementadas, seja para atender objetivos de instituições privadas ou até interesses pessoais.

O elenco dos direitos fundamentais previstos na CRFB/1988 tem ampla aplicabilidade nas relações privadas e têm estreita relação com a proteção dos dados pessoais e, por consequência, da privacidade, diz respeito: à intimidade, à vida privada, à imagem das pessoas, a casa, às comunicações de todos os tipos, mediante correspondência tradicional (carta) ou eletrônica (*e-mail*), telefônica (voz, ou mensagens eletrônicas), de dados, e telegráfica. Essa relação passou a ser mais intensa em face do avanço tecnológico nessa era chamada da sociedade da informação.

O direito fundamental à proteção de dados pessoais protege a privacidade, um dos direitos da personalidade. Aquela, por sua vez, engloba a intimidade e a vida privada, na perspectiva da teoria dos círculos concêntricos que, não obstante ser atualmente abominada pela doutrina que a originou, serve de esquema para estruturação da relação entre os atos da pessoa e a tutela de sua privacidade.

Dados pessoais não podem ser vistos simplesmente como informação que compõe dados estatísticos ou até mercadoria a ser negociada. Deve ser visto como um dos componentes da personalidade que deve ser protegido em termos diferentes do que já foi feito até então.

Nesse cenário de avanço tecnológico, dados pessoais que precisam de proteção jurídica podem ser uma imagem, uma conversa, uma filmagem, hábitos de consumo pessoal, registrados por meio de operações via Internet ou administradoras de cartões de crédito, dentre outras informações. As possibilidades são as mais diversas, principalmente devido tudo estar interconectado, como é o caso da Internet das Coisas, tendo em vista as circunstâncias sociais, mercadológicas e tecnológicas atuais.

A perda da privacidade é muito maior do que se imagina e do que se divulga. Os avanços nas técnicas de pesquisa inteligente de dados e de formação de base de dados estratosféricas demonstram que a expansão da rede é algo ilimitado. Os sistemas proporcionam a revelação de muitos aspectos da privacidade sem o conhecimento e consentimento da pessoa alvo, com base em informações pessoais mínimas existentes na rede.

É de suma importância a compreensão dos interesses subjacentes de toda essa superestrutura. Isso demanda uma visão sistêmica que consiste em ampliar o foco de observação, contextualizar o fenômeno e focalizar as interações recursivas. Juridicamente significa garantir o acesso mais amplo possível a todas as informações socialmente relevantes, públicas e privadas, por meio de uma nova geração de leis sobre o acesso às informações, mediante os mais diversos recursos tecnológicos; impedir que as coletas de dados pessoais se transformem em instrumentos de discriminação ou retaliação política; e reagir a qualquer forma de transformação da pessoa humana em número ou mercadoria.

Referente ao consentimento, este foi analisado tomando-se por base duas possíveis interpretações, com o intuito de verificar a sua eficácia jurídica. A análise dos elementos materiais e formais foi realizada de forma mais aprofundada, mas que, mais uma vez, devido a sua volatilidade, obsta que, na atualidade, seja aferido o real motivo por meio do qual a manifestação da vontade foi externada. Os requisitos previstos na legislação, tanto o diploma legal brasileiro (LGPD), quanto a paradigmática legislação europeia (GDPR), não são suficientes para que seja aferida a eficácia jurídica do consentimento bem como de sua natureza hipersubjetiva, especialmente nas relações de consumo.

O tratamento dos dados pessoais, alicerce de um capitalismo informacional e também de vigilância, demanda um regramento jurídico para garantir os direitos fundamentais dos titulares dos citados dados, o que, no Brasil, já está sendo feito com a LGPD. O consentimento, um dos arcabouços legais para o tratamento de dados pessoais, tem

fundamental função no estudo sobre a proteção legislativa, já que parte do protagonista da tutela jurídica, o titular dos dados, sendo, pois, um ato personalíssimo.

Apesar de o Brasil fazer parte da RIPD, a legislação sobre essa proteção ainda é incipiente, bem como a cultura jurídica do país ainda está mais voltada para a discussão das políticas públicas relacionadas ao mínimo existencial, porque parte substancial da população ainda carece de tais condições. Porém, não é de menos importância a proteção de outros direitos fundamentais, a exemplo dos que dizem respeito à privacidade, principalmente porque a informação tornou-se um bem de valor econômico incomensurável para determinadas instituições públicas ou privadas, uma riqueza fundamental da sociedade.

O MCI se limitou a proteção dos dados pessoais, quando previu a tutela somente para usuários da Internet. Tal tutela de direitos não deve ser somente do usuário, mas de qualquer pessoa. Há diversas situações nas quais a pessoa não é usuária da Internet momentaneamente, porém fatos que referem-se à sua privacidade são capturados, arquivados e processados na rede, sem que o titular desses dados tenha conhecimento. Com efeito, crê-se que o sistema legal de proteção de dados pessoais do país está muito aquém para ter efetividade, devido à falta de políticas públicas eficazes para essa proteção.

