UNIVERSIDADE NOVE DE JULHO
DEPARTAMENTO DE PÓS-GRADUAÇÃO *STRICTO SENSU*
PROGRAMA DE MESTRADO EM DIREITO

ELLEN CATARINO PALMEIRA

CONTRIBUIÇÃO PARA O ESTUDO DOS IMPACTOS DO TRATAMENTO DE DADOS PESSOAIS NA ATIVIDADE EMPRESARIAL SOB A ÓTICA DA ANPD

SÃO PAULO – SP
2023

ELLEN CATARINO PALMEIRA

CONTRIBUIÇÃO PARA O ESTUDO DOS IMPACTOS DO TRATAMENTO DE DADOS PESSOAIS NA ATIVIDADE EMPRESARIAL SOB A ÓTICA DA ANPD

Dissertação apresentada ao programa de pós-graduação *stricto sensu* em Direito da Universidade Nove de Julho, como requisito parcial para a obtenção do título de Mestre em Direito.

Orientação: Professor Doutor Walter Godoy dos Santos Júnior.

SÃO PAULO – SP
2023

FICHA CATALOGRÁFICA

Palmeira, Ellen Catarino.
Contribuição para o estudo dos impactos do tratamento de dados pessoais na atividade empresarial sob a ótica da ANPD. / Ellen Catarino Palmeira. 2023.
103 f.

Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2023.
Orientador (a): Prof. Dr. Walter Godoy dos Santos Júnior.

1. Proteção de dados. 2. Atividade empresarial. 3. Tratamento de dados. 4. Direito fundamental. 5. LGPD.
I. Santos Júnior, Walter Godoy dos. II. Título.

CDU 34

ELLEN CATARINO PALMEIRA

CONTRIBUIÇÃO PARA O ESTUDO DOS IMPACTOS DO TRATAMENTO DE DADOS PESSOAIS NA ATIVIDADE EMPRESARIAL SOB A ÓTICA DA ANPD

Dissertação apresentada ao programa de pós-graduação *stricto sensu* em Direito da Universidade Nove de Julho, como requisito parcial para a obtenção do título de Mestre em Direito.

Aprovado em: ____/____/2023

Banca Examinadora:

_____
Dr. Walter Godoy dos Santos Júnior
Orientador - UNINOVE

_____
Dr. Erickson Gavazza Marques
Examinador Interno - UNINOVE

_____
Dr. Marcelo Barbosa Sacramone
Examinador Externo – PUC/SP

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais, Eliane e Claudemir, que sempre me deram todo apoio necessário, tanto material como emocional, em minha trajetória acadêmica e, apesar de todas as dificuldades, sempre estiveram ao meu lado, e ao meu irmão, Enzo, acima de tudo, meu amigo.

Ao meu avô (*in memoriam*) que, seja de onde for, sei que está me olhando e se orgulhando de cada passo meu.

Agradeço ao meu namorado, Julio, meu parceiro afetuoso e confidente de todos os momentos.

Agradeço ao meu orientador, professor Dr. Walter Godoy dos Santos Júnior, por toda ajuda, dedicação, disponibilidade no auxílio desta pesquisa e por dividir comigo um pouco de sua sabedoria. A sua orientação foi fundamental durante todo o trabalho.

Aproveito também para agradecer a oportunidade concedida pela Universidade Nove de Julho, por fazer parte da minha trajetória acadêmica. A todos os outros professores e funcionários da universidade, pela ajuda, atenção e por terem contribuído imensamente para meu amadurecimento e crescimento acadêmico durante todo o tempo em que cursei o mestrado.

“Para ser grande, sê inteiro: nada
Teu exagera ou exclui.
Sê todo em cada coisa. Põe quanto és
No mínimo que fazes.
Assim em cada lago a lua toda
Brilha, porque alta vive.”

Fernando Pessoa

RESUMO

O compartilhamento, de dados cada vez, mais controla nossas vidas e causam um impacto significativo sobre a sociedade. Para regular e mitigar eventuais violações de direitos, as legislações nacionais e internacionais buscaram tutelar a proteção de dados pessoais, por meio de medidas que tragam a transparência da coleta de dados realizadas pelas organizações públicas e privadas. Neste sentido, a presente pesquisa realizou análise dos aspectos jurídicos da proteção de dados no Brasil, dedicando-se, especificamente, acerca do papel das empresas na busca pela proteção de dados e os impactos da legislação na atividade empresarial sob a ótica da Autoridade Nacional de Proteção de Dados – ANPD. Para tanto, será abordado panorama geral da evolução do direito à privacidade, resgatando o histórico sobre tema, até o surgimento da proteção de dados e promulgação da Lei Geral de Proteção de Dados – LGPD, no Brasil. Além disso, serão abordadas as adequações necessárias a serem implantadas pelas empresas, visando o integral cumprimento, bem como as hipóteses de sanções aplicáveis pela ANPD, em caso violações à proteção de dados e seus impactos na atividade empresarial. Desta forma, para o incremento do trabalho utilizou-se o método hipotético-dedutivo, por meio da técnica qualitativa com análise documental, legislativa e doutrinária.

Palavras-chave: proteção de dados; atividade empresarial; tratamento de dados; direito fundamental; LGPD.

ABSTRACT

The sharing of data increasingly controls our lives and has a significant impact on society. To regulate and mitigate any violations of rights, national and international legislation has sought to protect the protection of personal data, through measures that bring transparency to the collection of data carried out by public and private organizations. In this sense, this research carried out an analysis of the legal aspects of data protection in Brazil, dedicating itself specifically to the role of companies in the search for data protection and the impacts of legislation on business activity from the perspective of the National Protection Authority of Data - ANPD To this end, a general overview of the evolution of the right to privacy will be addressed, rescuing the history on the subject, until the emergence of data protection and the enactment of the General Data Protection Law - LGPD, in Brazil. In addition, the necessary adaptations to be implemented by companies will be addressed, aiming at full compliance, as well as the hypotheses of sanctions applicable by ANPD, in case of data protection violations and their impacts on business activity. Thus, for the increment of the work, the hypothetical-deductive method was used, through the qualitative technique with documental, legislative and doctrinal analysis.

Keywords: data protection; business activity; data processing; fundamental right; LGPD.

LISTA DE ABREVIATURAS E SIGLAS

ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
ANVISA	Agência Nacional de Vigilância Sanitária
AREsp	Agravo Regimental em Recurso Especial
CEP	Código de Endereçamento Postal
CF/88	Constituição Federal de 1988
CGI.br	Comitê Gestor de Internet no Brasil
CIS	Comunicados de Incidente de Segurança
CPF	Cadastro Pessoa Física
Dataprev	Empresa de Tecnologia e Informações da Previdência
DPA	Data Protection Authority
DPO	*Data Protection Officer*
EC	Emenda Constitucional
GDPR	*General Data Proteccion Regulation*
IBGE	Instituto Brasileiro de Geografia e Estatística
IBM	*International Business Machines*
ICO	*Information Commissioner's Office*
INSS	Instituto Nacional do Seguro Social
LGPD	Lei Geral de Proteção de dados
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PEC	Proposta de Emenda Constitucional
RIDP	Relatório de Impacto à Proteção de Dados
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça

SUMÁRIO

INTRODUÇÃO

Na sociedade atual, o compartilhamento de dados está presente no cotidiano de todas as pessoas, e, para manter essas informações seguras e transparentes, a legislação sobre proteção de dados ganhou destaque.

O desenvolvimento da disciplina da proteção de dados está fortemente ligado aos marcos regulatórios europeus, uma vez que as normas jurídicas sobre o tema vêm sendo discutidas há mais de meio século, desde a criação da Lei de Proteção de Dados do *Land*, em 1970.

Denota-se que a influência europeia foi intensificada a partir do surgimento do Regulamento Geral de Proteção de Dados, em 2016, inspirando o Brasil a desenvolver seu próprio sistema de proteção de dados.

Em 14 de agosto de 2018, adveio a Lei Geral de Proteção de Dados (LGPD) após diversas tentativas de regulação da privacidade e da proteção de dados no âmbito brasileiro, tais como o Código de Defesa do Consumidor, a Lei de Cadastro Positivo, a Lei de Acesso à Informação e o Marco Civil da Internet.

A LGPD é um marco regulatório brasileiro que visa criar regras uniformes sobre o fluxo e a proteção de dados pessoais no país, ao colocar o titular de dados pessoais no palco da legislação e atribuir ao agente de tratamento deveres a serem cumpridos.

Além disso, a LGPD trouxe, também, a previsão de uma autoridade de controle, a Autoridade Nacional de Proteção de Dados – ANPD. Esse órgão ficou responsável por regular e fiscalizar a coleta e o uso de dados, para garantir a eficácia da LGPD, bem como de aplicar sanções administrativas que podem chegar até R$ 50.000.000,00 (cinquenta milhões de reais).

Portanto, a LGPD tem natureza multissetorial, considerando que atinge todos os setores da sociedade, incluindo o setor público; e transversal, uma vez que incide sobre todas as atividades desenvolvidas de quem trata dados pessoais de pessoas físicas, em todos os níveis operacionais e organizacionais.

Sob esta perspectiva, a LGPD trouxe inúmeros desafios, em especial para as empresas, que devem se adequar às novas diretrizes por lidarem com tantos dados potencialmente lesivos à intimidade e a vida privada de seus clientes, funcionários e fornecedores.

Nesse trabalho, serão analisados os desafios enfrentados pelas empresas na busca pela adequação nos termos previstos pela LGPD, bem como quais os procedimentos a serem implantados pelas empresas e as consequências primárias do não cumprimento da lei, com a aplicação de sanções administrativas pela ANPD.

Por fim, serão colacionados casos semelhantes, que foram tratados e sancionados pelas autoridades de controle de outros países, na forma de direito comparado, ao que está previsto em nossa legislação. Ademais, será analisado como essas sanções poderão afetar o funcionamento das organizações, em especial, das empresas privadas.

Na primeira parte, será tratada a evolução do direito à privacidade e, posterior, surgimento do direito à proteção de dados em âmbito internacional e nacional, até o surgimento da LGPD.

Já na segunda parte, será analisada a Lei Geral de Proteção de Dados e seus principais aspectos. Essa análise mostra-se fundamental para definir os direitos envolvidos no assunto.

Buscar-se-á, no terceiro capítulo, demonstrar os desafios enfrentados pelas empresas na busca pela proteção dos dados pessoais, abordando as consequências e as regras que tratam o tema. Além disso, serão expostas as medidas necessárias para compatibilizar as atividades econômicas baseadas em dados pessoais com as diretrizes constitucionais e legais que regulam o tema.

Por fim, no quarto capítulo, serão analisadas as sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados, em razão do descumprimento dos preceitos legais da LGPD, em especial pelas organizações empresariais e seus impactos econômicos

1. DO DIREITO À PRIVACIDADE AO SURGIMENTO DA PROTEÇÃO DE DADOS PESSOAIS

Com a evolução dos meios de comunicação e crescente exposição do homem, o direito à privacidade ganhou grande destaque nas últimas décadas, em especial após a Segunda Guerra Mundial.

Por isso, vale contextualizar, suscintamente e para melhor elucidar o assunto, o direito fundamental à privacidade, que serviu de base para originar a tutela da proteção de dados.

O direito à privacidade tem inúmeros conceitos, que correspondem à evolução deste preceito fundamental que se moldou à cultura e aos costumes das sociedades ao longo dos séculos.

Historicamente, a proteção à privacidade na doutrina era definida com características de direito negativo, de modo que, para ser garantida, exigia-se absoluta abstenção do Estado na esfera privada individual.

Para alguns especialistas[1], privacidade é um conceito vago que engloba, dentre outros, o direito à liberdade de pensamento, à inviolabilidade do lar, do corpo, o controle sobre informações e a proteção contra a vigilância.

Para outros, como Tercio Sampaio Ferraz Júnior:

> A privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (o estar-só), o segredo, a autonomia. Na intimidade protege-se sobretudo o estar-só; na vida privada, o segredo; em relação à imagem e à honra, a autonomia. [2]

Um dos primeiros esforços doutrinários para definição de direito à privacidade, na história, foi o artigo publicado na *Harvard Law Review*, intitulado *The Right to*

---

[1] Dentre eles, Daniel Solove, que dedicou três livros sobre o tema. Neste capítulo, é trazida à tona a obra *Understanding Privacy*, em que o autor traça uma taxonomia do conceito de privacidade, a fim de melhor entender os elementos que a compõem e a efetivar sua aplicação prática. SOLOVE, Daniel J. **Understanding privacy**. Cambridge: Harvard University Press, ano, p. 1.

[2] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito.** Universidade de São Paulo, 88, 1993, p. 439-459. Disponível em: https://www.revistas.usp.br/rfdusp/article/download/67231/69841/88644. Acesso em: 17 abr. 2023.

Privacy (O Direito à Privacidade), elaborado e publicado em 15 de dezembro de 1890, pelos advogados estadunidenses, Samuel D. Warren e Louis D. Brandeis.[3]

No artigo, os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos invadiram os sagrados domínios da privacidade e da intimidade.

Ainda, nesse sentido, eles identificaram uma alteração do direito à vida (*right to life*), que passou a significar não só um direito a sobreviver, mas também, um direito a aproveitar a vida (*right to enjoy life*).

> Fotografias instantâneas e empreendimento jornalísticos têm invadido os recintos sagrados da vida particular e doméstica; e inúmeros dispositivos mecânicos ameaçam tornar verdadeiro o prognóstico de que "o que é sussurrado no armário será proclamado nos telhados.
> [...] A intensidade e complexidade da vida, continuadas com o avanço da civilização, tornaram necessário uma retirada do mundo – e o homem, sob refinada influência da cultura, tornou-se mais sensível à publicidade, tanto que solidão e a privacidade vem se tornando essenciais ao indivíduo.[4]

Por esse ângulo, os autores reconheceram direitos para além dos bens materiais e do próprio corpo do indivíduo, tutelando-se questões como a "natureza espiritual do homem, seus sentimentos, e seu intelecto"[5].

Nessa perspectiva, buscou-se o rompimento com a tradição anterior que associava a proteção da vida à privacidade, demonstrando a importância desse direito frente aos avanços da tecnologia e possibilitar o seu futuro reconhecimento, como um direito protegido constitucionalmente.[6]

Por essa razão, o artigo estadunidense é considerado um marco inicial na construção doutrinária de um direito à privacidade, em que pese não seja, de fato, o primeiro a abordar o assunto.

---

[3] WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, v. IV, dez. 1890, n. 5. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 10 jan. 2022.

[4] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. VI, n. 5, Dec. 15, 1890. (tradução nossa). Disponível em < https://groups.csail.mit.edu/mac/classes/6.805/articles/ privacy/Privacy_brand_warr2.html>. Acesso em: 27 out. 2022.

[5] *"Later, there came a recognition of man's spiritual nature, of his feelings and his intellect."* (Tradução livre). *Idem*, p. 193.

[6] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 139.

Entretanto, até hoje, ele é considerado o artigo mais influente e mais citado no que diz respeito à privacidade, em razão da sua moderação com o passar do tempo, à medida que a privacidade seria um aspecto fundamental da evolução da pessoa e do desenvolvimento de sua personalidade.[7]

Importa observar que a proteção à privacidade foi considerada, por muito tempo, como um direito tipicamente da burguesia. Nesse sentido, Danilo Doneda afirma que a associação do sentido de privacidade à imagem de mundo burguês se deu em decorrência de seu contexto ter se dado, principalmente, no ambiente judicial.

Isso porque, os primeiros casos judiciais em que se reconhece a violação à privacidade diziam respeito a grandes celebridades, como o caso Rachel (da famosa atriz Elisa Rachael Félix, na França, em 1858) e o caso de Benito Mussolini e de sua amante Clara Petacci (Itália, 1953).[8]

Na jurisprudência norte-americana, o caso *Olmstead v. United States,* de 1928, que contou com a presença de Louis Brandeis, então já juiz da Suprema Corte, traz sinais do lento reconhecimento do direito à privacidade.

O caso dizia respeito à aplicação da Quarta Emenda à Constituição norte-americana, referente ao direito contra a intromissão e buscas não autorizadas nas residências, documentos e bens de uma pessoa. No julgamento, o juiz Louis Brandeis destacou a necessidade da atualização da Quarta Emenda, conforme a realidade tecnológica:

> Na aplicação da Constituição, nossa preocupação não deve ser somente sobre o que foi, porém o que será. O progresso da ciência, ao munir o governo de meios automatizados de espionagem, não irá parar com a escuta telefônica. Um dia, surgirão meios para que o governo, sem ter que remover papéis de uma gaveta, possa utilizá-los em juízo, tornando possível expor os fatos mais íntimos ocorridos dentro de uma casa. O progresso científico proporcionará meios para explorar crenças, pensamentos e emoções sequer expressas. [...]. Será possível que a Constituição não nos ofereça meios de proteção contra tais invasões da segurança individual?[9]

---

[7] DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, ano 4, n. 16, out./dez., 2003, p. 30.

[8] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 11.

[9] *Olmstead v. United States*, 277 U.S. 438 (1928). Disponível em: https://billofrightsinstitute.org/e-lessons/olmstead-v-united-states-1927?gad=1&gclid=EAIaIQobChMIvcbomaTN_wIVBTaRCh3zhwsMEAAYASAAEgKR_PD_BwE Acesso em: 18 jun. 2023.

O voto de Louis Brandeis, ainda que vencido, tornou-se um poderoso argumento para, posteriormente, o caso *Katz v. United States* de 1967, a partir do qual a Quarta Emenda passou a ser aplicada diante de ameaças tecnológicas.

Mais adiante, após a Segunda Guerra Mundial, o tema privacidade foi discutido em diversos tratados e acordos internacionais, dentre eles, a Declaração Universal dos Direitos do Homem, de 1948, que reconheceu o direito à privacidade como direito fundamental.[10]

Ademais, o artigo II, da Declaração Universal determinou que o gozo dos direitos previstos nela não se daria mediante distinção de raça, cor, sexo, idioma, religião, opinião política, original nacional ou social, riqueza, nascimento ou qualquer outra condição.

O referido artigo serviu de inspiração após décadas, e os dados pessoais, tidos como sensíveis pela Lei Geral de Proteção de Dados, são justamente aqueles cujo processamento pode dar causa a categorização discriminatória dos titulares.

Por outro lado, ao elevar as características pessoais a um direito fundamental, a violação da privacidade deixou de ser um problema apenas de grandes celebridades e passou atingir a maioria dos cidadãos. Em razão disso, pela primeira vez, o direito à privacidade foi consagrado como um instrumento jurídico internacional.

Foi a Segunda Guerra Mundial que a proteção à privacidade ganhou reconhecimento no âmbito internacional, assim, a Declaração Universal dos Direitos do Homem, de 1948, dispõe, em seu art. 11.2 o direito à privacidade, o direito à honra e ao sigilo de correspondência, nos seguintes termos:

> Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques.

[10] Artigo 12: Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. ONU. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 9 mar. 2022.

O Pacto Internacional de Direitos Civis e Políticos, a Convenção Americana sobre Direitos Humanos e o Pacto de São José da Costa Rica também previram a proteção da vida privada nos mesmos termos.

Contudo, com o passar do tempo e as evoluções tecnológicas, novas questões surgiram em relação ao direito à privacidade, demandando novas soluções na preservação da personalidade do indivíduo[11], sobretudo a partir da década de 1960.

Mikhail Vieira de Lorenzi Cancelier leciona que, na década de 1960, com considerável rapidez, "o direito à privacidade vai expandindo suas fronteiras, alcançando novos sujeitos, englobando diferentes objetos e tornando-se presente em locais com ele antes incompatíveis".[12]

Desta feita, a privacidade ganha, então, um enfoque positivo, ao passo que devem ser propiciados meios aos indivíduos para controle e conhecimento sobre a informação veiculada sobre si.

Nesse sentido, Danilo Doneda expõe que:

> A privacidade nas últimas décadas passou a relacionar-se com uma série de interesses, o que modificou substancialmente o seu perfil. Chegamos assim ao ponto de verificar que, de acordo com a lição de Stefano Rodotà, que o direito à privacidade não se estrutura mais em torno do eixo "pessoa – informação – segredo", no paradigma da *zero-relationship*, mas sim em um eixo "pessoa-informação-circulação-controle".[13]

---

[11] José Afonso da Silva destaca que prefere usar a expressão direito à privacidade, "num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional [...] consagrou" (LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011, p. 80).

[12] CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**: Estudos Jurídicos e Políticos, Florianópolis, v. 38, n. 76, p. 213-240, 20 set. 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213/34870. Acesso em: 04 set. 2022.

[13] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 23.

Sobre o tema, elucida-nos Stefano Rodotà que:

> Talvez seja possível traçar um esquema deste processo, ressaltando que parece cada vez mais frágil a definição de “privacidade” como o “direito a ser deixado só”, que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito.
> [...] De sua tradicional definição como “direito a ser deixado só” passa-se, justamente pela influência da tecnologia dos computadores, àquela que constituirá um constante ponto de referência na discussão: “direito a controlar o uso que os outros façam das informações que me digam respeito”. Em fase mais recente surge um outro tipo de definição, segunda a qual a privacidade se consubstancia no “direito do indivíduo de escolher aquilo que está disposto a revelar aos outros.
> [...] pode-se dizer que hoje a segunda quantitativa mais relevante é “pessoa-informação-circulação-controle”, e não mais apenas “pessoa-informação-sigilo”, em torno da qual foi construída a noção clássica de privacidade. O titular do direito à privacidade pode exigir formas de ‘circulação controlada”, e não somente interromper o fluxo das informações que lhe digam respeito.[14]

Por fim, no ordenamento brasileiro, o tema foi abordado pela Constituição Federal de 1988, ao proteger, abstratamente, o direito à privacidade no artigo 5º, inciso X.

Para Laura Mendes, o referido artigo permite que seja:

> [...] possível extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra. Não faria sentindo excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais. Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos “tradicionais” [...]. Assim, não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.[15]

A seguir, serão abordados os desdobramentos do direito à privacidade para a criação da disciplina jurídica da proteção de dados, em âmbito nacional e internacional.

---

[14] RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 24.

[15] Art. 5º, inc. X: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

1.1. O Direito à Proteção de Dados Pessoais

Como exposto anteriormente, o direito à privacidade está em constante processo de evolução, devido aos avanços tecnológicos e suas implicações na esfera privada dos indivíduos.

Neste sentido, a proteção de dados pessoais surge mantendo uma ligação indireta com o direito à privacidade, sendo deste oriundo, mas atualizando-se e promovendo tutelas próprias, além de ganhar a natureza de direito autônomo.

A tecnologia tem, cada vez mais, ganhado relevância e, em especial, ao que tange à potencialização da coleta de dados. O recolhimento, o processamento e a análise constante, realizados pelos computadores, com o uso de inteligência artificial, permitem o mapeamento da personalidade das pessoas, por meio de máquinas que não se cansam, diferentemente dos seres humanos.

A exemplo, pesquisas afirmam que, com 250 curtidas, os algoritmos conseguem saber mais sobre uma pessoa do que seu companheiro.[16]

O fato é que os dados pessoais se tornaram objeto de um mercado em ascensão, servindo de insumos essenciais para a grande parte das atuais atividades econômicas. Portanto, evidencia-se a importância da existência de legislações, que busquem proteger a autonomia informativa dos titulares dos dados pessoais, garantindo o controle necessário para evitar que se tornem mercadorias.

Neste sentido, na obra “Vida para consumo: a transformação das pessoas em mercadoria”, Zygmunt Bauman afirma que na sociedade de consumidores não é possível se tornar sujeito sem, antes, virar mercadoria, uma vez que as questões de “subjetividade do sujeito, e a maior parte daquilo que essa subjetividade possibilita ao sujeito atingir, concentra-se num esforço sem fim para que ela própria se tornar, e permanecer, uma mercadoria vendável”.[17]

---

[16] LISSARDY, Gerardo. Despreparada para a era digital, a democracia está sendo destruída”, afirma o guru do “big data”. **BBC News Brasil**, 9 abr 2017. Disponível em: <https://www.bbc.com/portuguese/geral-39535650. Acesso em: 15 mar. 2023.

