**FACULDADES INTEGRADAS DE PONTA PORÃ**
**FIP/MAGSUL**

DANIEL RODRIGUES DUTRA

# O IMPACTO DA CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

PONTA PORÃ

2020

DANIEL RODRIGUES DUTRA

# O IMPACTO DA CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Curso de Direito das Faculdades Integradas de Ponta Porã como requisito à obtenção do título de Bacharel em Direito.

Orientadora: Profª Ma. Carolina Lückemeyer Gregorio

PONTA PORÃ

2020

DANIEL RODRIGUES DUTRA

# O IMPACTO DA CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Curso de Direito das Faculdades Integradas de Ponta Porã como requisito à obtenção do título de Bacharel em Direito.

**BANCA EXAMINADORA**

_____

Orientadora: Profª Ma. Carolina Lückemeyer Gregorio
Faculdades Integradas de Ponta Porã

_____

Profº Examinador
Faculdades Integradas de Ponta Porã

_____

Profº Examinador
Faculdades Integradas de Ponta Porã

## AGRADECIMENTOS

Agradeço primeiramente a Deus, pois sem a sua graça não seria capaz de alcançar a conclusão deste trabalho.

Meu agradecimento a esta instituição por ter me proporcionado a estrutura necessária para que pudesse crescer academicamente e pessoalmente.

Toda a minha gratidão ao corpo docente e, em especial, a minha orientadora, Carolina Lückemeyer Gregorio, por todo incentivo e apoio. Sem sua ajuda e ensino nada disso seria possível.

À minha família e amigos, por serem meu pilar, estarem ao meu lado e me fazer acreditar que tinha a força e as ferramentas necessárias para finalizar este trabalho.

E, por fim, agradeço todas as pessoas que, de alguma forma, foram essenciais para que alcançasse este objetivo com o qual sempre sonhei.

"A injustiça em qualquer lugar é uma ameaça à justiça por toda parte”.

Martin Luther King.

DUTRA, Daniel Rodrigues. **O impacto da criação da lei geral de proteção de dados**. 50 folhas. Trabalho de Conclusão do Curso de Direito – Faculdades Integradas de Ponta Porã, Ponta Porã/MS, 2020.

## RESUMO

O presente trabalho tem por objetivo examinar o impacto da criação da lei geral de proteção de dados. Cada ano que passa percebe-se a influência da tecnologia em nossas vidas, trazendo diversos benefícios, por outro lado, no que diz a respeito à privacidade adquirimos insegurança e exposição indevida. Dessa forma, a pesquisa demonstra a importância de uma lei para regulamentar a proteção de dados. Assim, será realizado um breve conceito histórico sobre a proteção de dados; analisaremos a internet como um direito fundamental; e também o tratamento jurídico da resposta às violações e, por fim, responsabilização e prestação de contas. Para tanto, será utilizada a metodologia de caráter hipotético dedutivo, utilizando-se a pesquisa bibliográfica como uma fonte de observação teórica, com o intuito de possibilitar a compreensão deste instituto, bem como verificar as hipóteses de multas e sanções previstas na lei como forma de penalização para os entes que não se adequaram a LGPD.

**Palavras-chave:** Lei nº 13.709. Direito eletrônico. Multas. Sanções. LGPD.

DUTRA, Daniel Rodrigues. **The impact of creating the general data protection law**. 50 pages. Undergraduate thesis of the Law Course – Faculdades Integradas de Ponta Porã, Ponta Porã/MS, 2020 (em inglês).


## ABSTRACT

This research aims to examine the impact of the creation of the general data protection law. Each year that passes we notice the influence of technology in our lives, bringing several benefits, on the other hand, with regard to privacy, we acquire insecurity and undue exposure. Thus, the research demonstrates the importance of a law to regulate data protection. Thus, a brief historical concept on data protection will be carried out; we will analyze the internet as a fundamental right; and also the legal treatment of the response to violations and, finally, accountability and accountability. Therefore, the hypothetical deductive methodology will be used, using bibliographic research as a source of theoretical observation, in order to enable the understanding of this institute, as well as to verify the hypotheses of fines and sanctions provided for in the law as a way of penalty for entities that did not conform to LGPD.



**Keywords:** Law No. 13,709. Electronic law. Fines. Sanctions. LGPD.

**SUMÁRIO**

## INTRODUÇÃO

A Lei Geral de Proteção de Dados foi promulgada em 14 de agosto de 2018 entrando em vigor em agosto de 2020. Essa lei traz grandes mudanças e regula punições aos agentes de tratamento de dados que desrespeitaram os direitos dos indivíduos previstos na legislação.

Essa lei irá trazer de punições, advertências, multas simples, multas diárias, publicização da inflação até medidas mais extremas como suspensão do tratamento de dados pessoais por até seis meses, ou então, a proibição do exercício deste tratamento específico que venha lesando os direitos dos titulares.

Desta forma, o objetivo geral do trabalho é discutir sobre a Lei Geral de Proteção de Dados e analisar o impacto que ela causa nas empresas, órgãos públicos e também pessoas físicas. A pesquisa fará uso da pesquisa bibliográfica, por meio de revisão bibliográfica e documental, em livros, artigos, teses e sites disponíveis na internet sobre o tema do estudo.

Assim, a pesquisa irá se dividir em três capítulos. O primeiro capítulo apresentará os aspectos iniciais, conceituando diversos termos extremamente importantes para a presente pesquisa, tais como dados pessoais, internet, metadados, entre outros.

O segundo capítulo discute sobre os aspectos jurídicos da internet. É averiguada também a internet como um direito fundamental e a proteção aos dados sendo um direito fundamental e autônomo. Nesse capítulo também faz um panorama das leis europeias e das concebidas na América Latina.

O terceiro capítulo irá discorrer sobre o impacto da criação da lei geral de proteção de dados, suas possibilidades de aplicação, principais alterações, desafios tecnológicos e as formas de multas e sanções.

Por fim, no âmbito desta pesquisa, pretende-se entender a dinâmica da lei geral de proteção de dados, desde a questões de as boas práticas e da governança dispostas no artigo 50 da Lei n. 13.709/2018 que incluem uma série de atividades, desde conscientização, formulários até pontos de contatos para que os titulares possam requerer seus direitos até as punições previstas no capítulo VIII da lei acima descrita.

# 1 ASPECTOS INICIAIS ACERCA DA LEI DE PROTEÇÃO DE DADOS PESSOAIS

Para uma melhor análise do tema proposto é necessário explorar preliminarmente o seu histórico, bem como algumas definições e elencar alguns pontos relacionados à proteção de dados pessoais na internet. É essencial também aclarar que as definições serão feitas com a finalidade de se ater ao assunto específico, ou seja, serão apresentados sob o prisma da internet.

## 1.1. BREVE CONCEITO HISTÓRICO

É notório que hoje vive-se o período que procede a "pós-modernidade[1]", isto é, trata-se daquele que os mais antigos apenas vislumbravam em maravilhados filmes: com um clique se pode ver ao vivo o que se passa até mesmo do outro lado do globo, sendo possível conversar com os amigos, além de divulgar em diversas mídias sociais o cotidiano e as experiências.

E tudo isso tem uma apenas uma razão de existir: a internet. Assim, possibilita por meio de equipamentos tecnológicos facilidades antes inimagináveis. No entanto, com toda a revolução tecnológica vislumbra-se, por isto, uma sociedade diferente, a qual se move em torno de todas as informações que circulam.

Fritz Machlup foi pioneiro em constatar, já em 1962, o valor econômico da informação, em seu livro "The Production and Distribution of Knowledge in the United States", o qual gerou o termo "sociedade da informação". Nesse sentido, corrobora Sérgio Amadeu da Silveira (2017, p. 13):

> As sociedades informacionais são sociedades pós-industriais que tem a economia fortemente baseada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais. Também é possível constatar que as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de informação e de controle, as quais apresentam consequências sociais bem distintas das tecnologias analógicas, tipicamente industriais.

À vista disso, é inegável que o fator decisivo para o surgimento da sociedade da informação é o advento do computador. Emergindo assim a "economia do

[1] O conceito de pós-modernidade foi um termo difundido principalmente por três teóricos e escritores, quais sejam: Jean François Lyotard, Fredric Jameson e Jean Baudrillard.

imaterial", substituindo todas as variáveis centrais anteriores, isto é, o trabalho e o capital por informação e conhecimento (GONÇALVES, 2003, p. 28).

É necessário mencionar que o computador surgiu no cenário da Segunda Guerra Mundial (1939-1945), na Alemanha, Inglaterra e Estados Unidos, praticamente simultaneamente. Eram máquinas bem diferentes das atuais e o seu uso era restrito aos governos e a sua principal função era bélica (GUGIK, 2009).

Desde o início os avanços tecnológicos proporcionaram enormes desenvolvimentos, e o seu uso expandiu para os cidadãos comuns, ou seja, computadores pessoais, e as suas funções passaram a englobar diversas coisas, como a comunicação, a pesquisa, a educação o lazer e alguns serviços, encontrando-se hoje no que se denomina de a "quarta geração" (GUGIK, 2009).

Salienta-se que o principal resultado do computador e consequentemente da internet a globalização, além de ser notório a profunda mudança na dinâmica da vida em sociedade. Os governos, as empresas e os próprios cidadãos acabaram se ajustando à nova realidade.

Nessa nova conjuntura, o sociólogo CASTELLS (2003, p. 225) afirma que:

> A Galáxia Internet é um novo ambiente de comunicação. Como a comunicação é a essência da atividade humana, todos os domínios da vida social estão sendo modificados pelos usos disseminados da Internet, como este livro documentou. Uma nova forma social, a sociedade de rede, está se construindo em torno do planeta, embora sob uma diversidade de formas e com consideráveis diferenças em suas consequências para a vida das pessoas.

