

DO DIGITAL AO DIREITO:

ENTENDENDO A LGPD E A NOVA ERA DA PRIVACIDADE



ORGANIZAÇÃO E COORDENAÇÃO:

ADRIANA ANTUNES WINKLER

PREFÁCIO: FABRÍCIO DA MOTA ALVES

VIVEMOS NA ERA DOS DADOS, EM QUE A INFORMAÇÃO PESSOAL É MOEDA VALIOSA — E, MUITAS VEZES, VULNERÁVEL. COMO EQUILIBRAR INOVAÇÃO E PROTEÇÃO DOS DIREITOS FUNDAMENTAIS NO CENÁRIO DIGITAL CONTEMPORÂNEO?

"Tema quente, relevante e de interesse não só profissional nacional, mas também global. Autores gabaritados e de bastante conhecimento técnico-prático, uma Coordenadora que dispensa elogios e o momento que continua pedindo por mais materiais de qualidade. Essa é a chamada de leitura deste novo livro que chega para marcar seu lugar no tempo e no espaço. Super recomendo!"

(Gustavo Godinho, CLO/DPO na Foggo Entertainment)

"Super recomendo esta obra incrível organizada pela talentosa Adriana, que reúne reflexões atuais e práticas sobre privacidade e proteção de dados, tão essenciais no nosso mundo digital acelerado. Os artigos são verdadeiros guias para quem lida com LGPD, segurança da informação e gestão de riscos. Leitura leve, rica e indispensável para quem quer navegar com confiança no universo da tecnologia!"

(Samanta Oliveira, DPO Brasil - Mercado Livre)

"Este livro é uma fonte indispensável para quem deseja compreender melhor a complexa relação entre proteção de dados e a realidade do mundo digital. Os capítulos da obra abordam diversos dos principais temas desafiadores no campo, como o impacto da proteção de dados no marketing digital, os riscos de discriminação algorítmica, os dilemas da inteligência artificial, novas questões como as heranças digitais, e a nada trivial interlocução entre proteção de dados, inovação e desenvolvimento econômico. Leitura obrigatória para os profissionais e estudantes da área."

(Rodrigo Ferreira, Encarregado de Dados da Casa da Moeda do Brasil)





Adriana Antunes Winkler, LL.M.,

é uma líder reconhecida em segurança da informação e encarregada de proteção de dados (DPO), com ampla experiência na implementação e gestão de estruturas de risco, privacidade e proteção de dados para corporações multinacionais em escala global. Atualmente, lidera iniciativas regulatórias de risco e privacidade na Accenture, nos Estados Unidos, onde auxilia clientes a navegarem em ambientes regulatórios complexos, implementarem estruturas de conformidade robustas e alinharem suas estratégias de negócios aos padrões globais em constante evolução. Seu trabalho oferece soluções inovadoras e eficazes que garantem a privacidade dos dados, a segurança e a eficiência operacional, capacitando as organizações a construírem confiança, mitigarem riscos e prosperarem em um mundo cada vez mais regulado e orientado por dados.

Anteriormente, Adriana liderou programas de privacidade e proteção de dados na América Latina, Oriente Médio e Ásia para uma empresa norte-americana avaliada em mais de 50 bilhões de dólares, atendendo clientes como McDonald's, Coca-Cola, Subway e Pizza Hut. Também presidiu a Comissão de Privacidade e Proteção de Dados da Ordem dos Advogados do Brasil, Seccional do Distrito Federal, nos últimos cinco anos, onde trabalhou com mais de 100 advogados e atuou como principal autoridade da organização em privacidade.

Adriana também atua como educadora, autora, palestrante e pesquisadora, orientando entidades públicas e privadas sobre uma ampla gama de legislações de privacidade e proteção de dados (incluindo LGPD, GDPR, HIPAA, NIST, DMA, DORA, PIPA, PDPA, CPRA e outras). Sua expertise inclui gestão de riscos, Privacy by Design, avaliação de terceiros, requisições de direitos dos titulares (DSARs), auditorias, fluxo de dados, governança, avaliações e condução de treinamentos e sessões educativas.

Ela possui certificações em privacidade pelas instituições IAPP, EXIN e ISACA, e é certificada como DPO pela Universidade de Maastricht, na Holanda.

Adriana está aberta a conexões profissionais por meio de seu perfil no LinkedIn:

<https://www.linkedin.com/in/adriana-winkler>.

**Do Digital ao Direito:
Entendendo a LGPD e a
Nova Era da Privacidade**
reúne especialistas
renomados para discutir os
principais desafios da
proteção de dados no Brasil.

Da publicação da LGPD aos
impactos práticos para
organizações públicas e
privadas, a obra oferece
reflexões profundas e
orientações concretas para
quem deseja compreender
— e aplicar — os pilares da
privacidade na prática.

Essencial para advogados,
profissionais de
compliance, gestores de
tecnologia, estudantes e
todos os interessados em
compreender os novos
contornos da cidadania
digital. Uma leitura atual,
crítica e necessária para os
tempos que vivemos.

COORDENAÇÃO

ADRIANA ANTUNES WINKLER

DO DIGITAL AO DIREITO

ENTENDENDO A LGPD E A NOVA
ERA DA PRIVACIDADE



EDITORA
IMPÉRIO

2026

COORDENAÇÃO

ADRIANA ANTUNES WINKLER

DO DIGITAL AO DIREITO

ENTENDENDO A LGPD E A NOVA ERA DA PRIVACIDADE

Adriana Antunes Winkler Joelane Rodrigues Carvalho

Adriana Carla Silva de Oliveira Luana Bueno Palma

Adriana da Costa Fernandes Luanna da Costa e Silva

Adriana Giuntini Viana Lucas Paglia

Arlene Pereira da Silva Sacco Marcela Calazans Medeiros Silva

Bibianna V. Versiani de Paula Peres Mariana Landim Carneiro

Daniela Lourenço de Oliveira Mariani Nazaré da Silva Costa

Daphne Kalyva de Almeida Rosa Matheus Resende da Silva Costa

Dayane Karine de S. Mendonça Neyanne Felipe Bezerra Araújo

Eduarda Moraes Chacon Rosas Paula de Paiva Santos

Fellipe Fernandes Duarte Raquel Elena Rinaldi Maciel

Graziella Angela Tinari Dell'Osa Roberto Arylton P. Ramos

Henriette Groenwold Monteiro Tatiana Venâncio de Rezende

Ivana Avellar N. de Lima e Silva



EDITORA
IMPÉRIO



Todos os direitos desta edição são reservados à Editora Império

Direção Executiva: Eduardo Cavalcante de Almeida Costa
Direção Editorial: Ana Paula Moraes Canto de Lima
Conselho Editorial: Ana Paula Moraes Canto de Lima
Anne Cristine Silva Cabral
Camila Henning Salmoria
Coriolano Aurélio de A. Camargo Santos
Cristiano Carrilho Silveira Medeiros
Ingrid Zanella Andrade Campos
Isabela Lessa de Azevedo Pinto Ribeiro
Maria Emília Miranda de Oliveira Queiroz
Schampou Bernardo Bezerra

Capa: Maxwell Douglas Pereira

Projeto Gráfico e Diagramação: Editora Império

Revisão: Carolina Antunes

Relacionamento com o cliente via WhatsApp: (81) 3203-6469

Dados Internacionais de Catalogação na Publicação (CIP)
Ficha Catalográfica

D598 Do digital ao direito: entendendo a LGPD e a nova era da privacidade. /
Adriana Antunes Winkler. – Recife: Editora Império, 2026.

395 p.

Contém bibliografia ao final de cada capítulo

ISBN 978-65-89291-71-8

1. Direito. 2. Proteção de dados pessoais. 3. Lei de proteção de
dados pessoais - LGPD. 4. Nova era da privacidade. 5. Proteção de dados -
Legislação. I. Winkler, Adriana Antunes. II. Título.

340:004 CDU (1999)

Fabiana Belo - CRB-4/1463

Printed in Brazil - Impresso no Brasil

Todos os direitos reservados. Nos termos da Lei que resguarda os direitos autorais é proibida a reprodução total ou parcial desta obra por qualquer forma ou meio, eletrônico ou mecânico, inclusive através de fotocópias e gravação, sem permissão por escrito do autor.

AGRADECIMENTOS

Escrever esta obra foi uma jornada intensa, marcada por vários desafios pessoais, mas profundamente gratificante — e ela só foi possível porque não estive sozinha. Cada página carrega a marca da generosidade, da confiança e do entusiasmo de pessoas que acreditaram neste projeto e caminharam ao meu lado.

Sou imensamente grata aos coautores, que dedicaram tempo, energia e conhecimento para compor este trabalho com excelência e sensibilidade. Foi um privilégio partilhar reflexões, dúvidas e conquistas com profissionais tão brilhantes, que tornaram esta caminhada mais leve e inspiradora.

Meu carinho e admiração ao querido Fabrício da Mota Alves, que aceitou prefaciar esta obra com a mesma elegância e sabedoria que sempre o acompanham. Ter suas palavras abrindo este livro é um presente que honra não apenas o trabalho desenvolvido aqui, mas toda a trajetória que me trouxe até este momento.

Agradeço de coração à Editora Império, especialmente ao Eduardo Costa, pela confiança e pelo acolhimento generoso. Obrigada por tratar este projeto com tanto zelo e profissionalismo, por acreditar no seu propósito e por viabilizar cada detalhe com tanto cuidado.

À talentosa Carolina Antunes, pela revisão criteriosa e pela sensibilidade ao registrar minha imagem na fotografia da biografia, deixo minha gratidão por ter dado forma, identidade e delicadeza ao que antes era apenas ideia.