[17] BAUMAN, Zygmunt. **Vida para consumo**: transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar Editor, 2008, p. 20.

É, em razão disso, que a proteção dos dados pessoais passou a ser encarada por meio de uma ótica mais abrangente, compreendendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais.

A proteção de dados pessoais pode ser entendida, como uma autodeterminação do indivíduo, na escolha de uso das informações geradas ao longo de sua existência e faz-se imperativo estabelecer garantias, com o escopo de impedir a utilização indevida desses dados, de forma que não se sirvam para causar danos ou discriminação a quem quer que seja.[18]

No entendimento de Bruno Ricardo Bioni, o direito à proteção de dados pessoais deve ser alocado como uma nova espécie dos direitos da personalidade, conferindo elasticidade à tutela da pessoa humana, viabilizando seu desprendimento do direito à privacidade e, consequentemente, uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana.[19]

Neste ínterim, para um debate aprofundado acerca da proteção de dados pessoais, deve-se ter em mente o conceito de dados pessoais. Todavia, esse conceito não é nada sólido, uma vez que esse direito não se restringe apenas ao ordenamento jurídico, mas deve ser analisado sob o prisma do contexto histórico.

Para Alexandre Souza Pinheiro, o termo “dado” adveio do alemão *Datenschutz*, utilizado no início dos 1970, como meio de proteger os direitos individuais frente aos avanços tecnológicos. O autor afirma que o termo é inadequado pela falta de clareza, tendo sido apenas a “palavra errada no momento certo”.[20]

---

[18] SOUZA, L. R. M. Proteção de dados pessoais: estudo comparado do regulamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016. **Revista IDP**, Brasília, v. 1, n. 41, 2018.
[19] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 100.
[20] PINHEIRO, Alexandre Sousa (coord.). Comentário ao Regulamento Geral de Protecção de Dados. Coimbra: Edições Almedina, 2018, p. 429 e 430.

No entendimento de Danilo Doneda, o conceito de dado é aquilo que:

> [...] apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza.[21]

Em suma, os dados, sozinhos, não acrescem conhecimento e são fatos brutos dependentes de processamento e organização para serem convertidos em algo decifrável: a informação.[22]

Para Raymond Wacks, "dado" é a informação em potencial, sendo apta a transformar-se em informação se for comunicada, recebida e compreendida. Todavia, se o dado requer a interpretação do receptor, ele permanece no estado de pré-informação, até que seja efetivamente compreendido.[23]

Segundo Marcel Leonardi:

> [...] dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontre registrado (escrita, imagem, som ou vídeo). Entende-se por identificado o indivíduo que já é conhecido, e por identificável a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros.[24]

Por fim, cumpre transcrever o entendimento de Bruno Ricardo Bioni sobre o conceito de "dado":

> De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham disso utilizado de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação.[25]

---

[21] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019, p. 136.
[22] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 13.
[23] WACKS, R. Personal information: Privacy and the law. Oxford: Clarendon Press, 1989, p. 25 apud MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 56.
[24] LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2011, p. 76.
[25] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020a, p. 31-32.

Diante desse contexto, verifica-se que, embora se reconheça a privacidade como direito da personalidade, esse direito não vinha sendo adequadamente respeitado, especialmente no que concerne à existência de bancos de dados e à utilização de informações pessoais sem o consentimento de seu titular.

Portanto, o indivíduo passou a ser titular de um direito quanto à circulação de seus dados pessoais, reconhecendo-se ser uma violação à dignidade da pessoa humana a utilização de suas informações pessoais sem a sua anuência, em atenção à autonomia privada.

Destaca-se, que a disciplina jurídica da proteção de dados pessoais, no direito europeu, é altamente desenvolvida e de vanguarda em relação à matéria, principalmente, em relação ao Regulamento Geral de Proteção de Dados.[26]

A partir da revolução dos meios digitais, houve a expansão das possibilidades de coleta e de exploração de dados e informações.[27] Por outro lado, o tratamento desses dados atribuiu valor a tais informações, permitindo que seja possível rastrear perfis de consumo, posições políticas e outras informações que podem ser usadas mercadologicamente.

Em razão dessas alterações na organização social, política e econômica, surgiu a chamada “sociedade da informação”, que motivou a necessidade de a União Europeia reconsiderar a tutela dos direitos de seus cidadãos, visando resguardar seus princípios fundamentais.

O principal marco quanto à proteção de dados pessoais, como um direito fundamental, é a Convenção Europeia dos Direitos Humanos, de 04 de novembro de 1950.

Todos os Estados que compõem a União Europeia são signatários da referida Convenção e aqui cabe destacar seu artigo 8º, que dispõe sobre o direito à vida privada e familiar, ao domicílio e à correspondência:

---

[26] Sobre o direito europeu em geral, consultar, dentre outros: STREINZ, R. Europarecht; OPPERMANN, Thomas. Europarecht.

[27] SOLOVE, Daniel. Privacy and Power: Computer Databases and Metaphors for Information Privacy. **Stanford Law Review**, v. 53, p. 1394, 2000-2001.

> Art. 8º da CEDH: 1. Qualquer pessoa tem direito à liberdade de pensamento, de consciência e de religião; este direito implica a liberdade de mudar de religião ou de crença, assim como a liberdade de manifestar a sua religião ou a sua crença, individual ou coletivamente, em público e em privado, por meio do culto, do ensino, de práticas e da celebração de ritos. 2. A liberdade de manifestar a sua religião ou convicções, individual ou coletivamente, não pode ser objeto de outras restrições senão as que, previstas na lei, constituírem disposições necessárias, numa sociedade democrática, à segurança pública, à proteção da ordem, da saúde e moral públicas, ou à proteção dos direitos e liberdades de outrem.

Nos anos subsequentes, surgiram leis nos demais países europeus. Em 1970, a Alemanha elaborou a Lei Hessiana de Proteção de Dados Pessoais[28], identificada como o primeiro diploma normativo que trata especificamente dessa matéria. Trata-se de uma lei sintética (composta por 17 artigos) e se concentrava em disciplinar a atividade de centros de processamento de dados de instituições e sujeitos submetidos à autoridade do Land.

A mencionada lei do Estado alemão utilizou pela primeira vez o termo “proteção de dados” (*Datenschutz)*, em vez que optar por fórmulas já estabelecidas na legislação alemã como a *Datensicherung* ou *Datensicherheit*, ambos referentes à segurança da informação.[29]

Neste sentido, Herbert Bukert explica:

> Na perspectiva anterior, a lei atendia aos receios de comunidades locais do que era visto como o poder inerentemente centralizador da máquina, que seria capaz de modificar o balanço de poderes a favor do Estado [...] A Lei de Hesse de 1970 era diferente porque, pela primeira vez, cláusulas de confidencialidade foram alçadas ao nível de lei, onde elas estavam par a par com outras cláusulas que abordavam outros conflitos de poder.[30]

---

[28] A Lei de Proteção de Dados do Land alemão de Hesse foi promulgada em 30 de setembro de 1970. Hessisches Datenschutzgesetz (The Hesse Data Protection Act), Gesetz und Verordungsblatt I (1970), p. 625.

[29] FUSTER, Gloria González. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Springer: Brussels, 2014, p. 56.

[30] The former law addressed the fear of local communities of what they saw as the inherent centralizing power of the machine that would shift their traditional power and influence to the Land [state]. […] The Hesse Law of 1970 was different because for the first time these confidentiality clauses were lifted to the level of a formal law, where they stood side by side with those clauses that addressed the other power conflicts mentioned above” (tradução livre) (BURKERT, Herbert. Privacy-Data Protection: a German/ European perspective. In: ENGEL, C.; KELLER, K. H. (ed.). **Governance of Global Networks in the Light of Differing Local Values**. Baden-Baden: Nomos, 2000, p. 46).

Na década seguinte, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[31] finalizou as diretrizes para a regulação de proteção de dados, com o *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[32], na busca por um ambiente seguro para a transferência de dados pessoais entre países.

Os seguintes países adotaram, parcialmente, as instruções do referido guia: Estados Unidos, Canadá, Alemanha, Suíça, Austrália e Nova Zelândia. A União Europeia adotou, também, parcialmente o modelo proposto pelas diretrizes.

No ano seguinte, foi dado o primeiro passo para um sistema integrado europeu de proteção de dados pessoais, com a Convenção n.º 108 de 1981, denominada Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais.

Essa Convenção exigia, em seu artigo 15, que os países signatários deveriam constituir uma ou mais autoridade responsável por assegurar a observância da convenção, com poderes de investigação e de sanção, atuando de forma independente e imparcial, o que se conhece, atualmente, por autoridade de controle.

Ademais, ela teve importância fundamental por se tratar do único tratado internacional sobre proteção de dados, levando os demais países a adequarem suas legislações e incentivando aqueles órfãos de leis de proteção de dados pessoais.

Além disso, elencou as competências e deveres dos titulares e dos responsáveis pelo tratamento, trazendo o princípio da qualidade do tratamento de dados.[33]

---

[31] Organização multilateral cujo objetivo é promover políticas que melhorem o bem-estar econômico e social, recomendando, com base em experiências empíricas, políticas por meio da cooperação e de ações coordenadas.

[32] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. **OECD** – Better Policies for better lives, 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 28 ago. 2022.

[33] Esse princípio consubstancia-se na garantia, assegurada aos titulares dos dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. A LGPD adotou esse princípio em seu artigo 6º, inciso V.

Segundo Danilo Doneda, a Convenção n.º 108, de 1981, também chamada de Convenção de Estrasburgo, é o:

> principal marco de uma abordagem da matéria [de proteção de dados] pela chave dos direitos fundamentais", considerando que conecta a proteção dos direitos humanos e das liberdades fundamentais diretamente à proteção de dados pessoais, ainda no preambulo e a percebe como pressuposto do estado democrático de direito, referenciando a já citada Convenção Europeia para os Direitos do Homem.[34]

Em 1995, a União Europeia, por meio da Diretiva n.º 95/46/CE[35], padronizou a proteção de dados pessoais e estabeleceu que os Estados-Membros deveriam inserir em suas legislações internas normas para resguardar os dados pessoais, definindo-os na seguinte forma:

> Artigo 2º
> Qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

Tal definição foi desenvolvida amplamente, com o intuito de abranger o maior número de situações possíveis. Além disso, estabeleceu a exigência da criação de autoridades públicas independentes, encarregadas pela fiscalização da aplicação do sistema regulatório de proteção de dados, as chamadas autoridades de controlo.

> Artigo 28º
> Autoridade de controlo
> 1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente directiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas. [...] (Tradução livre).[36]

---

[34] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, Joaçaba, v. 12, n. 2, jul./dez., 2011, p. 102.

[35] A imprescindibilidade de entidades tuteladoras dos dados pessoais já era prevista nas Diretrizes da OCDE, sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, de 1980, focada nas relações internacionais necessárias para a efetivação das Diretrizes; assim como na Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, datada de 1981. OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. **OECD** – Better Policies for better lives, 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 20 abr. 2020. CONSELHO DA EUROPA. **Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Estrasburgo**, 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em 19 fev. 2023.

[36] JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. **DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO**. De 24 de Outubro de 1995, relativa à protecção das pessoas singulares

Sem nenhuma dúvida, a Diretiva n.º 95/46/CE constituiu um marco histórico, estabelecendo um quadro geral na União Europeia sobre o tema proteção de dados. Todavia, a Diretiva foi instaurada em um período que a internet não fazia parte da sociedade no geral, apresentando obstáculos menores se comparados com os atuais, na busca pela proteção de dados.

Nos anos 2000, foi editada a Diretiva n.º 58 do Parlamento e Conselho Europeu, relativa ao tratamento dos dados pessoais e à proteção da privacidade no contexto das comunicações eletrônicas, ficando conhecida como *ePrivacy Directive*.

A esse respeito, Cintia Rosa Pereira de Lima ensina:

> A *ePricavy Directive* foi uma resposta à economia informacional acima destacada, na medida em que impõe limites à coleta, armazenamento e utilização de dados pessoais no contexto das comunicações eletrônicas, independemente da tecnologia utilizada. Assim, essa Diretiva traz como seu objetivo principal reduzir ao mínimo o tratamento de dados pessoais e de utilizar, quando necessário, mecanismos que assegurem o anonimato do usuário.[37]

Nos anos seguintes, a Comissão Europeia, em janeiro de 2012, preocupada com os desafios atuais do mundo digital, visou adequar as regras em vigor, por meio de uma reforma global do regramento presente na União Europeia.

Destaca Eduardo Magranique:

> Desta forma, iniciou-se estudos que se focavam (i) nos impactos das novas tecnologias; (ii) na falta de harmonia entre os Estados-Membros; (iii) na globalização e na internacionalização das transferências de dados; (iv) na necessidade de garantir cumprimento efetivo; e (v) na menor fragmentação dos instrumentos. O GDPR foi proposto em 2012 pela Comissão Europeia e seguiram quatro anos de intensas negociações entre o Parlamento Europeu e o Conselho da União Europeia, até que, em abril de 2019, a versão final foi publicada.[38]

---

no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046t&from=PT

[37] LIMA, Cíntia Rosa Pereira de. **A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.** 487 p. Tese (Livre Docência), Universidade de São Paulo, Ribeirão Preto-SP, 2015, p. 153-154.

[38] MAGRANI, Eduardo. **Entre dados e robôs**: Ética e privacidade na era da hiperconectividade, 2ª ed., Porto Alegre: Arquipélago Editorial, 2019.

Então, editou-se o Regulamento Geral de Proteção de Dados Pessoais Europeu n.º 679, identificado como *General Data Proteccion Regulation* (GDPR)[39], que serviu de inspiração para o surgimento de diversas legislações pelo mundo, com sua entrada em vigor em 25 de maio de 2018.[40]

Neste sentido, o GDPR consolidou os conceitos e unificou a legislação entre os Estados-membros, criando mecanismos efetivos para garantir o cumprimento de suas disposições.

Em razão da pluralidade de normas, os agentes com atuação em mais de um Estado-membro da União Europeia viam-se obrigados a adequar suas regras de *compliance* e o procedimento de tratamento dos dados pessoais, considerando as particularidades da legislação de cada um dos 28 Estados-membros.

Ademais, o regulamento geral causou um efeito cascata, uma vez que estabeleceu a exigência aos países e empresas que buscassem manter relações comerciais com a União Europeia, que já tivessem uma legislação proteção de dados robusta e estruturada.

Em contrapartida, aqueles que não tivessem tal regulamentação, passariam a sofrer algum tipo de impedimento econômico e comercial, em razão das dificuldades em estabelecer negócios com países integrantes da União Europeia.

Dentre as mudanças trazidas pelo GDPR, destaca-se que as empresas que oferecem bens e serviços na União Europeia e lidam com o tratamento de dados pessoais de pessoas residentes no seu território devem demonstrar claramente que podem processar esses todos, comprovando o consentimento do usuário.

---

[39] A despeito da diferença entre diretiva e regulamento. “Um Regulamento é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da EU, não carecendo de transposição para a ordem jurídica nacional. Tem um caráter geral e é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros (art. 288º, do Tratado sobre o Funcionamento da União Europeia). Uma directiva é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a país elaborar a sua própria legislação para dar cumprimento a esse objetivo (art. 288º do Tratado sobre o Funcionamento da União Europeia).” (FERREIRA, Manuel. **O Regulamento Geral sobre a Proteção de Dados**: os aspectos legais e organizativos de governança nas organizações. Aspectos legais e organizativos de governança nas organizações. 2018. 103 f. Dissertação (Mestrado) – Curso de Direito e Segurança, Direito, Universidade Nova de Lisboa, Lisboa, 2018, p. 23-24. Disponível em https://run.unl.pt/bitstream/10362/54953/1/ManuelFerreira_2018.pdf. Acesso em: 22 fev. 2023).

[40] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais** – comentários à Lei 13.709/2018. São Paulo: Saraiva, 2019, p. 19.

> Do ponto de vista operacional, a exigência de ter de comprovar a conformidade com o regulamento muda a forma de encarar a problemática da proteção de dados dentro das organizações. Até maio de 2018, a proteção de dados foi regulada numa perspectiva de hetero-regulação, em que a necessidade de garantir a licitude do tratamento, através dos princípios e condições de legitimidade, ocorria essencialmente na fase inicial, pelos meios definidos pela autoridade de controle (notificação, uma licença ou autorização, por exemplo). Após a entrada em aplicação do RGPD, estamos perante uma nova realidade. O responsável pelo tratamento tem que conseguir, em qualquer momento do processo de tratamento de dados pessoais, a sua licitude e cumprimento com a RGPD, criando evidências para que o possa comprovar, ficando assim sujeito à fiscalização e supervisão da autoridade de controle [...].[41]

Portanto, antes mesmo da LGPD, o Brasil sentiu os efeitos do GDPR. Apesar de ser restrita aos cidadãos da União Europeia, a norma afetou abundantemente empresas e organizações ao redor do mundo, uma vez que todas estão inseridas em uma sociedade amplamente globalizada e conectada.

Logo, todas as empresas que trabalham com informações de cidadãos europeus, precisam estar em conformidade com o GDPR, mesmo que sejam brasileiras. Em razão disso, muitas empresas brasileiras passaram a atender as exigências da lei europeia.

Desta forma, influenciado pela criação do regulamento europeu, o Brasil evoluiu sua legislação sobre o tema, como será abordado a seguir.

1.2. Evolução Legislativa Brasileira na busca pela Tutela da Proteção de Dados Pessoais

O tratamento de dados tornou-se um verdadeiro ativo do capitalismo da sociedade da informação, revisitando as discussões sobre o tema.

---

[41] FERREIRA, Manuel. **O Regulamento Geral sobre a Proteção de Dados**: os aspectos legais e organizativos de governança nas organizações. Aspectos legais e organizativos de governança nas organizações. 2018. 103 f. Dissertação (Mestrado) – Curso de Direito e Segurança, Direito, Universidade Nova de Lisboa, Lisboa, 2018. Disponível em https://run.unl.pt/bitstream/10362/54953/1/ManuelFerreira_2018.pdf. Acesso em: 22 fev. 2023.

No Brasil, o assunto era tratado, indiretamente, por diversos fragmentos espalhados pelo ordenamento jurídico, até o sancionamento da Lei Geral de Proteção de Dados. A Constituição Federal de 1988 deu ao direito à privacidade um *status* constitucional, em decorrência do artigo 5º, inciso X e XII.

> A Constituição de 1988 foi o primeiro texto normativo a positivar o direito à privacidade na estrutura legislativa brasileira. Fato que decorre principalmente de ela ter sido elaborada em um momento de retomada da democracia, após o término da ditadura militar, e o início da popularização das tecnologias de comunicação. Entretanto, "a ausência de um sistema normativo do direito à privacidade, alocado implicitamente na Constituição Federal (Art. 5º, inc. X) e transposto no art. 21, do CC/2002, dificultou sua promissora evolução, na medida em que restou subsidiário ao direito de personalidade, tido como regra, e aquele – intimidade e vida privada – pro instrumento deste".[42]

No âmbito infraconstitucional, o Código de Defesa do Consumidor (CDC), trouxe a proteção dos consumidores com relação à utilização de informações em banco de dados e cadastros de empresas.

Referida legislação consumerista provocou inúmeras mudanças, no ordenamento jurídico, como explica Silvio de Salvo Venosa, resumidamente:

> Seu caráter é interdisciplinar, daí porque se diz que criou um microssistema jurídico. Nele há normas de direito civil, direito comercial, direito administrativo, direito processual, direito penal. Seus princípios abarcaram direito privado e direito público, formando um terceiro gênero que a doutrina denomina direito social.[43]

O CDC, além de assegurar um melhor direito aos consumidores, preocupou-se com a regulamentação dos bancos de dados, em seu artigo 43, em razão da vulnerabilidade dos consumidores nas relações de consumo, principalmente, quando da coleta de dados para elaborar o perfil de consumo, acarretando eventual tratamento discriminatório.

---

[42] ROTUNDO, Rafael P. Proteção de Dados. **Revista de Direito Privado**, São Paulo, v. 74, ano 18, p. 133-158, fev. 2017, p. 146.
[43] VENOSA, Silvio de Salvo. **Direito Civil: Responsabilidade civil.** 7.ed. São Paulo: Atlas, v. 4, 2007.

Nesse sentido, ao abordar a questão, Laura Schertel Mendes expressa que:

> Ao se examinar o tratamento de dados pessoais realizado no âmbito da relação de consumo, é fundamental se considerar a vulnerabilidade do consumidor nesse processo. Isso porque os dados pessoais, assim como as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme a sua utilização. O risco ao consumidor que tem os seus dados coletados e processados ocorre, principalmente, quando o tratamento dos dados é realizado de forma equivocada ou discriminatória, acarretando a sua classificação e discriminação no mercado de consumo. Isso acaba por afetar expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais.[44]

Bruno Ricardo Bioni, por sua vez, afirma que “o CDC buscou conferir a autodeterminação informacional, o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento”.[45]

Nesta esteira, é possível verificar a intenção do legislador de garantir a maior proteção aos consumidores e relação de confiança entre fornecedores e consumidores.

Todavia, passados mais de trinta anos da criação do CDC, os desafios renovam-se, em especial ao progressivo surgimento de novas tecnologias, que impactam as operações das empresas, estremecendo as relações de consumo.

Retomando à evolução legislativa, em 2002, o Código Civil trouxe um rol de direito da personalidade, incluindo o direito à privacidade, em consonância aos dispositivos legais já existentes à época.

---

[44] MENDES, Laura Schertel. **Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor.** 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502218987/ >. cesso em: 31 mai. 2019.

[45] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 147.

Contudo, como Anderson Schreiber explica, o tema não adequadamente abordado pela legislação:

> A verdade é que o Código Civil brasileiro deu à privacidade um tratamento inadequado. Em primeiro lugar, dedicou um único artigo à matéria, cuja importância se renova a cada dia na sociedade contemporânea [...]. Não obstante isso, empregou a expressão vida privada, revelando certa indiferença à recente evolução do conceito de privacidade, que abandonou uma concepção mais restrita, limitada ao círculo de intimidade da pessoa humana, para abarcar a proteção aos dados e informações pessoais. Sobre esse último aspecto, a codificação não trouxe uma palavra sequer. Não é exagero dizer que o código civil ignorou a vasta amplitude do tema, cuja compreensão é essencial para perceber o importante papel reservado à tutela da privacidade no século XXI.[46]

No ano de 2011, foi promulgada a Lei do Cadastro Positivo[47] (Lei n.º 12.414/2011), a qual autorizou e regulamentou a formação e a consulta a banco de dados com informações de pessoas físicas e jurídicas adimplentes.

O Cadastro Positivo é um banco de dados, com informações relativas às operações de créditos de pessoas físicas e jurídicas e, após a promulgação da supracitada lei, as empresas elaboraram um histórico de crédito dos consumidores, definindo, assim, condições comerciais, preços e taxas ajustados ao perfil de cada consumidor.

A discussão acerca do cadastro positivo se deu por conta do *credit score*, um sistema de avaliação de risco de crédito, que utiliza diversos bancos de dados para aferir o grau de solvência do consumidor.

Em decorrência das controvérsias sobre o assunto, o Superior Tribunal de Justiça (STJ) editou a súmula n.º 550, que dispôs sobre o sistema de avaliação de crédito, que dispensa o consentimento do consumidor, o qual pode solicitar esclarecimentos sobre as informações pessoais valoradas e sua respectiva fonte.