Ainda, ressalta (CASTELLS, 2016, p. 84 e 85):

> Gostaria de fazer uma distinção analítica entre as noções de "sociedade da informação" e "sociedade informacional" com consequências similares para a economia da informação e a economia informacional. O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo por exemplo, como comunicação de conhecimentos, foi crucial a todas as sociedades, inclusive à Europa medieval que era culturalmente estruturada e, até certo ponto, unificada pelo escolatiscismo, ou seja, no geral uma infraestrutura intelectual (ver Southern 1995). Ao contrário, o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornaram-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. Minha terminologia tenta estabelecer um paralelo com a distinção entre indústria e industrial. Uma sociedade industrial (conceito comum na tradição sociológica) não é apenas uma sociedade em que há indústrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas de

> atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana. Meu emprego dos termos “sociedade informacional” e “economia informacional” tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para nossas sociedades. Porém o conteúdo real de “sociedade informacional” tem de ser determinado pela observação e análise. É exatamente esse o objetivo deste livro. Por exemplo, uma das características principais da sociedade informacional é a lógica de sua estrutura básica em redes, o que explica o uso do conceito de “sociedade em redes” [...].

Portanto, é com atenção as características contemporâneas da sociedade mencionadas *alhures* que se deve lançar olhar ao estudo aqui proposto. Afinal, todas as facilidades tecnológicas e os novos meios de comunicação e relações sociais também trazem consigo as suas facetas nocivas.

## 1.2. CONCEITOS NECESSÁRIOS

Para uma melhor compreensão da magnitude da imprescindibilidade de proteção dos dados pessoais na internet é, por certo, imprescindível precisar as definições relativas aos dados pessoais. Qualquer indivíduo que utiliza a ferramenta internet, em seus mais diversos propósitos, há de deixar rastros e informações a seu respeito, e, portanto, seus dados pessoais.

Nesse tópico, discorrer-se-á os conceitos de dados pessoais e as suas respectivas espécies, bem como da internet e os conceitos decorrentes deste, quais sejam: os metadados, o seu tratamento, os *cookies*, *big data*, algoritmos e *bots*.

### 1.2.1 Conceito de Dados Pessoais

Os dados pessoais foram definidos no Regulamento 2016/679 da União Europeia (General Data Protection Regulation – GDPR) no artigo 4º, n. 1, que *in verbis* estipula:

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular; (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, p. 5)

Ressalta-se que apesar da já entrada em vigor da Lei nº 12.965/2014 denominada de Marco Civil da Internet, não há definição legislativa para os dados pessoais nas leis brasileiras.

Ainda, é importante apontar que há outras leis internacionais, em especial na Europa, que precisam o seu conceito, no entanto, com a eminente entrada em vigor, em 25/05/2018 do Regulamento 2016/679 da União Europeia e no intuito de não dar margem aos conceitos defasados, será adotada no trabalho a definição mais recente estipulada pela Lei Europeia de Regulamentação de Dados Pessoais.

Nesse sentido, os dados pessoais coletados podem referir-se a uma universalidade de informações, desde a dados cadastrais tais como o nome, endereço, e-mail, endereço de IP, a dados biométricos, saúde e de raça (LIMA, 2014).

No que tange as redes sociais, em especial Facebook, Twitter e Instagram, é evidente que se destacam como plataformas de coleta de dados, o que se dá por meio de testes, elaborados de forma atraente aos usuários, e que induzem os usuários a "aceitar", levando ao acesso de diversos dados como nome, idade, e-mail, e todas as fotos contidas no perfil do usuário (MENDONÇA, 2018).

A fim de desenvolver o seu conceito, convém indicar alguns tipos de dados pessoais, quais sejam: dados biométricos, dados genéticos, dados relativos à saúde, e dados sensíveis.

Conceitua a GDPR, em seu artigo 4º, n. 14, que dados biométricos são "resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;" (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, p. 34).

Nesse sentido, representam características únicas, em outras palavras, variam a depender da pessoa em questão, permanentes não variam no tempo, acessíveis e quantificáveis. E permitem, dessa forma, a identificação ou a autenticação do indivíduo (CASTRO, 2005).

Ensina CASTRO (2005, p. 83) que os dados biométricos podem ser segmentados em dois grupos, quais sejam: os relativos a características físicas e os dados relativos a características comportamentais. Do primeiro grupo cita-se de exemplo "a impressão digital, a geometria da mão e dedos, das veias da face, ou da orelha, a íris, a retina, o odor, a voz, ou o DNA enquanto o outro engloba a sua assinatura escrita, a forma como toca nas teclas ou na forma como fala".

Ainda consoante a lei mencionada, os dados genéticos são definidos em seu artigo 4º, n. 13, sendo “relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;” (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, p. 34).

Com o intuito de se ilustrar a questão, menciona CASTRO (2005, p. 94) “estes dados podem demonstrar, v.g., se duas pessoas são ou não da mesma família, podem revelar a presença ou ausência de uma característica num individuo, assim como a presença ou ausência do risco/probabilidade de doença”.

No tocante aos dados relativos à saúde, a Lei Europeia de Proteção de Dados Pessoais em seu artigo 4º, n. 15, os define como “dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;” (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, p. 34).

Adverte-se que os dados relativos à saúde não se restringem apenas ao diagnóstico médico, mas contemplam “todos aqueles que permitem apurá-lo, incluindo resultados de análises clínicas, imagens de exames radiológicos, imagens vídeo ou fotografias que sirvam o mesmo fim” (CASTRO, 2005, p. 91).

Por fim, ainda encontramos na Lei Europeia de Proteção de Dados Pessoais outra distinção acerca deles: a de dados sensíveis, na qual se reserva uma proteção especial. Apesar de não instituir uma definição propriamente dita do termo, a referida lei assevera em sua consideração n. 51:

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluirse neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma

> obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais. (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, p. 10).

A Diretiva 95/46 da União Europeia em seu artigo 8º, n. 1, com a finalidade de complementar o entendimento, estabelece que:

> Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e a vida sexual.

Nesse sentido, pode-se extrair que a particularização de alguns dados conferida pela lei se fez pela necessidade de uma maior proteção a esses, porquanto o seu tratamento e utilização podem implicar em riscos significativos para os direitos e liberdades fundamentais, conforme apregoa a própria GDPR em sua consideração n. 51.

Frisa-se que essa classificação especial, dados sensíveis, compreende inclusive os dados biométricos e os genéticos (MONTEIRO, 2018). Dessa forma, superada a compreensão acerca dos dados pessoais, passa-se a discorrer a respeito da internet e as concepções dela decorridas.

### 1.2.2 Conceito de internet

A Lei nº 12.965/2014, Marco Civil da Internet, a conceitua a internet em seu artigo 5º, I, como “o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

A Lei Europeia de Regulamentação de Dados Pessoais, não possui qualquer definição acerca da nomenclatura internet.

Porém, conforme aponta Victor Hugo Pereira (GONÇALVES, 2017, p. 2):

> [...] a melhor conceituação não seria internet, mas tecnologias de informação e comunicação. Internet é um nome localizado no espaço e tempo restritos que pode, dentro em breve, ser ultrapassado por outras nomenclaturas melhores e mais atualizadas. Já há em curso uma revolução de convergências de mídias de comunicação, o que coloca em dúvida a utilização do conceito de internet, que foi formulado na década de 1990.

Dito isso, é necessário mencionar que para Naughton (2000), a internet não surgiu em um momento claro e específico, sendo diversos os estágios e os agentes que impactaram a sua criação. Entretanto, “um ponto que marca o estopim certamente é aquele ocorrido em 4 de outubro de 1957, o dia em que a União Soviética lançou o primeiro satélite artificial da história da humanidade, o Sputnik” (NAUGHTON, 2000, p. 77), dando início à exploração espacial durante a Guerra Fria.

### 1.2.3 Conceito de Metadados

Os metadados tem origem do grego “meta”, que significa “além de”, ou seja, atualmente designam as informações que acrescem aos dados, e tem por finalidade auxiliar a utilização dos dados (SAFERNET, 2018). Sendo portanto, as “informações a respeito de outras informações” (NETO; MORAIS; 2014, p. 418).

A fim de aprofundar seu conceito, cita-se os esclarecimentos de CABRAL (2018, p. 26):

> Praticamente todos os dispositivos digitais geram metadados a partir do uso que fazemos. Por exemplo, ao tirar uma foto, além de gravar a foto na memória da foto, metadados são associados a esta foto descrevendo informações sobre o modelo da câmera, tipo de ISO, data, tamanho e formato do arquivo e até o local de onde a foto foi tirada se o aparelho tiver GPS. Ao fazer login em um site de redes sociais ou de compras várias informações são registradas além daquelas que escrevemos diretamente nos sites, como por exemplo, o endereço IP, o nome e versão do navegador, horário exato de entrada e saída, bem como outros detalhes sobre os seus cliques durante aquela navegação. Os tipos mais comuns de metadados são: - Número de telefones, endereços de email e os nomes das pessoas que usam serviços; - Dados de Localização: onde está o seu telefone celular; - Data e hora em que foram feitas as ligações, emails, arquivos e fotos; - Informações do aparelho que você está usando.

Para melhor ilustrar suas implicações, cita-se o programa de computador “Immersion”, desenvolvido pelo físico César Hidalgo, pesquisador do Massachussetts Institute of Technology (MIT), em conjunto com seus parceiros, que após a permissão do usuário para acessar a sua conta do e-mail gera diversos gráficos interativos, ou

seja, evidenciando os períodos e quais relações sociais o mesmo possui, e até mesmo as pessoas que se comunicou ou se comunica. Apesar do software não ter acesso ao conteúdo das mensagens, ele tem o potencial de constatar as questões de extrema intimidade, como no caso de “sua namorada não gostar do grupo de amigos formado durante o seu relacionamento anterior, e o faz a partir de apenas informações como destinatário do e-mail, para quem ele foi enviado, quem está copiado e dados relativos ao horário do envio”. E o próprio pesquisador alerta que o uso de metadados pode implicar em uma violação à privacidade (CABRAL, 2018).

Além disso, devido ao seu extenso alcance, os metadados está por toda a internet e em dispositivos digitais, é necessário atenção quando se alia metadados à possível perspectiva de propósitos administrativos, comerciais e políticos sem a devida cautela.

### 1.2.4 Tratamentos

Com o fenômeno da “Dossier Society”, em que a informática concedeu poder às informações e os bancos de dados conquistaram valor de mercado, não tendo como não se debater também os tratamentos concebidos a esses últimos (WENDLING, 2018).