Ao criativo Maxwel Douglas, que traduziu em cores e traços a essência do livro na capa, meu sincero reconhecimento. Sua arte tornou visível a alma desta obra.

E, por fim, obrigada aos ilustres profissionais da área que gentilmente recomendaram este trabalho. Suas palavras de apoio significam

muito para mim — são sinal de confiança e também de compromisso coletivo com a construção de um futuro mais ético para a proteção de dados pessoais no Brasil.

A todos vocês, meu muito obrigada. Esta obra leva meu nome, mas carrega um pedacinho de cada um que acreditou em mim.

Adriana Antunes Winkler

PREFÁCIO

A transformação digital que vivenciamos nas últimas décadas trouxe desafios inéditos para o Direito e para a sociedade como um todo. A proteção de dados pessoais, antes uma preocupação restrita a especialistas em tecnologia, tornou-se uma questão central para a garantia dos direitos fundamentais na era digital. É neste contexto que surge esta obra coletiva, “Do Digital ao Direito: Entendendo a LGPD e a Nova Era da Privacidade”, coordenada pela competente Dra. Adriana Antunes Winkler, ex-presidente da Comissão de Privacidade e Proteção de Dados da OAB-DF.

Este livro representa muito mais do que uma coletânea de artigos sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018. Trata-se de um testemunho eloquente do papel fundamental que a advocacia brasileira desempenha na construção e consolidação dos novos direitos digitais. A obra é composta majoritariamente, embora não exclusivamente, por advogados e advogadas que integram ou integraram a Comissão de Privacidade e Proteção de Dados da Ordem dos Advogados do Brasil, Seção do Distrito Federal, demonstrando como a classe advocatícia se posiciona na vanguarda da proteção dos direitos fundamentais na sociedade da informação.

É importante recordar que os principais nomes que impulsionaram a legislação de proteção de dados no Brasil foram, em sua essência, juristas e advogados comprometidos com a defesa dos direitos fundamentais. Desde os primeiros debates sobre a necessidade de uma lei específica para a proteção de dados pessoais até a aprovação da LGPD, a advocacia brasileira esteve presente, contribuindo com sua expertise técnica e sua visão humanística do Direito. Estes mesmos profissionais continuam hoje trabalhando na governança de novos direitos digitais, especialmente no que se refere aos desafios apresentados pela inteli-

gência artificial e outras tecnologias emergentes. A advocacia, portanto, não apenas acompanha as transformações tecnológicas, mas atua como protagonista na construção do arcabouço jurídico necessário para proteger os cidadãos na era digital.

A Ordem dos Advogados do Brasil, conforme estabelecido no artigo 133 da Constituição Federal, é instituição essencial à função jurisdicional do Estado, sendo indispensável à administração da justiça. Esta missão constitucional ganha contornos ainda mais relevantes quando se trata da proteção de dados pessoais e da privacidade, direitos que se encontram no epicentro das discussões sobre direitos fundamentais na contemporaneidade. As Comissões de Privacidade e Proteção de Dados das diversas seccionais da OAB pelo país têm desempenhado papel crucial na disseminação do conhecimento sobre a LGPD, na capacitação de profissionais e na orientação da sociedade sobre seus direitos. A iniciativa da OAB-DF, materializada nesta obra, exemplifica como a advocacia organizada cumpre sua função social de guardiã dos direitos fundamentais.

A atuação da OAB na temática de proteção de dados não se limita à produção acadêmica. Inclui a participação ativa em consultas públicas, a elaboração de pareceres técnicos, a promoção de eventos educativos e a constante interlocução com os órgãos reguladores. Esta postura proativa demonstra como a advocacia brasileira compreende que a proteção de dados não é apenas uma questão técnica, mas um imperativo ético e constitucional.

A presente coletânea aborda de forma abrangente e aprofundada os principais aspectos da LGPD e seus desdobramentos práticos. Os autores, em sua maioria membros da Comissão de Privacidade da OAB-DF, oferecem uma visão multifacetada e especializada sobre os diversos aspectos desta legislação revolucionária. A obra inicia com uma análise fundamental sobre a privacidade por padrão, conceito central da LGPD que exige a integração da proteção de dados desde a concepção de sistemas e processos tecnológicos. Este tema estabelece as bases conceituais para compreender como a proteção de dados deve ser incorporada ao desenvolvimento tecnológico.

Os direitos dos titulares são examinados sob a perspectiva jurídica, oferecendo uma análise detalhada sobre como os cidadãos podem exercer seus direitos fundamentais na era digital. Complementando esta abordagem, a obra explora os princípios constitucionais da LGPD, demonstrando como a lei se alinha com os fundamentos constitucionais brasileiros. A interface entre tecnologia e direito é explorada em diversos capítulos, com análises sobre os efeitos da LGPD no marketing digital, tema de extrema relevância prática para empresas e profissionais da área. Esta perspectiva é complementada por trabalhos sobre marketing digital e proteção de dados pessoais, oferecendo uma visão abrangente sobre como conciliar estratégias comerciais com o respeito aos direitos dos titulares.

O aspecto sancionatório da legislação recebe atenção especial em trabalhos sobre sanções e penalidades na era da LGPD, tema crucial para a compreensão dos riscos e responsabilidades envolvidos no tratamento de dados pessoais. Esta abordagem é complementada por estudos sobre a aplicação do poder sancionatório da ANPD, oferecendo uma perspectiva atualizada sobre a atuação do órgão regulador. A dimensão educativa da proteção de dados é contemplada em trabalhos sobre educação digital, reconhecendo que a formação de uma sociedade preparada para a LGPD é fundamental para o sucesso da legislação. Este enfoque educativo reflete a compreensão de que a proteção de dados não é apenas uma questão técnica ou jurídica, mas também cultural e social.

A perspectiva internacional não foi negligenciada, com análises comparativas da LGPD com legislações internacionais, permitindo compreender como o Brasil se posiciona no cenário global de proteção de dados e quais lições podem ser extraídas de outras experiências legislativas. Aspectos técnicos especializados são abordados em estudos sobre segurança da informação e seu papel aliado à LGPD, demonstrando como a proteção técnica dos dados complementa a proteção jurídica. A obra também contribui com análises sobre a proteção de dados como direito constitucional, reforçando a fundamentação constitucional da matéria.

Temas emergentes e desafiadores também encontram espaço na obra. A complexa questão da herança digital, privacidade e proteção de dados é explorada, tema que ganha crescente relevância com a digitalização das relações sociais. A discriminação algorítmica na era da proteção de dados pessoais é abordada, questão que se torna cada vez mais relevante com o avanço da inteligência artificial. O impacto setorial da LGPD é examinado através de estudos sobre os impactos da legislação no e-commerce brasileiro, setor que experimentou crescimento exponencial durante a pandemia e que enfrenta desafios específicos na adequação à legislação.

Os aspectos práticos da implementação da LGPD recebem atenção especial. A obra aborda os desafios e soluções para a adequação de empresas à legislação, oferecendo orientações práticas para organizações de diversos portes e setores. A percepção dos riscos na proteção de dados é analisada, tema fundamental para a gestão adequada da privacidade nas organizações. A governança em privacidade é explorada através de estudos sobre governança em privacidade de dados, com foco no artigo 50 da LGPD. A obra também contribui com análises sobre a contratação do encarregado de dados, figura central na estrutura de governança estabelecida pela lei.

A coordenadora da obra, Dra. Adriana Antunes Winkler, contribui com capítulos fundamentais que tratam do exercício de direitos pelos titulares, oferecendo orientações sobre o que esperar e como se preparar para as solicitações dos cidadãos, além de abordar o futuro da privacidade e os desafios apresentados pela inteligência artificial, tema que representa a fronteira atual dos debates sobre proteção de dados.

Esta obra coletiva demonstra como a advocacia brasileira se posiciona como verdadeira guardiã dos direitos digitais. Os autores, em sua maioria advogados e advogadas, oferecem não apenas análises técnicas da legislação, mas também reflexões sobre os impactos sociais, econômicos e culturais da proteção de dados. A diversidade de temas abordados reflete a complexidade da matéria e a necessidade de uma abordagem multidisciplinar. Desde questões constitucionais fundamen-

tais até aspectos práticos de implementação, a obra oferece um panorama completo dos desafios e oportunidades apresentados pela LGPD.

É particularmente relevante observar como os autores equilibram rigor técnico com acessibilidade, oferecendo uma obra que serve tanto para especialistas quanto para profissionais que estão iniciando seus estudos na área. Esta característica reflete a vocação pedagógica da advocacia e seu compromisso com a disseminação do conhecimento jurídico. A LGPD representa apenas o início de uma jornada mais ampla rumo à construção de um arcabouço jurídico adequado para a era digital. Os desafios apresentados pela inteligência artificial, pela Internet das Coisas, pelo blockchain e por outras tecnologias emergentes exigirão constante atualização e aprofundamento do conhecimento jurídico.

A advocacia brasileira, como demonstra esta obra, está preparada para enfrentar estes desafios. A formação sólida em direitos fundamentais, combinada com a capacidade de adaptação às novas realidades tecnológicas, posiciona os advogados como protagonistas na construção dos direitos digitais do futuro. É fundamental reconhecer que a proteção de dados não é um fim em si mesmo, mas um meio para garantir a dignidade humana na era digital. A advocacia, com sua tradição humanística e seu compromisso com a justiça social, tem papel fundamental nesta missão.