Em 2012, a Lei Carolina Dieckman (Lei n.º 12.737/2012) veio para criminalizar a obtenção e uso indevido de dados pessoais por meio de aparelho eletrônico. Referida lei representou um marco inicial para a proteção dos dados pessoais dos cidadãos contra os criminosos virtuais.

---

[46] SCHREIBER, Anderson. **Direitos da personalidade.** 3. ed. São Paulo: Atlas, 2014, p. 136.

[47] O Cadastro Positivo é um banco de dados, com informações relativas às operações de crédito quitadas ou em andamento de todas as pessoas físicas e jurídicas.

Das legislações acima apresentadas, pode-se verificar que, até o ano de 2018, não existia, no ordenamento jurídico brasileiro, uma lei específica para a proteção de dados, como na União Europeia.

No entanto, reconhece-se que os casos relacionados à violação de proteção de dados ocorridos, no contexto internacional, em muito influenciaram os projetos de lei em tramitação perante o Congresso Nacional.

Dentre os quais, podem ser citados os documentos divulgados por Edward Snowden[48], em 2013, os quais demonstram que a agência de segurança nacional norte-americana monitorava milhões de telefones e dados de usuários *online*, coletando números de telefones, horário e duração de chamadas nos Estados Unidos e em países estrangeiros.

As denúncias de espionagem e violação de privacidade serviram de munição, para o governo brasileiro agilizar aprovação de um projeto de lei, visando regulamentar os direitos dos usuários da internet no Brasil.

O assunto já era discutido desde 1999, com a tramitação do Projeto de Lei n.º 84/1999, de autoria do ex-Deputado Luiz Piauhylino, sendo alvo de inúmeras críticas "devido ao seu potencial vigilantista". Porém, após dez anos, o Comitê Gestor da Internet no Brasil – CGI.br, vinculado ao Ministério das Comunicações, da Ciência e da Tecnologia, aprovou o "Decálogo do CGI.br" – documento que serviu de inspiração para a criação do Marco Civil da Internet e ampliação do nível de debate sobre o tema.[49]

[48] Edward Joseph Snowden é um ex-colaborador de agências de inteligência americanas (CIA e NSA), que tornou públicos detalhes dos programas de vigilância global do Governo dos Estados Unidos, com a divulgação de documentos internos confidenciais. Diante da acusação de diversos crimes pela retenção e divulgação de documentos internos pelo Estados Unidos, desde 2013 Snowden se encontra em asilo político (Hong Kong, Equador e Rússia), atualmente residindo em Moscou. No final de 2019, Snowden manifestou interesse em retornar para os Estados Unidos, desde que receba julgamento justo.

[49] OBSERVATÓRIO DO MARCO CIVIL DA INTERNET. **Histórico do Marco Civil**. Disponível em: http://www.omci.org.br/historico-do-marco-civil/timeline/#0. Acesso em 23 fev. 2023.

Em 2011, adveio o Projeto de Lei n.º 2.126, apresentado pelo Poder Executivo, com o escopo de “estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil”[50]. Assim, devido ao efeito Snowden, o Governo Federal pediu agilidade ao Congresso Nacional para aprovar o Projeto de Lei do Marco Civil da Internet no Brasil.

No ano de 2014, a Lei n.º 12.965, que ficou conhecida como Marco Civil da Internet, estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Essa lei foi o primeiro marco regulatória brasileiro específico para proteção dos direitos fundamentais da intimidade e da liberdade de expressão no uso da internet. Para Ronaldo Lemos, “a situação pré-Marco Civil era de completa ausência de regulamentação civil da internet no país”.[51]

Embora, o Marco Civil da Internet regulamentou e assegurou a liberdade de expressão, e, ao mesmo tempo, protegeu a intimidade e a vida privada, ele se absteve de regulamentar a proteção dos dados pessoais, restringindo-se apenas a dispor que tal proteção se dará na forma da lei.

Em seu artigo 7º, ficou assegurado ao usuário a inviolabilidade da intimidade e da vida privada, sua proteção e possível indenização pelo dano material ou moral decorrente de sua violação; garantiu o sigilo do fluxo de suas comunicações pela internet; manteve o sigilo das comunicações privadas armazenadas e proibiu o fornecimento a terceiros dos dados pessoais dos usuários, inclusive registros de conexão e de acesso a aplicações da internet, salvo mediante consentimento livre, expresso e informado.

---

[50] BRASIL. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 2126/2011**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255. Acesso em: 23 fev. 2023.

[51] LEMOS, Ronaldo (Org). **Marco Civil da Internet**. 1ª ed. São Paulo. Atlas, 2014.

No entanto, apesar do arcabouço protetivo disposto pelo Marco Civil da Internet, pode-se dizer que a proteção de dados pessoais era uma norma de eficácia limitada.[52] Logo, a norma carecia da edição de outra legislação para obter aplicação integral.[53]

Assim, pode-se dizer que, ao passo que o efeito Snowden influenciou na promulgação da Lei do Marco Civil da Internet, o caso da empresa *Cambrigde Analytica,* influenciou a LGPD no Brasil e, o GDPR na União Europeia.

Em síntese, a empresa *Cambrigde Analytica* teria coletado dados dos eleitores e traçado o perfil, na campanha presidencial, do presidente dos Estados Unidos da América, Donald Trump, eleito em 2016. Ele contratou a *Cambrigde Analytica* para fazer o gerenciamento de dados de potenciais eleitores nas redes sociais, revolucionando o modo de fazer campanha eleitoral.

> A polêmica pesquisa realizada pela *Cambridge Analytica,* a qual corroborou com a eleição de Donald Trump nos Estados Unidos da América, realizava a coleta de dados pessoais dos usuários e seus amigos no *Facebook*. Para tanto, um terceiro desenvolveu um aplicativo que por meio de um teste de personalidade na rede social, obteve os dados dos participantes e de sua rede de contato, mediante uma falsa promessa de uso fins acadêmicos e de ausência de qualquer menção ao compartilhamento de dados, a empresa vendeu os resultados obtidos para a *Cambridge Analytica* que os utilizou para personalizar campanhas pró Donald Trump e impulsionar notícias em desfavor de sua adversária, culminando, assim, para a eleição do então candidato republicano. Tal violação foi um dos pilares na aplicação de uma das multas mais altas acerca da proteção de dados pela agência federal dos Estados Unidos da América FTC (*Federal Trade Comission*). A rede social pagou US$ 5 bilhões e foi submetida a novas restrições sobre a privacidade de seus usuários, em sua decisão a FTC alegou que a rede violou uma ordem da agência americana ao ludibriar os usuários sobre sua capacidade de controlar a privacidade de suas informações pessoais.[54]

---

[52] MENDES, G. F.; BRANCO, P. G. G. **Curso de Direito Constitucional.** 13 ed. São Paulo: Saraiva Educação (Série IDP), 2018, p. 69-70. Sabe-se que o tema “aplicabilidade das normas constitucionais”, bem como que a eficácia limitada das normas se relaciona apenas à Constituição. Todavia, para o melhor esclarecimento acerca do tema, peço vênia para aplicar a conceituação através da doutrina constitucional de forma didática.

[53] Art. 3º, da Lei do Marco Civil: A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] III - proteção dos dados pessoais, na forma da lei.

[54] MONTEIRO, Renato Leite. **Cambridge Analytica e a nova era Snowden na proteção de dados pessoais.** El país. Brasil. 20 de março de 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/20/tecnologia/1521582374_496225.html. Acesso em 02 jun. 2023.

Por fim, a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709), mais conhecida por sua sigla – LGPD – foi sancionada em 14 de agosto de 2018, tornando-se a primeira lei brasileira com objetivo de tutelar dados pessoais[55].

Ela foi editada para proteger os dados de pessoas físicas, com fundamento nos direitos fundamentais da liberdade de expressão, privacidade e o livre desenvolvimento da personalidade da pessoa natural, *in verbis:*

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Importante destacar que a LGPD não visa proibir, tampouco impedir, qualquer tipo de operação com dados pessoais, mas sim protegê-los, por meio de regras específicas, para tais operações serem realizadas com segurança.

Nesse sentido, resta evidente que a LGPD não tem o intuito de engessar o desenvolvimento tecnológico e econômico, mas simplesmente regulamentar o tratamento dos dados para serem utilizados de forma ética, responsável e sob o amparo legal.

Importa destacar ainda que o direito fundamental à proteção de dados já havia sido reconhecido pelo Supremo Tribunal Federal (STF), no julgamento do caso do Instituto Brasileiro de Geografia e Estatística (IBGE), de relatoria da Ministra Rosa Weber.

---

[55] BIONI, Bruno R. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 344.

A decisão foi proferida quando referendada a medida cautelar nas Ações Diretas de Inconstitucionalidade n.º 6387, 6388, 6389, 6393, 6390, suspendendo a aplicação da Medida Provisória n.º 954/2018, que obrigava as operadoras de telefonia a repassarem ao IBGE dados identificados de seus consumidores de telefonia móvel e fixa, em nome do combate à pandemia de COVID-19.

O STF reverteu o entendimento histórico de trinta anos, de reconhecer o direito fundamental à proteção de dados com base nos incisos X e XII, do artigo 5º, da Constituição Federal.

Isso porque, até então, prevalecia uma interpretação cristalizada nos anos 1990 na Suprema Corte, segundo o qual o sigilo de dados era um sigilo sobre a transmissão de dados, e não sobre os dados em si.

Assim, um dos aspectos mais importantes da decisão é a consolidação do dado pessoal como merecedor da tutela constitucional, afastando-se a ideia de que existem dados pessoais neutros, insignificantes, desprovidos de proteção.[56]

1.3. Proteção de Dados Pessoais como Direito Fundamental no Brasil

Os direitos fundamentais destinam-se a estabelecer deveres, direitos e garantias dos cidadãos, normatizando as hipóteses que orientam a vida social, políticas e jurídica dos cidadãos[57].

---

[56] ADI n.º 6387. Rel. Min. Rosa Weber. Voto do Ministro Ricardo Lewandowski: “Aliás, todos nós sabemos que, nos dias que correm, o número de uma linha celular, por exemplo, tem a finalidade muito maior do que, singelamente, servir para que pessoas telefonem umas paras as outras. Na verdade, esse número serve como chave de identificação e de acesso a um universo de plataformas eletrônicas, como bancos, supermercados, serviços públicos e rede sociais, todos elas detentos das mais variadas informações sobre o titular daquela linha telefônica. [...] É preciso ficar claro, portanto, que não se está a falar de informações insignificantes, mas da chave de acesso a dados de milhões de pessoas, com alto valor para execução de políticas públicas, é verdade, mas também com provável risco de adoção de expedientes, por vezes, dissimulados, obscuros, que possam causar desassossego na vida diária do indivíduo”.

[57] LEONEL, Vilson; MOTTA, Alexandre de Medeiros. **Ciência e Pesquisa.** 3. ed. Palhoça: UnisulVirtual, 2011, p. 108.

Sobre o assunto, Noberto Bobbio ensina que:

> Os direitos fundamentais assumem posição de definitivo realce na sociedade quando se inverte a tradicional relação entre Estado e indivíduo e se reconhece que o indivíduo tem, primeiro, direitos, e, depois, deveres perante o Estado, e que os direitos que o Estado tem em relação ao indivíduo se ordenam ao objetivo de melhor cuidar das necessidades dos cidadãos.[58]

Em complemento, José Afonso da Silva leciona que os direitos fundamentais:

> [...] também são prerrogativas que garantem uma convivência digna, livre, igual entre as pessoas, e além disso, trata-se de uma situação jurídica sem a qual a pessoa humana não se realiza e são fundamentais no sentido de não apenas serem reconhecidos pelo ordenamento jurídico, mas também em serem concretamente efetivados.[59]

Portanto, pode-se dizer que os direitos fundamentais decorrem de um marco histórico que causou diversos impactos negativos, que levaram à positivação para a concretização destes direitos.

Neste sentido, antes mesmo da positivação da LGPD, a preocupação com a proteção de dados pessoais no Brasil, era um assunto em destaque. Em meados de 2019, o tema se tornou objeto da Proposta de Emenda Constitucional n.º 17[60], proposta pelos senadores Eduardo Gomes, de relatoria da senadora Simone Tebet, visando alterar a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais (artigo 5º, XX, CF) e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais (artigo 22, XXX, CF).

Entretanto, apenas no ano de 2022, a proteção de dados pessoais alcançou o título de direito fundamental[61], por meio da Emenda Constitucional n.º 115/22,[62] sendo publicada no dia 10 de fevereiro de 2022, no Diário Oficial da União.

---

[58] BOBBIO, Noberto. **A era dos direitos.** Rio: Campos, 1992, p. 4

[59] SILVA, José Afonso da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, 2014. p. 178.

[60] CÂMARA DOS DEPUTADOS. **PEC 17/2019**. Disponível em:< https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 20 dez. 2022.

[61] Art. 5º, inciso LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[62] Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Com a aprovação, a proteção de dados passou a ser considerada uma cláusula pétrea no ordenamento jurídico brasileiro (art. 60, § 4º, inciso IV, CF/88) e, portanto, está imune a qualquer supressão de seu predicativo normativo, uma vez que seu conteúdo axiológico ressalta valores protegidos constitucionalmente.

Além disso, a promulgação da EC n.º 115/2022 evidencia a distinção entre a proteção de dados e privacidade, essa última já prevista no inciso X, do artigo 5º da Constituição Federal.

A EC n.º 115/2022 é fruto de discussões históricas que levaram à elevação do direito à proteção de dados como direito fundamental.

Segundo Bobbio, os direitos fundamentais representam uma construção história, e por mais fundamentais que pareçam, são construídos por meio de lutas em defesa do reconhecimento de direitos, constituídos gradualmente com novas gerações de direitos.[63]

Neste sentido, Laura Schertel Mendes entende que reconhecer a proteção de dados como um direito fundamental não é apenas uma possibilidade, sendo também "uma necessidade para tornar efetivos os fundamentos e princípios do Estado Democrático de Direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal".[64]

Mas não foi só isso, a emenda em estudo também valorizou a atuação da Autoridade Nacional de Proteção de Dados, como entidade independente responsável pela uniformização e consistência na aplicação da LGPD, afastando eventuais incertezas quanto à competência para fiscalização da proteção de dados.

Portanto, a proteção de dados pessoais, com perspectiva de direito fundamental, incorpora à espera jurídica do titular mais um mecanismo de proteção aos direitos de personalidade, com foco na imagem e na honra da pessoa natural.

---

[63] BOBBIO, Noberto. **A era dos direitos.** Rio: Campos, 1992.

[64] MENDES, Laura Schertel. **Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor**. 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502218987/>. Acesso em: 23 mar. 2023.

Além disso, o reconhecimento da proteção de dados pessoais, como direito fundamental, também traz benefícios de ordem econômica, elevando o grau de segurança da informação, maior visibilidade junto à comunidade internacional, o que fortaleceu o relacionamento do Brasil com os países com alto nível de adequação à proteção de dados, como é o caso dos países da União Europeia.

Por fim, cabe aduzir que a Emenda Constitucional n.º 115/2022 ainda fixou a competência material para a União organizar e fiscalizar a proteção e o tratamento de dados pessoais e, também, conferiu competência privativa à União para legislar sobre a proteção de dados pessoais, buscando a uniformidade na produção legislativa, aumentando a segurança jurídica quanto ao tema.[65]

Nessa conjectura percebe-se a importância que concedida à defesa dos dados pessoais, equiparando esse direito à vida, liberdade, igualdade etc., além de potencializar a necessidade de as empresas tentarem se adequar o mais rápido possível às exigências da LGPD, já que, agora, não estão somente indo em desencontro com uma legislação infraconstitucional, mas sim, ferindo direito constitucional.

[65] Art. 21, inciso XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. Art. 22, inciso XXX - proteção e tratamento de dados pessoais.

2. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Após um longo trabalho multisetorial desde 2010, o tema proteção de dados passou a ser tratado no Congresso Nacional, a partir da propositura do Projeto de Lei n.º 4.060, de iniciativa do deputado Milton Monti e do Projeto de Lei do Senado n.º 330, do senador Antônio Carlos Valadares.

Todavia, apenas em 14 de agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), que passou a dispor sobre a proteção de dados pessoais, além de alterar a Lei n.º 12.695/2014 (Lei do Marco Civil da Internet).

A LGPD tornou-se a primeira lei brasileira, para regular o tema da proteção de dados pessoais, pois, até o momento, não havia uma lei específica em nosso ordenamento jurídico. Diante de tal cenário, o Brasil se nivelou a diversos modelos internacionais com um alto padrão de proteção de dados.[66]

Nesse sentido, o Brasil estabeleceu parâmetros normativos no que tange à proteção de dados pessoais, agregando maior segurança jurídica à coleta e ao tratamento de dados pessoais e aos demais aspectos ligados à inovação tecnológica, instituindo mecanismos para garantir seu cumprimento de forma igualitária, instituindo, por exemplo, a Autoridade Nacional de Proteção de Dados.

Para Patrícia Peck Pinheiro, a lei de proteção de dados “reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas, cujo lastro se funda na proteção de direitos humanos”.[67]

---

[66] “É perceptível que no Brasil não há uma cultura de proteção de dados como na União Europeia, por exemplo. E para que essa mudança ocorra, é necessário que o titular dos dados compreenda a importância de seus dados e o valor que possuem. Ações de conscientização serão imprescindíveis para que os titulares entendam seus direitos. Noutro giro, as empresas precisam internalizar a cultura de privacidade e de proteção de dados sem criar barreiras para o desenvolvimento e construção desse novo ecossistema.” LIMA, Ana P. M. C. de; ALMEIDA, Dionice de; MAROSO, Eduardo P. **LGPD – Lei Geral de Proteção de Dados: sua empresa está pronta?** São Paulo: Literare Books International, 2020, p. 48

[67] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2019 (LGPD). São Paulo: Saraiva, 2018, p. 15.

Neste mesmo viés, Bruno Ricardo Bioni define a Lei Geral de Proteção de Dados como:

> Uma lei que terá um impacto econômico-social e regulatório como poucas outras tiveram na história do país, suplantável ao que foi o Código de Defesa do Consumidor e a Consolidação das Leis Trabalhistas. (...) Em razão desse contexto, leis gerais de proteção de dados pessoais, como a Lei 13.709/2018, são elevadas, por vezes, ao patamar de um novo contrato social. Nelas se encontram as "regras do jogo" para o próprio funcionamento pacífico e democrática da sociedade.[68]

Portanto, pode-se dizer que o Estado perdeu seu monopólio do controle de dados para fornecer maior autonomia e protagonismo para outras entidades, como empresas privadas e até mesmo para o indivíduo, titular dos próprios dados pessoais.

2.1. Principais Aspectos Gerais

Após uma análise sobre a evolução mundial do direito à privacidade até o surgimento da LGPD, é necessário delimitar os principais aspectos gerais abordados pela referida lei, a fim de facilitar e conferir melhor compreensão do papel das empresas na proteção de dados pessoais, objeto do capítulo seguinte.

É importante destacar que a LGPD versa apenas tão somente sobre o tratamento de dados pessoais, aplicando-se à pessoa natural ou jurídica, seja de direito público ou privado, que realize tratamento de dados pessoais.

O artigo 3º, *caput*, da lei em comento dispõe sobre a sua aplicação material, deixando explícito que não importa o tipo de tecnologia empregada para a realização do tratamento, se por meio digital ou analógico.

---

[68] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020, p. 344.

Desta forma, a LGPD se aplica a todos os tratamentos de dados pessoais de qualquer pessoa física, quando ajustados em território nacional, para fins comerciais.[69]

Ela só não será aplicada, em algumas exceções, tais como: tratamento para fins exclusivamente pessoais; artísticos e jornalísticos ou acadêmicos; bem como para hipóteses de tratamento de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades e repressão de infrações penais.

Ademais, considerando que a LGPD se refere apenas ao tratamento de dados pessoais, se faz necessário definir o que são dados pessoais. Para isso, importa ressaltar que:

> O Brasil adotou o conceito expansionista de dado pessoal, pelo qual não somente a informação relativa à pessoa diretamente identificada estará protegida pela Lei, mas também aquela informação que possa – tem o potencial de – tornar a pessoa identificável.
> Assim, nome, prenome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, gênero, profissão, origem social e étnica; informações relativas à saúde, à genética, à orientação sexual, às convicções políticas, religiosas e filosóficas; números de telefone, registros de ligações, protocolos de internet, registros de conexão, registros de acesso a aplicações de internet, contas de e-mail, cookies, hábitos, gostos e interesses, são apenas alguns exemplos de dados pessoais que pautam a atual vida em sociedade.[70]

Portanto, para a lei, dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável (tal como um número de CPF ou o número do título de eleitor, por exemplo), ou ainda que indiretamente (como um CEP). Sobre o assunto, nos ensina Rony Vainzof:

---

[69] Art. 3º, da LGPD: 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; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

[70] MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019

> LGPD considera todos os meios suscetíveis de serem razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento, quer por outra pessoa, para identificar direta ou indiretamente a pessoa para determinar se ela é identificável. Também, que é necessária a avaliação de todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento e a evolução tecnológica, pata determinar se há uma possibilidade razoável de os meios serem utilizados para identificar a pessoa.[71]

Neste sentido, interessante destacar que o conceito apresentado no Regulamento Europeu 2016/679 também se limita ao conceito de dados pessoais às pessoas naturais, conforme definição constante do artigo 4º, "1":

> 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 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.

Neste sentido, Viviane Nóbrega Maldonado ensina:

> [...] observa-se que nem a LGPD nem o GDPR trazem uma listagem do que poderia constituir um dado pessoal, na medida em que a avaliação deve sempre ser levada a efeito de maneira contextual. Se uma determinada informação potencialmente é capaz de tornar uma pessoa identificável, então ela pode vir a caracterizar-se como dado pessoal naquele específico contexto[72].

Ademais, Danilo Doneda explica que é importante distinguir dados gerais de dados pessoais, pois estes últimos possuem um vínculo objetivo com a pessoa, justamente por revelar aspectos que lhe dizem respeito.[73]

Cíntia Rosa Pereira Leite, por sua vez, define que dados pessoais:

> São quaisquer informações que digam respeito a uma pessoa determinada ou determinável e que se refiram particularmente a um número de identificação, ou outros elementos que revelem sua identidade física, fisiológica, psíquica, econômica, cultural ou social.[74]

---

[71] Op. Cit, p. 90

[72] MALDONADO, Viviane Nóbrega (coord.). **LGPD:** Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Revista dos Tribunais, 2019, p. 15

[73] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. p. 157.

[74] LIMA, Cíntia Rosa Pereira de. A imprescindibilidade de uma entidade de garantia para a efetiva proteção de dados pessoais no cenário futuro do Brasil. **Tese de Livre-Docência apresentada à Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo.** Ribeirão Preto. Universidade de São Paulo. 2015, p. 145-146.

Além dos dados pessoais, são também objeto da LGPD, os dados sensíveis previstos em seu artigo 5º, inciso II, portanto, dado sensível é definido como dado pessoal sobre origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso; filosófico ou político; referente à saúde ou à vida sexual; genético ou biométrico; quando vinculado a uma pessoa natural.

Para Rafael Maciel, tais dados podem gerar riscos significativos para os direitos e liberdades fundamentais a depender do contexto de sua utilização e, por essa razão, são submetidos a um regime especial para tratamento mais rigoroso.[75]

Por serem dados íntimos e com valor social, econômico e político, eles requerem uma segurança especial, como explica Gabrielle Bezerra Sales Sarlet:

> Tratando-se de dados sensíveis, reafirma-se a exigência de uma proteção especial alicerçada no princípio da dignidade da pessoa humana, cuja fundamentalidade radica e sustenta a democracia e o atual molde de Estado de Direito. Este reforço antropológico encontra ainda amparo, e.g., no artigo segundo do Tratado da União Europeia, no qual se consagra, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos humanos.[76]

No mesmo sentido, Bruno Ricardo Bioni explica que dados sensíveis são uma espécie de dados que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação.[77]

Por fim, Patrícia Peck Pinheiro define dados pessoais sensíveis como dados relacionados às escolhas pessoais e características da personalidade da pessoa.[78]

A LGPD, também, traz o conceito de dados anonimizados, os quais já não são mais considerados pessoais, mas tal característica não é necessariamente permanente; e os dados pseudonimizado são definidos como:

---

[75] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:** Atualizado com a Medida Provisória nº 869/18. RM Digital Education. Edição do Kindle. Posição 594

[76] SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro In: LIMA, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados.** São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 13 mai. 2023.