O conceito de tratamento adotado nesse estudo será o mesmo definido na Lei Europeia de Proteção de Dados Pessoais em seu artigo 4º, n. 2. Veja-se:

> «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição; (JORNAL OFICIAL DA UNIÃO EUROPEIA, 2016, p. 33).

Ainda, a fim de complementar o entendimento CASTRO (2005, p. 187) aduz:

> Os tratamentos de dados pessoais pelos serviços públicos podem revestir um caráter muito diverso: do simples tratamento dos dados nome, morada e instituição a que alguém pertence, para efeitos de envio de convites ou para outros contactos, até ao tratamento de dados sensíveis como os dados de saúde, v.g., no caso dos estabelecimentos de saúde públicos, ou os dados relativos a condições socioeconômicas, v.g., por parte de organismos com

> funções sociais, etc, são hoje várias as possibilidades, graças à quase infinita capacidade de armazenamento de informações dos computadores e às suas faculdades de cruzamento e pesquisa de informação.

Por fim, esclarece-se que o Marco Civil Brasileiro da Internet não trouxe nenhuma definição específica a espeito da nomenclatura.

### 1.2.5 Cookies

Para esse estudo usaremos o conceito de cookies apresentado por Victor Gameiro (DRUMMOND, 2003, p. 98), que assim o define:

> Os cookies são pequenos programas colocados no computador do usuário sem a sua permissão durante uma navegação no ambiente da Internet. Em verdade, sem sequer seu conhecimento, visto que nenhum indicativo irá suceder-se na tela do computador que possa vir a evidenciar a sorrateira entrada daqueles programas de computador. Estes pequenos programas ficam armazenados, assim, no próprio computador do usuário.

Portanto, seu principal intuito é de colaborar a próxima utilização do usuário em um mesmo sítio cibernético. Esclarece-se ainda que essa ferramenta é utilizada para traçar o perfil do usuário, e assim, oferecer produtos de acordo (DRUMMOND, 2003, p. 100).

Observa-se que se trata de uma forma de coleta, possível armazenamento e tratamento de dados pessoais dos sujeitos que utilizam a internet. Uma das inúmeras maneiras de se usurpar de dados pessoais sem o devido consentimento do seu titular e mais uma para demonstrar o quanto os nossos dados pessoais são negligenciados e sua falta de proteção necessária.

### 1.2.6 Big Data

Apesar de não haver consenso entre os estudiosos da área a respeito do que se trata o *Big Data*, usar-se-á o conceito definido no relatório *Big Data* no projeto Sul

Global, Relatório sobre estudos, elaborado pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro. Veja-se:

> [...] é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores.

Ressalta-se que o termo "comporta diversas interpretações e variados significados, principalmente por ser utilizada por diversos setores, como especialistas em tecnologia, juristas e autoridades públicas" (GOMES, 2018, p. 233).

Esclarece-se também que para uma definição mais apropriada seria necessário um estudo complexo, ainda mais levando em conta que o termo envolve vários conceitos técnicos da Ciência da Informação e dedicação voltada às diversificadas áreas de uso, o que não é a proposta do trabalho.

Prosseguindo em seu conceito, percebe-se que o *big data* manifesta três atributos, denominados "3 V's", quais sejam:

> (i) volume – a sociedade atual é altamente conectada e tecnológica, todos os dias milhões de transações e comunicações são realizadas online, seja troca de e-mails, mensagens por comunicadores instantâneos, fotos, vídeos, digitalização de documentos, cadastros; (ii) velocidade – esses dados são criados de forma acelerada e praticamente instantânea, portanto, atualizadas; e (iii) variedade – os dados coletados são aleatórios, variados e advém das mais diversas ferramentas – mídias sociais, celular, gps, sistemas integrados etc (MCAFFE; BRYONJOELFSSON; apud SANTOS, 2018, p. 11).

Nesse mesmo sentido, pode-se afirmar que "o acúmulo de conhecimento e informação, que um dia significou estudar, conhecer e compreender o passado, está se transformando, significando, com o *big data*, a habilidade de prever o futuro" (MAYER-SCHONBERGER, Viktor; CUKIER, 2013, p. 190 apud GOMES, 2018, p. 236).

Portanto, após a elucidação desses apontamentos, é clara a importância do *Big Data* para os estudos e para o manuseio dos dados pessoais colhidos na internet. E, nesse sentido da complexa dinâmica da internet e das suas ferramentas, tecnologias e sua interação com os dados pessoais, frisa-se a primordialidade de voltar-se conjuntamente sobre todos os conceitos abordados nesse tópico para a plena compreensão de seu mecanismo.

### 1.2.7 *Bots*

Como pode-se perceber, a rede na atualidade é cheia de ferramentas, mecanismos e fenômenos que comprovam manipulações, disparidades entre os sujeitos, ou seja, usuário, provedor e a plataforma utilizada, sendo imprescindível a regulação para essas relações.

Outra ferramenta que vem sendo usada cada vez mais são os *bots*, em abreviação para robôs. E nada mais é do que alguns programas utilizados com objetivos específicos.

> [...] são programas de computador criados para executar tarefas específicas. Os primeiros robôs não tinham intenções maliciosas, e ainda hoje existem os bons bots, que têm como propósito exigir prestação de contas de políticos, viralizar causas para a igualdade de gênero ou ajudar a organizar as (muitas) tarefas diárias de seus usuários. Mas no final da década de 1990, os bots começaram a desenvolver uma reputação negativa. Alguns têm sido usados no envio de SPAMs por e-mail, no roubo de dados pessoais de usuários, em fraudes de cartão de crédito e em ataques de desinformação para manipulação da esfera pública. Esses bots têm como objetivo espalhar mentiras para influenciar narrativas, um fenômeno que desde 2014 vem ganhando escala global. E pior: eles estão por aí e quase ninguém sabe como funcionam, quem os desenvolve e por quem são financiados. (ITSRIO, 2018, p. 2)

Destaca-se que o seu uso é abundante em campanhas políticas. Nas redes sociais ele pode “seguir pessoas, postar e direcionar mensagens, inserir links ou hashtags. Eles muitas vezes servem para multiplicar as informações distribuídas na rede, passando-se por contas de pessoas reais” (ITAGIBA, 2017, p. 3).

E ainda, “com a evolução da inteligência artificial, bots terão a habilidade de mimetizar o comportamento humano de forma quase perfeita, o que dificulta o processo de checagem de fatos” (ITAGIBA, 2017, p. 4).

## 2 ASPECTOS JURÍDICOS DA INTERNET

Com o advento da internet, foram verificadas diversas mudanças em todos os âmbitos da sociedade, não apenas da sociedade brasileira, mas mundial. Os provedores de pesquisa começaram a existir, facilitando a busca por sites de conteúdo educacional e modificando o processo de aprendizado dos estudantes que buscavam

informação, não era mais preciso ir até uma biblioteca e ficar horas tentando localizar algum trecho específico de um livro, bastavam apenas alguns minutos de pesquisa utilizando as palavras-chave relacionadas ao tema. Houve assim também mudanças nos sistemas bancários, com a possibilidade de pagamentos online e até mesmo contas inteiramente digitais, o mercado de jogos eletrônicos, que já vinha em ascensão, não tendo tardado em obter um faturamento maior do que a consolidada Hollywood; as redes sociais surgiram, trazendo consigo um engajamento entre os usuários de forma a propagar inúmeros tipos de conteúdo e promovendo a socialização digital em um processo de globalização interno e externo.

O crescimento da internet aconteceu de forma significativa e em um período muito curto de tempo. Seu aspecto neutro, caótico e desvinculado de qualquer regulação estatal assustou, de certa forma, o direito. Neste mesmo teor, da globalização decorrente do surgimento da internet e das mudanças sociais trazidas pela mesma, o direito vem, incessantemente, se adaptando e encontrando as melhores formas de enfrentar as novas demandas e fatos jurídicos advindos dessa revolução tecnológica.

## 2.1 A INTERNET COMO DIREITO FUNDAMENTAL

Segundo o especializado site Internet World Stats, em pesquisa realizada em 30 de junho de 2018, mais de cerca de 4 bilhões de pessoas têm acesso a internet ao redor do mundo. A ferramenta que tem por finalidade de comunicação e principalmente sendo um meio para o acesso à informação, a internet começou a se tornar cada vez mais essencial para a vida humana, e, recentemente, sendo declarada pela ONU (2016) como um direito humano, inclusive advertindo as nações acerca da pertinência do acesso universal a ela.

Quanto aos direitos fundamentais, Luiz Alberto David Araújo e Vidal Serrano Nunes Júnior (2005, p. 109) esclarece:

> Os direitos fundamentais podem ser conceituados como a categoria jurídica instituída com a finalidade de proteger a dignidade humana em todas as dimensões. Por isso, tal qual o ser humano, tem natureza polifacética, buscando resguardar o homem na sua liberdade (direitos individuais), nas suas necessidades (direitos sociais, econômicos e culturais) e na sua preservação (direitos relacionados à fraternidade e à solidariedade).

Dessa maneira, apenas pela classificação supra, se nota que a rede mundial de computadores interligados abrange diversos aspectos dos direitos fundamentais, em especial supera as barreiras das diferentes gerações de direitos, as quais, pode-se exemplificar com a liberdade de expressão, o direito à informação e o direito à privacidade.

Nessa mesma linha, estava tramitando o Projeto de Emenda à Constituição 479/2010, proposta que “acrescenta o inciso LXXIX ao artigo 5º da Constituição Federal, para incluir o acesso à internet em alta velocidade entre os direitos fundamentais do cidadão" (BRASIL, 2010).

Ademais, conquanto o prejuízo social que pode trazer a disseminação de informações falsas em uma eleição presidencial, como verificado no ano de 2018, é de suma importância que seja garantida a liberdade de expressão online não apenas como um direito fundamental, mas como uma ferramenta democrática, afinal é de fácil percepção que países que possuem um acesso restrito ao mundo digital seguem uma forma de governo ditatorial ou com elementos poucos democráticos, como Cuba, China, Coréia do Norte, entre outros.