“Do Digital ao Direito: Entendendo a LGPD e a Nova Era da Privacidade” representa uma contribuição valiosa para a literatura jurídica brasileira sobre proteção de dados. A obra demonstra a maturidade e a competência da advocacia nacional para lidar com os desafios jurídicos da era digital. Aos colegas advogados que terão acesso a esta obra, recomendo uma leitura atenta e reflexiva. Os temas aqui abordados não são apenas questões técnicas especializadas, mas aspectos fundamentais da prática advocatícia contemporânea. A proteção de dados perpassa praticamente todas as áreas do Direito, desde o direito empresarial até o direito do consumidor, do direito trabalhista ao direito penal.

À Dra. Adriana Antunes Winkler, coordenadora desta iniciativa, e a todos os autores que contribuíram para esta obra, meus sinceros parabéns pela qualidade e relevância do trabalho apresentado. Esta co-

letânea certamente se tornará referência obrigatória para todos aqueles que desejam compreender a LGPD e seus desdobramentos. À Comissão de Privacidade e Proteção de Dados da OAB-DF, meu reconhecimento pelo trabalho desenvolvido e pelo exemplo oferecido às demais seccionais. Iniciativas como esta demonstram como a advocacia organizada cumpre sua missão constitucional de defesa dos direitos fundamentais.

Por fim, aos leitores desta obra, desejo que encontrem nas páginas seguintes não apenas conhecimento técnico, mas também inspiração para continuar construindo um futuro digital mais justo, mais seguro e mais respeitoso com a dignidade humana. A era digital chegou para ficar, e cabe a nós, advogados e advogadas, garantir que ela seja também uma era de direitos.

Fabício da Mota Alves

Advogado

SUMÁRIO

**O EXERCÍCIO DE DIREITOS PELOS TITULARES: O QUE ESPERAR
E COMO SE PREPARAR.....19**

Adriana Antunes Winkler

**A PERCEPÇÃO DOS RISCOS NA PROTEÇÃO DE DADOS: UM
ESTUDO SOBRE AS IMPLICAÇÕES E DESAFIOS NA ERA
DIGITAL.....39**

Adriana Carla Silva de Oliveira e Raquel Elena Rinaldi Maciel

**PRINCÍPIOS-BASE DA LGPD: REFLEXOS CONSTITUCIONAIS NA
SOCIEDADE DIGITAL.....67**

Adriana da Costa Fernandes

**A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO BRASIL E
SEU COMPARATIVO INTERNACIONAL.....85**

Adriana Giuntini Viana e Henriette Groenwold Monteiro

**DESAFIOS E SOLUÇÕES PARA A ADEQUAÇÃO DE EMPRESAS À
LGPD.....105**

*Arlene Pereira da Silva Sacco e Bibianna Valadares Versiani de
Paula Peres*

**CONTRATAÇÃO DO ENCARREGADO DE DADOS (DPO) –
DESAFIOS E RESPONSABILIDADES.....125**

Daniela Lourenço de Oliveira

**EDUCAÇÃO DIGITAL E CONSCIENTIZAÇÃO: FORMANDO UMA
SOCIEDADE PRONTA PARA A LGPD.....147**

*Dayane Karine de Sousa Mendonça e Daphne Kalyva de Almeida
Rosa*

HERANÇA DIGITAL, PRIVACIDADE E PROTEÇÃO DE DADOS.....	167
--	------------

Fellipe Fernandes Duarte

PROTEÇÃO DE DADOS COMO DIREITO CONSTITUCIONAL: A EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO CONSTITUCIONAL NO BRASIL.....	195
---	------------

Graziella Angela Tinari Dell’Osa

DIREITOS DOS TITULARES DE DADOS SOB A PERSPECTIVA DA LGPD.....	211
---	------------

Ivana Avellar Nicolau de Lima e Silva

A APLICAÇÃO DO PODER SANCIONATÓRIO PELA AUTORIDADE NACIONAL DE DADOS PESSOAIS (ANPD) NA ERA DA GOVERNANÇA DIGITAL.....	221
---	------------

Joelane Rodrigues Carvalho e Eduarda Moraes Chacon Rosas

ANÁLISE SOBRE A DISCRIMINAÇÃO ALGORÍTMICA NA ERA DA PROTEÇÃO DE DADOS PESSOAIS.....	243
--	------------

Luanna da Costa e Silva

GOVERNANÇA EM PRIVACIDADE DE DADOS: A LGPD E SEU ARTIGO 50.....	263
--	------------

Lucas Paglia

IMPACTOS DA LGPD NO E-COMMERCE BRASILEIRO: DESAFIOS E BOAS PRÁTICAS PARA A PROTEÇÃO DE DADOS DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO.....	289
---	------------

Mariana Landim Carneiro

MARKETING DIGITAL E PROTEÇÃO DE DADOS PESSOAIS: ANÁLISE DA PERCEPÇÃO DOS CONSUMIDORES QUANTO À PROTEÇÃO DE SEUS DADOS E A CONSTRUÇÃO DA CONFIANÇA NA MARCA.....	307
--	------------

Mariani Nazaré da Silva Costa e Matheus Resende da Silva Costa

**PRIVACIDADE POR PADRÃO: INTEGRANDO A LGPD AO
DESENVOLVIMENTO TECNOLÓGICO.....323**

Neyanne Felipe Bezerra Araújo e Marcela Calazans Medeiros Silva

**SEGURANÇA DA INFORMAÇÃO E SEU PAPEL ALIADO À LGPD:
UMA PERSPECTIVA JURÍDICA.....337**

Paula de Paiva Santos e Luana Bueno Palma

SANÇÕES E PENALIDADES NA ERA DA LGPD.....357

Roberto Arylton P. Ramos

**A LGPD E SEUS EFEITOS NO MARKETING DIGITAL: ANÁLISE
DAS PRINCIPAIS PRÁTICAS DE MERCADO E SUAS IMPLICAÇÕES
NA PRIVACIDADE DE DADOS.....379**

Tatiana Venâncio de Rezende

O EXERCÍCIO DE DIREITOS PELOS TITULARES: O QUE ESPERAR E COMO SE PREPARAR

Adriana Antunes Winkler¹

INTRODUÇÃO

O advento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) trouxe à tona uma nova dinâmica na relação entre titulares de dados e agentes de tratamento. Inserida em um contexto de consolidação de direitos fundamentais e da crescente digitalização das relações sociais, a LGPD passou a reconhecer de forma expressa os direitos dos titulares de dados pessoais, estruturando um arcabouço jurídico robusto destinado a assegurar transparência, controle e segurança no tratamento de informações.

A previsão dos direitos no art. 18 do diploma legal, tais como o acesso, a correção, a portabilidade, a eliminação e a revogação do consentimento, tem gerado desafios práticos significativos para os controladores, exigindo adaptações tecnológicas, procedimentais e culturais. O reconhecimento do direito à autodeterminação informativa — fundamento também previsto no art. 2º da LGPD — está em consonância com tendências internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e legislações similares, como o *California Consumer Privacy Act* (CCPA).

Diante disso, este artigo tem como objetivo analisar o exercício dos direitos dos titulares, por meio da “Requisição de Direitos do Titular” (ou DSAR – *Data Subject’s Access Request*) sob as óticas jurí-

¹ **CIPM, CIPP-E, CDPO-BR, CDPSE, LL.M.**, Advogada, professora, autora e palestrante. Líder global de risco e privacidade na Accenture (EUA). Foi Vice-Presidente da Comissão de Direito Digital, Start ups e Tecnologias Disruptivas (OAB/DF; 2019-2020) e Presidente da Comissão de Privacidade e Proteção de Dados Pessoais (OAB/DF; 2020-2025).

dica, prática e normativa, identificando os principais pontos de atenção, bem como os caminhos para que as organizações públicas e privadas se preparem adequadamente para responder a essas demandas em conformidade com a lei e as boas práticas internacionais.

Mais adiante, será apresentada uma breve análise sobre os requisitos mínimos para que as empresas, órgãos públicos e demais entidades devem adotar para que não somente estejam aptas a receber e responder tais requisições, mas também o façam em conformidade com os princípios da boa-fé, transparência, segurança e responsabilização previstos na Lei Geral de Proteção de Dados Pessoais, garantindo o pleno exercício dos direitos dos titulares e a mitigação de riscos jurídicos decorrentes de eventuais inadequações.

Por fim, serão explorados casos reais relacionados a requisições de acesso realizadas por titulares de dados, com o intuito de ilustrar os principais desafios enfrentados na prática por controladores e operadores. A partir desses casos, serão extraídas as lições aprendidas (*lessons learned*), com enfoque nas boas práticas de governança, na adoção de mecanismos eficientes de resposta e na importância de processos internos bem estruturados para assegurar a conformidade com a LGPD e minimizar riscos reputacionais e regulatórios.

1. FUNDAMENTOS E EVOLUÇÃO HISTÓRICA DA REQUISIÇÃO DE ACESSO DOS TITULARES

Desde a publicação, em 15 de dezembro de 1890, do artigo intitulado *The Right to Privacy*¹, pelos advogados (e amigos desde a faculdade de Direito) Samuel Warren e Louis Brandeis, inaugurou-se um marco teórico e jurídico fundamental para a concepção moderna do direito à privacidade, estabelecendo as bases para a proteção da vida privada frente aos avanços tecnológicos e à crescente exposição promovida pelos meios de comunicação.