[77] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 85.

[78] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2021, p. 16.

> [...] dado pessoal, que, por meio de tratamento, perde a possibilidade de ser associado direta ou indiretamente a um indivíduo, a menos que o controlador use uma informação adicional que era mantida separadamente em ambiente seguro. Exemplo: dados criptografados e uso de *hash* como autenticação.[79]

Posteriormente, é definido outro importante conceito que é o tratamento de dados, caracterizado por sua amplitude conceitual ao compreender operações de tratamento de dados realizados tanto pelo setor o público quanto pelo setor privado.

O conceito de tratamento de dados pessoais disposto no artigo 5º, inciso X, da LGPD engloba diversas operações com dados pessoais, incluindo-se a coleta, o acesso, distribuição, armazenamento, eliminação, a estes não se limitando.

Segundo *General Data Protection Regulation* (GDPR), tratamento é uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não, tais como a recolha, o registro, 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.[80]

Ademais, para ser possível a realização de qualquer tipo de tratamento de dados pessoais, o controlador precisa ter um motivo legítimo para esse tratamento. Esse motivo legítimo é considerado pela lei, como a base legal para o tratamento de dados pessoais.

Isso quer dizer que a LGPD determina que para cada operação que a empresa fizer com o dado pessoal, deve haver uma base legal que sustente essa operação, dentre elas, o cumprimento de obrigação legal, o interesse legitimo e o próprio consentimento do titular.

---

[79] MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

[80] UNIÃO EUROPEIA. General Data Protection Regulation (GDPR). Artigo 4, item 2 – Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 maio 2023.

As bases legais correspondem a dez hipóteses previstas na LGPD[81], que autorizam o tratamento de dados pessoais não sensíveis, através do seu rol taxativo[82], sendo dotados de algumas hipóteses mais amplas e com certo grau de subjetividade, como do legítimo interesse. Dentre as hipóteses, o consentimento é a principal base legal, sendo que as demais independem do consentimento para serem tidas como válidas.

[81] 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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
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.

[82] No regulamento europeu de proteção de dados (GDPR), utiliza-se a mesma sistemática para a aplicação das bases legais para o tratamento de dados pessoais: “The principle of ‘lawful processing’, which is one of several data protection principles under Article 5 GDPR, requires that every processing operation involving personal data must have a legal basis. Article 6(1) stipulates what may constitute such a legal basis. At the same time, it must be kept in mind that legally sound processing of personal data will necessitate fulfilling also all other of the core principles for processing personal data set out by Article 5(1). The list of legal grounds for processing contained in Article 6(1) must be understood as exhaustive and final – it can neither be supplemented nor otherwise amended by interpretation. As far as Member States’ legislators are, at all, allowed to act under Article 6(1),1 all legislative activities must keep within the strict boundaries it sets. The elements in the list must be seen to be legally equal. There is no ranking between Article 6(1)(a) to (f) in the sense that one ground has normative priority over the others.3 However, in the private sector, consent (Article 6(1)(a)) may in practice play a salient role as a potential substitute whenever there is no contractual context, no detailed legal rules about a fitting legal basis, or the scope of ‘legitimate interests of the controller or of a third party’ is particularly difficult to assess. This may also be the reason why it was deemed necessary in the GDPR to define valid consent more extensively than the other legal grounds for processing and – compared to the DPD – to add two articles (Articles 7 and 8) dealing with specific aspects of consenting” (KOTSCHY, Waltraut. Lawfulness of processing. 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019). Oxford University Press, 2018, p. 37. Disponível em: <https://works.bepress.com/christopher-kuner/1/>. Acesso em: 13 mai 2023).

Para a LGPD, o consentimento é caracterizado como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5.º, XII, Lei n.º 13.709/2018), seguindo a mesma linha do regulamento europeu.[83]

Contudo, a LGPD traz hipóteses para o tratamento de dados que vão muito além do consentimento. Em razão disso, as empresas precisam avaliar sua situação específica antes de decidir em qual base legal se enquadrar, além de ter conhecimento de quais possibilidades são essas, para evitar atividades indevidas, evitando-se punições severas pela ANPD.

Claramente que, estar em conformidade com a LGPD, ajudará a mitigar riscos financeiros e reputacionais, além de ser um diferencial no mercado, por mostrar compromisso com a privacidade e proteção de dados pessoais dos clientes, funcionários e fornecedores.

2.2. Princípios da LGPD

A LGPD possui um capítulo dedicado aos seus fundamentos, princípios e conceitos aplicáveis. O artigo 6º elenca dez princípios, em seu rol exemplificativo, considerando que a LGPD[84] determina que os direitos e princípios ali expressos, não excluem outros previstos no ordenamento jurídico relacionados à matéria ou nos tratados internacionais.

---

[83] “The GDPR does not provide for formal requirements as to the consent. Whereas under the former legislative situation some EU Member States’ legislation laid down such requirements, consent under the GDPR could be given by oral or written statement, including by electronic means. Nevertheless, written form is advisable regarding the controller’s burden of proof. Given its practicability, a lot of entities might opt for obtaining consent by electronic means in the future. In order to be able to demonstrate that valid consent has been obtained, entities will have to protocol the declared electronic consent” (VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR**). A Practical Guide. Springer, 2017, p. 94).

[84] Art. 64. LGPD. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Conforme ensina Celso Antônio Bandeira de Mello:

> Os princípios jurídicos constituem mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e sentido servindo de critério para sua exata compreensão e inteligência, exatamente por definir a lógica e a racionalidade do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico.[85]

Como exposto, a LGPD impõe expressamente os seus princípios jurídicos, dentre eles, destaca-se 5 (cinco) princípios fundamentais para a proteção de dados: princípio da finalidade; princípio da necessidade; princípio da não discriminação; princípio da boa-fé; e princípio da segurança.

O princípio da finalidade estabelece que todo tratamento de dados cumprirá os "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", conforme disposição do artigo 6º, inciso I, da LGPD.

Esse princípio é fundamental a todas as atividades de processamento de dados, bem como essencial para limitar o acesso de terceiros ao banco de dados da empresa detentora dos dados.

Neste sentido, a título de exemplo, uma empresa não poderá operar um tratamento de dados sem existir uma justificativa ou finalidade para tanto. Por isso, a comunicação da finalidade deverá ser declarada antes do processamento e, caso exista mais de uma finalidade para o tratamento dos dados pessoais, todas elas deverão ser declaradas ao titular dos dados de forma transparente e que não gere dúvidas em seu tratamento.

> Lojas *on-line* coletam informações de visitantes. Embora nem todos os tipos de dados coletados sejam estritamente necessários para fornecer acesso e realizar compras, são muito uteis para o controlador analisar o comportamento de seus clientes e potenciais clientes em seu comércio eletrônico. Tais dados permitem o aprimoramento de serviços aos clientes, seja quanto à performance do *site*, seja da avaliação de produtos mais acessados, por exemplo. Assim poderia ser defensável a legitimidade da finalidade, apesar de tais dados não serem essenciais para a venda do produto ou serviço, desde que haja consentimento prévio.[86]

---

[85] MELLO, Celso Antônio Bandeira. Curso de direito administrativo. 26 ed. São Paulo: Malheiros, 2009.
[86] MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019

Para Danilo Doneda[87], o referido princípio é, provavelmente, o que carrega de forma mais incisiva os traços característicos da matéria de proteção de dados pessoais, pois o motivo da coleta deve ser compatível com o objetivo final do tratamento de dados.

> O princípio da finalidade dispõe que o motivo da coleta deve ser compatível com o objetivo final do tratamento de dados. A sua utilização sempre estará vinculada ao motivo que fundamentou essa coleta, nascendo uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, de modo que esta deva ser levada em consideração em qualquer tratamento posterior. Como o dado pessoal é expressão direta da personalidade do indivíduo, nunca perde seu elo com este, pois sua utilização pode refletir diretamente para seu titular.

A sua utilização sempre estará vinculada ao motivo que fundamentou essa coleta, nascendo uma ligação entre a informação e a sua origem, vinculando-se ao fim de sua coleta, de modo que esta deva ser considerada em qualquer tratamento posterior.

Como o dado pessoal é expressão direta da personalidade do indivíduo, nunca perde seu elo com este, pois sua utilização pode refletir diretamente para o seu titular.

Ademais, as informações devem atender ao princípio da necessidade. Este princípio instituiu uma limitação do tratamento mínimo necessário para realização das finalidades estipuladas, visando minimizar a coleta de dados, além disso, ele guarda relação direta com o princípio da finalidade.

Por isso, o controlador pode questionar, antes do início do tratamento, se é possível atingir a finalidade de outro modo que não seja com o uso de dados pessoais (*data minimisation*), e mediante a avaliação de quais gêneros de dados são imprescindíveis.

---

87 DONEDA, Danilo. Princípios de Proteção de Dados. In: MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019

87 DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. In*:* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direitos & Internet III:** Marco Civil da Internet. Quartier Latin, 2015, t. I, p. 378.

> Assim, quaisquer políticas empresariais baseadas em “reter tudo” possivelmente serão consideradas ilícitas. Para atingir um certo grau de segurança jurídica, o controlador deverá realizar um teste de razoabilidade e adequação. Se a natureza e a quantidade dados pessoais forem proporcionais em relação aos objetivos do tratamento, o procedimento será lícito.[88]

O princípio da não discriminação tem como finalidade evitar a segregação pela criação de estereótipos, seja pela limitação de direitos por meio de forma automatizada, ou não.

À vista disso, ele se mostra fundamental, prevendo a impossibilidade do tratamento de dados para fins discriminatórios, seja de forma automatizada ou não, avistando a limitação e permissões no processamento de dados, de modo a mitigar o risco do determinismo tecnológico.[89]

Laura Schertel Mendes explica que o consumidor, em razão de informações armazenadas em banco de dados, caso tenha oportunidades diminuídas ou lhe seja negado acesso a bens ou serviços, está sujeito ao risco de ser discriminado.[90]

Ou seja, caso haja discriminação de adquirentes por meio de fixação diferenciada de preços, poderá ser considerada ilícita, do ponto de vista concorrencial, se houve aumento arbitrário dos lucros, domínio do mercado ou limitação da concorrência.

Ademais, quanto à oferta do produto ou serviço com a utilização de dados pessoais do consumidor, as empresas precisam respeitar tanto a LGPD bem como respeitam o CDC, o qual assegura, dentre outros direitos, a liberdade de escolha e igualdade nas contratações, a proteção contra a publicidade abusiva e enganosa além de métodos desleais.

---

[88] MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

89 É a tecnologia que amolda a sociedade, e não o inverso, segundo tal corrente, “e são vistas como a condição fundamental de sustentação do padrão da organização social. Os deterministas tecnológicos interpretam a tecnologia como a base da sociedade no passado, presente e até mesmo no futuro. Novas tecnologias transformam a sociedade em todos os níveis, inclusive institucional, social e individualmente. Os fatores humanos e sociais são vistos como secundários” CHANDLER, Daniel Technological or Media Determinism. 25.04.2000. Disponível em: <http://www.wolearn.org/pluginfile.php/2185/mod_page/content/6/chandler2002_PDF_full.pdf>. Acesso em: 03 jun. 2023.

[90] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 92-93.

Para Fabíola Meira de Almeida Santos e Rita Taliba, dos princípios da boa-fé e da segurança decorrem os demais princípios que deverão guiar o comportamento das empresas que coletam e tratam, de alguma forma, dados pessoais:

> (i) minimização dos dados – não estamos mais na era da coleta irrestrita de dados. Os princípios da Lei impõem, que sejam coletados apenas dados mínimos para a finalidade do serviço a ser prestado ou produto. Isso se aplica, também, às autoridades, ainda que, nesses casos, se dispense o consentimento expresso do tratamento (art. 7º). Esse conceito deve ser incorporado desde a concepção do serviço ou produto a ser ofertado (*Privacy by Design*), devendo o controlador sempre efetuar a pergunta "é preciso coletar esse dado? Para qual finalidade?", na medida em que, inexistindo finalidade clara e adequação, o tratamento poderá ser considerado abusivo; (ii) adequação do tratamento dos dados à finalidade para os quais foram coletados - na mesma esteira da minimização, ainda que a hipótese seja a da dispensa do consentimento inequívoco, os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares, e o tratamento não pode estar dissociado daquilo que o titular razoavelmente espera ao fornecê-lo.[91]

Portanto, o princípio da segurança garante ao titular dos dados a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Os agentes de tratamento, como, por exemplo, empresas, devem utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de eventuais violações, por meio da adoção de boas práticas e da governança corporativa.

Sobretudo por que, como pontua Marcelo Benacchio e Tatiana de Almeida Campos, "toda empresa deve ter uma gestão inteligente preocupada no impacto que sua atividade negocial pode causar no meio social".[92]

Cumpre ressaltar, que toda essa preocupação se dá em razão do elevado risco dos direitos dos titulares, em especial quando da formação de grande banco de dados, mormente caso ocorram invasões ou situações que podem gerar graves prejuízos às pessoas. Ainda, pode gerar degradação da imagem do agente de tratamento – a empresa – perante o mercado, sujeitando-se, também, às penalidades previstas na LGPD.

---

[91] SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. **Lei Geral de Proteção de Dados no Brasil e os possíveis impactos.** São Paulo: Revista dos Tribunais, 2018, p. 988.

[92] BENACCHIO, Marcelo; CAMPOS, Tatiana de Almeida. A Importância da Governança Corporativa no Pacto Global e na Concretização dos Princípios Ruggie. In: CAVALCANTI, Thais Novaes; CONCI, Luiz Guilherme Arcaro (Orgs.) **Proteção jurídica da pessoa, direitos humanos e desenvolvimento regional**. São Bernardo do Campo: Ed. Universitária FDSBC, 2022, p. 90.

2.3. Autodeterminação Informativa

Como visto, o conceito de privacidade acendeu e ganhou força ao longo das décadas, mas foi no ano de 1982, que a Alemanha assumiu posição de protagonismo no regramento da coleta e tratamento de dados pessoais, quando foi palco de uma decisão judicial que revolucionou a forma como o mundo entende a privacidade e a proteção aos dados pessoais.

Naquele ano, o governo federal alemão aprovou uma lei de censo populacional, chamada de *Volkszählungsgesetz*, conhecida como Lei de Censo Populacional, que previa gigantesca coleta de dados sobre os cidadãos, por meio de questionários a compreender perguntas sobre gênero, estado civil e religião.

Entretanto, o povo alemão reagiu de forma negativa e o tema foi levado a julgamento no Tribunal Constitucional Alemão, que reconheceu o direito à autodeterminação informativa, inaugurando um dos mais importantes conceitos sobre privacidade.

Na ocasião, o tribunal entendeu que para o indivíduo exercer sua liberdade de decisão junto às ações praticadas em relação aos seus dados, era necessário garantir que ele tivesse autonomia e pudesse escolher a forma como seus dados seriam utilizados.

A autodeterminação informativa é conceituada como o "direito que cabe a cada indivíduo de controlar e de proteger os próprios dados pessoais, tendo em vista a moderna tecnologia e processamento de informação".[93]

Para Rony Vainzof, a autodeterminação informativa é:

> "o controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático; e a moderna, em que a intervenção (proteção) é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular.[94]

---

[93] MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** Montevidéu: Fundação Kontad Adenauer, 2005, p. 233.

[94] VAINZOF, Rony. Conceito, perfil, papéis e responsabilidade do encarregado. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (coord.). **Data Protection Officer:** teoria e prática de acordo com a LGPD e o GDPR. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. E-book.

Portanto, o direito à autodeterminação informativa se constitui como direito intrinsecamente ligado ao direito à privacidade, permitindo a toda pessoa exercer, de algum modo, controle sobre seus dados pessoais, garantindo-lhe, exceto algumas circunstâncias, decidir se a informação pode ser objeto de tratamento por terceiro, ou, até mesmo, acessar banco de dados com o intuito de exigir correção ou cancelamento de informações.

Nesse sentido, o exercício do direito à autodeterminação informativa visa garantir a cada cidadão ser o senhor das suas informações, ante as múltiplas possibilidades de coletas e tratamento de dados oferecidos na sociedade atual.

> Não há sobreposição, contudo, entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar uma dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão dos seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*). Dito de outro modo, “a proteção de dados é, enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal”. No concernente às suas interfaces com o direito à privacidade, também inexiste, como já adiantado, superposição completa dos respectivos âmbitos de proteção. Proteção de dados pessoais e, da mesma forma, autodeterminação informativa, vão além da privacidade e de sua proteção, ao menos no sentido tradicional do termo, caracterizado por uma lógica de “recolhimento” e "exposição".[95]

Portanto, a autodeterminação informativa reconhece que as pessoas têm o direito de decidir sobre suas próprias informações, além de serem informadas sobre como esses dados estão sendo coletados, usados, armazenados e ou compartilhados.

Com o avanço da tecnologia e da informação, bem como da crescente preocupação com a privacidade, a autodeterminação informativa se tornou o princípio central nas discussões sobre privacidade e proteção de dados nos dias atuais.

---

[95] SARLET, Ingo W.; DONEDA, Danilo; MENDES, Laura S. **Estudos sobre proteção de dados pessoais**. Ebook. São Paulo: Editora Saraiva, 2022. (Coleção Direito, tecnologia, inovação e proteção de dados num mundo em transformação). Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620810/. Acesso em: 14 mai. 2023. p. 23.

> No tocante à autodeterminação informativa, é certo que as evoluções tecnológicas trazem inúmeros benefícios, em sua contraposição há a problemática paradoxal da consequência da promoção de uma maior exposição dos dados pessoais, gerando assim constante violação no que concerne às informações pessoais dos indivíduos. E é neste cenário que surge o direito à autodeterminação informativa ou informacional, traduzindo-se como um desmembramento do direito à privacidade, visando essencialmente tutelar de forma efetiva os dados/informações pessoais das pessoas naturais garantindo-lhes o controle sob eles, sendo, portanto, imperiosa a necessidade de seu reconhecimento como um novo direito fundamental.[96]

Neste escopo, a autodeterminação informativa se torna pilar fundamental para fortalecer o direito à proteção de dados, especialmente, no sentido de incluí-la no rol de direitos fundamentais previstos na Constituição Federal.

2.4. Agentes de Tratamento

Como já exposto, a LGPD traz os conceitos tratados pela legislação em seu artigo 5º e, dentre eles, tem-se o conceito acerca dos agentes de tratamento, controlador e operador, que serão objeto de estudo a seguir.

A LGPD conceitua controlador, como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, inciso VI, Lei n.º 13.709/2018).

É notável a relevância imposta pela LGPD ao controlador, considerando sua responsabilidade pela tomada de decisões sobre o tratamento de dados pessoais, visando o cumprimento da lei, na prática.

Nesse sentido, a ANPD publicou o “Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado” destacando o peso jurídico do controlador:

---

[96] VIGLIAR, José Marcelo M. **LGPD e a Proteção de Dados Pessoais na Sociedade em Rede**. E-book. São Paulo: Grupo Almedina (Portugal), 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556276373/. Acesso em: 13 mai. 2023. p. 72

> O conceito possui elevada importância prática, uma vez que a LGPD atribui obrigações específicas ao controlador, como a de elaborar relatório de impacto à proteção de dados pessoais (art. 38), a de comprovar que o consentimento obtido pelo titular atende às exigências legais (art. 8º, § 2º) e a de comunicar à ANPD a ocorrência de incidentes de segurança (art. 48). Além disso, a atribuição de responsabilidade em relação à reparação por danos decorrentes de atos ilícitos é distinta de acordo com a qualificação do agente de tratamento, isto é, se controlador ou operador, conforme disposto nos arts. 42 a 45.[97]

Portanto, é fundamental que as organizações compreendam e cumpram suas obrigações legais para garantir a proteção adequada dos dados pessoais, sob sua responsabilidade.

O operador, por sua vez, também pessoa física ou jurídica, é mero executor das ordens do controlador (art. 39, da LGPD), ou seja, é uma atividade procedimental, operacional (locação de servidores, provimento de infraestrutura e tecnologia para armazenamento de dados, desenvolvimento ou manutenção de *softwares* etc.) das decisões tomadas pelo controlador.[98]

O operador faz o tratamento dos dados pessoais em nome e aos comandos do controlador sem, contudo, alterar a finalidade dos dados relacionados a determinado tratamento.[99] Logo, este não poderá tratar dados pessoais senão em virtude das determinações do controlador ou de previsão legal.

A LGPD, em seu artigo 39, determina que o operador deverá realizar o tratamento, segundo as instruções fornecidas pelo controlador, o qual verificará a observância das normas.

Desta forma, neste cenário, o que diferencia o operador do controlador, é o poder de decisão, uma vez que o operador somente pode agir no limite das finalidades determinadas pelo controlador.

---

[97] ANPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo**. Tratamento de Dados Pessoais pelo Poder Público. 2021, p. 7. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico Acesso em: 20/06/2023.

[98] PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. Lei Geral de Proteção de Dados Pessoais. 1.ed. São Paulo: Thomson Reuters Brasil, 2021. p. RB-5.4. In: NOHARA, Irene Patrícia Diom, ALMEIDA, Luiz Eduardo de. **Compliance digital e LGPD.** Coleção Compliance; v. 5. 1. ed. em e-book baseada na 1. ed. impressa).

[99] LEONARDI, Marcel. Controladores e operadores: papéis, distinções, mitos e equívocos. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. **A Lei Geral de Proteção de Dados Pessoais:** Aspectos práticos e teóricos relevantes no setor público e privado. 1. Ed. e-book baseada na 1. ed. Impressa. São Paulo: Thomson Reuters Brasil, 2021, p. RB-5.4.

2.5. Autoridade Nacional de Proteção de Dados

A LGPD concedeu à Autoridade Nacional de Proteção de Dados um papel de protagonista na tutela dos dados pessoais no Brasil, incumbindo-a de editar normas e procedimentos sobre a proteção de dados, além de possuir a função de conscientizar os titulares e os responsáveis pelo tratamento, fiscalizar a aplicação da legislação de proteção de dados brasileira e aplicar medidas coercitivas no caso de descumprimento. Pode-se dizer, em outras palavras, que a ANPD é o eixo central de um ecossistema de proteção de dados no Brasil.

Há de se registrar, também, que a criação da ANPD viria ao encontro do exigido pelo Regulamento Europeu, sendo elemento relevante à preservação dos dados pessoais, evitando-se o uso indevido de dados pessoais, além de assegurar os direitos fundamentais dos indivíduos.

Contudo, apesar de sua importância, a ANPD enfrentou percalços até alcançar o seu formato atual no Brasil. Os debates em torno da necessidade de uma autoridade nacional, como figura centralizadora para fins de controlar o uso dos dados pessoais, iniciaram-se com as primeiras consultas legislativas propostas a respeito da criação da LGPD.

O Projeto de Lei n.º 53/2018, da Câmara dos Deputados, trouxe a figura da autoridade nacional, como órgão integrante da administração pública federal indireta, submetida ao regime autárquico especial, vinculado ao Ministério da Justiça e regida pela Lei das Agências Reguladoras (Lei n.º 9.986, de 18 de julho de 2000).