O direito à autodeterminação informativa surge como consectário do direito à proteção de dados pessoais, em face da TI. Tal direito considera ilegítima toda coleta de informações pessoais que seja realizada sem o prévio conhecimento e explícito consentimento da pessoa. Consiste ainda que determinadas informações coletadas não devem circular fora da instituição pública ou privada que tenha coletado essas informações originalmente para certa finalidade.

A LGPD ingressa tardiamente no ordenamento pátrio, mas visa à proteção de dados pessoais do indivíduo. Para isso, trouxe diversos fundamentos relacionados com a personalidade, especialmente o respeito à privacidade, a inviolabilidade da intimidade, da honra e imagem, os direitos humanos, a dignidade e o exercício da cidadania por pessoas naturais. Esses fundamentos estão intimamente ligados à cidadania do novo milênio e não foram pensados para servir às relações de consumo, mesmo em fase do consentimento do consumidor, já que os contratos firmados *online*, em sua maioria são contratos de adesão.

Nesses termos, apesar de a informação ter mudado de roupagem em tempos de *e-commerce* e ter passado de ser um direito/dever para o objeto da relação de consumo, o princípio da vulnerabilidade do consumidor não mudou e há a necessidade de se reconhecer a

fragilidade deste diante das novas relações de consumo, da sociedade informacional, impondo ao fornecedor limites para o uso das informações coletadas, ainda que exista a concordância.

Uma das formas que vislumbra-se seria obrigar os fornecedores a não condicionar a aquisição do produto à concordância com a divulgação dos dados, coibindo efetivamente o abuso do poder econômico e permitindo que a concordância seja consciente por parte do consumidor.

Ademais, há que proteger também o consumidor de situações de atuação criminosa – ainda que o fornecedor também seja vítima – o consumidor tem o direito de ser indenizado e reparado em todos os danos que vier a sofrer em função dessa ação. Nesse caso, a responsabilidade é do fornecedor por não assegurar que os dados do consumidor estivessem totalmente protegidos.

Dito isto, é possível concluir que não obstante o tratamento jurídico dispensado aos dados pessoais dos consumidores brasileiros não tenha sido suficiente para resguardar o direito fundamental à privacidade em tempos de evolução tecnológica e massificação dos dados, o posicionamento jurisprudencial dominante antes do advento da Lei nº 13.709/2018 se esforçava em assegurar que o direito à privacidade fosse resguardado, sem, no entanto, obstar o desenvolvimento da TIC, também de grande importância para as relações de consumo travadas *online*.

Sabe-se que nas compras realizadas pela internet sempre são exigidos dados como nome completo, números de documentos pessoais, endereços, dados de cartão de crédito. A expectativa é que esses dados serão protegidos e guardados pelos fornecedores e que não serão usados. Entretanto, na nova sociedade informacional, essas informações têm valor e servem, em um primeiro momento, para direcionar o consumo, além de se ter notícia de venda desses dados para outros fornecedores ou pessoas que tenham interesse quaisquer.

Embora não fosse esse o foco da LGPD, essa Lei buscou regulamentar o uso dos dados de natureza pessoal consignando que esses somente podem ser usados ou comercializados com o consentimento do titular. Contudo, em razão da LGPD não ser uma legislação consumerista, ela não aborda o problema da vulnerabilidade do consumidor, que é a parte mais frágil da relação por se ver compelido a firmar contratos de adesão, não tendo a oportunidade, na maioria das vezes, de discutir os termos do contrato. Assim, ou aceita os termos pré-determinados ou não compra ou contrata o produto ou serviço.

Outra situação que se mostra preocupante é o armazenamento dos dados dos consumidores nas nuvens e a exposição desses a atos criminosos. Nesse ponto, a responsabilidade é do fornecedor, que ainda que também seja vítima, tem o dever de reparar os danos suportados pelo consumidor.

Dessa forma, encarar a informação como um produto/serviço possibilita o reconhecimento de que ao seu uso devem ser aplicadas as regras de proteção do consumidor, pois esse continua sendo a parte vulnerável na relação de consumo com o fornecedor.

Entende-se que cada empresa possui as suas especificidades, a depender dos seus modelos de negócio, do mercado em que atua e do seu relacionamento com os clientes e parceiros e que, em virtude disso, o compartilhamento dos dados e a celebração de contratos podem ganhar diferentes nuances. Todavia, a base, em todos eles, deve consistir na transparência e na responsabilidade, por meio de demonstração de clara e evidente preocupação com a segurança dos dados e de atitudes que possam assegurá-la. Por isso, a importância de um bom termo de confidencialidade e de uma boa política de segurança empresarial, devidamente disseminada, difundida e conhecida por todos os funcionários, parceiros e colaboradores.