No referido artigo², os juristas evidenciam sua preocupação com o uso indiscriminado das novas “tecnologias” da época; a *câmera fotográfica* e o *gravador de áudio*. Tais equipamentos eram constantemente utilizados por, principalmente, repórteres, que publicariam, posteriormente, conteúdos de cunho íntimo e pessoal nos jornais impressos e rádios, causando, muitas vezes, constrangimento às pessoas envolvidas. Tais práticas deram início a debates sobre os limites entre o interesse público e a esfera privada, haja vista que a crítica central dos autores residia na ausência de consentimento e na invasão da privacidade, o que evidenciava a necessidade urgente de reconhecimento jurídico de um direito autônomo à privacidade frente aos avanços tecnológicos. Assim, esse embrião doutrinário abriu caminho para que, décadas depois, se estruturasse o campo da proteção de dados pessoais, incluindo o direito de acesso como mecanismo concreto de garantia da privacidade.

No contexto europeu, tais fundamentos ganharam dimensão já na década de 1970, quando os primeiros debates sobre bancos de dados centralizados suscitaram preocupações quanto ao controle do cidadão sobre seus próprios dados. A **Convenção 108 do Conselho da Europa (1981)**³ é considerada um marco inaugural ao reconhecer expressamente o direito dos indivíduos de conhecer e retificar informações pessoais mantidas em sistemas automatizados. Posteriormente, a **Diretiva 95/46/CE**⁴ consolidou esse direito como eixo da proteção de dados na União Europeia, sendo mais tarde reforçado pelo **Regulamento Geral**

2 WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, Dec. 1890.

3 CONSELHO DA EUROPA. Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108). Estrasburgo: Conselho da Europa, 1981.

4 UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, Luxemburgo, n. L 281, p. 31-50, 23 nov. 1995.

de Proteção de Dados (GDPR – 2016/679)⁵, que lhe conferiu amplitude, detalhamento procedimental e força sancionatória.

Fora do eixo europeu, legislações como a **Privacy Act de 1974**⁶ (EUA), o **Data Protection Act de 1984**⁷ e **1998**⁸ (Reino Unido) e a **Lei Federal de Proteção de Dados Pessoais em Posse de Particulares de 2010**⁹ (México) também refletiram a preocupação com a transparência e o controle individual. Em muitos desses diplomas, o direito de acesso constituiu a porta de entrada para o exercício de outros direitos relacionados ao tratamento de dados, como a retificação, exclusão ou oposição.

No Brasil, ainda que a Constituição de 1988¹⁰ tenha assegurado o **direito à intimidade, à vida privada e ao habeas data** (art. 5º, incisos X e LXXII), foi apenas com a **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**¹¹ que o direito de acesso ganhou contornos específicos, vinculados a uma disciplina própria de governança de dados.

A trajetória histórica, resumidamente traçada nos parágrafos anteriores, demonstra que a requisição de acesso não é apenas um direito instrumental, mas um pilar estruturante da proteção de dados. Sem ele, a autodeterminação informativa seria inviabilizada, uma vez que o titular só pode exercer controle sobre seus dados se conhecer de forma clara e tempestiva como e por quem eles estão sendo tratados.

5 UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Proteção de Dados – GDPR). Jornal Oficial da União Europeia, Luxemburgo, L 119, p. 1-88, 4 maio 2016.

6 UNITED STATES. Privacy Act of 1974. Public Law 93-579, 88 Stat. 1896, 31 Dec. 1974.

7 UNITED KINGDOM. Data Protection Act 1984. London: Parliament of the United Kingdom, 1984.

8 UNITED KINGDOM. Data Protection Act 1998. London: Parliament of the United Kingdom, 1998.

9 MÉXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación, Ciudad de México, 5 jul. 2010.

10 BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

11 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

(I) FUNDAMENTOS CONSTITUCIONAIS E JURISPRUDENCIAIS NO BRASIL

Como vimos anteriormente, no contexto brasileiro, a Constituição de 1988 foi o marco inaugural para o reconhecimento do direito de acesso a informações pessoais. Ao prever a inviolabilidade da intimidade e da vida privada (art. 5º, X), bem como o habeas data (art. 5º, LXXII), a Carta Magna não apenas assegurou proteção contra abusos estatais, mas também criou um instrumento processual específico para garantir que o cidadão pudesse conhecer e corrigir dados relativos a si, mantidos em registros públicos ou de caráter público. Embora pouco utilizado, o habeas data foi crucial como matriz jurídica da autodeterminação informativa no país, revelando o entendimento de que o acesso à informação pessoal é condição para o exercício pleno da cidadania. Esse fundamento foi reforçado por legislações setoriais, como o Código de Defesa do Consumidor (1990)¹², que tratou do acesso a cadastros de crédito; a Lei de Acesso à Informação (2011)¹³, que ampliou a transparência no setor público; além de normas específicas nos setores bancário^{14 15}, de telecomunicações^{16 17} e de saúde^{18 19}.

12 BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 12 set. 1990.

13 BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal. *Diário Oficial da União*: seção 1, Brasília, DF, 18 nov. 2011.

14 BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 11 jan. 2001.

15 BRASIL. Lei nº 12.414, de 9 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 (Cadastro Positivo). *Diário Oficial da União*: seção 1, Brasília, DF, 10 jun. 2011.

16 BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento da Agência Nacional de Telecomunicações (Anatel). *Diário Oficial da União*: seção 1, Brasília, DF, 17 jul. 1997.

17 BRASIL. Agência Nacional de Telecomunicações (ANATEL). Resolução nº 632, de 7 de março de 2014. Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações. *Diário Oficial da União*: seção 1, Brasília, DF, 10 mar. 2014.

18 BRASIL. Lei nº 8.080, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes. *Diário Oficial da União*: seção 1, Brasília, DF, 20 set. 1990.

19 BRASIL. Lei nº 9.656, de 3 de junho de 1998. Dispõe sobre os planos e seguros privados de assistência à saúde. *Diário Oficial da União*: seção 1, Brasília, DF, 4 jun. 1998.

A jurisprudência do Supremo Tribunal Federal (STF) também foi decisiva para dar efetividade a esses preceitos. Desde os anos 1990, a Corte reconheceu que o habeas data é um remédio constitucional voltado à proteção da informação pessoal, garantindo não apenas o acesso a registros públicos, mas também o direito de retificação de dados incorretos (como no HD 22/DF, Rel. Min. Celso de Mello, julgado em 1992)²⁰.

Mais recentemente, em 2020, o STF consolidou um marco histórico ao reconhecer expressamente os dados pessoais como direito fundamental autônomo, no julgamento da ADI 6.389/DF (Rel. Min. Rosa Weber)²¹. Na ocasião, a Corte declarou a inconstitucionalidade de dispositivos da Medida Provisória nº 954/2020, que obrigava o repasse de dados de usuários de telecomunicações ao IBGE. A decisão afirmou que a proteção de dados pessoais possui estatura constitucional, ainda que não estivesse expressamente prevista até então, e deve ser entendida como desdobramento direto dos direitos à privacidade e à autodeterminação informativa.

Esse reconhecimento jurisprudencial fortaleceu o arcabouço da LGPD, publicada em 2018 e em vigor desde 2020. A lei positivou, no art. 18, o direito de acesso do titular, alinhando-se não apenas ao texto constitucional e à prática judicial brasileira, mas também às tendências internacionais. Assim, a requisição de acesso em território nacional passou a ocupar posição central no sistema de proteção de dados, sendo vista como instrumento fundamental de cidadania, transparência e *accountability*.

2. O DIREITO DE ACESSO NA LGPD: CONTEÚDO, ALCANCE E LIMITES

O art. 18 da Lei nº 13.709/2018 (LGPD) estabelece o rol dos direitos assegurados ao titular de dados pessoais, conforme pode-se ler a seguir o seu caput e incisos:

20 BRASIL. Supremo Tribunal Federal. *Habeas Data nº 22/DF*. Relator: Min. Celso de Mello. Brasília, DF, 19 maio 1992. Disponível em: <http://portal.stf.jus.br>. Acesso em: 8 set. 2025.

21 BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6.389/DF*. Relatora: Min. Rosa Weber. Brasília, DF, 7 maio 2020. Disponível em: <http://portal.stf.jus.br>. Acesso em: 8 set. 2025.

“Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

O presente artigo abordará, dentre esse rol de direitos, o direito de confirmação da existência de tratamento e, mais especificamente, o de acesso aos dados pessoais (incisos I e II). Tais dispositivos concretizam, em âmbito infraconstitucional, os fundamentos já delineados pela Constituição Federal de 1988 e pela jurisprudência do Supremo Tribunal Federal, ao conferir ao indivíduo um instrumento normativo claro e detalhado para o exercício da autodeterminação informativa.

A redação do inciso II evidencia que o direito de acesso não se limita à mera ciência sobre a coleta de dados, mas impõe ao controlador a obrigação de fornecer informações claras, completas e acessíveis ao titular. Isso inclui, além da confirmação da existência de tratamento, a disponibilização de dados pessoais que estejam sendo tratados, bem como informações complementares sobre as finalidades, a forma e a duração do tratamento, a identificação dos controladores e eventuais compartilhamentos com terceiros.

O acesso previsto na LGPD deve, ainda, ser facilitado e preferencialmente fornecido em formato eletrônico seguro e estruturado (art. 19), de modo a permitir a portabilidade e o uso efetivo dos dados pelo titular. Trata-se de um avanço em relação ao habeas data e às legislações setoriais anteriores, pois amplia o alcance do direito, adaptando-o ao contexto tecnológico contemporâneo e às exigências de interoperabilidade de sistemas.

Desse modo, o art. 18, II, não apenas garante o conhecimento sobre o tratamento de dados, mas também estabelece um dever de transparência ativa por parte dos controladores. Essa característica faz do direito de acesso a porta de entrada para os demais direitos previstos na LGPD (como retificação, anonimização, bloqueio ou eliminação), funcionando como condição de possibilidade para o exercício pleno da cidadania digital.