Contudo, o Presidente da República à época, Michel Temer, vetou a criação na forma proposta, considerando que estava eivada de vício de inconstitucionalidade formal, uma vez que a criação do órgão é prerrogativa do Poder Executivo e, como se tratava de órgão que integraria o Poder Executivo, caberia a este poder legislar sobre o tema, nos termos do artigo 61, §1º, alíneas “a” e “e”, da Constituição Federal.

Destaca-se que, o veto foi objeto de diversas polêmicas, havendo severas críticas no sentido de que tenha sido feito de forma estratégica, haja vista não ser de interesse de alguns governantes que a autoridade funcionasse de forma independente, pois, uma vez que isso ocorresse, também o Poder Executivo estaria a ela submetido.

Ao revogar, em uma tacada só, os dois dispositivos previstos na LGPD original, eliminou-se o comando legal que previa importante mecanismo de informação transparência ao titular de dados pessoais para garantia de seus direitos.

Revogou-se, também, competência regulamentar prevista à ANPD, que poderia disciplinar de forma eficiente e eficaz a forma pela qual o direito à informação do titular de dados pessoais seria protegido sem inviabilizar o bom desenvolvimento de políticas públicas.

Posto isso, diante da importância da criação da Autoridade Nacional de Proteção de Dados, foi publicada a Medida Provisória n.º 869/2018 e, posteriormente, convertida na Lei n.º 13.853, de 2019, para vincular a ANPD à Presidência da República.

Essa alteração comprometeu severamente a independência da referida autoridade, na medida em que, nessa configuração, o Poder Executivo passou a assumir os papéis de regulador e de regulado.

A MP 869/2018 criou, dessa maneira, assimetria regulatória injustificável e perigosa, ao exigir do Poder Público reduzido grau de *accountability* diante de eventual tratamento de dados pessoais.

A crítica é no sentido de se alertar para a reduzida capacidade legal de a ANPD regular e fiscalizar a atuação do Poder Público no tratamento de dados pessoais. Essa deficiência não nos parece casual, mas, sim, desenhada com claro intuito limitador. Apontando preocupante possibilidade de propósitos distorcidos no tratamento de dados de cidadãs e cidadãos por órgãos e entidades pública.

Nesse sentido, Beto Vasconcelos e Felipe de Paula asseveram que:

> [...] a vinculação à Presidência da República, por si só problemática, carrega em si dificuldades especificas: pode não haver suficiente autonomia e independência institucional exigidas de outros países de modo a assegurar a cooperação jurídica internacional para a transferência de dados pessoais entre nações. Pode ser o caso, em especial, para os Estados-Membros da União Europeia sob a disciplina da GPDR. Outra crítica com a qual alinhamos, diretamente relacionada à primeira, diz respeito à inescapável redução da capacidade de regulação e fiscalização, por parte da ANPD, do tratamento de dados pessoais pelo Poder Público. Se o ente perdeu importante parcela de autonomia e independência, em especial dada a inexistência de mecanismos mínimos estabelecidos internacionalmente, como garantir que haverá proteção de direitos individuais frente a atuação do Poder Público? [100]

Todavia, a implementação da ANPD, como órgão integrante da Presidência da República, foi a solução encontrada naquele momento. Contudo, ficou consignado que a autoridade teria natureza transitória, por um período de dois anos da sua criação, após o que deveria ser realizada a sua transformação em outro órgão público, dotado de autonomia e independência.

Em 1º de agosto de 2021, a ANPD foi legalmente autorizada, dando início à fiscalização de denúncias e apontamentos de eventuais irregularidades quanto ao uso indevido de dados, em face de órgãos públicos e privados.

No ano seguinte, a Medida Provisória n.º 1.124, de 13 de junho de 2022, foi assinada pelo então Presidente da República, Jair Messias Bolsonaro, para transformar a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial, com patrimônio próprio, sede e foro no Distrito Federal.

Diante disso, a ANPD deixou de ser subordinada hierarquicamente a ministérios ou à Presidência da República, adquirindo autonomia técnica e decisória, tal qual os demais órgãos regulatórios, como a Agência Nacional de Vigilância Sanitária (ANVISA) e Agência Nacional de Telecomunicações (ANATEL).

Ademais, com a transformação da ANPD, o Brasil atenderá às exigências para obter decisão de adequação da Comissão Europeia e para indicadores positivos junto à Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

---

[100] VASCONCELOS, Beto. PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Coordenação). **Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro**. 1. Ed. São Paulo: Revista dos Tribunais, 2019, p. 733.

> A atração de investimentos externos e credibilidades internacional também tendem a ser favorecidas através da aproximação do modelo brasileiro com o posicionamento europeu e eventual reconhecimento do grau de adequação de proteção aos dados pessoais da LGPD pela União Europeia, já que essa convergência de entendimentos potencialmente criaria mais chances de entrada do Brasil na OCDE.[101]

Notavelmente, a estruturação de uma autoridade independente tem o potencial de gerar efeitos econômicos e políticos ao Brasil, principalmente no fluxo de dados intra-Mercosul, considerando que a Argentina e o Uruguai dispõem de sistemas robustos de proteção de dados pessoais, com restrições à transferência internacional de dados.

> Como referido neste relatório, eventual reconhecimento do Brasil, pela União Europeia, como um país que possui mecanismos que asseguram um adequado grau de proteção aos dados pessoais poderá representar ganhos econômicos e sociais de significativa monta, pelo que se mostra recomendável que se postule a obtenção de uma decisão de adequação junto à Comissão da União Europeia.[102]

Então, em 25 de outubro de 2022, foi sancionada a Lei n.º 14.460/2022, tornando a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio e com sede e foro no Distrito Federal.

Feitas tais considerações sobre a estruturação da ANPD, a seguir será destacada suas principais competências previstas no artigo 55-J, da LGPD, em razão de um extenso rol de atribuições que promove a centralização de atividades em um órgão pretensamente forte, para a efetiva proteção de dados pessoais.

Dentre suas funções, a ANPD deverá realizar a fiscalização e aplicação da LGPD, por parte das organizações públicas e privadas. Isso envolve a verificação do cumprimento das normais de proteção de dados, a aplicação de sanções em caso de violações e a promoção de medidas coercitivas.

---

[101] ARAGÃO, Isabella de C. S. **Contexto brasileiro pós-Scherms I e II:** influências de limitações geográficas no fluxo transnacional de dados pessoais e aspectos práticos. Direito Digital e O Setor Público, Rio de Janeiro, n. 2, 2020, p. 13.

[102] VIOLA, Mario. **Transferência de Dados entre Europa e Brasil**: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: Instituto de Tecnologia & Sociedade do Rio, 2019, p. 18.

Além disso, a ANPD tem o papel de fornecer orientações e aconselhamentos sobre questões relacionadas à proteção de dados, tais como: responder a consultar de empresas e indivíduos; esclarecer dúvidas sobre a aplicação da LGPD; e fornecer diretrizes para o cumprimento das obrigações previstas em lei.

A atuação preventiva da ANPD tem como escopo promover o fortalecimento da cultura de proteção de dados para a sociedade civil em geral, baseada na construção conjunta e dialogada de soluções e medidas que visam a recondução dos agentes de tratamento à conformidade ou de maneira a evitar situações de risco ou danos aos titulares de dados pessoais ou agentes de tratamento.

O órgão, também, tem a competência de elaborar diretrizes, guias e regulamentos complementares à LGPD, como os já elaborados: Guia Orientativo Cookies e Proteção de Dados Pessoais e Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.[103]

Além das funções mencionadas, a ANPD também poderá desempenhar outras atividades direcionadas para promoção da proteção dos direitos dos titulares de dados, em razão do seu rol exemplificativo de competências delegadas.

Portanto, o que se espera é que a ANPD possa não apenas zelar pela privacidade e proteção de dados, mas também, tenha condições de atuar ativamente na regulamentação e fiscalização da LGPD, tudo de forma eficaz e impessoal, sem interferências hierárquicas e políticas.

[103] ANPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico Acesso em: 20/06/2023.

3. OS DESAFIOS ENFRENTADOS PELAS EMPRESAS NA BUSCA PELA ADEQUAÇÃO À LGPD

A partir da promulgação da Lei Geral de Proteção de Dados, as empresas foram afetadas e sentiram a necessidade de se adequarem ao quanto previsto na referida Lei, sob pena de sanções administrativas e pecuniárias, aplicáveis pela ANPD, como será exposto no próximo Capítulo.

Tudo isso se dá, em razão das discussões da ameaça às violações de dados pessoais, que passa a ser representada pelas milhares de empresas que coletam, armazenam e processam dados de seus clientes, fornecedores e funcionários.

Neste sentido, Benedikt Buchner citando Winfried Hassemer afirma que:

> O Estado ainda aparece em algumas áreas... em outras, o tema se desloca para distintos demônios, que são muito piores que ele: por meio de uma potente tecnologia da informação nas mãos de qualquer um, essa força se desloca (...) de forma ágil, oculta, voraz e por toda a Terra, coletando, classificando, repreendendo, reunindo, comercializando e utilizando dados pessoais.[104] (tradução livre).

Antes das regulamentações, as organizações públicas e privadas tinham o uso indiscriminado dos dados pessoais para as mais diversas finalidades.

Os dados coletados pelas empresas, a partir do momento que configuravam em sua base de dados, ficavam sob sua posse de forma indefinida, sendo utilizados para diversas finalidades, diferentes daquela que originou sua coleta, sem o menor conhecimento de seu titular.

Porém, diante do novo cenário, os impactos da LGPD fazem-se sentir de forma transversal, principalmente no que tange às organizações empresariais, que urgem pela adoção das adequações necessárias.

Neste sentido, Ricardo Oliveira pontua que:

> Para sua aplicação basta termos diante de nós dados pessoais, simples assim. E de tão simples, o problema é comum, pois empregar uma única pessoa, ter pessoas físicas como clientes ou ser uma pessoa jurídica já torna a empresa um órgão público um controlador, ou seja, o responsável na linha

104 BUCHNER, Benedikt. **Informationelle Selbstbestimmung im Privatrecht. Tübingen:** MohrSiebeck, 2006, p. 26.

> de frente pelo tratamento de dados pessoais realizado, atraindo para si a responsabilidade principal por eventuais violações de direito.[105]

Ao passo em que, o tratamento de dados tem um grande potencial de geração oportunidades e novos modelos de negócios, também se trata de uma atividade que oferece ameaças e riscos à proteção dos dados pessoais, com a possibilidade de exposição e utilização indevida ou abusiva de dados pessoais.

Destaca-se que, a atividade empresarial, antes mesmo da promulgação da LGPD, já tinha obrigações impostas pela Constituição Federal, como por exemplo, o respeito aos princípios da dignidade humana e os valores sociais do trabalho e da livre iniciativa.

À vista disso, destaca-se a lição de Gilberto Haddad Jabur, o qual menciona ser:

> O direito constitucional à livre concorrência, arrimo inegável da ordem econômica nacional (CF, art. 170, V), não abandona a obtenção ilícita de dados pessoais nem a entrega de produtos ou serviços que dela ordinariamente decorre sob a invocação de *oferta comercial*. A oferta saudável e revestida de liceidade não serve de subterfúgios que a preparam (obtenção de dados pessoais à revelia ou à sorrelfa) nem de métodos que a introjetam no domicílio ou ambiente alheio. A privacidade é zona reserva, é santuário que reclama isolamento é, numa expressão, círculo do qual participam somente aqueles a quem se quer dar a revelar.[106]

Todavia, com a vigência da LGPD, a carga de obrigações para com a sociedade aumentou e muitas empresas sofreram e ainda sofrem o grande impacto causado para a adaptação das novas regras trazidas pela legislação em comento, em razão da cultura existente no Brasil.

> Os impactos desta nova norma são expressivos, tanto no aspecto da tutela da privacidade e proteção dos dados pessoais de seus respectivos titulares, quanto, naturalmente, para a atividade empresarial, considerando que a LGPD impõe uma série de diretrizes para que o tratamento de dados seja realizado de forma lícita.[107]

No mesmo sentido, Diego de Lima Gualda destaca:

---

[105] OLIVEIRA, Ricardo. **LGPD:** Como evitar as sanções administrativas. São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 04 jun. 2023.

[106] JABUR, Gilberto Haddad. A dignidade e o Rompimento de privacidade. In: Martins, Ives Gandra da Silva; PEREIRA JR, Antonio Jorge. **Direito à Privacidade.** 1 ed. Aparecida: Editora Ideias & Letras, 2005, p. 98.

[107] OLIVEIRA, A. P. de. et al. A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, Curitiba, v. 4, n. 1, maio, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wpcontent/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 24 mai. 2023.

> O Brasil não detém uma cultura de proteção de dados pessoais e isso repercute nas práticas corporativas. Continua corriqueira a existência de bases de clientes em planilhas sem controle de acesso, trocas de e-mails com essas bases, uso de dados pessoais de clientes para fins distintos do propósito da coleta, manutenção de dados pessoais por períodos indefinidos e sem controle de segurança, atividades de marketing não regulares etc. As organizações devem investir em revisitar cada uma de suas linhas de negócio e práticas a elas inerentes, além de treinamento contínuo para colaboradores. A grande maioria dos problemas de violação de dados pessoais e segurança da informação têm por causa condutas inadequadas e a mudança de cultura corporativa é muito mais lenta e muito mais difícil que a troca ou implantação de um software. Não devemos subestimar a importância e o desafio cultural que a LGPD traz consigo.[108]

Diante deste panorama, as empresas têm a necessidade de se adaptarem à legislação, mudando seu *modus operandi* atual quando da coleta e tratamento de dados de clientes e fornecedores.

É por esse motivo que a LGPD ainda é vista como um grande desafio paras as empresas brasileiras e vem sendo uma das maiores aflições das organizações e empresas atualmente.

Sobre os impactos produzidos pela nova legislação, Patrícia Peck Pinheiro observa:

> Tanto porque traz exigências que aumentam os custos empresariais e passam a ter que entrar na prioridade dos gestores (*road map*) mas como também exigem alguns processos de governança corporativa (de TI, de Segurança de Informação, de Gestão de Dados) que não eram tão comuns neste ambiente e que podem até dificultar (burocratizar) suas atividades que estão mais acostumadas com leveza e velocidade.[109]

Notavelmente, novas legislações dessa envergadura abalam grandemente os alicerces de hábitos empresariais, e não basta simplesmente escrever no texto legal o que deverá se fazer, ou não, para que se produza efeitos, é preciso lastrear a construção de uma nova cultura empresarial, visando proteger os direitos individuais.

Portanto, em que pese as medidas serem custosas, as empresas precisam compreender que as disposições trazidas pela LGPD proporcionam aspectos positivos, como a construção de uma relação com o cliente mais saudável e na base da confiança, com maiores níveis de transparência e proteção.

---

[108]GUALDA, Diego de Lima. **Desafio Cultural da Proteção de Dados.** Disponível em: https://www.aarb.org.br/desafio-cultural-da-protecao-de-dados/. Acesso em: 24 mai. 2023.

[109] PINHEIRO, Patrícia Peck. **Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o impacto nas instituições públicas ou privadas**. RT 1.000. Ano 108. Vol. 1.000. São Paulo: Revista dos Tribunais, 2019.

Assim, com a estruturação dessas informações de forma consciente, permite-se, por exemplo, criar uma vasta gama de novas aplicações, tornando os processos de comércio mais produtivos e eficazes.

Entretanto, as exigências impostas pela lei, ainda, são vistas com ônus, por muitas organizações, em razão do grande custo operacional, eventual aumento do número de colaboradores e criação de setores responsáveis pela privacidade e proteção de dados, com a finalidade de suprir as exigências.

Além disto, desde que a referida lei entrou em vigor, casos de vazamentos de dados têm ganhado cada vez mais destaque na mídia. O que se justifica, não apenas por conta da frequência com que ocorrem, mas a falta de observância da lei, que passou a tutelar os dados pessoais.

O relatório da IBM sobre vazamento de dados, feito com 524 empresas em 17 países, incluindo o Brasil, concluiu que cerca de 80% dos vazamentos de dados em empresas envolvem a perda ou roubo de dados pessoais de clientes.[110]

Possíveis falhas com o vazamento de dados foram ocasionadas de diversas maneiras, como por exemplo, ataques cibernéticos, hackers, funcionários mal-intencionados, além de falhas de programação.

Diante disso, além do vazamento de dados causar danos aos titulares, ele também impacta drasticamente as operações de negócio das empresas e exigindo a adoção de medidas preventivas.

Nesse sentido, a responsabilidade social de empresas, passa a adotar também, os princípios basilares da LGPD, no que tange a proteção de dados.

A respeito do tema, o Instituto Ethos, organização da sociedade civil de interesse público, define o instituto da responsabilidade social como:

> Responsabilidade social empresarial é a forma de gestão que se define pela relação ética e transparente da empresa com todos os públicos com os quais ela se relaciona e pelo estabelecimento de metas empresariais compatíveis com o desenvolvimento sustentável da sociedade, preservando recursos ambientais e culturais para as

[110] IBM. Relatório do Custo de uma Violação de Dados 2021. Disponível em: https://www.ibm.com/downloads/cas/RBJ6BJVN#:~:text=Figura%201-,O%20custo%20total%20m%C3%A9dio%20de%20uma%20viola%C3%A7%C3%A3o%20de%20dados%20aumentou,4%2C24%20milh%C3%B5es%20em%202021 Acesso em: 20 jun. 2023.

> gerações futuras, respeitando a diversidade e promovendo a redução das desigualdades.[111]

Rodrigo Almeida Magalhães[112], por sua vez, conceitua que a responsabilidade social das empresas engloba todas as atividades não relacionadas ao objeto social da empresa, mas que são geradoras de benefícios para a sociedade, tanto no âmbito interno quanto ao externo.

Em outras palavras, as empresas devem se posicionarem “estrategicamente como substitutas do papel do Estado, apresentando-se como voluntárias à promoção do bem-estar”, isso porque, a “responsabilidade social da empresa está intimamente ligada ao movimento de valoração da ética nas relações empresariais”, como bem assevera Caio Pacca de Castro e Marcelo Benacchio.[113]

Desta forma, as empresas têm o compromisso com a sociedade na busca pela proteção de dados no Brasil, para fortalecer os Direitos Humanos. E o principal elemento propulsor será a adoção das medidas exigidas pela LGPD, cumuladas com a conscientização de seus funcionários e consumidores, por meio de ações corporativas internas, desenvolvimento de modelos de gestão e comunicações transparências.

Tudo isso, além de contribuírem para o processo de desenvolvimento com justiça social, as empresas adotantes das medidas necessárias passarão a ter grande diferencial, criando vantagens competitivas e, consequentemente, maiores níveis de sucesso.

Claramente, uma empresa responsável, provida de credibilidade e compromisso com a proteção de dados, tanto no mercado interno como externo, se adequará aos novos interesses da sociedade e garantirão uma gestão livre de concorrência justa.

Portanto, em que pese os desafios enfrentados pelas empresas para se adequarem à LGPD, adianta-se desde já que os benefícios inúmeros.

---

[111] INSTITUTO ETHOS. Disponível em: <http://www.ethos.org.br>. Acesso em 20 mai. 2023.
[112] MAGALHÃES, Rodrigo Almeida**. A função social da empresa e a responsabilidade social**. Disponível em: http://direito.newtonpaiva.br/revistadireito/docs/prof/13_prof_rodrigo2.pdf. Acesso em 20 mai. 2023.
[113] DE CAMARGO, Caio Pacca Ferraz; BENACCHIO, Marcelo. Função social e responsabilidade social empresarial: convergências e divergências. **Revista Thesis Juris**, v. 8, n. 2, p. 119-148, 2019.

3.1. Adequações Necessárias das Empresas à LGPD

Como anteriormente exposto, o papel das empresas e organizações é bastante significativo e implica diversas responsabilizações e ações a serem tomadas em relação ao uso de dados pessoais. Isso porque, a LGPD estabelece uma cultura de responsabilidade em relação aos dados pessoais, visando coibir o uso indevido e o vazamento de dados.

No Brasil, adotou-se o sistema de gerenciamento de risco chamado *risk-based approach*, em contraposição ao sistema rígido de prescrição de direitos e deveres (*right-based approach*), conforme explica Filipe Fonteles Cabral.[114]

O autor afirma que a abordagem de gerenciamento de riscos se mostra como um modelo apropriado para regular a proteção de dados pessoais, uma vez que o objetivo da tutela jurídica deve ser baseado no fomento do livre fluxo de dados, porém, sem descuidar dos direitos dos indivíduos.[115]

Neste sentido, cada caso empresarial deverá passar por um processo interno de avaliação para melhor adotar as medidas necessárias para compatibilização com os ditames legais.

Todavia, diferentemente do que acontece na Europa, o Brasil possui uma cultura de proteção de dados incipiente. Antes do advento da LGPD, o ordenamento jurídico brasileiro era composto por diversas leis setoriais, causando imensa insegurança jurídica, não somente aos titulares de dados, como também às empresas.[116]

Desta forma, é imprescindível a alteração do comportamento tanto do setor público como do privado, para trazer maior segurança no tratamento de dados e oferecendo maior autonomia para o titular de dados.

---

[114] CABRAL, Filipe Fonteles. **Proteção de dados pessoais na atividade empresarial**: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.
[115] CABRAL, Filipe Fonteles. **Proteção de dados pessoais na atividade empresarial**: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.
[116] DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469- 483, nov.-dez. 2018.

Sobre o tema, Danilo Doneda e Laura Schertel Mendes ensinam que:

> A Lei aprovada proporciona ao cidadão garantias em relação ao uso dos seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor público possam utilizar esses dados pessoais, dentro dos parâmetros e limites de sua utilização. [...], introduzindo o paradigma do controle- pelo qual se garante ao cidadão o controle sobre seus dados, inclusive para que os divulgue e use, em oposição ao paradigma do segredo e do sigilo. A ideia é a de que, com o empoderamento do cidadão e com a institucionalização de mecanismos de controle e supervisão sobre o uso de seus dados, o cidadão passe a ser protagonista das decisões sobre o uso de seus dados, em linha com o conceito de autodeterminação informativa, consagrada em decisão histórica da Corte Constitucional alemã, e agora também positivado como princípio na LGPD.[117]

Para isso, as empresas devem se adaptar às exigências da legislação, implementar práticas de segurança adequadas, criação de políticas interna de proteção de dados, conscientização sobre a importância da privacidade e da segurança das informações pessoais, obter consentimento válido e estarem preparadas para responder as solicitações dos titulares dos dados e às exigências dos órgãos reguladores, como a ANPD.

Em suma, todo o processo de tratamento de dados deverá ser documentado e justificado, garantindo assim maior prestação de contas por parte da empresa, que ficará responsável por informar os processos e meios de segurança que são utilizados, além de resguardar que as informações que foram coletadas são de fato verdadeiras e condizem com a realidade, preservando assim os direitos dos titulares dos dados.

Sobre o tema, Alexandre Prata anota:

> Esses aspectos apontam para a necessidade de endereçar ações com o objetivo de consolidar a proteção de dados e privacidade no seio da organização. Ações que corroborem naturalmente para a mudança de cultura, mas que de início estabeleçam os fundamentos da estrutura formal e investida de autoridade no tema privacidade. Um conjunto de princípios que declare de maneira inequívoca e ampla qual é a postura da organização no que diz respeito à proteção de dados privados. Todo risco de interpretação subjetiva por parte da “tripulação” deve ser mitigado. A malha social da organização deve estar coesa e partilhar de um mesmo objetivo no que tange à proteção de dados e privacidade. Isso só é possível organizando o assunto e abordando questões como as que estão relacionadas a seguir de modo não exaustivo: estrutura; papéis e responsabilidade; engajamento dos

[117] DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. **Revista do Consumidor,** São Paulo, vol. 120, p, 22.