Assim, como é importante mencionar que atualmente a internet não é apenas uma ferramenta voltada para o lazer, ainda mais com as consequências da pandemia de COVID-19 que sujeitaram todos os alunos brasileiros a se adequarem as aulas online.

## 2.2 PROTEÇÃO AOS DADOS: UM DIREITO FUNDAMENTAL E AUTONÔMO

No âmbito jurídico há inúmeros institutos e princípios que se propõem a proteger aspectos e direitos da vida do cidadão. Dessa maneira, os direitos que originaram a proteção aos dados pessoais foram o direito à vida privada e o direito à intimidade.

Dessa forma, a teoria dos direitos da personalidade surgiu nos países de língua germânica, “a qual se baseava na ideia de um direito subjetivo além dos direitos reais e pessoais” (GIACCHETTA; MENEGUETTI, 2014, p. 377).

Ressalva-se que muitos autores distinguem o direito à intimidade do direito à vida privada, ambos relacionados a uma noção de privacidade, direito à privacidade, no sentido mais geral. A fim de se aclarar a questão, destaca-se alguns entendimentos acerca da definição de intimidade, quais sejam: “a esfera secreta do indivíduo na qual este tem o poder legal de evitar os demais” (DOTTI, 1980, p. 69).

“Modo de ser de determinado indivíduo, consistindo fundamentalmente na exclusão do conhecimento pelos demais daquilo que somente a ele diz respeito” (FARIAS, 1996, p. 104). “A esfera mais secreta da vida de cada um” (MOTTA; BARCHET, 2007, p. 180).

Já o jurista brasileiro José Afonso da Silva (2005, p. 206) prefere utilizar a expressão direito à privacidade, “num sentido amplo e genérico, de modo a abarcar todas as manifestações de esfera íntima, privada e da personalidade”.

Desse modo, devido as diferentes posições acerca da diferenciação entre o direito à vida privada e o direito à intimidade, esclarece-se que adotaremos a visão mais ampla, referindo-se de maneira geral por direito à privacidade. Além disso, referidas distinções não prejudicam o tema específico, isto é, a proteção devida aos dados pessoais dentro da internet.

Assim, verifica-se que a Carta de Direitos Fundamentais da União Europeia, promulgada em 2000, culminou em uma verdadeira divisão do direito à privacidade e da proteção de dados pessoais, em especial ao conhecer este último como um direito autônomo (RODOTÀ, 2008).

> Suas diferenças estão esculpidas principalmente porquanto a proteção à vida privada embasa-se numa proteção estática e negativa, caracterizada pela objeção em se interferir na vida privada e familiar de um singular, enquanto que a proteção de dados pessoais é mais ativa, regra os instrumentos de processamento de dados e designa legitimidade para os atores necessários a fim de se cumprir as medidas de proteção (RODOTÀ, 2008, p. 17).

Á vista disso, foi assentada nessas circunstâncias favoráveis à “autonomia do indivíduo na sociedade de informação, [que] uma decisão histórica da Corte Constitucional Alemã de 1983 reconheceu a autodeterminação informativa” (RODOTÁ, 2008, p. 15).

Ademais, no contexto atual, verifica-se presente, em relação à proteção de dados pessoais, interesses contrapostos, ou seja, por um lado, há a proteção da vida

privada dos indivíduos e por outro, questões relativas à segurança interna e internacional, reorganização da administração pública e interesses de mercado (RODOTÀ, 2008).

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso de dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". (RODOTÀ, 2008, p. 37)

Nesse contexto, o autor defende também a proteção coletiva dos dados coletados, para o qual prescreve (RODOTÀ, 2008, p. 50):

> [...] um alargamento da perspectiva institucional, superando a lógica puramente proprietária e integrando os controles individuais com aqueles coletivos; diferenciando a disciplina de acordo com as funções para as quais são destinadas as informações coletadas; analisando com maior profundidade os interesses envolvidos nas diversas operações e colocando em funcionamento novos critérios para o equilíbrio de tais interesses. Em síntese: a proteção de dados pessoais não pode mais se referir a algum aspecto especial, mesmo que seja em si muito relevante, porém requer que sejam postas em operações estratégias integradas, capazes de regular a circulação de informações em seu conjunto.

CASTRO (2005), ao observar a Convenção do Conselho da Europa, 28 de janeiro de 1981, e a Recomendação da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), 23 de setembro de 1980, elencou alguns princípios em comum no trato dos dados pessoais, quais sejam:

> 1. princípio da correção na coleta e no tratamento das informações; 2. princípio da exatidão dos dados coletados, acompanhado pela obrigação da atualização; 3. princípio da finalidade da coleta de dados, que deve poder ser conhecida antes que ocorra a coleta, e que se específica na relação entre os dados colhidos e a finalidade perseguida (princípio da pertinência); na relação entre a finalidade da coleta e a utilização dos dados (princípio da utilização não-abusiva); na eliminação, ou na transformação em dados anônimos das informações que são mais necessárias (princípio do direito do esquecimento); 4. princípio da publicidade dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público; 5. princípio do acesso individual, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente; 6. princípio da segurança física e lógica da coletânea de dados. (CASTRO, 2005, p. 229)

O autor ao analisar demais legislações estipulou outras características necessárias a fim de proteger os dados pessoais, das quais se citam algumas (CASTRO, 2005, p. 230):

> 1.a previsão de colocar à disposição dos usuários não somente instrumentos jurídicos, mas também meios técnicos de controle direto. [...] 2. extensão da obrigação de pedir o consentimento dos interessados não apenas para a coleta de dados que lhe digam respeito, mas também para utilização especificas destes [...]. 4. proibição de compartilhar os dados coletados com terceiros [...].

Nessa toada, cita-se que Catarina Sarmento aponta os princípios da finalidade e da transparência como fundamentais no tratamento de dados pessoais. “E quanto aos relativos às qualidades dos dados pessoais cita os princípios da licitude e lealdade; e os princípios da exatidão e atualização dos dados” (2005, p. 237).

Em relação aos direitos dos titulares dos dados assegura os direitos ao esquecimento, assim como à curiosidade, à informação, ao acesso, de retificação e atualização, do apagamento ou bloqueio dos dados, e o de oposição.

A fim de se desenvolver suas implicações, tem-se que o princípio geral da transparência. Veja-se:

> [...] implica que o responsável de um tratamento de dados, devidamente identificado, deve dar a conhecer ao titular dos dados a realização do tratamento que lhe respeite, indicando, nomeadamente, os seus fins, categorias de dados tratados, período de conservação dos dados, eventuais comunicações dos mesmos, etc. (CASTRO, 2005, p. 229)

Dessa forma, conclui-se que a preocupação com as possibilidades infinitas de combinações de dados pessoais dos usuários, associadas a poderosas habilidades de pesquisa e a impressionantes habilidade de armazenamento, todas potenciadas pelo uso da informática, “levaram a construção deste direito, que foi sendo acolhido como um novo direito fundamental” (CASTRO, 2005, p. 29).

## 2.3 O TRATAMENTO JURÍDICO DA RESPOSTA ÀS VIOLAÇÕES

Como visto *alhures* é evidente a necessidade de uma maior regulamentação a fim de resguardar os usuários de passiveis abusos. Assim, uma legislação bem detalhada e protetiva, principalmente se houver prenúncio de alguma penalidade

quando não contemplada tende a ser um meio efetivo de resposta às possíveis violações.

Destarte, a doutrina inclusive aponta alguns princípios que precisam ser mencionados, que vem se desenvolvendo e consolidando desde as primeiras gerações de leis de proteção de dados e para a privacidade e que se encontram inerentemente ligados aos direitos fundamentais, e que se averiguam presentes nas normas paradigmáticas a serem comentadas no presente capítulo (DONEDA, 2011). Sendo eles:

> a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos; b) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade; c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade); d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos; e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. (DONEDA, 2011, p. 100)

Desse modo, a proteção aos dados é indispensável para a segurança dos direitos humanos, das liberdades, e, portanto, que a tendência internacional, em especial na legislação europeia, tem sido conceber mecanismos próprios de proteção a fim de garantir estes direitos conforme as necessidades novas da vida contemporânea.

Diante disto, esse tópico explorará alguns formatos de leis internacionais de proteção de dados.

### 2.3.1 Diretiva Europeia 45/96/CE

Esta diretiva foi extremamente importância para salvaguarda da privacidade nos Estado-Membros europeus. Pois, ela comprova a proteção aos dados como uma forma de defesa dos direitos fundamentais e conduzia a criação de leis que englobassem tanto o setor privado quanto o público, e por sua vez acabou influenciando diversos outros países, tal qual o Canadá e a Austrália na criação de suas próprias bases legais (DONEDA, 2011).

Em seguida também editaram as seguintes diretivas, de modo a ampliar a regulamentação quanto aos dados para alguns setores mais específicos, sendo elas: a Diretiva 97/66/CE9, 1997, cujo foco é justamente o tratamento dos dados pessoais e a defesa da privacidade no setor das telecomunicações; e a Diretiva 2002/58/CE10, 2002, que alude sobre o tratamento de dados pessoais e à proteção da privacidade nas comunicações que são eletrônicas.

> A legislação em tela foi um dos mais significativos avanços em matéria de proteção dos dados pessoais, e consequentemente da privacidade dos cidadãos que ela contempla, conforme já mencionado anteriormente ao analisar a evolução histórica destas leis no primeiro capítulo. Esta e outras leis serviram para formar as bases do que hoje vem sido chamado pela doutrina como um verdadeiro direito fundamental à proteção de dados. (MENDES, 2010, p. 134)

Desse modo, de uma norma geral a diretiva se referia a proteção das pessoas singulares, ainda mais no que diz respeito ao tratamento de dados pessoais e à sua livre circulação. Assim, a sua finalidade era justamente a harmonia entre o seu texto e as outras normas setoriais de proteção que complementassem a norma mais completa, com a finalidade de incluir os setores mais específicos, sendo notável pela razão da construção de uma arquitetura regulatória.