2.1. Alcance

O direito de acesso previsto no art. 18, inciso II, da LGPD possui um alcance que transcende a mera disponibilização de informações. Ele se configura como condição de possibilidade para o exercício de todos os demais direitos dos titulares. Sem conhecer quais dados estão sendo tratados, por quem, para quais finalidades e com quais destinatários, o titular não dispõe dos elementos necessários para decidir sobre eventual retificação, eliminação, oposição ou portabilidade. Por essa razão, a doutrina e a prática regulatória reconhecem o acesso como a

porta de entrada para a autodeterminação informativa. Doneda (2006)²² já havia destacado que, sem conhecimento prévio acerca do tratamento, o titular não consegue exercer seus demais direitos de forma efetiva. Nessa mesma linha, Bygrave (2002)²³ descreve o acesso como um verdadeiro *gateway right*, por ser o ponto de partida para a proteção efetiva dos dados pessoais. Mendes, Doneda e Monteiro (2020)²⁴, em comentários à LGPD, reforçam essa compreensão ao salientar que o art. 18 organiza o núcleo de prerrogativas do titular justamente a partir da garantia de acesso. Wimmer (2020)²⁵, por sua vez, enfatiza que o reconhecimento do direito fundamental à proteção de dados pelo STF somente se torna concreto na prática quando acompanhado da efetividade do direito de acesso, que viabiliza transparência e controle social sobre o tratamento de dados pessoais.

No contexto brasileiro, essa função ganha relevo adicional, pois a LGPD universaliza um direito antes restrito ao habeas data e a legislações setoriais específicas. A lei amplia sua aplicabilidade para todos os agentes de tratamento, públicos e privados, independentemente de setor econômico, consolidando um regime geral e uniforme de tutela. Dessa forma, o acesso não se limita a proteger contra abusos estatais ou práticas de mercado isoladas, mas assegura ao titular um controle contínuo e ampliado sobre seus dados em diferentes esferas sociais e econômicas.

Além disso, a função do acesso na LGPD está diretamente vinculada ao princípio da transparência (art. 6º, VI) e ao princípio da responsabilização e prestação de contas (art. 6º, X). O controlador, ao atender à requisição de acesso, não apenas satisfaz um direito subjetivo,

22 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da legislação brasileira*. Rio de Janeiro: Renovar, 2006.

23 BYGRAVE, Lee A. *Data protection law: approaching its rationale, logic and limits*. The Hague: Kluwer Law International, 2002.

24 MENDES, Laura Schertel; DONEDA, Danilo; MONTEIRO, Fabrício da Mota Alves (org.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. São Paulo: Thomson Reuters Brasil, 2020.

25 WIMMER, Miriam. O direito fundamental à proteção de dados pessoais e a sua implementação no Brasil: fundamentos, desafios e perspectivas. *Revista de Direito Civil Contemporâneo*, v. 23, p. 61-91, 2020.

mas também demonstra conformidade com o regime de proteção de dados, fortalecendo a confiança dos titulares e contribuindo para a consolidação de uma cultura de proteção da privacidade no país.

Assim, o direito de acesso deve ser compreendido como eixo estruturante do ecossistema da LGPD: é simultaneamente um direito instrumental, pois possibilita a efetividade dos demais direitos; e um direito substantivo, porque concretiza o valor da transparência e da dignidade da pessoa humana no ambiente digital.

2.2. Limites

Embora o art. 18 da LGPD assegure ao titular o direito de acesso aos seus dados pessoais, trata-se de um direito que não é absoluto. Como ocorre com outros direitos fundamentais, seu exercício deve ser conciliado com interesses igualmente legítimos, a fim de evitar colisões ou comprometimento de valores constitucionais relevantes.

Em primeiro lugar, a própria LGPD estabelece hipóteses que limitam a plenitude do acesso, como nos casos em que a requisição possa comprometer segredos comerciais e industriais (art. 18, V) ou envolver dados anonimizados, já fora do escopo da lei (art. 18, §7º). Essa limitação decorre da necessidade de proteger não apenas os interesses do titular, mas também a esfera jurídica do controlador e de terceiros que possam ser afetados.

Em segundo lugar, é preciso reconhecer que o acesso deve ser harmonizado com outros direitos fundamentais, tais como a liberdade de expressão e informação (art. 5º, IX, CF/88), a segurança nacional e a ordem pública. A divulgação irrestrita de informações em certas situações poderia gerar riscos a investigações em curso, à segurança de sistemas tecnológicos críticos ou até à proteção da intimidade de outros indivíduos.

No âmbito internacional, esses limites já foram reconhecidos por diversos ordenamentos. O GDPR, por exemplo, prevê que o direito

de acesso pode ser restringido em situações que envolvam segurança do Estado, defesa nacional ou prevenção de infrações penais (art. 23). A LGPD, embora não detalhe hipóteses tão amplas, deve ser interpretada de forma sistemática com a Constituição e com legislações especiais, permitindo a adoção de restrições proporcionais e fundamentadas.

Cabe ressaltar, ainda, que a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel relevante nesse equilíbrio, uma vez que possui competência para regulamentar a forma de exercício dos direitos dos titulares (art. 55-J, XIII, LGPD) e para dirimir potenciais conflitos envolvendo pedidos de acesso, especialmente em casos de alegação de excesso ou inviabilidade técnica.

Portanto, o direito de acesso, embora central e estruturante, deve ser exercido dentro de um regime de proporcionalidade e razoabilidade, que assegure sua efetividade sem comprometer a proteção de outros direitos fundamentais ou interesses jurídicos legítimos. Essa ponderação é indispensável para consolidar uma cultura de proteção de dados que seja, ao mesmo tempo, eficaz e equilibrada.

3. OPERACIONALIZAÇÃO DO DIREITO DE ACESSO NA LGPD: PROCEDIMENTOS, PRAZOS E DESAFIOS PRÁTICOS

3.1. Procedimentos para o exercício do direito de acesso

A LGPD prevê que o titular pode exercer seus direitos mediante requisição expressa ao controlador (art. 18, §3º). Essa solicitação pode ser feita diretamente pelo titular ou por representante legalmente constituído, devendo o controlador disponibilizar mecanismos gratuitos e facilitados para tanto, tais como: portais eletrônicos com formulários padronizados; endereços de e-mail específicos para o recebimento de requisições de titulares (exemplos: “privacidade”, “dpo”, “encarregadodedados”, “solicitacaoolgpd” seguidos do arroba e domínio da empresa ou instituição); centrais telefônicas ou canais de atendimento

ao consumidor; aplicativos móveis; e, quando aplicável, atendimento presencial em unidades físicas de atendimento ao público. O objetivo é assegurar que o exercício do direito não seja oneroso nem dependa de barreiras técnicas, linguísticas ou financeiras, permitindo que titulares com diferentes perfis socioeconômicos tenham meios efetivos para exercer suas prerrogativas.

3.2. Formatos e requisitos de resposta

A resposta a ser fornecida pelo Controlador deve ser clara, inteligível e gratuita, observando-se o dever de fornecer informações completas e atualizadas. O art. 19 exige que sejam entregues não apenas os dados em si, mas também informações sobre:

- a) a origem dos dados;
- b) os critérios utilizados no tratamento;
- c) a finalidade específica;
- d) os agentes de tratamento com os quais houve compartilhamento.

A seguir, um modelo de resposta à requisição do titular (fictício):

Prezado(a) [Nome do Titular],

Em atendimento à sua solicitação de acesso aos dados pessoais, nos termos do art. 18, II, da Lei nº 13.709/2018 (LGPD), informamos o seguinte:

1. Dados pessoais tratados:

Nome completo: João da Silva

CPF: *.456.789-

Endereço de e-mail: joaosilva@email.com

Histórico de compras no período de 2021 a 2023

2. Finalidades do tratamento:

Os dados são utilizados para fins de cadastro, gestão de pedidos, emissão de notas fiscais, atendimento pós-venda e envio de comunicações relacionadas a produtos e serviços.

3. Forma e duração do tratamento:

Os dados são tratados em sistemas eletrônicos seguros, com acesso restrito a colaboradores autorizados. O prazo de retenção é de 5 (cinco) anos, contado da última transação, em conformidade com a legislação fiscal.

4. Compartilhamento com terceiros:

Os dados foram compartilhados com:

Empresa XPTO Ltda. (serviços de logística e entrega)

Empresa ABC Ltda. (serviços de tecnologia em nuvem)

5. Direitos do titular:

Você poderá, a qualquer tempo, solicitar a retificação de informações, a portabilidade para outro fornecedor, ou a eliminação de dados excessivos ou tratados em desconformidade, entre outros direitos previstos na LGPD.

6. Canal de contato:

Para exercer seus direitos ou esclarecer dúvidas adicionais, entre em contato pelo e-mail privacidade@empresa.com.br ou pelo telefone 0800-000-000.

Atenciosamente,

[Nome do DPO ou responsável pela privacidade]

Encarregado de Proteção de Dados – [Nome da Empresa]

Esse detalhamento visa a assegurar transparência e *accountability*, permitindo que o titular compreenda de modo abrangente como suas informações são tratadas. Importa destacar que o conteúdo da res-

posta pode e deve ser customizado de acordo com a natureza da atividade comercial ou institucional do controlador. Empresas do setor financeiro, por exemplo, tendem a fornecer informações mais detalhadas sobre dados cadastrais, histórico de transações e critérios de análise de crédito; já instituições de saúde, em atenção à legislação setorial, podem incluir dados sensíveis relativos a prontuários, diagnósticos e tratamentos, observando padrões de sigilo médico. Órgãos públicos, por sua vez, precisam compatibilizar o acesso individual com as regras da Lei de Acesso à Informação (Lei nº 12.527/2011), garantindo transparência sem expor dados de terceiros. Essa adaptação contextual reforça a ideia de que o direito de acesso, embora uniformemente previsto na LGPD, não é exercido de forma padronizada, mas sim em diálogo com a atividade desempenhada pelo controlador e com os princípios da razoabilidade e da proporcionalidade.