> funcionários; comprometimento da alta administração; políticas; comunicação; controles; e processos.[118]

As empresas devem, inicialmente, estabelecer seus objetivos em relação à proteção de dados, com a implementação de um programa completo de privacidade e proteção de dados, por meio do qual serão traçados os passos a serem percorridos de forma assertiva.

Como medidas exigidas pela LGPD, na fase inicial, as empresas deverão nomear um encarregado da proteção de dados. Este profissional, pessoa natural ou jurídica, também conhecido como DPO (*Data Protection Officer*) atuará efetivamente como um mediador entre os agentes de tratamento (empresa) e os titulares dos dados, bem como com a Autoridade Nacional de Proteção de Dados.

O encarregado é peça fundamental nas organizações pela adequação à LGPD, assim, Rony Vainzof ensina:

> Uma das mais importantes medidas de governança das organizações é justamente avaliar sua nomeação, posição e atribuições, com autonomia e recursos para poder desempenhar, de forma eficaz, a sua função, pois é peça-chave, para não dizer fundamental, no devido cumprimento das leis aplicáveis na mitigação de riscos.[119]

Em complemento, as autoras Filipa Matias Magalhães e Maria Leitão Pereira explicam:

> Pessoa designada pela organização que estará envolvida em todas as questões relacionadas com a proteção de dados pessoais cujas principais funções envolvem informar e aconselhar a empresa sobre a conformidade da proteção de dados, aconselhar sobre a avalição de impacto da proteção de dados, monitorizar a conformidade da proteção de dados, que inclui por exemplo formar equipe e realizar auditorias relacionadas com esta área e cooperar e atuar como ponto de contato com as autoridades de proteção de dados.[120]

As atribuições do encarregado consistem em: (I) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providencias; (II) receber comunicações da ANPD e adotar providências; (III) orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas em relação à

---

[118] PRATA, Alexandre. Organização. In: **Lei Geral de Proteção de Dados:** manual de implementação. São Paulo: RT, 2019, p. 107.
[119] VAINZOF, Rony. Conceito, perfil, papéis e responsabilidade do encarregado. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (coord.). **Data Protection Officer:** teoria e prática de acordo com a LGPD e GDPR. 1. Ed. São Paulo: Thomson Reuters Brasil, 2020, *Ebook*.
[120] MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** Manual Prático. 3 ed. Porto: Vida Econômica, 2020, p. 10.

proteção de dados pessoais, e (IV) executar as demais atribuições determinadas pelo controlador ou normas vigentes.

Portanto, a principal função do encarregado é justamente de servir de ponto de referência para que saiba a quem as demandas relacionadas ao tratamento de dados pessoais devem ser direcionadas, na forma do artigo 41, da LGPD.

Neste sentido, Márcio Cots entende que:

> [...] segundo a nova lei, o encarregado não responderá civilmente perante os titulares ou a autoridade nacional em relação ao tratamento de dados realizados pelo controlador, pois, é este último que concentra todo o poder decisório sobre o tratamento de dados, atuando o encarregado, apenas, como comunicador de tais decisões aos terceiros interessados.[121]

Ademais, a ANPD publicou em 28 de maio de 2021 e atualizou em 2022, o Guia Orientativo para Definições dos Agentes de Tratamento e do Encarregado[122], o qual fornece exemplos práticos e explica quem pode exercer a função do controlador, do operador e do encarregado, além de suas responsabilidades.

É clara a atuação orientativa da ANPD, na busca da adequação das organizações, nos moldes exigidos pela LGPD, visando sanar todas e quaisquer dúvidas existentes, sem deixar margem para eventuais alegações de desconhecimento das normas.

Neste sentido, as organizações empresas que, ainda, não publicaram os dados de seu encarregado, estão em desconformidade com a legislação e sujeitas às sanções administrativas.

A LGPD exige, também, que as empresas obtenham o consentimento explícito e livre dos indivíduos para coletar, armazenar e processar seus dados pessoais, na forma do artigo 6º, inciso VI:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> [...]

---

[121] COTS, Márcio**. Lei Geral de Proteção de Dados comentada**. São Paulo: RT, 2018, P. 220.

[122] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 03 jun. 2023.

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Portanto, as empresas devem informar claramente aos usuários sobre como seus dados serão utilizados, bem como obter uma autorização válida destes.

No mesmo sentido, as empresas devem ser transparentes sobre suas práticas de coleta e tratamento de dados pessoais, como por exemplo, fornecer informações claras sobre os propósitos da coleta de dados, como eles serão usados, por quanto tempo serão retidos e com quem serão compartilhados.

Ademais, também, é necessário que sejam desenvolvidas políticas de privacidade e termos de uso, destinados a regular o acesso aos sites, aplicativos, lojas virtuais e outros meios de atendimento das empresas. Além de realizarem uma análise e gestão de riscos no tratamento de dados pessoais, com a adoção de ações coordenadas, com o objetivo de controlar os possíveis impactos que um determinado tratamento pode gerar.

Ainda, como exigência da LGPD, as empresas devem adotar medidas adequadas de segurança para proteger os dados pessoais que coletam e armazenam, por meio de um conjunto de boas práticas e diretrizes de governança, análogo a um programa de *compliance*.

Nesta esteira, a LGPD se tornou um pilar do *compliance*, em razão de se tratar de uma forma de controle e cumprimento das leis e normas que todas as empresas estão sujeitas.

Estar em *compliance* representa estar em conformidade com as normas e regulamentos vigentes, minimizando riscos e mantendo a organização dentro da legalidade.

Portanto, diante da preocupação das empresas quanto à possibilidade de arcar com as sanções administrativas, aplicáveis pela ANPD, o *compliance* se torna um instrumento de controle de processos e sustentabilidade empresarial.

A expressão *compliance* provém do verbo inglês *to comply*, que indica “estar de acordo”. Trata-se da adoção das normas legais e regulamentares de uma

determinada instituição ou empresa. Em outros termos, é agir de acordo com a lei, regulamentos e preceitos éticos.[123]

Neste sentido, Henrique Correia define o *compliance* como prática empresarial que “consiste na criação de um sistema de controle e fiscalização interno na empresa para reduzir os riscos à imagem do negócio por meio do correto cumprimento das normas aplicáveis à instituição”.[124]

Sobre essa jornada de planejamento, Lygia Maria Moreno Molino Henrique indica:

> [...] para um bom compliance com a Lei Geral de Proteção de Dados Pessoais, a empresa deve: (i) definir o seu papel em relação ao tratamento de dados; (ii) promover engajamento dos colaborares com a questão, visando uma mudança cultural; (iii) ajustar as bases legais de acordo com o tipo de tratamento a ser realizados; (iv) ser transparente e honesta em suas relações; (v) investir em sua confiabilidade (por meio de certificações, boas práticas e outras garantias); (vi) investir em segurança da informação; (vii) escolher bem seus parceiros; (viii) zelar por todos os relacionamentos advindos do tratamento de dados, do modo mais transparente possível.[125]

Claramente, o *compliance* traz grandes vantagens econômicas e reputacionais para as empresas que adotam, dentre elas podem ser citados:

> [...] (i) vantagens reputacionais, (ii) o estímulo para maior investimento em inovação e qualidade, em razão da sua supressão dos benefícios decorrentes de vantagens ilícitas, que alteram a dinâmica concorrencial, (iii) melhorias do padrão de gestão organizacional, que podem contribuir para a eficiência da empresa, (iv) aumento das oportunidades de negócio, e, por fim, (v) a própria economia decorrente da prevenção do ilícito e/ ou da minoração de seus danos.[126]

Todavia, para que o programa de *compliance* seja de fato eficaz, é necessário que sejam elencados os principais riscos aos quais a empresa está sujeita ao realizar o tratamento de dados pessoais.

> [...] bons programas de compliance baseiam-se na correta identificação dos riscos e implementação de procedimentos que a eles respondam adequada e proporcionalmente; na reavaliação periódica dos riscos, com o implemento de adaptações; no comprometimento da alta administração; na capacidade

---

[123] BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. **Manual de Compliance**. Rio de Janeiro: Forense, 2019. p. 35

[124] CORREIA, Henrique. Compliance e sua aplicação no direito do trabalho. **Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região**, Brasília, DF, ano IX, n. 91, ago./2020. Disponível em:https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/151250/2020_correia_henrique_compliance_aplicacao.pdf?sequence=1&isAllowed=y. Acesso em: 2 jun. 2023. p. 17

[125] HENRIQUE, Lygia Maria Moreno Molina. **LGPD:** cuidados na implementação. Revista Forense, v. 429, 2019.

[126] FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance:** perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 80.

> de a organização identificar e agir para minimizar os riscos; e no estabelecimento de eficientes canais de comunicação (internos e externos).[127]

Sob essa ótica, o plano de *compliance* visa gerenciar adequadamente os riscos das atividades, identificar possíveis não conformidades e danos causados, contribuir para a redução de perdas, fortalecer o estabelecimento de uma cultura corporativa que atenda aos padrões legais e proporcione um serviço de redução de riscos.[128] Ou seja, a implementação de programas de *compliance* de dados pessoais é essencial para garantir a observância da LGPD.

De modo geral, as organizações assumem perante seus funcionários e clientes um compromisso de implantar um programa de integridade, em especial, no que tange a proteção dos dados coletados e tratados, para propiciar o bem oferecido.

Ademais, em determinadas situações, a LGPD requer a realização de um Relatório de Impacto à Proteção de Dados (RIDP), previsto no artigo 38, da LGPD, o qual é instrumento de importante valia para determinar o fluxo de dados e a sua relação com a empresa, sendo fundamental na instituição de um programa de *compliance*.

Segundo a *Information Commissioner's Office* (ICO), autoridade de controle do Reino Unido, conceitua RIPD como:

> Um processo projetado para ajudar a analisar, identificar e minimizar sistematicamente os riscos de proteção de dados de um projeto ou plano. É uma parte fundamental de suas obrigações de responsabilidade sob o GDPR e, quando feito de forma adequada, ajuda a avaliar e demonstrar como são cumpridas as obrigações de proteção de dados.[129]

Este documento com o objetivo de analisar os riscos associados ao tratamento de dados pessoais e identificar medidas para mitigar esses riscos, eliminando os processos que possam configurar ameaça ou possibilidade de ocorrência de eventos danosos.

---

[127] FRAZÃO, Ana. Compliance de dados pessoais. In.: **Lei Geral de Proteção de Dados Pessoas e suas repercussões no direito brasileiro** (coord. Gustavo Tepedino, Ana Frazão e Milena Donato Oliva). São Paulo: Thomson Reuters Brasil, 2019, p. 699.

[128] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 686.

[129] INFORMATION Commissioner's Office. **Whats is a DPIA?** Disponível em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/#:~:text=A%20Data%20Protection%20Impact%20Assessment,a%20high%20risk%20to%20individuals. Acesso em 20 mai de 2023.

> Nesse sentido, a finalidade principal do relatório de impacto à proteção de dados pessoais é de apontar qualquer risco que possa advir daquela operação de tratamento de dados pessoais, e direcionar o controlador e/ou o operador à mitigação daqueles riscos mapeados.
> Trata-se de uma avaliação de risco similar à prevista na norma técnica ISO 27.001, de modo que empresas que já passaram pela adequação à referida norma, que já identificaram dados pessoais como um ativo da companhia, e realizaram o levantamento dos riscos ao redor desses dados, estão muito próximas com o cumprimento do requisito do artigo 38 da Lei Geral de Proteção de Dados.[130]

Contudo, a LGPD já sinaliza a necessidade do Relatório de Impacto nas atividades que envolvem o tratamento de dados sensíveis, bem como nas operações de tratamento de dados envolvendo legítimo interesse, na forma do artigo 10, § 3º da referida lei.

Todavia, se a empresa não está certa quanto à necessidade de um relatório de impacto para determinada atividade de tratamento de dados, o recomendável é por fazê-lo, com o intuito de mitigar riscos e sanções futuras.

> Importante salientar que, do ponto de vista da proteção de dados pessoais, é recomendável à empresa conduzir a elaboração do relatório de impacto não apenas nas hipóteses em que a Lei Geral de Proteção de Dados e o futuro regulamento exigem, mas em todas as situações em que possa antever riscos aos titulares dos dados pessoais tratados. Trata-se da postura mais segura, e recomendável, notadamente em operações que possam envolver avaliações sistemáticas de aspectos pessoais, tratamento de dados pessoais em grande escala, decisões automatizadas com efeitos significantes, monitoramento automática, processamento de dados pessoais de titulares vulneráveis, limitação no exercício dos direitos dos titulares, entre outras operações onde o risco ao titular seja potencial.[131]

Como outro passo importante para a adequação das empresas, após a identificação dos riscos, é a elaboração interna de um código de conduta, ou como a LGPD nomeia de código de boas práticas e governança, em seu artigo 50.

Ressalta-se que a implementação de boas práticas de governança de dados Brasil, ao contrário da Europa, não é obrigatória.

Segundo o entendimento de John Ladley,

> [...] a governança de dados é a organização e implementação de políticas, procedimentos, estrutura, papéis e a responsabilidade que delineiam e

---

[130] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados comentada [livro eletrônico/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. - 2. ed. - São Paulo: Thomson Reuters Brasil, 2019.

[131] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 245.

> reforçam regras de comprometimento, direitos decisórios e prestação de contas para garantir o gerenciamento apropriado dos ativos de dados.[132]

Por isso, é preciso que as práticas de governança permeiem todas as área e relacionamentos da empresa, mostrando o integral comprometimento desta com as legislações em vigor.

Por fim, a LGPD prevê a necessidade de que o programa de governança contenha um plano de resposta a incidente e remediação. Portanto, as empresas precisam estar prontas e saibam agir em caso de um incidente de segurança. Para isso, é necessário que seja criado um plano de resposta a incidentes, para ser iniciado assim que o incidente de segurança ocorrer.

Neste sentido, a ANDP define incidente de segurança de dados pessoais como:

> Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamentos de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.[133]

O descumprimento das exigências impostas pela LGPD não são apenas uma faculdade, mas sim, obrigações a serem cumpridas. O não cumprimento sujeitará as empresas às sanções impostas, que são severas e poderão impactar profundamente a reputação da empresa.

3.2. A Responsabilidade das Empresas nos Casos de Incidentes de Segurança e Vazamento de Dados

Antes de adentrarmos especificamente no tema da responsabilidade do agente de tratamento de dados, deve-se conceituar, com base na doutrina e legislação, o que é um incidente de segurança da informação categorizado como vazamento de dados, conhecido também como *data breach*.

---

[132] LADLEY, John. Data Governance: how to desig, deploy and sustain na effective data Governance program. **The Morgan Kaufmann Series on Business Inteligence**, 2012.

[133] ANPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico Acesso em: 20/06/2023.

O Regulamento Geral de Proteção de Dados Europeu, uma vez que LGPD não definiu, conceitua o incidente de segurança como:

> [...] uma violação que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.[134]

Para o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, é "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas, modificações em um sistema de computação ou de rede de computadores".[135]

Portanto, os incidentes de vazamento de dados pessoais ocorrem quando a violação de segurança acaba por expor informações de pessoas naturais, protegidos ou confidenciais, que são copiados, transmitidos ou roubados por pessoas não autorizadas. Eles são muito diversificados, podendo ser varreduras em redes de computadores, ataques *web*, invasões ou acesso não autorizado a computadores e redes.

Segundo informações trazidas pela ANPD em seu sítio eletrônico, desde o dia 01/01/2023 até 20/05/2023, foram protocolados 71 (setenta e um) Comunicados de Incidentes de Segurança - CIS, tendo 13 (treze) CIS decorrentes de sequestro de dados (os *ransomware*[136]) sem transferência de informações e 9 (nove) CIS causados por sequestro de dados (*ransomware*) com transferência de informações e/ou publicação de informações.[137]

---

[134] Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt Acesso em: 20 jun. 2023.

[135] Núcleo de Informação e Coordenação do Ponto BR. **Estatísticas dos Incidentes Reportados ao CERT.BR.** Disponível em: < https://www.cert.br/stats/incidentes/2018-jandec/tipos-ataque.html >. Acesso em 13 mai. 2023.

[136] *Ransomware* trata-se do uso de software malicioso, que se utiliza de criptografia e compactação de dados com senha e torna reféns as informações digitais das vítimas – principalmente empresas. Em outra perspectiva, *ransomware* é um pedido de resgaste em troca de desbloquear o acesso aos dados de um sistema, usado para atingir, com algumas exceções notáveis, empresas relativamente pequenas, quase sempre sem sistemas de segurança sofisticados ou especialistas em pessoal nesse assunto. A palavra *ransom*, em inglês, significa resgate; caso ele não seja pago, os dados são apagados ou então tornados públicos, causando danos aos seus proprietários.

[137] Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/numeros_fiscalizacao. Acesso em: 21 mai. 2023.

O *ransomware* é um instrumento principal de forma de chantagem dos criminosos, que ao privarem as vítimas de seus dados, cobram valores exorbitantes para descriptografar os arquivos raptados.

Na maioria das vezes, os criminosos estipulam prazos curtos para o pagamento em dinheiro ou até mesmo em criptomoedas, sem margem para que a vítima possa refletir sobre o ataque.

Nesse sentido, algumas empresas cedem a esses pedidos de resgate, pagando valores elevados, na ilusão de que essa é a maneira mais rápida de voltar a operar normalmente.

O site *Flowti* veiculou que os criminosos virtuais encontraram na LGPD, uma forma a mais de compelir as empresas a pagarem pelo resgate de seus dados, considerando que ao invadirem os computadores das corporações e raptarem os dados críticos e pessoais de cooperadores ou clientes.

Os criminosos expõem as falhas de segurança da empresa, o que revela uma falha na adequação aos requisitos impostos pela referida lei, dando margem para que a empresa seja multada pela ANPD, ou ainda, acionada judicialmente.

Sob a ótica das empresas, um ataque cibernético, além de causar complicações com dados e informações sigilosas, também pode causar prejuízo financeiro às empresas, podendo levá-las a uma perda, muitas vezes, sem retorno. Não esquecendo das eventuais ações judiciais e processos administrativos.

Desse modo, as empresas devem estar preparadas para eventuais ações judiciais individuais e coletivas, para cooperar com investigações administrativas e judiciais, processos administrativos, auditorias, multas, resposta à incidentes, danos à imagem e reputação empresarial, dentre outros.

Não é só. O tratamento de dados inadequado pode acarretar o vazamento de dados pessoais, além de penalizações que, fatalmente, gerará diversos prejuízos e infortúnios de várias sorte ao seu titular, como dano moral, patrimonial e moral.

Essa violação, dá ensejo à obrigação de reparação pelo dano causado, conforme determina o artigo 42 da LGPD, bem como os responsáveis estarão sujeitos às punições estabelecidas diante da inobservância de normas jurídicas previstas em leis esparsas, como o Código Civil e o Código de Defesa do Consumidor.

Em razão da essencialidade da segurança da informação, atualmente, a LGPD conceitua, no artigo 44, o tratamento de dados pessoais irregular, como aquele em que o agente de tratamento incide nos comportamentos de “deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar”.

O que se tem que ter em mente é que, muitas vezes o vazamento de dados ocorre por causa de ataques cibernéticos, de *hackers*, que trazem diversos prejuízos à empresa, que muitas vezes desembolsa valores milionários, à título de resgate do “sequestro de dados”, mas também, acaba sendo acionada pelos titulares de dados lesados, na busca pela reparação por danos morais e materiais.

Um vazamento de dados pode acarretar diversas consequências danosas às empresas, tais como: sanções administrativas, como multas; perdas financeiras por conta de negócios cancelados, fuga de investidores e vazamento de informações sensíveis à empresa; quebra de confiança na relação com o consumidor e com os titulares de dados em geral; danos de reputação e imagem; ações judiciais individuais e coletivas por parte de titulares de dados e de entidades de defesa do consumidor. Exemplos não faltam ao redor do mundo.

Em 2016, nos Estados Unidos, a Uber teve dados vazados de 57 milhões de usuários e motoristas em todo o mundo. O fato resultou em um acordo com governo daquele país, no importe de R$ 500.000.000,00 (quinhentos milhões reais), além de multa por Autoridades de Controle do Reino Unido e da Holanda, no valor aproximado de R$ 4.500.000,00 (quatro milhões e quinhentos mil reais).

Salienta-se que, em caso de violação de dados que possa resultar em risco ou danos aos titulares dos dados, a LGPD estabelece que o responsável pelo tratamento de dados deve estar preparado para reagir aos casos de incidentes.

Nesse sentido, a LGPD prevê o dever de notificação à ANPD e ao titular, na forma do seu artigo 48, fornecendo informações claras sobre a natureza da violação, as medidas adotadas para mitigar os impactos e as recomendações para proteção dos titulares dos dados. Caso a empresa permaneça inerte, tal inércia na adoção de notificação aos titulares de dados, poderá acarretar sanções administrativas.

A título de exemplo, tem-se o caso da empresa Altaba, que entre os anos de 2013 e 2016, foi alvo de violações de segurança que resultaram no vazamento de dados de mais de 1 bilhão de usuários, que permitiu o vazamento de identidades e o uso indevido dos dados pelos criminosos.

Nesse caso, a falta de divulgação ao mercado, que poderia evitar ou mitigar os danos, gerou um acordo com autoridades governamentais envolvendo o pagamento de R$ 190 milhões, além de multas e acordos com os investidores da empresa.

Sobre o tema, destaca-se que, no Brasil, nem todo vazamento de dados será considerado como incidente de segurança punível sob a égide da LGPD. A título de exemplo, caso ocorra o vazamento de um segredo industrial, ele será punido a partir da Lei de Propriedade Intelectual.

Por isso, para que haja a configuração de infração à LGPD, o incidente de segurança deverá envolver o vazamento de dados pessoais, que possa acarretar risco ou dano relevante aos titulares.[138]

Portanto, ao passo em que a empresa tomar conhecimento de uma violação de dados, é fundamental a realização de uma avalição completa do incidente, incluindo a identificação da natureza dos dados afetados, o escopo da violação, as possíveis consequências para os titulares dos dados e a gravidade do incidente.

A ocorrência de um incidente que resulte no vazamento de dados, além de ser absolutamente indesejado pelas empresas, por expor informações de todos os gêneros, ferindo direitos fundamentais, pode acarretar inúmeras repercussões negativas ao negócio.

Por isso, a segurança do ambiente de dados é uma responsabilidade da empresa, que deve ter o comprometimento e investir em sistemas de proteção e correção de vulnerabilidades a que os processos se encontrem de alguma forma expostos, além de demonstrar o empenho e a atenção com que lida com a proteção de dados pessoais.

[138] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

4. OS IMPACTOS DAS SANÇÕES ADMINISTRATIVAS PREVISTAS NA LGPD NA ATIVIDADE EMPRESARIAL

O presente capítulo pretende perquirir a responsabilização administrativa dos agentes de tratamento de dados pessoais, em especial empresas, em razão de violações à Lei Geral de Proteção de Dados Pessoais, sob a ótica das sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados.

Diante disso, como já extensivamente narrado, a preocupação acerca da privacidade pelas instituições públicas e privadas, se dá pelo fato de que a proteção de dados pessoais não ser apenas uma escolha, e sim, uma adequação aos termos da LGPD.

Neste contexto, as organizações públicas e empresas que não se adequarem à legislação e violarem seus preceitos, se submeterão às suas sanções, que serão aplicadas pela ANPD.

O artigo 52, da LGPD, elenca referidas sanções administrativas, que incluem desde advertências até a aplicação de multas sobre o faturamento da pessoa jurídica de direito privado, limitadas ao valor de R$ 50.000.000,00 (cinquenta milhões de reais), por infração.

Com exceção das multas, todas as demais sanções poderão ser aplicadas ao Poder Público.

Por óbvio, e como é ressaltado pelos membros da ANPD, as sanções buscam desmotivar, de forma responsiva, aqueles que realizam o tratamento de dados pessoais, com objetivos econômicos e financeiros. E, certamente, a multa pecuniária é de grande valor, em razão do intuito de coibir a prática indevida do tratamento de dados, que causem danos a terceiros.