O desafio mostra-se imenso, mas percebe-se que o Brasil caminha e dá seus passos no sentido de proteger os dados dos seus cidadãos, ao mesmo tempo em que permite a continuação da evolução tecnológica pela qual se passa atualmente. No entanto, para que essa efetividade aconteça, é necessária a realização de políticas públicas, a exemplo da criação de plataformas educacionais com vistas à educação e conscientização da sociedade.

As empresas brasileiras e os cidadãos precisam assimilar a cultura da proteção de dados pessoais e devem entender o direito à privacidade como um princípio e não como uma obrigação. É princípio da lei o desenvolvimento econômico e a inovação e não apenas a proteção de dados. Então não se pode permitir que certas atividades inovadoras sejam impedidas pela LGPD. O que é preciso (e está na lei) é estabelecer responsabilidades para essas pessoas que querem avançar, que querem desenvolver o país, mas que agora, com a LGPD precisarão fazer isso de forma responsável, levando em conta as boas práticas, com governança e segurança.

Portanto, aliando a positivação dessa conscientização e educação, o direito será capaz - como já vem se esforçando - de responder às novidades propostas pela tecnologia da informação, com a realização do seu valor fundamental: a pessoa humana e sua dignidade.

Por derradeiro, considerando que o ciberespaço é um ambiente digital, cuja matéria-prima para sua sustentação, e fomento do capitalismo informacional, é o dado pessoal, evidente que o seu uso de maneira irrestrita e incondicionada, pode afetar direitos individuais e de grupos determinados ou não. Posto isto, em sede de sugestão, entende-se que a proteção da privacidade do indivíduo poderia ser alçada a patamar de direito difuso, e protegida como tal, mediante os mecanismos processuais respectivos, haja vista a possibilidade de um único ato ou conduta afetar um número indeterminável de pessoas.

Em tempo, considerando a recente vigência da LGPD no ordenamento jurídico pátrio, a jurisprudência decerto terá uma função fundamental na análise da eficácia jurídica do consentimento aplicado a casos concretos, procedendo-se à análise dos meios de prova que eventualmente são produzidos, bem como se a verdadeira intenção do titular dos dados pessoais é passível de ser verificada e, em caso afirmativo, se a mesma será efetivamente compreendida como uma autorização para o tratamento dos dados.

REFERÊNCIAS

ACUNHA, Fernando José Gonçalves. Colisão de Normas – Distinção entre Ponderação e Juízo de Adequação. **Revista de Informação Legislativa**, a. 51, n. 203, jul./set., 2014. Disponível em: https://www12.senado.leg.br/ril/edicoes/51/203/ril_v51_ n203_p165.pdf. Acesso em: 16 Julho 2022.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgilio Afonso da Silva. São Paulo: Malheiros, 2008.

AMARAL, João Ferreira do. **Economia da informação e do conhecimento**. Coimbra: Almedina, 2009.

AMARAL, Ana Cláudia Correa Zuin Mattos do; FERREIRA, Jussara Borges. Negócio Jurídico e juízo arbitral: modulação da autonomia da vontade e da autonomia privada. In: MUNIZ, Tania Lobo; ARAUJO JUNIOR, Miguel Etinger de (Orgs.). **Estudos em direito negocial e mecanismos contemporâneos de resolução de conflitos**. Birigui, SP: Boreal Editora, 2014.

BARRETO NETO, Cândido Alexandrino. **O direito de criticar na jurisprudência do Supremo Tribunal Federal**. 113 f. 2015. Dissertação (Mestrado em Direito). Fortaleza, Universidade Federal de Fortaleza, 2015.

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução Plínio Dentzien. Rio de Janeiro: Jorge Zahar Editor, 2001.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. São Paulo: Forense, 2019.

BIRITI, Carlos Roberto. **Proteção de Dados Pessoais em Face do Estado**. Curitiba: Juruá Editora, 2021.

BANNWART JÚNIOR, Clodomiro José. Perspectiva Evolucionária na Teoria Social Crítica De Habermas. **TRANS/FORM/AÇÃO: Revista De Filosofia**, v. 36, n. 1, p. 67–86, 2013.

BARBIERI, Carlos. **Governança de Dados**: práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019.

BÉRRIUS, Carmen Gloria Arriagada; WOLF, Nathália Mello Américo. Compliance e LGPD (Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018). In: GIONÉDIS, Louise Rainer Pereira; VIANNA, Maria Amélia Mastrorosa. **Lei Geral de Proteção de Dados e o *Compliance*.** Curitiba: Juruá, 2021, p. 55-68.

BOBBIO, Norberto. **Teoria do ordenamento jurídico**. 6. ed. Brasília: UnB, 1995.