Assim, nas constituições dos países europeus após a ela, muitas já acrescentaram em seu texto todas as previsões quanto a este gênero de informação, como a dos Países Baixos, Suíça, Grécia e Espanha. Salienta que a Carta Magna de Portugal consagrou inclusive a proteção das informações pessoais face às ameaças provocadas pelo uso da informática, criando assim um inovador rol de direitos fundamentais intrinsecamente ligados à proteção da dignidade da pessoa humana.

Verifica que esta diretiva dispõe de dois relevantes enfoques (MENDONÇA, 2016). Por um lado, pretende amparar as pessoas físicas ao indicar as normas de

proteção quanto ao seu tratamento de dados e, ademais, também pretende compelir o comércio, criando regras comuns, e harmoniza as abordagens legais, à vista disso contribuiu para o sistema de mercado unificado da União Europeia, reduzindo os custos das transações eventualmente.

> A norma em questão aplica-se ao tratamento de dados pessoais, sendo feito de forma automatizada ou não quando contidos em um ficheiro, um conjunto estruturado de dados, ou a ele destinados tendo em vista que o risco de danos aos direitos da personalidade não está na informatização em si, mas sim na potencialidade de obtenção de informações dos titulares dos dados a partir do tratamento deles. De fato, a automatização possibilita uma organização muito maior dos dados, realizando seu cruzamento a fim de obter ainda mais informações relevantes, no entanto, tal resultado pode ser obtido também sem o uso de recursos tecnológicos tão avançados. A mera organização e análise de cadastros e registros de compras de forma não automatizada pode render os mesmos resultados, porém em escala menor, mas ainda assim gerando consequências na vida dos indivíduos analisados. (MENDONÇA, 2016, p. 299)

Dessa forma, percebe que esse documento foi um marco legal de relevância quanto a proteção de dados nos últimos anos. Porém, a sociedade evoluiu desde então, devido aos inúmeros avanços tecnológicos, e com isto a abordagem legal renovou-se para manter-se eficiente. Assim sendo, foi editado em 2016 o Regulamento Geral Sobre a Proteção de Dados, o qual passa-se a elucidar.

### 2.3.2 Regulamento (UE) 2016/679 – O Regulamento Geral Sobre a Proteção de Dados (RGPD)

Esta nova regulamentação foi feita para suceder a Diretiva Europeia 45/96/CE, adequando a legislação quanto à sua proteção aos dados pessoais pela Europa. Portanto, é uma atualização, ainda levando em conta que muito mudou desde a edição da diretriz editada na década de 90, ou seja, tanto a tecnologia quanto as formas de relacionamento entre as pessoas e ainda as táticas de mercado tiveram uma profunda mudança.

O principal objetivo da norma é obter maior controle aos cidadãos europeus no que tange ao tratamento de seus dados quando relacionados às ofertas de bens, de serviços e até mesmo no que se refere ao controle de seu comportamento, tanto com relação a empresas europeias e até mesmo as estrangeiras, unificando e simplificando as normas, modernizando os princípios já consagrados na Diretiva Europeia 45/96/CE.

Tendo sido promulgado em 2016, o regulamento concedeu às empresas o prazo de até 2 (dois) anos para se adequarem às exigências novas, passando assim a surtir os seus efeitos plenamente em 2018. Além disso, esse novo regulamento influenciou principalmente as empresas que cuidam e tratam dos dados pessoais de europeus, estando elas na União Europeia ou em outro país, e de pessoas localizadas na União Europeia, sendo está última uma de suas maiores novidades, isto é, a extraterritorialidade.

Este regulamento moderniza ao incluir definições quanto as proteções aos dados genéticos e aos biométricos, traz também consigo uma série de direitos, contidos no Capítulo III, para os titulares dos dados.

Ainda há o direito à definição do tratamento permitido, e ainda inova ao permitir que o titular limite o uso de seus dados em algumas situações que são especificadas em lei. Quanto a obrigação de notificação, essa faz-se necessárias por parte do responsável do tratamento, aos terceiros que sejam destinatários dos dados caso os seus supostos dados tenham sido retificados, limitados ou apagados, com a finalidade de que estes também estejam alinhados com a política instituída e com a informação atualizada.

> Além disto, passa a haver uma diretriz a ser seguida em caso de violação de dados pessoais. Caso isto ocorra, por razões internas ou por fato de terceiro, o responsável pelo tratamento deverá notificar o ocorrido à autoridade de controle competente em até 72 horas após ter tido conhecimento da violação, devendo a notificação vir acompanhada dos motivos do atraso se o prazo determinado for excedido, é a inteligência do art. 33 do regulamento. Além disto, quando tal violação representar elevado risco aos direitos e liberdade do titular dos dados, este deverá ser notificado. A instituição de tal obrigatoriedade mostra-se necessária pois, por vezes, havendo uma falha na segurança e sem a necessidade de prestação de contas, muitas empresas preferiam não divulgar informação a fim de se resguardar, tendo em vista o abalo na confiança que isto poderia gerar e com isto os eventuais efeitos no mercado, assim pondo em risco a privacidade dos titulares dos dados para manter sua imagem. (MENDES, 2010, p. 135)

Isto posto, o RGPD demonstra ser uma norma extensa, que busca uma harmonia com as outras leis elaboradas anteriormente pelos estados membros com o intuito de se adequar melhor às suas especificidades e regular os setores específicos. O regulamento vem para conduzir e tende inclusive a influenciar outros países, tal qual a Diretiva Europeia 45/96/CE, nas elaborações e atualizações de suas normas próprias.

Além disto, dado o aspecto da extraterritorialidade, as empresas que possuem a intenção de continuar negociando bens e serviços com os europeus devem reformular-se para estar em conformidade com as novas regras, e pouco antes da entrada em vigor dessa norma muitas companhias já estão começando a notificar os usuários das alterações nas suas políticas de privacidade, o que acaba afetando os usuários de fora da união europeia que utilizam dos mesmos serviços, demonstrando assim que desde logo a norma já está tendo um perceptível impacto.

### 2.2.3 Modelo de regulação dos Estados Unidos da América

Os Estados Unidos possuem diversas leis sobre a privacidade e a segurança da informação por todo o seu território nacional, podendo até mesmo bem diferentes entre si. Nesse contexto, com o grande aumento da relevância da informação, e a inevitabilidade de se resguardar a privacidade, os EUA, através de diversas construções legislativas e jurisprudências originou um novo conceito de "*informational privacy*", cujo objetivo é a proteção ao direito de acesso à informação, ainda mais quanto aos dados armazenados em órgãos públicos e a sua disciplina de proteção ao crédito, conferindo uma maior segurança ao consumidor (DONEDA, 2011).

Percebe-se então que modelo de proteção de dados norte-americano é estruturalmente diverso do europeu. "No modelo americano o processamento de dados é permitido, favorecendo o livre mercado, a não ser que isto cause algum dano ou que seja expressamente limitado pela lei americana" (MELTZER, 2015, p. 90). Na União Europeia o que ocorre é justamente o oposto, a regulação do tratamento de dados é extremamente detalhada, prevendo todas as hipóteses em que ele é permitido e ainda como deve ser feito.

> Diferentemente do panorama europeu, não há uma lei maior que sirva como diretriz para as normas setoriais. Há, porém, duas leis básicas quanto à política interna, o Fair Credit Reporting Act, de 1970, e o Privacy Act, de 1974. A primeira aplica-se à emissão de relatórios sobre os consumidores, para fins de análise de perfis quanto ao risco de crédito, seguros e contratação de empregados. Já a segunda trata das empresas ou agências governamentais que administram um sistema de registro para o governo. (MELTZER, 2015, p. 95)

No que tange à política externa, à frente das diferenças entre os Estados Unidos e a União Europeia, contudo, tendo em vista que o defluxo internacional dos

dados entre os dois era essencial algumas modificações para as relações comerciais, portanto, eles negociaram o *Safe Harbor Agreement of 2000* que, de forma resumida, “deveria proteger os dados de cidadãos europeus se estes fossem guardados por companhias americanas para serem tratados nos EUA”. Entretanto, o acordo foi em 2015 anulado pela União Europeia, dessa maneira, o Tribunal de Justiça da União Europeia reconheceu que o acordo não alcançava os padrões de proteção de dados da União Europeia. Com isto, muitas empresas que estavam sob a amparo desse acordo tive que implementar outras medidas alternativas. Criando assim certa insegurança jurídica (WEISS, 2018, p. 134).

Em 2016, em resposta à essa situação, o acordo foi revisto, dando origem assim ao *Privacy Shield*, que foi concebido através da influência do RGPD e é mais longo e detalhado que seu antecessor. Assim, essa legislação contém uma série de princípios relativos às transações comerciais e em especial aos dados sensíveis e reformulou quanto ao papel das autoridades responsáveis pela proteção dos dados. Portanto, as empresas americanas que possuem o objetivo de trabalhar com os dados de cidadãos europeus comprometem a estar em conformidade com este padrão estabelecido.

WEISS (2018, p. 134) aduz:

> Os EUA têm uma forte regulamentação quanto à privacidade dos dados para o setor público. O Privacy Act de 1974, seria um exemplo de legislação aplicável somente à esfera federal, e ainda sim tendo sua abrangência limitada, conforme leciona Colin Bennett.65 O setor privado, por outro lado, apenas agora tem sido alvo de maior atenção, especialmente após o escândalo do tratamento desvirtuado dos dados do Facebook pela empresa Cambridge Analytica. Dada a forte base liberal norte-americana, no entanto, a intervenção do estado tende a ser mínima, mesmo com o icônico caso, as previsões são de que as providências tomadas pelo governo americano não sejam extensivas como na União Europeia.

No entanto, os Estados Unidos, com o seu sistema federalista e com o posicionamento liberal, preferiram tutelar alguns setores em vez de criar um único regulamento como no modelo europeu. Mas, o país escolheu por fazer concessões, como o “*Privacy Shield*”, já mencionado anteriormente, de modo a se alinhar com a política internacional com o objetivo de manter boas relações com o mercado europeu.

### 2.2.4 Regulação em países da América Latina

Na América Latina, são vários os países que já possuem um arcabouço jurídico avançado no tocante à proteção de dados pessoais, em especial alguns são inspirados no modelo europeu. Diante disto, alguns exemplos merecem aqui serem elucidados, mostrando a experiência dos países mais próximos ao Brasil.