Todavia, a LGPD traz, também, a previsão do agravamento das punições com a suspensão parcial ou total das atividades de tratamento de dados pessoais pelo agente responsável.

Nos casos de suspensão total, a proibição da atividade de tratamento de dados pessoais, em empresas que seja imprescindível em seu objeto social, poderá ocasionar no fechamento da empresa, em razão do encerramento de suas atividades.

Neste sentido, Ricardo Oliveira:

> [...] as sanções administrativas previstas na LGPD variam, mas as mais graves podem resultar na quebra de um negócio. Quando digo mais graves não me refiro aquelas que são pecuniárias. Imagine que um prestador de serviços seja penalizado com a sanção estabelecida no artigo 52, inciso IV, que prevê a "publicização da infração após devidamente apurada e confirmada a sua ocorrência". Dependendo do segmento no qual atue, a perda dos contratos dos demais clientes pode ser consequência natural pois, quem confiaria em um prestador de serviços que não trata adequadamente os dados pessoais que lhe são confiados?
> Naturalmente que evitar as sanções legais não deveria ser a tônica dos projetos de adequação, assim como utilizar o cinto de segurança não deveria se dar por mero receio do recebimento de multas. Há uma questão de fundo que deve ser preservada e, no caso da LGPD, é o tratamento de dados pessoais adequado, colocando a proteção e a privacidade do titular em primeiro lugar.
> Entretanto, o recebimento de multas nesse momento pode comprometer a melhor das intenções. Isso porque, com a economia em frangalhos, os recursos financeiros devem ser bem utilizados e canalizados, não havendo espaço para desperdícios como poderia ser o custo de uma penalidade administrativa. Em outras palavras, uma multa pode comprometer o investimento que se poderia fazer para criar ambiente mais seguro e adequado de tratamento de dados pessoais.[139]

Há de se ressaltar, que a LGPD entrou em vigor no dia 18 de setembro de 2020, data em que todos os agentes de tratamento de dados pessoais já estavam sujeitos aos processos judiciais individuais e coletivos sobre o tema.

Todavia, apenas em 1º de agosto de 2021, passou a valer as sanções previstas na LGPD, restando pendente regulamento próprio sobre sanções administrativas. Portanto, o período de quase um ano, entre a entrada em vigor da LGPD e início das sanções previstas, serviu de tempo para a sociedade, em especial, as empresas se adequarem às exigências e afastarem as sanções administrativas que são possíveis desde agosto de 2021.

---

[139] OLIVEIRA, Ricardo. **LGPD:** Como evitar as sanções administrativas. São Pialo Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 04 jun. 2023.

Em razão do período entre a entrada em vigor da LGPD e o início das sanções, o papel do judiciário foi de grande importância. A título exemplificativo, tem-se a sentença proferida no Processo n.º 1080233-94.2019.8.26.0100, no dia 29/09/2020, oriunda da 13ª Vara Cível do Tribunal de Justiça do Estado de São Paulo, em face da empresa Cyrela Brazil Realty S/A Empreendimentos e Participações.

Na ocasião, a empresa, companhia do ramo imobiliário, foi condenada a indenizar em R$ 10.000,00 (dez mil reais) um cliente que teve informações enviadas para outras empresas (instituições financeiras e empresas de decoração), que passaram a importunar o consumidor. Tal decisão foi fundada na violação aos dispositivos da LGPD e tutela constitucional.

Outro caso recente foi a decisão proferida pela 8ª Câmara de Direito Público do Tribunal de Justiça do Estado de São Paulo, que condenou a empresa Via Quatro, concessionária da Linha 4 (Amarela) do metrô da capital paulista, a pagar indenização de R$ 500.000,00 (quinhentos mil reais) por dano moral coletivo, devido ao uso do sistema de câmeras de segurança para captação, sem consentimento, de imagens dos usuários para fins comerciais e publicitários, em 2018.

Em suma, a ação foi movida pelo Instituto de Defesa do Consumidor, que pediu uma indenização total de R$ 100.000.000,00 (cem milhões de reais), em razão da detecção facial não consentida em sete estações da Linha 4 (Amarela). O sistema de câmeras implantado identificava emoção, gênero e faixa etária das pessoas posicionadas em frente anúncios publicitários.

No acordão, o desembargador Antônio Celso Faria, relator do caso, criticou a captação de imagens para fins comerciais, bem como afirmou que incumbe a empresa arcar com o risco das atividades econômicas que explora, especialmente por envolver os direitos fundamentais à intimidade, à privacidade, à imagem e a honra dos usuários, o que não ocorreu.

Ademais, também observou que os usuários do metrô não foram comunicados prévia ou posteriormente sobre a captação ou o uso de sua imagem. Segundo o desembargado, isso “afronta, claramente, o direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos e desleais”.

Contudo, em levantamento realizado pelo escritório Opice Blum, na produção do Relatório Anual de Jurimetria 2022, nem todos os processos há o acolhimento de indenização por danos morais.

Isso se justifica, em razão da maioria dos processos judiciais analisados, envolvendo a LGPD, não resultarem em condenação, ou seja, cerca de 57% das decisões em segunda ou superior instância, que trataram da matéria trazida pela Lei Geral de Proteção de Dados, não resultaram qualquer condenação (mantendo-se ou determinando a improcedência ou extinção do feito).[140]

Ademais, cerca de 65% das decisões em segunda ou superior instância exigiram comprovação do dano moral, indicando tendência de que ele não possui natureza *in re ipsa* (presumido), portanto, os danos morais devem ser comprovados na maior parte dos casos para gerar condenação.[141]

Em consonância com referido Relatório, o STJ ao julgar o AREsp 2.130.619, entendeu que o vazamento de dados pessoais comuns não gera dano moral presumido, ao argumentar que, os dados pessoais vazados geram dano moral, mas este não pode ser presumido, devendo haver comprovação de dano para que a indenização seja aplicada.[142]

---

[140] RELATÓRIO ANUAL DE JURIMETRIA 2022. Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf. Acesso em 03 jun. 2023.

[141] RELATÓRIO ANUAL DE JURIMETRIA 2022. Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf. Acesso em 03 jun. 2023.

[142] Ementa: PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. *In casu*, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais, mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o

Portanto, frente às decisões judiciais, verifica-se que ainda não há entendimento uniforme sobre o assunto e aplicação de condenações em razão de danos extrapatrimoniais em virtude de vazamentos de dados sensíveis.

4.1. Sanções Administrativas Aplicáveis pela ANPD

No ordenamento jurídico, há diversos tipos de sanções nas esferas penal, civil, regulatória, entre outras. E, no mesmo sentido, a LGPD, trouxe em seu artigo 52, uma lista de sanções administrativas que pretendem estimular o cumprimento de uma determinada regra, que serão aplicadas pela Autoridade Nacional de Proteção de Dados.

Em que pese a ANPD ressaltar sua atuação responsiva, visando, em princípio, orientar as empresas, suas sanções administrativas, em geral, têm dois objetivos: (i) punir o causador do dano, independentemente do dano gerado; (ii) ressarcir do dano gerado pela violação da norma, visando retribuir o agente pelo descumprimento.

Neste sentido, Rafael Munhoz de Mello ensina que:

> [...] a sanção administrativa retributiva se destina a imputar um mal ao infrator de acordo com o ato ilícito praticado. Esse tipo de sanção não está voltado ao ressarcimento dos danos causados pela conduta delituosa. A sua finalidade é evitar a repetição de novos atos ilícitos. Tem, assim, caráter repressivo.[143]

Na mesma linha, Fábio Medina Osório esclarece:

> Sanção (administrativa retributiva) é um mal, um castigo, e, portanto, implica um juízo de privação de direitos, imposição de deveres, restrição de liberdades, condicionamentos, ligados, em seu nascedouro e existência, ao cometimento de um ilícito administrativo. [...] consequência de conduta ilegal, tipificada em norma proibitiva, com uma finalidade repressora ou disciplinar, no âmbito de aplicação formal e material do Direito Administrativo.[144]

---

titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.

[143] MELLO, Rafael Munhoz de. **Princípios constitucionais de direito administrativo sancionador:** as sanções administrativas à luz da Constituição Federal de 1988. São Paulo: Malheiros, 2007.

[144] OSÓRIO, Fábio Medina. **Direito administrativo sancionador**. São Paulo: Ed. RT, 2010.

Portanto, as sanções trazidas pela LGPD, são claramente sanções retributivas, considerando que não visam desfazer um mal, mas sim de se desencorajar a infração legal, por meio de multas, advertências, cassação de autorização, entre outras hipóteses previstas.

A título de exemplo, uma empresa milionária pode pagar uma multa de até R$ 50.000.000,00 (cinquenta milhões de reais), de acordo com o seu faturamento, sem causar danos financeiros, porém, essa sanção não “doeria” e não teria a mesma eficácia. Contudo, se a sanção fosse em relação ao bloqueio da base de dados, ela seria extremamente danosa e, talvez, a empresa não sobrevivesse.

Diante disso, a LGPD estabeleceu critérios para dosimetria da sanção, por meio do Regulamento de Dosimetria Aplicação de Sanções Administrativas, publicado em 27 de fevereiro de 2023, com o objetivo de garantir a proporcionalidade entre a sanção aplicada e a gravidade da conduta do agente, além de proporcionar segurança jurídica aos processos fiscalizatórios, bem como garantir o direito ao devido processo legal e ao contraditório.

Segundo, Antônio José Calhau de Resende as sanções administrativas devem respeitar ao princípio da razoabilidade que:

> [...] é um conceito jurídico indeterminado, elástico e variável no tempo e no espaço. Consiste em agir com bom senso, prudência, moderação, tomar atitudes adequadas e coerentes, levando-se em conta a relação de proporcionalidade entre os meios empregados e a finalidade a ser alcançada, bem como as circunstâncias que envolvem a prática do ato.[145]

Sendo assim, o que se espera da a ANPD, na aplicação das sanções administrativas, é punição das organizações infratoras, porém, sem as levar à falência ou interrupção de suas atividades econômicas.

A advertência é a primeira sanção prevista e mais branda delas. Ela poderá ser aplicada pela ANPD de forma condicionada ou não a adoção de medidas coercitivas. Em seguida, há previsão da multa simples e multa diária, dois tipos de sanções pecuniárias.

---

[145] RESENDE, Antonio José Calhau. **O princípio da razoabilidade dos atos do Poder Público.** Revista do Legislativo, abr. 2009.

A multa simples tem o caráter indenizatório, visando reparar o dano causado pelo agente de tratamento pelo cometimento de uma infração. Contudo, a multa diária tem natureza de medida coercitiva, com o intuito de compelir o agente de tratamento de dados a cumprir com uma obrigação legalmente imposta.

Para José Rogério Cruz e Tucci, multa diária é:

> Tal sanção não tem caráter indenizatório ou ressarcitório. Trata-se exclusivamente de técnica impositiva do cumprimento de decisões judiciais de modo mais célere e adequado. Possui, pois, conotação coercitiva, objetivando atuação ou abstenção específica do sujeito processual que se encontra obrigado a um fazer ou não fazer.[146]

Em ambas as situações, a LGPD estabelece um limite de 2% do faturamento da pessoa jurídica de direito privado, no último exercício, excluído os tributos, com teto máximo de R$ 50.000.000,00 (cinquenta milhões de reais).

Há, ainda, a penalidade de publicização da infração. Ela impõe ao agente de tratamento o dever de tornar pública a condenação que sofreu em razão da infração, o que sugere potenciais implicações reputacionais às organizações, com reflexos na perda de receita, aumento de custo operacional, queda na confiança dos *stakeholders* (clientes, fornecedores e outras partes interessada), entre outros

Neste sentido, Fabrício da Mota Alves destaca que esta penalidade se assemelha àquele chamado de *shame sanction* (penas criminais infamantes), próprios do Direito Penal econômico moderno, apresentada como alternativa de penalização mais severas. Destaca-se que a lei espanhola[147] e a lei francesa[148] de proteção de dados pessoais, também, adotam a sanção de publicização da infração.

---

[146] CRUZ E TUCCI, José Rogério. **Natureza, compatibilidade e limites subjetivos da multa coercitiva**. 2018. Disponível em: https://www.conjur.com.br/2018-jan-09/paradoxo-corte-naturezacompatibilidade-limites-subjetivos-multa-coercitiva. Acesso 13 mai 2023.

[147] A lei espanhola de proteção de dados estabelece que serão publicadas as infrações cuja multa seja superior a € 1.000.000, nos seguintes termos do art. 76, em tradução livre: 4. Será objeto de publicação no Diário Oficial do Estado a informação que identifica o infrator, a infração cometida e o montante da sanção aplicada quando a autoridade competente for a Agência Espanhola de Proteção de Dados, a sanção exceder um milhão de euros, e o infrator for uma pessoa jurídica. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673. Acesso em 13 mai. 2023.

[148] A autoridade francesa também pode determinar a publicação de sua decisão, o que poderá acontecer imediatamente à notificação, em publicações, jornais ou mídias de sua escolha, às custas do autuado. Neste caso, o autuado poderá recorrer da decisão.

Em continuidade, os agentes de tratamento também estão sujeitos ao bloqueio e eliminação dos dados pessoais. Tal sanção visa impedir o tratamento dos dados pessoais envolvidos na infração, de forma temporária no caso de bloqueio e de forma permanecente no caso de eliminação.

No mesmo sentido, há previsão legal sobre a possibilidade de suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Diante das sanções administrativas, previstas pela LGPD, tem-se que a melhor forma de evitá-las é, obviamente, a adequação à referida lei. Ou seja, as empresas devem criar programas efetivos em atendimento à LGPD, analisar como é feito o tratamento de dados dentro da organização e adequá-lo às exigências legais.

4.2. As Sanções Previstas Podem vir a Inviabilizar a Atividade Empresarial?

Como visto anteriormente, as sanções administrativas podem ser aplicadas aos agentes de tratamento em razão do descumprimento de qualquer preceito da LGPD, e não somente o famoso vazamento de dados pessoais.

As empresas podem ser punidas por ofensa a um princípio eventualmente não observado em determinada atividade de tratamento, como por exemplo, coletar dados pessoais sem informar ao titular qual a finalidade daquela coleta ou obter o consentimento deste.

Caso similar ao exemplo acima exposto ocorreu com a empresa Microsoft, que terá que arcar com multa de US$ 20 milhões, aproximadamente R$ 98.400.000,00 (noventa e oito milhões e quatrocentos mil reais), aplicada pelo *Federal Trade Comission*, em razão da empresa ter coletado informações pessoais de crianças menores de 13 anos que criaram contas na *Xbox Live* (jogos de videogame), sem notificar ou obter consentimento dos pais, entre os anos de 2015 e 2020.

Ademais, em que pese as previsões estabelecidas na LGPD, no Brasil, ainda não se verifica na prática a aplicação de sanções pecuniárias previstas na LGPD, porém, é possível se basear pelas experiências de outros países que possuem as mesmas previsões.

O ICT Legal Consulting lançou relatório contendo o resumo das sanções administrativas aplicadas por autoridades de proteção de dados da União Europeia entre 2018 e 26 de março de 2022, em razão de violações ao princípio da segurança e de notificações obrigatórias às autoridades e aos titulares de dados.[149]

Na Itália, em 11 de dezembro de 2019, a Autoridade Italiana de Proteção de Dados (*Garante per la protezione dei dati personali*) multou em € 8,5 milhões a *Enis Gas e Luce* (EGL) após constatação de processamento ilegal de atividades de *telemarketing* e televendas.[150]

As denúncias recebidas pela DPA (*Data Protection Authority)* decorriam de chamadas publicitárias feitas sem consentimento do titular, ausência de medidas técnicas e organizacionais capazes de acomodar as manifestações de vontade dos usuários, bem como aquisição de dados de potenciais clientes sem consentimento deles.

A despeito, a LGPD tem previsão de sanções para casos semelhantes, todavia, somente há processos fiscalizatórios que estão sob investigação da ANPD, sem nenhuma aplicação concreta das medidas coercitivas. Como exemplo, cita-se o Processo n.º 001688/2022-98, tendo como agente de tratamento, Instituto Nacional do Seguro Social (INSS) e Dataprev, e o escopo da análise é a verificação de conformidade do tratamento de dados pessoais, em razão do compartilhamento para oferta de empréstimos consignado.[151]

---

[149] Disponível em: https://www.ictlegalconsulting.com/?lang=en Acesso em: 20 jun. 2023.
[150] Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/report_multas_VF.pdf Acesso em: 20 jun. 2023.
[151]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2023. **Relação atualizada dos processos administrativos sancionatórios instaurados pela ANPD**. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao. Acesso em 03 jun. 2023.

No que tange ao vazamento de dados, temos inúmeros exemplos de sanções aplicadas por outras Autoridades Nacionais, como ocorreu, na Eslováquia, o Gabinete de Proteção de Dados da Eslováquia multou em € 40 mil a *Slovak Telekom,* após vazamento envolvendo dados da própria empresa e de 22 clientes.

Para a DPA, a empresa não implementou medidas técnicas e organizacionais adequadas para garantir a segurança das informações, distribuindo contratos a destinatários incorretos (ou seja, pessoas não autorizadas), que incluíam dados pessoais como nome, residência, data de nascimento, número de carteira de identidade, número de telefone e *e-mail.*

Como visto, a multa é a sanção mais frequentemente aplicada pelas autoridades europeias de proteção de dados pessoais e é esperado cenário similar no Brasil, em razão da forte influência europeia na Lei Geral de Proteção de Dados brasileira.

Neste sentido, presume-se que para as empresas serão aplicadas sanções pecuniárias em razão de eventuais descumprimentos dos preceitos da LGPD, ao menos no primeiro momento.

Além disso, a mera aplicação de multa já pode ser uma considerável ameaça às empresas, já que estas, frequentemente, apresentam dificuldades financeiras, em especial após a pandemia do COVID-19, que abalou diversas organizações.

Como mencionado, haverá casos, em que, além do pagamento da multa, a empresa pode ter pagado, também, resgate exigido por *hackers*, em decorrência de ataques, causando enorme abalo financeiro à empresa, além de eventuais ações judiciais.

Porém, o impacto maior que qualquer pagamento, é a publicização da infração, que causa danos reputacionais. Eles poderão perdurar por anos, já que o mercado como um todo perde a confiança no agente de tratamento que frequentemente se envolve em incidentes com dados pessoais.

E, para aplicação da pena de proibição do tratamento de dados pessoais, esta só poderá ocorrer após ter sido imposta ao menos uma das seguintes sanções administrativas: multa simples, multa diária, publicização da infração, bloqueio e eliminação dos dados pessoais a que se refere a infração. Diante deste cenária, certamente que as empresas penalizadas não terão alternativa a não ser a interrupção de suas atividades.

Relevante reiterar que as sanções previstas serão aplicadas somente mediante processo administrativo, respeitado os princípios da ampla defesa, do contraditório e com direito a recurso.

Ademais, na aplicação de sanções serão considerados parâmetros e critérios previstos em lei, como, por exemplo, a cooperação do infrator, a pronta adoção de medidas corretivas e a implementação de mecanismos internos para o tratamento adequado dos dados.

Portanto, a empresa, responsável pelo tratamento de dados, deverá criar evidências das medidas adotadas na busca pelo cumprimento da LGPD, que servirão como fator de gradação para aplicação de eventuais sanções.

Novamente, a LGPD é obrigatória para todas as empresas que tratam dados pessoais para fins econômicos, independente do seu tamanho. Entretanto, para integral cumprimento das exigências impostas pela lei, poderá acarretar investimentos de fundos financeiros, já escassos para empresas de pequeno porte, por exemplo.

Todavia, em que peses os investimentos dispensados para a adequação quanto ao tratamento dos dados, conforme a Lei Geral de Proteção de Dados, as empresas precisam ter a conscientização dos benefícios, bem como das sanções administrativas que poderão ser evitadas ou mitigadas.

CONCLUSÃO

Diante da análise do panorama atual de proteção de dados pessoais no Brasil, restou evidenciado que as grandes mudanças ocorridas pelo crescente uso da *internet* no decorrer dos anos, impactaram, indiscutivelmente, na necessidade de uma mudança de cultura das organizações que realizam o tratamento de dados pessoais.

Sem dúvidas, o objeto da pesquisa aqui tratado possui extrema relevância jurídica frente as mudanças tecnológicas de captação e registro de informações que têm crescido exponencialmente, à medida que aumenta a necessidade de proteger a privacidade dos indivíduos, no âmbito da atividade empresarial.

A evolução da tecnologia trouxe mudanças nas relações pessoais e econômicas, e como resultado, o comportamento humano está sendo influenciado pelo aumento do volume de dados pessoais.

Essas mudanças levantam discussões sobre os danos causados pelo processamento e fluxo de dados na sociedade, incluindo a coleta em massa de informações sobre consumidores, seus hábitos e comportamentos. É evidente que o uso desses dados permite a extração de informações valiosas.

A União Europeia já abordava o assunto, de forma primitiva, e deu início às legislações sobre privacidade e proteção de dados no mundo, a partir da Diretiva de Proteção de Dados criada em 1995, e em 2016, com a promulgação do *General Data Protection Regulation* (GDPR) despontou no mundo no que se refere ao tema da proteção de dados.

No tocante à Lei Geral de Proteção de Dados, vale salientar que esta se inspirou na legislação europeia e, por um lado, estabeleceu regras específicas para regulamentação imediata do tratamento de dados pessoais, mas, por outro, prestou-se a estabelecer fundamentos, princípios e objetivos do tratamento de dados.

Diante do novo cenário legislativo, as empresas e entidades públicas precisam se adaptar à Lei Geral de Proteção de Dados, em razão de estarem sujeitas a diversas penalidades, aplicáveis pela Autoridade Nacional de Proteção de Dados, em razão do descumprimento dos preceitos legais da LGPD.

É evidente os desafios enfrentados pelas empresas na busca pela adequação à LGPD, que se torna fundamental não somente para a empresa estar em conformidade com a legislação vigente, garantir o respeito aos direitos dos titulares de dados, mas também para minimizar o risco de incidentes, possíveis ações judiciais e eventuais e irreparáveis prejuízos.

Os desafios se dão em razão da falta de cultura de proteção de dados, no Brasil, por não guardar laços históricos com a referida tutela de proteção de dados.

Além do mais, mesmo que diante dos percalços encontrados pelas empresas, se faz necessária tal adequação, considerando que milhares de empresas coletam, armazenam e processam dados de seus clientes, fornecedores e funcionários.

Importa lembrar que as empresas têm papel inestimável para fomentar a cultura de proteção de dados, mas para isso, ainda se vislumbra a necessidade de diversos estímulos por parte do Poder Público, além de uma vigilância severa para que de fato essa nova realidade de conformidade seja exercida.

Neste sentido, como medidas de incentivo, há Projeto de Lei n.º 4, de 2022, em tramitação perante o Senado, que tem como objetivo estimular a realização de investimentos em atividades de caráter pedagógico-educacionais e de implantação, adequação e operacionalização da LGPD, nas empresas, por meio de descontos de créditos relativos a valores despendidos com investimentos em atividades de adequação, da base de cálculo do PIS, PASES, CONFINS, PIS/PASEP Importação e CONFINS – Importação.

Tais medidas servem de estímulo para as empresas que necessitam se adequar aos termos da LGPD, porém, por meio de investimentos vultosos para tanto, como por exemplo, custos para a adoção de um programa efetivo de *compliance*, que servirá como mecanismo para afastar ou diminuir sua responsabilidade e dar maior segurança em possíveis futuras ações, além de ser critério atenuante na imposição das sanções administrativas pela Autoridade Nacional de Proteção de Dados.