3.3 .Prazos legais e regulamentação da ANPD

O art. 19 da LGPD estabelece dois regimes de prazo distintos para o atendimento às requisições de titulares:

Confirmação imediata da existência de tratamento – quando solicitada de forma simplificada, a lei impõe que o controlador dê resposta imediata sobre se realiza ou não o tratamento de dados do titular. Esse dever de prontidão busca evitar que o titular fique em situação de incerteza quanto à posse ou uso de suas informações.

Disponibilização do acesso aos dados – deve ser fornecida em até 15 (quinze) dias, contados da data do requerimento, em formato eletrônico seguro e estruturado ou, quando solicitado, em meio físico. Esse prazo é aplicável também às demais requisições do art. 18, salvo previsão específica em regulamento.

A Autoridade Nacional de Proteção de Dados (ANPD), em seu Guia Orientativo sobre Direitos dos Titulares (2022)²⁶, esclareceu que

26 BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Guia orientativo sobre direitos dos titulares*. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-sobre-direitos-dos-titulares>. Acesso em: 8 set. 2025.

os prazos devem ser contados em dias corridos, e não úteis, reforçando a obrigação de celeridade no atendimento. Além disso, eventuais prorrogações só são admitidas em hipóteses excepcionais e devem ser justificadas de maneira transparente ao titular, demonstrando as razões de fato ou de direito que impedem a resposta imediata.

Essa sistemática representa um avanço em relação ao habeas data, cujo processamento judicial naturalmente implicava maior morosidade. A previsão de prazo certo e reduzido na LGPD reforça a natureza procedimental e administrativa do direito de acesso, facilitando o exercício cotidiano desse direito sem a necessidade de judicialização.

Dessa forma, a operacionalização do direito de acesso demonstra que a LGPD não se limita a consagrar direitos em abstrato, mas impõe aos controladores a criação de mecanismos concretos de resposta, em prazos definidos e com padrões de clareza e transparência. A efetividade desse direito depende, portanto, da capacidade das organizações de mapear seus fluxos de dados, estabelecer canais acessíveis de comunicação com os titulares e internalizar rotinas administrativas capazes de atender às requisições de forma tempestiva e segura. A ausência de tais mecanismos transforma o direito em “letra morta”, fragilizando a confiança social e expondo controladores a riscos jurídicos, regulatórios e reputacionais.

Ao mesmo tempo, a experiência brasileira mostra que o direito de acesso deve ser visto como um instrumento de governança e cidadania digital. É muito mais do que uma obrigação legal, mas sim uma oportunidade para fortalecer a relação entre controladores e titulares, consolidando uma cultura de prestação de contas e de respeito à privacidade. Nesse sentido, a operacionalização adequada do direito de acesso funciona como um verdadeiro termômetro do nível de maturidade de proteção de dados no país, pavimentando o caminho para debates futuros sobre a efetividade dos demais direitos dos titulares e a evolução do regime regulatório nacional.

4. CONSIDERAÇÕES FINAIS

A proteção de dados pessoais no Brasil, consolidada pela LGPD, representa uma das mais significativas conquistas normativas da sociedade contemporânea. Assim como os principais diplomas internacionais, a lei brasileira foi concebida sob a lógica de que o cidadão é o centro do sistema e que a privacidade, a dignidade e a autonomia individual não são concessões, mas direitos inalienáveis. Ao reconhecer que o tratamento de dados não pode se sobrepor à pessoa, a LGPD se coloca como uma barreira jurídica contra práticas abusivas e como um alicerce ético para a sociedade da informação.

Todavia, a eficácia desse arcabouço protetivo ainda depende de um processo de amadurecimento coletivo. Embora em vigor desde 2020, a LGPD permanece pouco conhecida pela grande maioria da população brasileira, o que limita a efetividade dos direitos dos titulares e mantém lacunas na consolidação de uma cultura de privacidade. O exercício de direitos como o acesso, a retificação e a eliminação só será pleno quando houver consciência social difusa, isto é, quando cada cidadão tiver clareza de sua condição de titular de dados e do poder que lhe foi conferido pela lei. Sem essa apropriação coletiva, a LGPD corre o risco de permanecer restrita a círculos jurídicos, empresariais e acadêmicos, afastando-se de seu objetivo maior de empoderamento da sociedade.

De igual modo, a lei desafia os controladores a repensarem sua postura. Longe de ser apenas um instrumento de fiscalização ou de gerar custos de conformidade, a LGPD deve ser vista como oportunidade estratégica. Ao assegurar direitos de forma transparente e responsiva, organizações podem transformar a privacidade em valor agregado, consolidando uma relação de confiança com seus clientes, parceiros e cidadãos em geral. Nesse sentido, conformidade não é apenas cumprimento legal, mas também vantagem competitiva: empresas que internalizam práticas éticas de governança de dados tendem a conquistar maior fidelização, reputação sólida e acesso a novos mercados.

Por isso, é preciso reconhecer que a LGPD funciona como um duplo vetor de transformação. Para os cidadãos, é instrumento de eman-

cipação, que possibilita maior controle sobre o ciclo de vida de suas informações pessoais. Para os agentes econômicos e institucionais, é oportunidade de alinhar inovação tecnológica e modelos de negócio a princípios de confiança, transparência e responsabilidade. O futuro da proteção de dados no Brasil dependerá dessa convergência: de um lado, da apropriação social dos direitos; de outro, da internalização da privacidade como valor estratégico.

Assim, a efetividade da LGPD será medida não apenas pela quantidade de sanções aplicadas ou intermináveis relatórios de conformidade apresentados, mas pelo quanto ela conseguirá transformar a cultura brasileira em torno do uso ético de dados. O desafio é grande, mas a promessa é maior: construir um ambiente em que a tecnologia e a inovação caminhem lado a lado com o respeito à pessoa humana, consolidando a privacidade como um dos pilares da democracia digital no Brasil.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 12 set. 1990.

BRASIL. Lei nº 8.080, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes. *Diário Oficial da União*: seção 1, Brasília, DF, 20 set. 1990.

BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações e cria a Agência Nacional de Telecomunicações (Anatel). *Diário Oficial da União*: seção 1, Brasília, DF, 17 jul. 1997.

BRASIL. Lei nº 9.656, de 3 de junho de 1998. Dispõe sobre os planos e seguros privados de assistência à saúde. *Diário Oficial da União*: seção 1, Brasília, DF, 4 jun. 1998.

BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras. *Diário Oficial da União*: seção 1, Brasília, DF, 11 jan. 2001.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento (Cadastro Positivo). *Diário Oficial da União*: seção 1, Brasília, DF, 10 jun. 2011.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto na Constituição Federal. *Diário Oficial da União*: seção 1, Brasília, DF, 18 nov. 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Supremo Tribunal Federal. *Habeas Data nº 22/DF*. Relator: Min. Celso de Mello. Brasília, DF, 19 maio 1992. Disponível em: <http://portal.stf.jus.br>. Acesso em: 8 set. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6.389/DF*. Relatora: Min. Rosa Weber. Brasília, DF, 7 maio 2020. Disponível em: <http://portal.stf.jus.br>. Acesso em: 8 set. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Guia orientativo sobre direitos dos titulares*. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-sobre-direitos-dos-titulares>. Acesso em: 8 set. 2025.

BYGRAVE, Lee A. *Data protection law: approaching its rationale, logic and limits*. The Hague: Kluwer Law International, 2002.

CONSELHO DA EUROPA. Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108). Estrasburgo: Conselho da Europa, 1981.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da legislação brasileira*. Rio de Janeiro: Renovar, 2006.

MENDES, Laura Schertel; DONEDA, Danilo; MONTEIRO, Fabricio da Mota Alves (org.). *Comentários à Lei Geral de Proteção de Dados*

Pessoais. São Paulo: Thomson Reuters Brasil, 2020.

MÉXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*, Ciudad de México, 5 jul. 2010.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. *Jornal Oficial das Comunidades Europeias*, Luxemburgo, n. L 281, p. 31-50, 23 nov. 1995.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados – GDPR). *Jornal Oficial da União Europeia*, Luxemburgo, L 119, p. 1-88, 4 maio 2016.

UNITED KINGDOM. Data Protection Act 1984. London: Parliament of the United Kingdom, 1984.

UNITED KINGDOM. Data Protection Act 1998. London: Parliament of the United Kingdom, 1998.

UNITED STATES. Privacy Act of 1974. Public Law 93-579, 88 Stat. 1896, 31 Dec. 1974.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, Dec. 1890.

WIMMER, Miriam. O direito fundamental à proteção de dados pessoais e a sua implementação no Brasil: fundamentos, desafios e perspectivas. *Revista de Direito Civil Contemporâneo*, v. 23, p. 61-91, 2020.