BOFF, Salete Oro; FORTES, Vinicius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção e um marco regulatório para o Brasil. **Revista Sequência**, Florianópolis, n. 68, p. 109-127, jun., 2014.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRAMANTE, Ivani Contini; DE MARTINO, Ana Cecilia Sampaio; ALVES, Leonardo Gutierrez. **Proteção de Dados Pessoais na Relação de Trabalho**. Curitiba: Juruá Editora, 2021.

BRASIL. **Decreto-Lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução as Normas do Direito Brasileiro – LINDB. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 16 Julho 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 Julho 2022.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** pra além da informação creditícia. Brasília: SDE/DPDC, 2010.

BRASIL. **Projeto de Lei nº 4.060, de 13 de Junho de 2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012. Acesso em: 14 Julho 2022.

BRASIL. **Decreto nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm. Acesso em: 14 março 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 Julho 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 Julho 2022.

BRASIL. **Projeto de Lei nº 1515, de 7 de junho de 2022**. Altera as Leis nº 12.850 de 2013; 12.965 de 2014; 9.613 de 1998 e 12.037 de 2009. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#:~:text=PL%201515%2F2022%20Inteiro%20teor,Projeto%20de%20Lei&text=Lei%20de%20Prote%C3%A7%C3%A3o%20de%20Dados,1998%20e%2012.037%20de%202009. Acesso em: 10 março 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.316.921-RJ**. Relatora: Ministro Nancy. Julgado em: 26 de junho de 2012. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/22026857/recurso-especial-resp-1316921-rj-2011-0307909-6-stj/inteiro-teor-22026859. Acesso em: 16 Julho 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança 55.019/DF**. Relator: Min. Joel Ilan Paciornik. Julgado em: 12.12.2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1646430&num_registro=201202108054&data=20171130&formato=HTML. Acesso em: 16 Julho 2022.

BRASIL. Superior Tribunal de Justiça. **Agravo Interno no Agravo em Recurso Especial 704.886/SP.** Relator: Min. Paulo de Tarso Sanseverino. Julgado em: 07.03.2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?Componente=ITA&sequencial=1576703&num_registro=201500839516&data=20170313&formato=HTML. Acesso em: 16 Julho 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.348.532/SP**. Relator: Min. Luís Felipe Salomão. Julgado em: 10.10.2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1646430&num_registro=201202108054&data=20171130&formato=HTML. Acesso em: 16 Julho 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Habeas Corpus 75.055/DF**. Relator: Min. Ribeiro Dantas. Julgado em: 21.03.2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1583195&num_registro=201602198887&data=20170327&forma to=HTML. Acesso em: 16 Julho 2022.

BRASIL. Superior Tribunal de Justiça. **REsp 1.348.532-SP**. Relator: Min. Luis Felipe Salomão, por unanimidade. Julgado em: 10/10/2017. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/526809457/recurso-especial-resp-1348532-sp-2012-0210805-4. Acesso em: 15 Julho 2022.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6390/DF 0090595-58.2020.1.00.0000**. Relator: Min. Rosa Weber. Julgado em: 17/04/2020. Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/862328256/medida-cautelar-na-acao-direta-de-inconstitucionalidade-mc-adi-6390-df-distrito-federal-0090595-5820201000000. Acesso em: 15 Julho 2022.

BRASIL, Emanuelle. **Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional**. Câmara dos Deputados, 12.08.2022. Disponível em: https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/. Acesso em: 14 março 2023.

CANOTILHO, Gomes; MACHADO, Jónatas; GAIO JR., Antônio. **Biografia não autorizada *versus* Liberdade de Expressão**. Curitiba: Juruá, 2015.

CAPPELLI, Cláudia; CARVALHO, Luiz Paulo; MAJER, violeta; OLIVEIRA, Jonice. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais**. Universidade Federal do Rio de Janeiro, 2020. Disponível em: desafios da LGPD.pdf. Acesso em: 16 Julho 2022.

CARDOSO, Henrique Ribeiro. **Proporcionalidade e argumentação**: a Teoria de Robert Alexy e seus pressupostos filosóficos. Curitiba: Juruá Editora, 2009.

CHAVES, Luís Fernando Prado. Bélgica: Empresa é multada por ter nomeado *head* de *compliance*, auditoria e riscos como DPO. **Migalhas**, 04.06.2020. Disponível em: https://www.migalhas.com.br/depeso/328258/belgica--empresa-e-multada-por-ter-nomeado-head-de-compliance--auditoria-e-riscos-como-dpo. Acesso em: 16 Julho 2022.

COLAÇO, Hian Silva; MENEZES, Joyceane Bezerra de. Quando a Lei de Proteção de Dados não se aplica? *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters, 2019.

CONSULTOR JURÍDICO. **Empresa é condenada em R$ 1,5 mil por excesso de ligações de telemarketing.** 05.06.2021. Disponível em: https://www.conjur.com.br/2021-jun-05/empresa-condenada-excesso-ligacoes-telemarketing. Acesso em: 14 março 2023.