Logo, torna-se de extrema importância que a empresa crie um time qualificado no assunto referente à proteção de dados para guiar as decisões que a empresa como um todo tomará, mapeamento dos dados que são utilizados e coletados e os riscos que permeiam.

Como visto, é crucial que as empresas informem claramente aos usuários como seus dados serão utilizados e obtenham uma autorização válida para isso. Além disso, devem ser transparentes sobre suas práticas de coleta e tratamento de dados pessoais, fornecendo informações claras sobre os propósitos da coleta, do uso dos dados, do período de retenção e mencionar as partes com as quais serão compartilhados os dados.

Em outras palavras, as empresas devem assumir um papel de garantidoras dos direitos fundamentais envoltos no tema ora tratado nessa dissertação, pois a responsabilidade social da empresa está intimamente ligada a essas questões.

Dessa forma, as empresas têm o compromisso de buscar a proteção de dados no Brasil em prol dos Direitos Humanos, sendo certo que, a adoção das medidas exigidas pela LGPD, juntamente com a conscientização dos funcionários e consumidores por meio de ações corporativas internas, desenvolvimento de modelos de gestão e comunicações transparentes, contribuirá para o processo de desenvolvimento da proteção com justiça social.

De todo modo, sob a ótica das empresas, percebe-se que muitas se preocupam com os custos que serão dispendidos para as adequações sistêmicas e procedimentais para firmarem-se em conformidade com a norma em estudo.

Contudo, a falta de adequação da conduta empresarial em relação dados pessoais, pode gerar, além do comprometimento de negociações comerciais, grandes prejuízos de reputação, que tem potencial de gerar consequências drásticas em participação e valor de mercado.

Ademais, é sensato afirmar que as empresas que adotarem as medidas trazidas no bojo da Lei Geral de Proteção de Dados certamente terão uma grande vantagem competitiva e, consequentemente, alcançarão maior sucesso e lucratividade.

REFERÊNCIAS

ANPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo.** Tratamento de Dados Pessoais pelo Poder Público. 2021, p. 7. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico Acesso em: 20/06/2023.

ARAGÃO, Alexandre Santos de. **Agências Reguladoras e a evolução do Direito Administrativo Econômico**. 3ª ed. Rio de Janeiro: Forense, 2013.

ARAGÃO, Isabella de C. S. **Contexto brasileiro pós-Scherms I e II:** influências de limitações geográficas no fluxo transnacional de dados pessoais e aspectos práticos. Direito Digital e O Setor Público, Rio de Janeiro, n. 2, 2020.

ARGENTINA. **Lei nº 25.326/2000**, de 04 de octubre de 2000. Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Buenos Aires: Senado y Cámara de Diputados de la Nación Argentina, 04 out. 2000. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acesso em: 13 mar. 2023.

ARGENTINA. Presidente de la Nación Argentina. **Decreto n. 746/2017**, de 25 de septiembre de 2017. Modificación. Decretos N° 1558/2001, N° 357/2002 y N° 1172/2003. Buenos Aires, 25 set. 2017. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm. Acesso em: 13 mar 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2023. **Relação atualizada dos processos administrativos sancionatórios instaurados pela ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao. Acesso em 03 jun. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf Acesso em 3 jun. 2023.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 20. ed. atual. São Paulo: Saraiva, 1999.

BAUMAN, Zygmunt. **Vida para consumo**: transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar Editor, 2008.

BENACCHIO, Marcelo; MACIEL, Renata Mota. A LGPD sob a Pespectiva de Regulação do Poder Econômico. In: DE LIMA, Cíntia Rosa Pereira (Org.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

BENACCHIO, Marcelo; CAMPOS, Tatiana de Almeida. A Importância da Governança Corporativa no Pacto Global e na Concretização dos Princípios Ruggie. In:

CAVALCANTI, Thais Novaes; CONCI, Luiz Guilherme Arcaro (Orgs.). **Proteção jurídica da pessoa, direitos humanos e desenvolvimento regional.** São Bernardo do Campo: Ed. Universitária FDSBC, 2022.

BERTOCCELLI, Rodrigo de Pinho. **Compliance.** In: CARVALHO, André Castro et. al. Manual de Compliance. Rio de Janeiro: Forense, 2019.

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

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

BLUM, Renato Opice; ARANTES, Camila Rioja. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018.

BOBBIO, Noberto. **A era dos direitos**. Rio: Campos, 1992.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 abr. 2023.

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Diário Oficial da União, Brasília, 27 ago. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de2020-274389226. Acesso em: 10 set. 2021.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planaltogov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 16 abr. 2022.

BRASIL. **Lei n. 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, 09 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 10 maio 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 26 abr. 2023.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26 abr. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados**. Disponível em**:** https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 abr. 2023.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 fev. 2022.

BRASIL. **Lei nº 9.986, de 18 de julho de 2000**. Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9986.htm. Acesso em: 26 abr. 2023.

BRASIL. **Medida Provisória nº 1.124, de 13 de junho de 2022.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm**.** Acesso em: 10 abr. 2023.

BUCHNER, Benedikt. Informationelle Selbstbestimmung im Privatrecht. Tübingen: MohrSiebeck, 2006.

BURKERT, Herbert. Privacy-Data Protection: a German/ European perspective. In: ENGEL, C.; KELLER, K. H. (ed.). **Governance of Global Networks in the Light of Differing Local Values**. Baden-Baden: Nomos, 2000.

CABRAL, Filipe Fonteles. **Proteção de dados pessoais na atividade empresarial**: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.

CÂMARA DOS DEPUTADOS. **PEC 17/2019**. Disponível em:< https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>Acesso em: 20 dez. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 2126/2011**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255. Acesso em: 23 fev. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje:** perspectiva histórica e o cenário brasileiro. SeqUência: Estudos Jurídicos e Políticos, Florianópolis, v. 38, n. 76, p. 213-240, 20 set. 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213/34870. Acesso em: 04 set. 2022.

CASTRO, Maria Eugênia Bordinassi de. A estrutura e a natureza jurídica da Autoridade Nacional de Proteção de Dados com base na lei n° 13.853/2019. In: MAGRO, Américo Ribeiro; TEIXEIRA, Tarcísio (coords.). **Proteção de Dados Fundamentos Jurídicos**. 1. ed. Salvador; JusPODIVM, 2019, p. 199-227.

COMISSÃO EUROPEIA. **Adequacy decisions**: How the EU determines if a non-EU country has an adequate level of data protection. European Comission, [2021]. Disponível em: https://ec.europa.eu/info/law/lawtopic/data-protection/international-dimension-data-protection/adequacy-decisionspt. Acesso em: 10 jan. 2023.

COMPARATO, Fábio Konder. **Rumo à justiça**. São Paulo: Saraiva, 2010.

CONSELHO DA EUROPA. **Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Estrasburgo**, 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em 19 fev. 2023.

CORREIA, Henrique. Compliance e sua aplicação no direito do trabalho. **Revista Eletrônica do Tribunal Regional do Trabalho da 9ª Região**, Brasília, DF, ano IX, n. 91, ago./2020. Disponível em:https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/151250/2020_correia_henrique_compliance_aplicacao.pdf?sequence=1&isAllowed=y. Acesso em: 2 jun. 2023.

COTS, Márcio. **Lei Geral de Proteção de Dados comentada**. São Paulo: RT, 2018.

CRUZ E TUCCI, José Rogério. **Natureza, compatibilidade e limites subjetivos da multa coercitiva.** 2018. Disponível em: https://www.conjur.com.br/2018-jan-09/paradoxo-corte-naturezacompatibilidade-limites-subjetivos-multa-coercitiva. Acesso 13 mai 2023. Acesso em: 28 mai. 2023.

DE CAMARGO, Caio Pacca Ferraz; BENACCHIO, Marcelo. Função social e responsabilidade social empresarial: convergências e divergências. **Revista Thesis Juris**, v. 8, n. 2, p. 119-148, 2019.

DE LUCCA, Newton; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e Privacidade. In: LIMA, Cintia Rosa Pereira de (Coordenação). **Comentários à Lei Geral de Proteção de Dados**. 1. Ed. São Paulo: Almedina, 2020.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, jul./dez., 2011.

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

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thompson Reuters Revista dos Tribunais, 2019.

DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, ano 4, n. 16, out./dez., 2003.

ESTADOS UNIDOS DA AMÉRICA. **Children´s Online Privacy Protection Act**. **15 U.S.C** §6501-6506, Public Law, Washinton D.C., 21 out. 1998.

ESTADOS UNIDOS DA AMÉRICA. **Federal Trade Comission Act**. **15 U.S.C**. §41-58., Public Law, Washinton D.C., 1914.

ESTADOS UNIDOS DA AMÉRICA. **Olmstead v. United States**, 277 U.S. 438, 1928.

FADANELLI, Isadora C. Nova Lei Geral de Proteção de Dados: perspectiva e desafios sob a ótica dos princípios de proteção de dados no contexto europeu e brasileiro. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). **Lei Geral de Proteção de Dados**: aspectos relevantes. Indaiatuba: Editora Foco, 2021.

FERRAZ JÚNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito.** Universidade de São Paulo, 88, 1993, p. 439-459. Disponível em:

https://www.revistas.usp.br/rfdusp/article/download/67231/69841/88644. Acesso em: 17 abr. 2023.

FERREIRA, Manuel. **O Regulamento Geral sobre a Proteção de Dados**: os aspectos legais e organizativos de governança nas organizações. Aspectos legais e organizativos de governança nas organizações. 2018. 103 f. Dissertação (Mestrado) – Curso de Direito e Segurança, Direito, Universidade Nova de Lisboa, Lisboa, 2018. Disponível em https://run.unl.pt/bitstream/10362/54953/1/ManuelFerreira_2018.pdf. Acesso em: 22 fev. 2023.

FRAZÃO, Ana. Compliance de dados pessoais. In.: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Danato (coords.). **Lei Geral de Proteção de Dados Pessoas e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Coordenação). **Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro**. 1ª ed. São Paulo: Revista dos Tribunais, 2019.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. **Desafios para a efetividade dos programas de compliance**. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

FURTADO, L. R. **Curso de Direito Administrativo**. 5ª ed., rev. e atual. Belo Horizonte: Fórum, 2016.

FUSTER, Gloria González. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Springer: Brussels, 2014.

GOV.BR. **ANPD divulga lista de processos sancionatórios**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios Acesso em: 10 abr. 2023.

GRAU, Eros Roberto. **A ordem econômica na constituição de 1988.** São Paulo: Malheiros, 2006.

GUALDA, Diego de Lima. **Desafio Cultural da Proteção de Dados**. Disponível em: https://www.aarb.org.br/desafio-cultural-da-protecao-de-dados/. Acesso em: 24 mai. 2023.

HENRIQUE, Lygia Maria Moreno Molina. **LGPD**: cuidados na implementação. Revista Forense, v. 429, 2019.

IBM. **Relatório do Custo de uma Violação de Dados 2021.** Disponível em: https://www.ibm.com/downloads/cas/RBJ6BJVN#:~:text=Figura%201-,O%20custo%20total%20m%C3%A9dio%20de%20uma%20viola%C3%A7%C3%A3o%20de%20dados%20aumentou,4%2C24%20milh%C3%B5es%20em%202021 Acesso em: 20 jun. 2023.

INFORMATION Commissioner's Office. **Whats is a DPIA?** Disponível em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-

assessments/#:~:text=A%20Data%20Protection%20Impact%20Assessment,a%20high%20risk%20to%20individuals. Acesso em: 20 mai. de 2023.

INSTITUTO ETHOS. **Direitos Humanos, Gestão para o Desenvolvimento sustentável, Integridade e Meio Ambiente**. Disponível em: <http://www.ethos.org.br>. Acesso em: 20 mai. 2023.

JABUR, Gilberto Haddad. A dignidade e o Rompimento de privacidade. In: MARTINS, Ives Gandra da Silva; PEREIRA JR, Antônio Jorge. **Direito à Privacidade.** 1 ed. Aparecida: Editora Ideias & Letras, 2005.

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. **DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO**. De 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT Acesso em: 28 mai. 2023.

KOTSCHY, Waltraut. Lawfulness of processing. 2018. Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019). **Oxford University Press**, 2018, p. 37. Disponível em: <https://works.bepress.com/christopher-kuner/1/>. Acesso em: 13 mai. 2023.

LADLEY, John. Data Governance: how to desig, deploy and sustain na effective data Governance program. **The Morgan Kaufmann Series on Business Inteligence**, 2012.

LEMOS, Ronaldo (Org). **Marco Civil da Internet.** 1ª ed. São Paulo. Atlas, 2014.

LEONARDI, Marcel. Controladores e operadores: papéis, distinções, mitos e equívocos. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. **A Lei Geral de Proteção de Dados Pessoais:** Aspectos práticos e teóricos relevantes no setor público e privado. 1. Ed. e-book baseada na 1. ed. Impressa. São Paulo: Thomson Reuters Brasil, 2021.

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

LEONEL, Vilson; MOTTA, Alexandre de Medeiros. **Ciência e Pesquisa**. 3. ed. Palhoça: Unisul Virtual, 2011.

LIMA, Ana P. M. C. de; ALMEIDA, Dionice de; MAROSO, Eduardo P. **LGPD – Lei Geral de Proteção de Dados**: sua empresa está pronta? São Paulo: Literare Books International, 2020.

LIMA, Christina Aires Correa; BARBOSA, Júlio César Moreira. Autoridade Nacional de Proteção de Dados precisa de independência técnica. **CONJUR.** Disponível em: https://www.conjur.com.br/2019-abr-11/opiniao-autoridade-protecao-dados-requer-autonomia-tecnica. Acesso em: 3 fev. 2023.

LIMA, Cíntia Rosa Pereira de. **A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.** 487 p. Tese (Livre Docência), Universidade de São Paulo, Ribeirão Preto - SP, 2015.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**: De Acordo com a Lei Geral de

Proteção de Dados (Lei n. 13.709/2018 do CDC (PL 3.514/2015). Coimbra: Grupo Almedina, 2020. E-book.

LIMA, Cíntia Rosa Pereira de. **Parecer Técnico sobre o tema:** "Modelo Regulatório: órgão, agência e autorregulamentação". Disponível em https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-emporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp. Acesso em: 12 dez. 2021.

LIMA, Cintia Rosa Pereira de; PEROLI, Kelvin. Desafios para a Atuação Independente da Autoridade Nacional de Proteção de Dados Pessoais Brasileira à Luz das Exigências Internacionais para a Adequada Proteção dos Dados Pessoais. In: SIMÃO FILHO, Adalberto et al (org.). **Direito & Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

LISSARDY, Gerardo. Despreparada para a era digital, a democracia está sendo destruída, afirma o guru do "big data". **BBC News Brasil**, 9 abr 2017. Disponível em: <https://www.bbc.com/portuguese/geral-39535650. Acesso em: 15 mar. 2023.

MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:** Atualizado com a Medida Provisória nº 869/18. RM Digital Education. Edição do Kindle.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. **Regulamento Geral de Proteção de Dados:** Manual Prático. 3 ed. Porto: Vida Econômica, 2020, p. 10.

MAGALHÃES, Rodrigo Almeida. **A função social da empresa e a responsabilidade social.** Disponível em: http://direito.newtonpaiva.br/revistadireito/docs/prof/13_prof_rodrigo2.pdf. Acesso em 20 mai. 2023.

MAGRANI, Eduardo**. Entre dados e robôs**: Ética e privacidade na era da hiperconectividade, 2ª ed., Porto Alegre: Arquipélago Editorial, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada [livro eletrônico/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. --2. ed. -- São Paulo: Thomson Reuters Brasil, 2019.

MARQUES NETO, Floriano Peixoto de Azevedo. **Agências Reguladoras Independentes:** Fundamentos e seu Regime Jurídico. 1. Ed. Belo Horizonte: Editora Fórum, 2005.

MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Kontad Adenauer, 2005.

MATTOS, Paulo Todescan Lessa. **O novo Estado regulador no Brasil**: eficiência e legitimidade. 1. Ed. São Paulo: Revista dos Tribunais, 2017.

MELLO, Celso Antônio Bandeira. **Curso de direito administrativo.** 26 ed. São Paulo: Malheiros, 2009.

MELLO, Rafael Munhoz de. **Princípios constitucionais de direito administrativo sancionador:** as sanções administrativas à luz da Constituição Federal de 1988. São Paulo: Malheiros, 2007

MENDES, G. F.; BRANCO, P. G. G. **Curso de Direito Constitucional.** 13 ed. São Paulo: Saraiva Educação (Série IDP), 2018.

MENDES, Laura Schertel. **O direito fundamental à proteção de dados pessoais**. Revista de Direito do Consumidor, v. 79, p. 45-81, jul./set. 2011.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. **Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor**. 2014. Disponível em:<https://integrada.minhabiblioteca.com.br/#/books/9788502218987/ >. Acesso em: 23 mar. 2023.

MIRANDA, Francisco Cavalcanti Pontes de. **Tratado de direito privado**. 4. ed. São Paulo: Ed. RT, 1983.

MONTEIRO, Renato Leite. **Cambridge Analytica e a nova era Snowden na proteção de dados pessoais.** El país. Brasil. 20 de março de 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/20/tecnologia/1521582374_496225.html. Acesso em 02 jun. 2023.

NESTER, Alexandre Wagner; MÜLLER, Nicole Mendes. Regime sancionatório da LGPD (arts. 52 a 54 da Lei 13.709/2018. **Informativo Justen, Pereira, Oliveira e Talamini**, Curitiba, n. 163, set. 2020. Disponível em: https://justen.com.br/pdfs/IE163/IE163-NesterNicole-RegSancionatorioLGPD.pdf. Acesso em: 30 nov. 2022.

Núcleo de Informação e Coordenação do Ponto BR. **Estatísticas dos Incidentes Reportados ao CERT.BR**. Disponível em: < https://www.cert.br/stats/incidentes/2018-jandec/tipos-ataque.html >. Acesso em 13 mai. 2023.

OBSERVATÓRIO DO MARCO CIVIL DA INTERNET. **Histórico do Marco Civil**. Disponível em: http://www.omci.org.br/historico-do-marco-civil/timeline/#0. Acesso em: 23 fev. 2023.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. **OECD** – Better Policies for better lives, 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 28 ago. 2022.

OLIVEIRA, A. P. de. et al. A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, Curitiba, v. 4, n. 1, maio, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wpcontent/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 24 mai. 2023.

OLIVEIRA, Ricardo. **LGPD:** Como evitar as sanções administrativas. São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 04 jun. 2023.

ONU. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em:

<http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 9 mar. 2022.

OSÓRIO, Fábio Medina. **Direito administrativo sancionador.** São Paulo: Ed. RT, 2010.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Lei Geral de Proteção de Dados Pessoais**. 1.ed. São Paulo: Thomson Reuters Brasil, 2021. p. RB-5.4. In: NOHARA, Irene Patrícia Diom, ALMEIDA, Luiz Eduardo de. Compliance digital e LGPD. Coleção Compliance; v. 5. 1. ed. em e-book baseada na 1. ed. impressa.

PAULA, Felipe de; VASCONCELOS, Beto. A Autoridade Nacional de Proteção de Dados. In: FRAZÃO, ANA; OLIVA, Milena; TEPEDINO, Gustavo (Coords.). **Lei Geral de Proteção de Dados Pessoais e a suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters do Brasil; 2019.

PIETRO, Maria Sylvia Zanella Di. **Direito Administrativo**. São Paulo: Editora Atlas, 2019.

PINHEIRO, Alexandre Sousa (coord.). **Comentário ao Regulamento Geral de Protecção de Dados**. Coimbra: Edições Almedina, 2018.

PINHEIRO, Patrícia Peck. **Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o impacto nas instituições públicas ou privadas**. RT 1.000. Ano 108. Vol. 1.000. São Paulo: Revista dos Tribunais, 2019.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018 – LGPD. São Paulo: Saraiva Educação, 2020. E-book.

PRATA, Alexandre. Organização. In: **Lei Geral de Proteção de Dados**: manual de implementação. São Paulo: RT, 2019.

RESENDE, Antonio José Calhau. **O princípio da razoabilidade dos atos do Poder Público**. Revista do Legislativo, abr. 2009.

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

ROTUNDO, Rafael P. Proteção de Dados. **Revista de Direito Privado**, São Paulo, v. 74, ano 18, p. 133-158, fev. 2017.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1988.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. **Lei Geral de Proteção de Dados no Brasil e os possíveis impactos**. Revista dos Tribunais, vol. 988, ano 107. São Paulo: RT, 2018.

SARLET, Gabrielle Bezerra Sales. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro In: LIMA, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados.** São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 13 mai. 2023.

SARLET, Ingo W.; DONEDA, Danilo; MENDES, Laura Schertel. **Estudos sobre proteção de dados pessoais.** Ebook. São Paulo: Editora Saraiva, 2022. (Coleção

Direito, tecnologia, inovação e proteção de dados num mundo em transformação). Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620810/. Acesso em: 14 mai. 2023.

SENADO FEDERAL. Comissão de Assuntos Econômicos. **Relatório Legislativo n. SF183412917700-20180629**, de 29 de junho de 2018. Relator: Ricardo Ferraço. Brasília, 29 jun. 2018, p. 10. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1594012451098&disposition=inline. Acesso em: 26 fev. de 2022.

SHAPIRO, Fred. “The Most-Cited Law Review Articles Revisited.” In: **71 Chicago-Kent Law Review 751** (1996) apud DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

SHARMA, Sanjay. **Data Privacy and GDPR Handbook**. New Jersey: Wiley, 2020.

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

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 2014.

SOLOVE, Daniel. Privacy and Power: Computer Databases and Metaphors for Information Privacy. **Stanford Law Review**, v. 53, p. 1394, 2000-2001.

SOLOVE, Daniel. **Understanding privacy**. Cambridge: Harvard University Press, 2004.

SOUZA, L. R. M. Proteção de dados pessoais: estudo comparado do regulamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016. **Revista IDP**, Brasília, v. 1, n. 41, 2018.

SUNDFELD, Carlos Ari. Introdução as Agências Reguladoras. In: SUNDFELD, Carlos Ari. **Direito Administrativo Econômico.** São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

TEFFÉ, Chiara Spadaccini de. Por que precisamos de uma Autoridade Nacional de Proteção da Dados? **Jota.** Brasil, 07 de janeiro de 2020. Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020. Acesso em: 21 set. 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01)**. Disponível em: https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf. Acesso em: 15 de ago. de 2022.

UNIÃO EUROPEIA. Comissão das Comunidades Europeias. Decisão da Comissão n. 2003/490/CE, de 30 de junho de 2003. Decisão da Comissão de 30 de junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina. **Jornal Oficial da União Europeia**, Bruxelas, 30 jun. 2003. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32003D0490&from=EN. Acesso em: 13 mar. 2023.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Artigo 4, item 2 – Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 maio 2023.

VAINZOF, Rony. Conceito, perfil, papéis e responsabilidade do encarregado. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (coord.). **Data Protection Officer**: teoria e prática de acordo com a LGPD e o GDPR. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. E-book.

VASCONCELOS, Beto. PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Coordenação). **Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro**. 1. Ed. São Paulo: Revista dos Tribunais, 2019.

VENOSA, Silvio de Salvo. **Direito Civil**: Responsabilidade civil. 7.ed. São Paulo: Atlas, v. 4, 2007.

VIGLIAR, José Marcelo M. **LGPD e a Proteção de Dados Pessoais na Sociedade em Rede**. E-book. São Paulo: Grupo Almedina (Portugal), 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556276373/. Acesso em: 13 mai. 2023.

VIOLA, Mario. **Transferência de Dados entre Europa e Brasil**: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: Instituto de Tecnologia & Sociedade do Rio, 2019.

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

WACKS, Raymond. Personal information: Privacy and the law. Oxford: Clarendon Press, 1989, p. 25 apud MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, v. IV, dez. 1890, n. 5. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 10 jan. 2022.