A PERCEPÇÃO DOS RISCOS NA PROTEÇÃO DE DADOS: UM ESTUDO SOBRE AS IMPLICAÇÕES E DESAFIOS NA ERA DIGITAL

Adriana Carla Silva de Oliveira¹

Raquel Elena Rinaldi Maciel²

INTRODUÇÃO

Na era digital, a coleta, o armazenamento e o tratamento de dados pessoais tornaram-se aspectos centrais da dinâmica econômica e social. Tecnologias emergentes, como inteligência artificial, *block-chain* e a Web 3.0, estão remodelando a maneira como os indivíduos interagem com o mundo digital, ao mesmo tempo em que oferecem novas oportunidades e desafios para a privacidade e a segurança dos dados. Esse cenário de transformação é acompanhado por uma crescente conscientização da sociedade sobre a importância da proteção de dados, impulsionada por regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Este artigo busca explorar a percepção dos riscos associados à proteção de dados, analisando as implicações para indivíduos, organizações e o poder público. O objetivo é examinar como os diferentes atores reconhecem e enfrentam os desafios apresentados por um ambiente digital cada vez mais complexo e interconectado, além de destacar as principais ameaças e as estratégias de mitigação que garantem a conformidade com as legislações de proteção de dados.

1 Pós-doutorado em Direito. Doutorado em Ciência da Informação. Mestre em Engenharia de Produção. MBA em Data Protection Officer. Servidora Pública e Membro integrante do Comitê Gestor de Privacidade de Dados do TJRN. Membro convidada da Comissão de Privacidade de Dados da OAB/DF e Coordenadora Científica da Associação Brasileira de Governança Pública de Dados Pessoais (govDADOS).

2 Doutora em Teoria e Filosofia do Direito. Mestre em Teoria e Filosofia do Direito. Especialização em Lei Geral de Proteção de Dados - LGPD. Diretora Executiva da Associação Brasileira de Governança Pública de Dados Pessoais (govDADOS).

Também serão discutidas as responsabilidades compartilhadas na governança de dados e a importância de uma cultura organizacional robusta voltada para a segurança da informação.

Dividido em seções, o artigo apresenta inicialmente os fundamentos teóricos que norteiam os conceitos de privacidade, proteção de dados e gestão de riscos. Em seguida, aborda o impacto das regulamentações como a GDPR e a LGPD na percepção de riscos e no comportamento organizacional. Por fim, analisa como a percepção de riscos influencia as decisões de indivíduos e organizações, apontando para a necessidade de alinhar práticas operacionais e estratégicas à conformidade regulatória e à construção de confiança em um mundo digital.

1. FUNDAMENTOS TEÓRICOS: PRIVACIDADE, PROTEÇÃO DE DADOS E RISCOS

O avanço das tecnologias digitais tem intensificado o debate sobre privacidade, proteção de dados e os riscos cibernéticos como temas fundamentais na sociedade contemporânea.

Nesta seção revisaremos a literatura sobre tais conceitos, considerando teóricos renomados e suas contribuições para a compreensão dos riscos associados à manipulação e tratamento de dados pessoais. Serão abordados os conceitos de privacidade e proteção de dados, a definição e a classificação de riscos, além dos principais referenciais teóricos sobre percepção de riscos.

1.1. Conceitos de privacidade e proteção de dados

A privacidade pode ser compreendida como o direito de um indivíduo de controlar o acesso a suas informações pessoais e limitar a exposição de sua vida privada e intimidade. É um conceito associado à autonomia, dignidade e liberdade individual, permitindo que cada pessoa decida o que deseja compartilhar ou manter restrito, conforme suas preferências e necessidades de proteção. De acordo com Warren

e Brandeis (1890), a privacidade é o direito do indivíduo de preservar seus dados e informações pessoais contra qualquer intrusão. É o controle que a ele se assegura sobre a divulgação ou exposição de manifestações próprias de sua vida, por isso íntima e privada. Em suma, segundo os autores supracitados, é o direito à privacidade dentro da categoria mais geral do direito de o indivíduo ser deixado em paz. Seguramente é uma discussão atualizada para os dias atuais.

Historicamente, Alan Westin (1967) definiu a privacidade como o “direito de controlar a informação sobre si mesmo”, enfatizando que ela garante ao indivíduo uma esfera pessoal e o poder de definir como e com quem se comunica. Segundo tal autor, a privacidade é uma condição de controle seletivo sobre a interação social e sobre a comunicação das informações pessoais. Essa visão destaca a privacidade como um direito individual de autonomia, alinhado ao conceito de “autodeterminação informacional”.

Daniel Solove (2008), no entanto, aponta que a privacidade é multifacetada e não pode ser completamente capturada por um único conceito. Em vez disso, envolve diferentes dimensões e aspectos que vão desde a proteção contra vigilância, coleta e uso indevido de dados até o controle de informações sensíveis. O autor amplia a compreensão de privacidade ao propor que a mesma não pode ser reduzida a um conceito único; sendo uma construção jurídica e social que se manifesta em diferentes dimensões, como coleta, tratamento monitoramento, vigilância, e segurança da informação, afetando tanto a dignidade pessoal quanto a liberdade do indivíduo.

Helen Nissenbaum (2004) com sua teoria da “Privacy as Contextual Integrity”, argumenta que a privacidade deve ser entendida em termos de normas sociais que determinam o que é apropriado compartilhar em cada contexto. Dessa forma, a privacidade é vista não apenas como uma proteção contra a exposição, mas como a conformidade com expectativas individuais, sociais e contextuais.

Esses enfoques refletem que a privacidade é um direito dinâmico e culturalmente variável, fundamental para a autonomia e o bem-estar dos indivíduos, especialmente em uma sociedade digital onde dados

peçoais são constantemente processados e analisados por empresas e governos.

No contexto da proteção de dados, a privacidade torna-se mais complexa, uma vez que envolve não apenas o controle de informações, mas também as práticas e políticas que regulam o tratamento dos dados pessoais. A proteção de dados surge, então, como um conjunto de normas e práticas destinadas a garantir que o uso das informações seja realizado de maneira ética e segura, respeitando a privacidade dos indivíduos.

No contexto europeu, o GDPR (*General Data Protection Regulation*) estabelece princípios como o direito ao esquecimento, a transparência e o consentimento, que definem os direitos dos titulares dos dados. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) adota uma abordagem semelhante, ao definir os papéis e as responsabilidades das empresas e organizações no tratamento de dados pessoais. Assim, a proteção de dados aparece como um esforço para assegurar a privacidade do indivíduo no ambiente impresso e digital, especialmente nos ambientes de práticas tecnológicas que, por sua natureza, têm o potencial de violar a autonomia informacional dos indivíduos.

Essas regulamentações definem a privacidade em termos de:

(i) Controle sobre Dados Pessoais: A privacidade é garantida pelo direito dos titulares de controlar quem pode acessar seus dados e para qual finalidade. Isso inclui o direito de consentir ou negar o uso de seus dados, e de revogar o consentimento, se desejado.

(ii) Direitos do Titular dos Dados: A LGPD e o GDPR reforçam direitos como o direito ao acesso, à retificação, à exclusão (direito ao esquecimento), à portabilidade e à transparência. Salienta-se que no caso da lei brasileira, não há dispositivo legal para o Direito ao Esquecimento. Esses direitos garantem que os indivíduos possam controlar seus dados, corrigir informações incorretas e excluir dados que não sejam mais necessários ou que tenham sido tratados de forma inadequada.

(iii) Princípios e Normas de Tratamento: Ambas as regulamentações estabelecem princípios para o tratamento de dados, como finalidade, adequação, necessidade, qualidade, segurança, prevenção, responsabilização e transparência. Esses princípios determinam que o tratamento dos dados deve ser feito apenas para finalidades específicas, de maneira proporcional e com medidas de segurança adequadas, evitando o uso indiscriminado, indevido ou desproporcional dos dados.

Assim, a privacidade sob o prisma da LGPD e do GDP, é um direito que envolve o respeito à integridade, à informação e a autonomia do indivíduo, considerando a coleta, uso e compartilhamento dos dados pessoais de maneira ética e dentro dos limites estabelecidos pela lei específica.

1.2. Definição e classificação de riscos na proteção de dados

A definição e a classificação de riscos na proteção de dados são fundamentais para entender como empresas e organizações podem prevenir e mitigar incidentes de segurança. Risco, no contexto da proteção de dados, refere-se à probabilidade de um evento adverso – como uma violação de dados ou um acesso não autorizado – que possa comprometer a confidencialidade, integridade e disponibilidade das informações pessoais.

O risco na proteção de dados é comumente definido como a combinação entre a probabilidade de ocorrência de um evento adverso e o impacto que ele pode causar sobre a privacidade e os direitos dos titulares dos dados. Um risco de proteção de dados pode incluir desde a perda ou o vazamento de informações pessoais até o uso indevido de dados por terceiros, podendo afetar tanto indivíduos quanto organizações. A definição de risco é central para as regulamentações de proteção de dados, como o GDPR e a LGPD, que exigem que as organizações identifiquem e gerenciem riscos associados ao tratamento de dados pessoais, tomando medidas adequadas para garantir sua segurança e integridade.

Para gerir esses riscos de maneira eficaz, as empresas adotam estratégias de análise e avaliação de impacto de risco, como a *Data Protection Impact Assessment* (DPIA). O DPIA é uma avaliação de impacto exigida em certos casos pelo GDPR e recomendada pela LGPD para identificar e mitigar potenciais riscos antes do lançamento de um novo projeto ou de um tratamento de dados sensíveis. A identificação precisa de riscos permite que as organizações implementem controles específicos e priorizem recursos para as áreas de maior vulnerabilidade.

A gestão de riscos é um processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles diante de uma matriz de riscos. As diretrizes gerais do processo de gestão de risco de privacidade e proteção de, além de estarem alinhadas à política de segurança da informação, poderão considerar, entre outros aspectos, objetivos estratégicos, processos, estrutura organizacional, requisitos da LGPD e demais normativos aplicáveis. A identificação e análise dos fatores de risco devem ser documentadas e justificadas para que possam demonstrar que as decisões tomadas em relação à gestão de riscos foram as medidas mais adequadas com base nas informações disponíveis. Comumente ela é normatizada por uma Política de Gestão de Riscos ou incorporada na Política de Segurança da Informação e na Política de Privacidade e Proteção de Dados Pessoais.