À vista disso, o Uruguai possui a Lei nº 18.331 de 2008, que dispõe sobre a proteção de dados e quanto ao habeas data no país. A garantia da proteção de dados é um direito fundamental para os uruguaios, remetendo-se à sua própria Constituição, motivo pela qual o país foi inclusive reconhecido pela própria União Europeia como um país juridicamente progressista no tema, tendo sido convidado até mesmo pela União Europeia a aderir à Convenção 108 da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), “que traz em seu texto os princípios essenciais da proteção de dados, e assim sendo considerado apto a receber os dados dos cidadãos europeus” (MENDONÇA, 2016, p. 298).

Por sua vez, o Chile publicou a Lei nº 19.628 em 1999, sendo assim o primeiro país da América Latina a normatizar a matéria em tela, abrangendo tanto normas procedimentais quanto as substantivas, prevendo a necessidade de autorização do uso dos dados por seus titulares e até à adstrição de seu uso para a finalidade informada e consequentemente pactuada, dentre outros. Em 2012 a referida lei foi atualizada, com o objetivo de adequar aos desafios que a internet apresentou ao potencializar a transferência de dados.

A Argentina é outro exemplo latino, cuja Lei nº 25.326 de 2000 foi editada a fim de tutelar o uso de informações pessoais no ambiente virtual. Tendo sido incluído todos os temas basilares, desde os conceitos, às suas garantias conferidas e eventuais as sanções em caso de descumprimento da lei. Buscando assim orientação no modelo europeu, tendo a sua legislação sido considerada apropriada quanto ao tema.

Diante do que foi aqui comentado brevemente nos países latinos, e tendo em vista a necessidade de se estudar o tema, ainda mais dado o novo contexto tecnológico administrado pelo *Big Data*, é verificado que diversos países, inclusive os de histórico semelhante ao do Brasil, legislaram sobre o tema muito antes que o Brasil. Segundo um levantamento feito pelo Graham Greenleaf, professor da Law & Information Systems, UNSW Australia, em janeiro de 2015 já eram 109 (cento e nove) países com leis voltadas para a proteção da privacidade dos dados (GREENLEAF, 2015).

# 3 O IMPACTO DA CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Esse capítulo buscará fazer uma análise da Lei Geral de Proteção de Dados brasileira, em seus pontos mais essenciais, não se pretendendo esgotar a matéria.

## 3.1 A PROTEÇÃO DE DADOS NO ORDENAMENTO NACIONAL

Em 2014, o Marco Civil da Internet, MCI - Lei 12.965, entrou em vigor no país, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Foi uma forma de reconhecer e regulamentar todas as novas relações jurídico-virtuais, em razão da existência de inúmeros usuários e consequentemente provedores, bem como de empresas que trabalham online, dado que grande parte não estava adaptada à essa nova realidade digital.

Portanto, o MCI trata dos delitos praticados online, isto é, crimes cibernéticos e da neutralidade da rede, estabelecendo direitos e garantias para liberdade de expressão, apesar de cuidar da privacidade, acabou restando uma lacuna sobre o tratamento de dados pessoais, pois não foi dada a devida atenção a sua utilização, destino, comercialização etc.

Com uma clara influência da entrada em vigor do novo Regulamento Geral sobre a Proteção de Dados (RGPD), da União Europeia, e dos recentes escândalos de vazamento de dados, foi sancionado o texto que trata do uso de informações pessoais de modo específico no ordenamento nacional, visando desenvolver a proteção da privacidade no meio eletrônico.

Assim, com o período de *vacatio legis* de 18 (dezoito) meses, a nova Lei Geral de Proteção de Dados (LGPD) passa a ter eficácia plena em todo território nacional em fevereiro de 2020, consagrando assim princípios e garantias semelhantes àqueles do Regulamento europeu e reforçando, ainda, o controle do titular sobre os seus dados pessoais pela exigência do consentimento, o direito ao acesso e à informação, o direito de retificação e apagamento. Dispondo sobre o modo pelo qual informações pessoais podem ser coletadas e tratadas, seja a partir de cadastros, no fechamento de compras ou até mesmo em imagens publicadas, estabelecendo requisitos para que os dados possam ser tratados, repassados, publicados e até comercializados

Assim, a Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que determina como os dados dos cidadãos podem ou não ser coletados e tratados, e que prevê punições para transgressões. Foi sancionada no dia 14 de agosto de 2018 pelo Congresso Nacional, o PLC 53/2018, o qual dispõe sobre a proteção de dados pessoas e altera algumas situações trazidas pela Lei 12.965 de 16, isto é, o Marco Civil da Internet, consolidando-se assim como a Lei Geral de Proteção de Dados brasileira.

Vale destacar que, “apesar de versar sobre temas similares, o MCI se mantém integralmente vigente, tendo sido alterado apenas naqueles artigos que dizem respeito expressa e especificamente aos dados pessoais, quais sejam os artigos 7, X e 16, II” (CAVALCANTI, 2018, p. 3).

Assim a LGPD cria toda um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito offline quanto online, nos setores privados e públicos. Salienta-se que o país já dispunha de mais de 40 normas que diretamente e indiretamente tratavam da proteção à privacidade e aos dados pessoais. Todavia, foi a LGPD que substituiu e/ou complementou esse arcabouço regulatório setorial, que era conflituoso, trazia insegurança jurídica e tornava o país menos competitivo no contexto de uma sociedade cada vez mais movida em torno de dados. Ao ter uma Lei Geral, o Brasil entra para o rol de mais de 100 (cem) países que hoje podem ser considerados adequados para proteger a privacidade e o uso de dados.

> Os principais fatores que motivaram a criação de uma lei de proteção de dados foram: Uso cada vez maior de dados pessoais • O recurso mais valioso do mundo não é mais petróleo, mas dados. (The Economist). Era digital, redes sociais, “analytics”. Possibilidade de impactos nas vidas das pessoas, negócios e até eleições. Ausência de um marco regulatório nacional quanto à proteção de dados. Acontecimentos recentes e outros fatores. Cambridge Analytic. GDPR (General Data Protection Regulation - União Européia). OCDE (Organização para a Cooperação e Desenvolvimento Econômico). Lei do Cadastro Positivo. Ano Eleitoral Composta por 65 artigos divididos em 10 capítulos, abaixo segue uma descrição sucinta dos conceitos que a LGPD aborda. (LEMOS, 2018, p. 16)

Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD) é composta por 65 (sessenta e cinco) artigos divididos em 10 (dez) capítulos.

Assim, ficou evidente que o direito à privacidade sempre foi uma matriz constitucional na era dos dados físicos e agora com a LDPR teve a devida estatura legal no ambiente eletrônico, fazendo assim com que o Brasil passe, então, a integrar

o seleto time de países que reconhecem positivamente a relevância dos dados digitais e a necessidade de protegê-los.

Nesse contexto, podemos afirmar que a palavra-chave é justamente o consentimento, ou seja, o titular deve expressamente concordar, tendo que ser de forma inequívoca e explícita, permitindo que os seus dados sejam tratados. Portanto, o empresário deve conceber esse tratamento tendo em conta os princípios da LGPD, isto é, os princípios da transparência, finalidade, livre acesso, adequação, qualidade dos dados, prevenção, não discriminação e responsabilização.

Nas palavras de Viviane Nóbrega Maldonado e Renato Opice Blum (2019, p. 52):

> De modo geral, você não poderá enviar ofertas se o consumidor não permitir isso explicitamente. As exceções em que não é preciso o consentir é quando tratar dados for indispensável em situações relacionadas: a uma obrigação legal; a políticas públicas; a estudos via órgão de pesquisa; a um direito, em contrato ou processo; à preservação da vida e da integridade física de uma pessoa; à tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; à prevenção de fraudes contra o titular; à proteção do crédito; a interesses legítimos da empresa, desde que esses interesses não firam direitos fundamentais do titular.

A LGPD vem como um primeiro e importante passo para o ingresso definitivo do Brasil no estabelecimento de garantias e principalmente na preservação dos direitos fundamentais do novo cidadão que surgiu com o meio digital.

## 3.2 POSSIBILIDADES DE APLICAÇÃO

O artigo 1º da Lei nº 13.709 LGPD 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” (BRASIL, 2018, p. 1).

A Lei aplica-se a todas as empresas, inclusive nas pequenas e médias, alcançando também aquelas que possuem sede no exterior e a operação e o tratamento de dados são feitos no Brasil. Após inúmeros adiamentos, a expectativa era de que a LGPD entrasse em vigor apenas em 2021, com o fim do período de calamidade pública causado pela pandemia de coronavírus. No entanto, foi aprovada pelo Senado Federal, encontra-se em pleno vigor desde 18 setembro de 2020, ficando apenas adiada para agosto de 2021 a vigência das sanções administrativas. Veja-se:

> A LGPD se aplica a empresas que ou têm estabelecimento no Brasil, e/ou oferecem produtos e serviços ao mercado brasileiro, e/ou coletam e tratam dados de pessoas que estejam no país. Vale lembrar que não interessa: se o titular dos dados é brasileiro ou não; qual o meio de operação de tratamento dos dados (físico ou digital); qual o país sede da empresa; se os dados estão hospedados em *datacenters* no país ou não. Vale reforçar que a LGPD permite a transferência de dados além-fronteira, desde que seja: com o consentimento específico do titular; a pedido do titular para que esse possa executar pré-contrato ou contrato; para proteção da vida e da integridade física do titular ou de terceiro; para ajudar na execução de política pública; para país ou organismo internacional que projeta dados pessoais de forma compatível com o Brasil; para cooperar juridicamente com órgãos públicos de inteligência, investigação, ou por conta de compromisso assumido via acordo internacional; para cumprir obrigação legal; com a autorização da ANPD; comprovado que o controlador segue a LGPD na forma de normas globais, selos, certificados e códigos de conduta. (GOVERNO FEDERAL, 2019, p. 1)

Desse modo, conforme o artigo 1º da já mencionada lei, há a possibilidade de aplicação da mesma em pessoas jurídicas de direito público ou privado e até mesmo por pessoas naturais. *In verbis* o artigo 3º que corrobora com esse entendimento:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. (BRASIL, 2018, p. 1)

A Lei Geral de Proteção de Dados é apenas restrita ao que já foi mencionado anteriormente, mas pode ser utilizada no campo das relações trabalhistas, já que disciplina o respeito à privacidade, a inviolabilidade da intimidade, da honra e da imagem. Portanto, se aprofundarmos o estudo, será notório que o tema em si não é nenhuma novidade, afinal em 1988 a Constituição Federal em seu artigo 5º, incisos X e XII exaltou tais direitos à posição de “direitos fundamentais”.