COTS, Márcio; OLIVEIRA, Ricardo. **Legítimo Interesse e a LGPD**. São Paulo: RT, 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. São Paulo: Editora Revista dos Tribunais, 2021.

COUTO E SILVA, Clóvis do. **Principes Fondamentaux de La Responsabilité Civile em Droit Brésilien et Comparé:** cours fait à la Facultè de Droit e Scientes Politiques de St. Maur. Paris XII: Porto Alegre, 1988.

DESLANDES, Maria S. S.; ARANTES, Álisson R. Os perigos dos crimes virtuais nas redes sociais. **Sinapse Múltipla**, v. 6, n. 2, p. 175-178, dez., 2017.

DIAS, Clara Angélica G.; SILVA, Raquel Torres de Brito. A aplicabilidade dos direitos fundamentais sob a ótica horizontal: um supino fruto do constitucionalismo democrático contemporâneo. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ**, Rio de Janeiro, v.3, n.1, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ESPOLADOR, Rita de Cássia Resquetti Tarifa. **Necessidade de controle jurídico nos negócios:** algumas considerações envolvendo a manipulação embrionária humana e o papel da legislação consumerista. Birigui, SP: Boreal Editora, 2013.

ESTADO DE MINAS. Vulnerabilidade no CDC. **Jornal Estado de Minas**, 03/10/2016. Disponível em: https://www.em.com.br/app/noticia/direito-ejustica/2016/10/03/interna_direito_e_justica,828595/vulne rabilidade-no-cdc.shtml. Acesso em: 15 Julho 2022.

FEIGELSON, Bruno; SIQUEIRA, Antônio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados:** Lei 13.709/2018. São Paulo: RT, 2019.

FERGUSON, Andrew Guthrie. Big Data and Predictive Reasonable Suspicion. **Univesity of Pensylvania Law Review**, v. 163, n. 327, Jan., 2015.

FERREIRA, Natália Braga. Notas Sobre a Teoria dos Princípios de Robert Alexy. **Revista Eletrônica do Curso de Direito – PUC Minas Serro,** n. 2, 2010. Disponível em: http://periodicos.pucminas.br/index.php/DireitoSerro/article/view/1290. Acesso em: 15 Julho 2022.

FILOMENO, José Geraldo Brito. **Manual de Direito do Consumidor**. 10. ed. São Paulo: Atlas, 2010.

FLIPSIDE. **Caso C&A**: o que muda com a Lei Geral de Proteção de Dados? 03.09.2018. Disponível em: https://www.flipside.com.br/blog/2018/9/2/caso-cea-o-que-muda-com-a-lgpd. Acesso em: 15 Julho 2022.

FLUMIGNAN, Wévertton Gabriel Gomes; FLUMIGNAN, Silvano José Gomes. Princípios que regem o tratamento de dados no Brasil. Princípios que regem o tratamento de dados no Brasil. In: LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**: Lei nº 13.709/2018, com alteração da Lei nº 13.853/2019. São Paulo: Almedina, 2020. 123-141.

FORTES, Vinícius Borges. **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. Rio de Janeiro: Lumen Juris, 2016.

FRANCO, Benedito Luiz. **Proteção Constitucional do Sigilo da Fonte na Comunicação Jornalística**. São Paulo: Celso Bastos, 1999.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters, 2019.

GAMIZ, Mario Sergio de Freitas. **Privacidade e Intimidade**. Curitiba: Juruá Editora, 2012.

GIARLLARIELLI, Gustavo. Base legal do legítimo interesse – LGPD. **Jus.com.br**, 07.10.2021. Disponível em: https://jus.com.br/artigos/93546/base-legal-do-legitimo-interesse-lgpd. Acesso em: 15 Julho 2022.

GIONÉDIS, Louise Rainer Pereira; VIANNA, Maria Amélia Mastrorosa. **Lei Geral de Proteção de Dados (LGPD) e o *Compliance***. Curitiba: Juruá Editora, 2021.

GLOBO.COM. **Mônica Iozzi é condenada a pagar R$ 30 mil a ministro Gilmar Mendes.** 03.10.2016. Disponível em: http://g1.globo.com/distrito-federal/noticia/2016/10/monica-iozzi-e-condenada-pagar-r-30-mil-ministro-gilmar-mendes.html. Acesso em: 13 Julho 2022.

GRANERO, Arlete Eni; COUTO, Tatiane Cione. Consumo no ciberespaço: a explosão de aplicativos de dispositivos móveis que ajudam a controlar a vida na palma da mão. **Revista GEMInIS**, v. 4, n. 2, p. 89-105, Dez., 2013. Disponível em: https://www.revistageminis.ufscar.br/index.php/geminis/article/view/147. Acesso em: 15 Julho 2022.

GUIMARÃES, Maria Carolina Soares; NOVAES, Sylvia Caiuby. Autonomia Reduzida e Vulnerabilidade: Liberdade de decisão, diferença e desigualdade. **Revista Bioética**, 2009 Disponível em: http://revistabioetica.cfm.org.br/index.php/revista_bioetica/article/view/288. Acesso em: 15 Julho 2022.

HOFFMANN-RIEM, Wolgang. **Teoria geral do direito digital:** transformação digital: desafios para o direito. Rio de Janeiro: Forense, 2021.

JUSBRASIL. **Sexta Turma anula prova obtida pelo *WhatsApp Web* sem conhecimento do dono do celular**. 2018. Disponível em: https://stj.jusbrasil.com.br/noticias/653496663/sexta-turma-anula-prova-obtida-pelo-whatsapp-web-sem-conhecimento-do-dono-do-celular. Acesso em: 15 Julho 2022.

KANT, Immanuel. **Fundamentação da metafísica dos costumes**. Trad. Paulo Quintela. Lisboa: Edições 70, 1997.

LEAL, Luziane de Figueiredo Simão. **Crimes Contra os Direitos da Personalidade na Internet**. Curitiba: Juruá Editora, 2015.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LISBOA, Roberto Senise. **Confiança contratual**. São Paulo: Atlas, 2012.

LONGHI, João Victor Rozatti. **Processo Legislativo Interativo**. Curitiba: Juruá Editora, 2017.

LUFT, Mayumi Iguchi; POLLI, Fernando Gabbi. Sociedade de Informação, ambiente virtual e Código de Defesa do Consumidor: possibilidade de responsabilização das redes sociais em razão dos danos causados aos usuários através da ótica consumerista. **Revista Eletrônica do Curso de Direito da UFMS**. v.7, n.2, 2012. Disponível em: https://periodicos.ufsm.br/revistadireito/citationstylelanguage/get/apa?submissionId=7425&publicationId=5503. Acesso em: 16 Julho 2022.

MACHADO, André Luiz Sienkievicz. **As práticas de discriminação em razão de condição de saúde do trabalhador e o sistema jurídico para a concretização do direito fundamental a receber tratamento não discriminatório no mercado de trabalho**. 328f. 2019. Dissertação (Mestrado em Direito). Universidade de Fortaleza, Fortaleza, 2019.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 6. ed. São Paulo: Revista dos Tribunais, 2011.

MARTINS, Guilherme Magalhães. **Responsabilidade Civil por acidente de consumo na internet**. 2. ed. São Paulo: Revista dos Tribunais, 2014.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**. 2. ed. São Paulo: Saraiva Educação, 2018.

MEDEIROS, Amanda. **Os limites dos algoritmos para evitar a manipulação do comportamento do consumidor.** 22.11.2022. Disponível em: https://www.consumidormoderno.com.br/2022/11/22/algoritmos-manipulacao-comportamento-consumidor/. Acesso em: 14 março 2023.

MEIRELES Edilton. **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Thomson Reuters Brasil, 2020.

MÈLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019.

MELO, Caroline Dantas; DIAS, Clara Angélica Gonçalves. A refundamentação da responsabilidade civil através do princípio da prevenção. **REIDESE: Revista Eletrônica do Instituto Sergipano de Direito do Estado**, v. 03, p. 01-01, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, nov./dez. 2018.

MINAS GERAIS. Tribunal de Justiça de Minas Gerais. **AC 1.0471.16.012594-7/001**. Relatora: Desa. Juliana Campos Hora, 12ª Câmara Cível, Dje. 08/08/2019. Disponível em: http://www.idealsoftwares.com.br/ idealnewsjd/noticia.php?id=7937. Acesso em: 15 Julho 2022.

MIRAGEM, Bruno. A Lei Geral de Proteção de dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, v. 1009, Nov., 2019. Disponível em: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 15 Julho 2022.

MIZIARA, Raphael; PESSOA, André; MOLLICONE, Bianca. **Reflexos do LGPD no Direito e no Processo do Trabalho**. São Paulo: Revista dos Tribunais, 2020.

MONTEIRO, Carina Villela de Andrade. Direito à Privacidade versus Direito à Informação. **Revista de Informação Legislativa,** Brasília, n. 173, jan./mar., 2007.

MORAES, Alexandre de. **Direitos Humanos Fundamentais***:* Teoria Geral. 11. ed. São Paulo: Atlas, 2016.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa. **Cadernos Adenauer**, Rio de Janeiro, a. XX, p. 113-135, n. 3, 2019.

MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial Ltda., 2020.

NANNI, Giovanni Ettore. Evolução do direito civil obrigacional: concepção do direito civil constitucional e a transição da autonomia da vontade para autonomia privada. In: LOTUFO, Renan (Coord.). **Cadernos de autonomia privada**. Curitiba: Juruá, 2001.