Por conseguinte, na relação trabalhista, o empregador pode armazenar os dados dos seus trabalhadores necessários para o desemprenho de suas obrigações legais, regulamentadas pelo próprio contrato de trabalho, dessa forma, é claro que o empregador muitas vezes tem acesso a informações relacionadas com a origem racial, saúde opinião política e orientação sexual do trabalhador, considerados pelo artigo 11º dados sensíveis.

Ademais, a discriminação ou o constrangimento dos trabalhadores devido a distribuição dos dados deve ser sempre evitado, podendo tais situações serem objetos de judicializações com pedido de ressarcimento de danos morais. Sempre que houver necessidade do empregador da utilização dos dados sensíveis que não seja para o cumprimento de obrigação legal regulatória, deverá ser logrado com o consentimento do trabalhador, que deverá ser categoricamente informado de forma inequívoca, evitando prejuízos ao mesmo.

Dessa maneira, é importante ressaltar quanto a privacidade nas relações de trabalho, que alguns trabalhadores, pela natureza das suas próprias funções, têm acesso as informações de clientes que não podem ser difundidas, essas informações recebem o nome de dados comerciais. Essa situação requer que a empresa ocorra preventivamente, buscando assim treinar e capacitar os seus empregados, evitando acidentes como vazamentos e, além disso, há o pagamento de possíveis sanções que podem ser impostas pelo Departamento Estadual de Proteção e Direito do Consumidor (Procon) como pela Autoridade Nacional de Proteção de Dados (ANPD).

Ainda na seara trabalhista, outra questão que requer uma conformidade com a LGPD é justamente o recebimento de currículos em processos seletivos. A recomendação que a lei traz é que a empresa não trate os dados desnecessários, ou seja, não tratem dos dados sensíveis, minimizando assim possíveis riscos de vazamento e, de preferência, não armazene tais documentos, seja em meios digitais como em meios físicos.

Assim, é necessário informar que a adequação às novas regras impostas pela LGPD requer que a empresa possua seu próprio mapeamento de fluxo de dados, podendo realizar todas as alterações contratuais primordiais e treine os seus empregados conforme uma política de privacidade que a partir de agora se torna obrigatória.

Outra área que será afetada é a área da saúde. Dessa maneira, ressalta-se que o setor de saúde engloba desde hospitais públicos e privados, consultórios, clínicas médicas, laboratórios, farmácias, agentes de saúde e toda a esfera pública – o Sistema Único de Saúde – SUS e pacientes, que possibilita o acesso universal ao sistema público de saúde. Portento, esse é um setor com a coleta de dados em proporções elevadas, que poderiam possibilitar a comparação de dados de saúde de indivíduos de diversas localidades, em especial nas grandes estruturas.

Pode-se afirmar que o compartilhamento de dados na área da saúde “é importante para que sejam reduzidos os custos assistenciais, tanto para disponibilizar dados mínimos dos pacientes aos que integram toda a cadeia de assistência à saúde quanto para possibilitar um tratamento mais assertivo” (ARAUJO; NUNES, 2005, p. 35).

De acordo com o artigo 5º, II, da Lei Geral de Proteção de Dados, os dados referentes à saúde são considerados dados pessoais sensíveis. Dessa maneira, as organizações que tratarem desses dados pessoais sensíveis devem se subordinar aos artigos 7º e 11 da LGPD. *In verbis*:

> Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; *(Redação dada pela Lei nº 13.853, de 2019)*
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. [...]

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. [...] (BRASIL, 2018, p. 5)

Isto posto, embora não seja um ordenamento nova para o setor de Saúde Suplementar, cumpre informar que o §5º, do artigo 11, da Lei Geral de Proteção de Dados proibe que as operadoras de planos de saúde do setor privado utilizem os meios de tratamento dos dados de saúde para apurar quais casos trariam riscos na contratação de qualquer modalidade que seja, bem como na contratação e na exclusão de beneficiários.

Faz-se necessário salientar que a LGPD aponta que o tratamento dos dados sensíveis deve estar em conformidade com a finalidade e com o benefício do titular dos dados pessoais. Da mesma maneira, que em algumas situações, quando for indispensável o tratamento para proteção da vida ou incolumidade física do seu titular ou de terceiros, a mencionada lei autoriza o tratamento dos dados sem o devido consentimento. Entretanto, devem ser respeitados os princípios indicados no artigo 6º, da LGPD.

### 3.1.1 Poder público e a LGPD

A Lei Geral de Proteção de Dados Pessoais se aplica as empresas que têm estabelecimento no Brasil, ou as que estejam localizada em outros países mas que oferecem produtos e serviços ao mercado brasileiro, e até aquelas que coletam e tratam dados de pessoas que estejam no país.

Nesse seguimento, não interessa se o titular dos dados é ou não brasileiro, qual o meio de operação de tratamento dos dados, isto é, podendo ser físico ou digital, ou qual o país sede da empresa. Vale reforçar que a LGPD possibilita a transferência de dados além-fronteira, desde que com o consentimento do titular, a pedido do titular

para que o mesmo possa efetuar algum contrato, para salvaguardar a vida e a integridade física do seu titular ou até mesmo de terceiro.

Há outras hipóteses, tais como “ajudar na execução de política pública; para país ou organismo internacional que projeta dados pessoais de forma compatível com o Brasil; para cooperar juridicamente com órgãos públicos de inteligência”, assim como “investigação, ou por conta de compromisso assumido via acordo internacional; para cumprir obrigação legal; com a autorização da ANPD; comprovado que o controlador segue a LGPD na forma de normas globais, selos, certificados e códigos de conduta” (MORAES, 2017, p. 98).

## 3.2 MULTAS E SANÇÕES

Primeiramente, temos que nos atender que o órgão responsável para aplicação de multas e sanções previstas na LGPD é a autoridade nacional de proteção de dados, no qual estas penalidades são aplicadas para os agentes de tratamentos de dados.

Vale ressaltar que, são considerados agentes de tratamento de dados o operador e controlador, conforme dispõe o artigo 5º, da lei n. 13.709/18:

> Art. 5º Para os fins desta Lei, considera-se:
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Quando a autoridade nacional de proteção de dados verificar que algum agente de tratamento de dados descumpriu a LGPD poderá aplicar as seguintes sanções, quais sejam: advertência, no qual indicará um prazo para realizações de correções; multa simples, no valor de dois por cento do faturamento da pessoa jurídica, que deve ser limitada até cinquenta milhões de reais por infração; multa diária, que também seguirá o limite da multa simples; publicização da infração, neste caso ocorrerá após ser devidamente apurada; bloqueio do  dados pessoais da referida infração até sua regularização; eliminação dos dados, apenas aqueles que se referem a infração; suspenção parcial do funcionamento do banco de dados pelo período máximo de seis meses, podendo ser prorrogável por igual período até a regularização da atividade de tratamento ou a suspensão total da atividade; e por fim, a proibição total de tratamento de dados.

Sobre o valor da multa diária o artigo 54 da mencionada lei define, que:

> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.
> Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (BRASIL, 2018)

Essas sanções são aplicadas pela ANDPD através de processos administrativos, que devem garantir o exercício da plena defesa dos acusados. Ademais, estas penalidades devem cumprir critérios que estão elencados no artigo 52, § 1º, inciso I a XI na LGPD, tais como:

> [...] I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Assim vemos, que para o enquadramento de cada uma dessas penalidades, a autoridade nacional vai avaliar cada caso concreto e utilizar os critérios acima descritos.

É importante frisar, que a responsabilidade é solidaria entre os agentes de tratamentos de dados, ou seja, o controlador e o operador são solidários nesse tipo de processo administrativo, podendo os dois sofrerem as sanções.

Outro ponto, que deve ser levado em consideração é que se sua empresa não implementar as normas da LGPD, só pela falta de inconformidade, já estará passível de aplicações de multas. Então, não precisa esperar ter um vazamento de dados ou de informações da empresa para receber uma sanção ou multa que será prejudicial ao seu negócio.

Por fim, as sanções administrativas aplicadas pela autoridade nacional, conforme a lei, não excluem as responsabilidades cíveis, penais ou relativas ao direito do consumidor dos agentes de tratamento de dados, assim sendo, podemos entender

que além dessas sanções, os agentes poderão sofrer processos judiciais nas outras esferas do direito.

Em relação a responsabilidade civil prevista em nosso ordenamento jurídico, quando houver caso onde envolva a violação das normas na LFPD, o agente de tratamento de dados será imputado pela reparação do dano, podendo este dano ser patrimonial, moral, individual ou coletivo. Assim, aqueles que descumprirem a lei responderá civilmente pelos danos que ocasionalmente ocorrerem.

Nesse cenário, se torna primordial esclarecer que o texto legal em seu artigo 52 determina as punições severas para quem comete infrações já mencionadas, que vão desde a advertência, com a indicação do prazo para a adoção de medidas corretivas até a aplicação de multa simples, isto é, de 2% (dois por cento) sobre o faturamento da pessoa jurídica, podendo atingir o limite de R$ 50 (cinquenta) milhões pela infração. Assim, podemos até mesmo afirmar que a falta de conformidade e proteção de dados poderá fechar uma empresa.

Além disso, a lei já em vigor e, com previsão das sanções começarem a ser aplicadas em 2021, mais especificamente em agosto, o Ministério Público e os Procons, com o devido fundamentação no Código de Defesa do Consumidor já estão atuando na defesa dos direitos daqueles titulares que tiveram qualquer problema com os seus dados pessoais e contra os incidentes de segurança, tais como algum tipo de vazamentos de dados.