NOVAIS, Jorge Reis. **As restrições aos direitos fundamentais não expressamente autorizadas pela constituição**. 2. ed. Coimbra: Coimbra Editora, 2010.

NUNES JUNIOR, Vidal Serrano. **Direito e jornalismo**. São Paulo: Verbatim, 2011.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de **Proteção de dados pessoais e sua repercussão no direito brasileiro**. São Paulo: Ed. RT, 2019, p. 566.

OLIVEIRA, José Roberto Pimenta. **Os Princípios da Razoabilidade e da Proporcionalidade no Direito Administrativo Brasileiro**. São Paulo: Malheiros, 2006.

PASQUALINI, Renata. **O devido processo legal e a liberdade de imprensa**. Porto Alegre: Sergio Antonio Fabris, 2009.

PEREIRA, Caio Mário da Silva. **Instituições do Direito Civil**. 30. ed. Rio de Janeiro: Forense, 2018. v. 3.

PILAU SOBRINHO, Liton Lanes; MIGUEL, A.E. O direito do consumidor como instrumento de cidadania em uma sociedade contemporânea altamente consumista. In: PILAU SOBRINHO, Liton Lanes; SILVA, Rogério. (Orgs.). **Balcão do Consumidor:** Diálogos Internacionais. Itajaí: Editora Univali, 2013, v. 1, p. 52-74.

PILAU SOBRINHO, Liton Lanes; PIAIA, Thami Covatto. Mudanças Institucionais e Cidadania: da participação social ao Marco Civil da Internet. **Revista Eletrônica de Direito e Política**. v. 10, p. 616-637, 2015.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2020.

PONTES, Sérgio. O que fala a Lei Geral de Proteção de Dados Pessoais. **JusBrasil**, 2018. Disponível em: https://sergiopontes.jusbrasil.com.br/artigos/614642198/o-que-fala-a-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 16 Julho 2022.

RIBEIRO, André Carvalho. **Proteção de Dados Pessoais e *Big Data***: coexistência possível? 2020. 184f. Dissertação (Mestrado - Direito da Sociedade da Informação) – São Paulo, Faculdades Metropolitanas Unidas, 2020.

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

RODRIGUES, Gustavo. **Rastrear e atrair**: armadilhagem, geolocalização e vulnerabilidades no aplicativo Grindr. 2018. Disponível em: file:///E:/TRABALHO/Mestrado/Direito%20Penal%20Econômico/Artigos%20para%0elaboração%20do%20artigo%20final/00.pdf. Acessado em: 12 de Julho de 2022.

RODRIGUES, Laura Secfém. A tutela jurídica dos dados pessoais. **Consultor Jurídico**, 03.10.2021. Disponível em: https://www.conjur.com.br/2021-out-03/laura-rodrigues-tutela-juridica-dados-pessoais. Acesso em: 14 Julho 2022.

ROSA, Jorge Chagas. **Abusividade contratual na era digital sob a ótica do Código de Defesa do Consumidor**: aspectos teóricos, práticos e reflexos da LGPD. Belo Horizonte: Dialética, 2021.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional.** São Paulo: Revista dos Tribunais, 2014.

SARMENTO, Daniel. A liberdade de Expressão e o problema do "Hate Speech". In: FARIAS, Cristiano Chaves de (Org.). **Leituras Complementares de Direito Civil**. Salvador: JusPodivm, 2009, p. 39-95.

SARMENTO, Daniel. Liberdade de expressão, pluralismo e o papel promocional do Estado. **Revista Diálogo Jurídico**. Salvador, n.16, mai.-ago., 2007. Disponível em: http://www.direitopublico.com.br. Acesso em: 15 Julho 2022.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Editora Atlas S.A., 2014.

SCHULMAN, Gabriel. A proteção do consumidor digital em face das redes sociais. **Consultor Jurídico,** 01.12.2021. Disponível em: https://www.conjur.com.br/2021-dez-01/garantias-consumo-protecao-consumidor-digital-face-redes-sociais. Acesso em: 14 março 2023.

SEABROOK, Jeremy. **The Leisure Society**. Oxford: Blackwell, 1988.

SILVA, Edson Ferreira da. **Direito à intimidade**: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de 2002. São Paulo: Juarez Soares, 2003.

SILVA, Lucas Gonçalves da; CERQUEIRA, E.C. Dimensão Jurídica da Liberdade de Imprensa a partir da noção instrumental da liberdade de expressão. In: ORSINI, Adriana Goulart de Sena; SANTIAGO, Mariana Ribeiro; FÉLIX, Ynes Da Silva (Org.). Teorias dos Direitos Fundamentais. Florianópolis: CONPEDI, 2015, v. 1, p. 1-22.

SILVA, Lucas Gonçalves da; COSTA, Ilton. **Direitos e garantias fundamentais II**. Florianópolis: CONPEDI, 2020. v. 1.