Ademais, pautando pela segurança nas informações e pela transparência, o Supremo Tribunal de Justiça tem admitido diversas iniciativas para assegurar o pleno cumprimento de todas as disposições da Lei Geral de Proteção de Dados Pessoais. Nesse sentido, a Portaria STJ/DG 590/2020 instituiu uma comissão com a específica finalidade de elaborar o estudo e identificar as medidas necessárias para à implementação da LGPD no Supremo Tribunal de Justiça.

## CONSIDERAÇÕES FINAIS

Com o uso cada vez maior de tecnologia e principalmente dados pessoais em todas as esferas da sociedade mundo a fora, o compartilhamento não autorizado e até mesmo a venda destes dados tem ocorrido de forma indiscriminada há muito tempo.

Especialmente no Brasil, carecíamos de uma regulamentação nacional que regulamentasse o uso indevido de dados pessoais, tendo em vista a prerrogativa constitucional de privacidade do cidadão. Todo cidadão merece que suas informações pessoais sejam tratadas com devido cuidado e necessita que corporações e órgãos governamentais tomem precauções na coleta, gravação, uso e até mesmo no descarte deste tipo de informação.

Em razão disto, em agosto de 2018 foi aprovada a LGPD, objeto do nosso estudo, que trouxe como principais finalidades os seguintes pontos: proteção de dados pessoais do cidadão; direitos dos cidadãos titulares em possuir maior controle sobre o uso de seus dados em qualquer empresa; segurança da informação; boas práticas de prevenção de vazamento de informações; comunicação de incidentes de vazamento e fiscalização do uso destes dados.

Em resumo, a lei visa estabelecer direitos fundamentais ao cidadão, tais como privacidade; direito a informação; defesa do consumidor; liberdade, dignidade e cidadania.

Sob o ponto de vista de como a lei irá impactar as organizações brasileiras, destaca-se a oportunidade única de elevar a postura de segurança a um nível nunca antes imaginável, tendo em vista que a lei é bastante abrangente, não apenas no aspecto jurídico, quanto no técnico, especialmente tratando sobre a segurança cibernética, surge então a chance de os times de gestão de segurança da informação terem papeis de protagonismo nas estratégias de proteção de dados, podendo tornar-se referência nas organizações onde atuam como diferenciais em seu mercado.

A lei inclui em seu escopo toda e qualquer pessoa jurídica e física quando trata-se sobre qual dados pessoais realizados em território nacional independente deste tratamento ser feito por meios digitais ou não.

Por fim, vale afirmar que a lei geral de proteção de dados existe com o propósito de garantir o direito a privacidade prevista em nossa constituição federal, para que não seja utilizado para fins indevidos.

**REFERÊNCIAS BIBLIOGRÁFICAS**

ARAUJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano**. Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2005.

BRASIL, PEC 479/2010. **Acrescenta o inciso LXXIX ao art. 5º da Constituição Federal, para Incluir o acesso à Internet em alta velocidade entre os direitos fundamentais do cidadão,** Brasília, DF, abril 2010. Disponível em: < https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=47382 7#marca cao-conteudo-portal>. Acesso em: 12 de dezembro de 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 12 de dezembro de 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 12 de dezembro de 2020.

BRASIL. **Guia de Boas Práticas Lei Geral de Proteção de Dados. Comitê Central de Governança de Dados.** 23 de março de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guialgpd.pdf. Acesso em: 12 de dezembro de 2020.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005.

CAVALCANTI, Eduardo de Hollanda. P**roteção de dados, a vez do Brasil.** Disponível em: https://www.migalhas.com.br/dePeso/16,MI286295,71043-Protecao+de+dados+a+vez+do+Brasil. Acesso em: 12 de dezembro de 2020.

DOTTI, Renè Ariel. **Proteção Da Vida Privada e Liberdade de Informação.** São Paulo: RT, 1980.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** EJJL-Espaço Jurídico: Journal of Law, v. 12, n. p. 100-101. 2011.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda..Brasília: SDE/DPDC, 2010.

_____. **Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro RBRS10-4**. Revista Brasileira de Risco e Seguro. Disponível em: www.rbrs.com.br/paper/_.../RBRS10-4%20Danilo%20Doneda.pdf. Acesso em: 12 de dezembro de 2020.

DRUMMOND, Victor. **Internet, Privacidade e Dados Pessoais**. Rio de Janeiro: Lumen Juris, 2003.

GOVERNO BRASILEIRO. **Como cumprir a LGPD? Mais que multas que afetem o caixa, não aplicar a nova lei pode abalar a reputação diante dos clientes e a confiança em seus produtos e serviços.** Brasília: Serpro, 2019. Disponível em: <https://www.serpro.gov.br/lgpd/empresa/como-cumprir-a-lgpd> . Acesso em: 12 de dezembro de 2020.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. São Paulo: Atlas, 2017.

GUGIK, Gabriel. **A história dos computadores e da computação**. Disponível em: https://informaticaeadministracao.wordpress.com/2014/04/18/os-computadores-e-sua-historia/. Acesso em: 12 de dezembro de 2020.

GOMES, **Rodrigo Dias de Pinho. Privacidade em perspectivas: Desafios à privacidade: Big Data, Consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de Dados Pessoais.** Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

GABRIEL, Martha. **A ilusão da conexão.** Disponível em: http://campuse.ro/social/resource/38995/view.cp. Acesso em: 12 de dezembro de 2020.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. **Marco Civil da Internet: A garantia constitucional à inviolabilidade da intimidade e da vida**

**privada como direito dos usuários no marco civil da internet.** Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GREENLEAF, Graham. **Global data privacy laws 2015: 109 countries, with european laws now a minority.** 2015. Disponível em: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529> Acesso em: 12 de dezembro de 2020.

HALF, Robert. **O que muda para o consumidor com a LGPD? 2019**. Disponível em: https://itforum365.com.br/colunas/o-que-muda-para-o-consumidor-com-a-lgpd/. Acesso em: 12 de dezembro de 2020.

ITAGIBA, Gabriel. **Fake news e Internet: esquemas, bots e a disputa pela atenção.** 2017. Disponível em: https://itsrio.org/wp-content/uploads/2017/04/v2_fake-news-e-internet-bots.pdf . Acesso em: 12 de dezembro de 2020.

**JORNAL OFICIAL DA UNIÃO EUROPEIA**, 2016, p. 5 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 12 de dezembro de 2020.

LIMA, Caio César Carvalho. **Marco Civil da Internet: Garantia da privacidade e dados pessoais à luz do marco civil da internet**. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

LOTTENBERG, Fernando; VAINZOF, Rony. **Discurso de ódio, redes sociais e o Marco Civil da Internet (parte 1). Revista Consultor Jurídico, 13 de julho de 2018, 6h14**. Disponível em: <https://www.conjur.com.br/2018-jul-13/opiniao-discurso-odioredes-sociais-marco-civil-parte> Acesso em: 12 de dezembro de 2020.

LEMOS, R.; ADAMI, M.P.; SUNDFELD, P. **Proteção de dados na Administração Pública.** Jota. 14 de maio de 2018.Online. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados- administracaopublica-14052018#sdfootnote3anc . Acesso em: 12 de dezembro de 2020.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. p. 134. 2010.

MENDONÇA, Fernanda Graebin. **Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e em Países Latino-Americanos.** Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA, v. 11, n. 1. p. 298. 2016.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. **Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet.** Revista Pensar, v. 22, n. 1 2017.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais?**, Instituto Igarapé, Artigo Estratégico nº 39, Dezembro de 2018, p. 11.

MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. **Marco Civil da Internet: A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance.** Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MOTTA, Sylvio; BARCHET; Gustavo. **Curso de direito constitucional: atualizado até a Emenda constitucional nº 53/2006.** Imprenta: Rio de Janeiro, Elsevier, Campus, 2007.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big Data: A Revolution That Will Transform How We Live, Work, and Think. New York.** Houghton Mifflin Harcourt, 2013, p. 190 apud GOMES, Rodrigo Dias de Pinho. Desafios à Privacidade: Big Data, Consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de Dados Pessoais, 2018, p. 236.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor: O novo regime das relações contratuais**. 5. ed. São Paulo: Revista dos Tribunais, 2006.

MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman V.; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor.** 2. ed. ver., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2006.

MELTZER, Joshua Paul. **The Internet, Cross-Border Data Flows and International Trade**. Asia & the Pacific Policy Studies, v. 2, n. 1. p. 90-102. 2015.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados.** São Paulo: Revista dos Tribunais, v. 107, n. 5970, jan. 2019.

NADER, Ralph. **"The Dossier Invades the Home"**, in: NADER, Ralph. The Ralph Nader Reader. Seven Stories Press, 2000, 407.

NAUGHTON, John, 2000, **A brief history of the future: from radio days to Internet years in a lifetime.** Woodstock, NY, Overlook Press.

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

ROCHFELD, Judith. **Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet.** Revista de Direito, Estado e Comunicações, Brasília, v. 10, n. 1, maio 2018. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_ servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-Dir-Est-Telecom_v.10_n.01.04.pdf. Acesso em: 12 de dezembro de 2020.

STJ, **Recurso Especial n. 22.337/RS,** rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p.6119.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais.** São Paulo: Edições Sesc, 2017.

SAFERNET. **O que são os Metadados?** Acesso em: https://new.safernet.org.br/content/o-que-s%C3%A3o-os-metadados#mobile 12 de dezembro de 2020.

SOARES, Rafael Ramos. **Lei geral de proteção de dados – lgpd: direito à privacidade no mundo globalizado. 2020,** Goiânia. Disponivel em: < https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1201/1/RAFAEL%20RAMOS%20SOARES%20-%20Artigo.pdf >. Acesso em: 12 de dezembro de 2020.

VAINZOF, Rony. **Lei 13.709/2014 de 14 de agosto de 2018 – disposições preliminares.** In In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords).

LGPD – Lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

WENDLING, Mike. **Como o termo 'fake news' virou arma nos dois lados da batalha política mundial.** Disponível em: https://www.bbc.com/portuguese/internacional-42779796. Acesso em: 12 de dezembro de 2020.