SILVA, Lucas Gonçalves da; CURY, Jacqueline Taís Menezes Paez. Proteção jurídica dos direitos à privacidade e à intimidade diante das novas tecnologias informáticas. **Relações Internacionais no Mundo Atual**, v. 3, p. 111-132, 2020.

SILVA, Lucas Gonçalves da; SIQUEIRA, Alessandra Cristina de Mendonça. A (Há) liberdade de expressãqo na sociedade em rede (?): Manipulação na era digital. **Relações Internacionais no Mundo Atual**, v. 2, p. 195-217, 2020.

SILVA, Lucas Gonçalves da; MELO, Brício Luís da Anunciação. A Lei Geral de Proteção de Dados como instrumento de concretização da autonomia em um mundo cada vez mais tecnológico. **Revista Jurídica Unicuritiba**, Curitiba. V.03, n.53 , p.354-377, Jul-Set. 2019, p. 357.

SILVA, Lucas Gonçalves da; CURY, Jaqueline Taís Menezes. Proteção Jurídica dos Direitos à Privacidade e à intimidade diante das novas tecnologias informáticas. **Relações Internacionais no Mundo Atual**, v. 3, p. 111-132, 2020.

SILVA, Lucas Gonçalves da; SANTOS, Carla V. P. N. Discurso do ódio no Estado Democrático do Direito: intolerância ou direito à liberdade de expressão? In: LINS JÚNIOR,

George Sarmento; BRITO FILHO, José Claudio Monteiro de; SILVA, Lucas Gonçalves da (Org.). **Direitos e garantias fundamentais I.** Florianópolis: CONPEDI, 2018, v. 1, p. 63-80.

SILVEIRA, Vinicius Loureiro da Mota. Ponderação e proporcionalidade no direito brasileiro. **Conteúdo Jurídico**, Brasília, 26.09.2020. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/34807/ponderacao-e-proporcionalidade-no-direito-brasileiro. Acesso em: 16 Julho 2022.

SILVEIRA JUNIOR, Hermano Marques da. **A Legitimidade Passiva dos Fornecedores do Serviço Rede Social nas Ações de Dano Moral Decorrentes do seu Ambiente Virtual**. 2011. Disponível em: http://www.forumjuridico.org/topic/13672-a-legitimidadepassiva-dos-fornecedores-doservico-rede-social-nas-acoes-de-dano-moraldecorrentes-do-seu-ambiente-virtual/. Acesso em: 16 Julho 2022.

SOLOVE, Daniel J; ROTENBERG, Marc; SCHWARTZ, Paul M. **Privacy, information, and technology**. New York: Aspen Publishers, 2006.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade de proteção de dados:** pluralismo jurídico e transparência em perspectiva. São Paulo: Revista dos Tribunais, 2019.

TAKANO, Camila Cardoso; SILVA, Lucas Gonçalves de. O constitucionalismo digital e as novas Tecnologias da Informação e Comunicação (TIC). **Revista de Direito, Governança e Novas Tecnologias**, v. 6, n. 1, p. 1-15, Jan.-Jun., 2020.

TEIXEIRA, Guilherme Carvalho. **O papel social da Lei Geral de Proteção de Dados**. 59 f. 2020. Trabalho de Conclusão de Curso (Curso de Graduação em Direito) – Araranguá, Universidade do Sul de Santa Catarina, 2020. Disponível em: https://1library.org/document/qvrv3w1y-o-papel-social-lei-geral-protecao-dados-bra sil.html. Acesso em: 16 Julho 2022.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados pessoais e sua repercussão no direito brasileiro**. São Paulo: Ed. RT, 2019, p. 300.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **Comentários ao GDPR**. São Paulo: Revista dos Tribunais, 2018.

VÉLIZ, Carissa. Entrevista. In: VELASCO, Irene Hernández. Falta de privacidade mata mais que terrorismo': o surpreendente alerta de professora de Oxford. **BBC News**, 16.10.2020. Disponível em: https://www.bbc.com/portuguese/geral-54558878. Acesso em: 15 Julho 2022.

WALDMAN, Ricardo Libel. A teoria dos princípios de Ronald Dworkin. **Direito e Democracia,** v. 2, n. 2, p. 425-477, 2001.

WALDMAN, Ricardo Libel; FUJITA, Maíra de Oliveira Lima Ruiz. A base legal do legítimo interesse na proteção de dados pessoais. In: LISBOA, Roberto Senise. **O Direito na Sociedade da Informação V**. São Paulo: Almedina, 2020.

ZANFIR-FORTUNA, Gabriela et al. Processing personal data on the basis of legitimate interests under the GDPR: practical cases. **Future of privacy Forum**, 2018. Disponível em: https://www.ejtn.eu/PageFiles/17861/Deciphering_Legitimate_Interests_Under_the_GDPR%20(1).pdf. Acesso em: 16 Julho 2022.