A avaliação de risco dificilmente irá representar a totalidade dos fatores de risco envolvidos no tratamento. Cabe ao controlador identificar o maior número possível de fatores, principalmente os mais relevantes, que possam afetar os dados pessoais que serão tratados. Para cada fator identificado deve-se estimar a probabilidade de materialização do risco e o impacto inerente. Esse impacto dependerá dos possíveis danos que possam ser causados aos titulares, em particular no âmbito dos seus direitos e liberdades individuais e coletivos.

Destaca-se que a existência de múltiplos fatores de risco pode aumentar o nível de risco do tratamento considerado individualmente. Quando existem diferentes fatores de risco, é necessário interpretar como esses fatores podem interagir entre si para aumentar o nível de risco do tratamento, analisando suas dependências e efeitos combinados ou as interações mútuas.

Nesse contexto, a gestão de riscos pode ser conduzida por diversas metodologias. No entanto, é recomendável optar por aquelas amplamente reconhecidas como boas práticas pela comunidade técnica de segurança, privacidade e proteção de dados e a escolha da mais adequada é uma responsabilidade do controlador de dados. A avaliação do nível de risco deve considerar os possíveis impactos sobre os titulares dos dados pessoais, incluindo a perda de confidencialidade, integridade e disponibilidade dos dados, a reversão de anonimização ou pseudonimização, o uso indevido das informações, a violação de direitos e liberdades individuais, ou qualquer forma de tratamento inadequado ou ilícito.

Os riscos de proteção de dados podem ser classificados de diversas maneiras, mas, em geral, são categorizados em três grupos principais: riscos técnicos, riscos humanos e riscos organizacionais. Cada um desses tipos de risco apresenta particularidades que influenciam o modo como as empresas lidam com a segurança dos dados.

Riscos técnicos referem-se a vulnerabilidades nos sistemas tecnológicos que podem comprometer a segurança dos dados. Esse tipo de risco inclui falhas em softwares, ausência de atualizações de segurança, vulnerabilidades em redes e sistemas expostos a ataques cibernéticos, como o *phishing* e o *ransomware*. Em muitos casos, os riscos técnicos são explorados por *hackers* e *cyber* criminosos que aproveitam brechas tecnológicas (*data breach*) para acessar dados pessoais ou para interceptar informações sensíveis. Para mitigar esses riscos, as empresas utilizam medidas como criptografia, *firewalls* e sistemas de detecção de intrusões (IDS).

Os riscos humanos estão relacionados a erros ou atitudes de usuários e funcionários que podem comprometer a segurança dos dados. Esses riscos incluem, por exemplo, a manipulação inadequada de informações, o compartilhamento de dados de maneira insegura e o descuido com senhas e dispositivos de trabalho. O fator humano é amplamente reconhecido como uma das principais causas de incidentes de segurança e de violação de dados pessoais, pois mesmo uma estrutura tecnológica robusta pode ser vulnerável a comportamentos descuidados

e sem capacitação adequada. Para reduzir esses riscos, as organizações investem em treinamento e conscientização acerca da LGPD, Segurança da Informação, Riscos e outros temas que promovem uma cultura de privacidade e proteção de dados entre todos os colaboradores da empresa.

Os riscos organizacionais derivam de políticas internas e práticas administrativas que não são adequadas para garantir a segurança dos dados. Incluem a ausência de políticas de privacidade e proteção de dados claras, a falta de controles internos, a inadequação das práticas de segurança e a ausência de uma estrutura de governança de dados. Esses riscos podem surgir, por exemplo, em empresas que não realizam avaliações de risco periodicamente ou que falham em definir responsabilidades sobre a proteção de dados. Para mitigar esses riscos, é necessário que as empresas desenvolvam políticas de governança de dados, designem responsáveis, como o Encarregado pelo Tratamento de Dados Pessoais, também conhecido como DPO (*Data Protection Officer*) e adotem práticas de auditoria para assegurar a conformidade com as regulamentações.

Classificar os riscos na proteção de dados permite que as empresas identifiquem com precisão as áreas que precisam de maior proteção e invistam de maneira mais eficaz em medidas de mitigação e primordialmente, as preventivas. As regulamentações de proteção de dados, como o GDPR e a LGPD, enfatizam a necessidade de gestão de riscos, incentivando as empresas a compreenderem e classificarem os riscos com base na sensibilidade dos dados tratados e na criticidade dos processos envolvidos. Essa análise detalhada ajuda a priorizar ações de segurança, alocar recursos para medidas de mitigação e definir procedimentos que minimizem o impacto de possíveis incidentes.

Além disso, a classificação dos riscos também facilita a comunicação e a conscientização interna, pois cada tipo de risco pode ser abordado de maneira específica. Riscos técnicos, humanos e organizacionais demandam estratégias e controles distintos, bem como uma estrutura de classificação de riscos que auxiliem as organizações desenvolvam políticas de gestão de riscos, medidas de segurança da

informação e diretrizes na governança organizacional que englobem todos os aspectos do tratamento de dados pessoais e a minimização de riscos em um processo de melhoria contínua.

1.3. Percepção de riscos no âmbito individual e organizacional

A percepção de risco é um aspecto subjetivo que envolve não só o entendimento técnico dos riscos, mas também fatores psicossociais e culturais que influenciam a maneira como indivíduos e organizações interpretam e respondem aos riscos associados ao tratamento de dados pessoais. Autores como Ulrich Beck (1986) e Anthony Giddens (1991) destacam que a sociedade contemporânea é caracterizada pelo aumento de riscos, muitos dos quais resultam do próprio desenvolvimento tecnológico. Essa sociedade do risco é marcada por uma crescente consciência das vulnerabilidades associadas ao uso de tecnologias digitais, o que impacta diretamente a percepção pública e organizacional sobre privacidade e proteção de dados.

Shoshana Zuboff (2019) em sua obra “A Era do Capitalismo de Vigilância” explora como o poder das grandes empresas de tecnologia em controlar informações pessoais criou formas de exploração, monitoramento e vigilância, resultando em uma percepção de risco que envolve perda de autonomia e invasão de privacidade do indivíduo. Os dados pessoais passaram a ser utilizados como uma mercadoria e, por consequência, a privacidade tornou-se um bem explorado no mercado (ZUBOFF, 2019). Esse fenômeno intensifica a vulnerabilidade dos indivíduos, ao passo que diminui o controle sobre o uso das suas informações, criando um ambiente de risco contínuo.

Daniel Solove (2020) também contribui para a compreensão da percepção de risco ao desenvolver a teoria da “Arquitetura da Privacidade”. Solove argumenta que a relação de poder entre indivíduos e empresas se reflete na maneira como os dados são tratados, com as organizações geralmente exercendo maior controle sobre as informações pessoais, o que gera uma assimetria informacional e dificulta a percepção crítica sobre as práticas de privacidade.

Já Helen Nissenbaum (2004), com sua teoria da “Privacy as Contextual Integrity”, propõe que a privacidade deve ser analisada a partir do contexto em que os dados são utilizados, pois a percepção de risco está relacionada à conformidade das práticas de tratamento de dados com as normas sociais estabelecidas para cada contexto.

Assim, a percepção de risco em relação à proteção de dados é complexa e multifacetada, sendo influenciada pela confiança nas instituições, pelo histórico de vazamentos e pela transparência das práticas organizacionais. A literatura mostra que a capacidade dos indivíduos para avaliar os riscos de maneira crítica é frequentemente limitada, em parte pela complexidade dos sistemas de tratamento de dados, mas também pela falta de informações e pela assimetria de poder entre os titulares dos dados e as organizações que os coletam e tratam.

2. LEGISLAÇÃO E REGULAMENTAÇÃO: IMPACTOS DO GDPR E LGPD NA PERCEPÇÃO DE RISCOS

As regulamentações de proteção de dados, especialmente a GDPR na União Europeia e a LGPD no Brasil, são marcos legais que mudaram profundamente a forma como as organizações públicas e privadas e os indivíduos lidam com os dados pessoais. Ambas as legislações têm como objetivos principais fortalecer a proteção à privacidade e garantir que os dados pessoais sejam tratados com responsabilidade e transparência, promovendo uma conscientização maior sobre os riscos associados ao tratamento de informações pessoais. Nesta seção exploraremos a evolução e o impacto dessas regulamentações na percepção de riscos, analisando as responsabilidades impostas às organizações e o papel das autoridades de proteção de dados.

2.1. Breve histórico do GDPR e LGPD

A evolução da proteção de dados pessoais tem origem na Europa, onde o conceito de privacidade já estava presente em convenções e legislações desde o final do século

XX. A GDPR (*General Data Protection Regulation*) foi implementada oficialmente em 25 de maio de 2018 pela União Europeia, mas sua origem remonta a 1995, quando a Diretiva 95/46/CE estabeleceu as bases para a proteção de dados pessoais no contexto europeu. No entanto, com o crescimento acelerado da Internet, o surgimento de tecnologias digitais avançadas e o aumento do uso de dados pessoais por empresas e governos, tornou-se claro que a legislação de 1995 não atendia mais às demandas de proteção de dados na era digital.

Em resposta, a União Europeia começou, em 2012, um extenso processo de reforma para substituir a diretiva de 1995 por uma legislação mais robusta e abrangente. O GDPR foi aprovado em abril de 2016 e implementado em maio de 2018, com o objetivo de fortalecer o controle dos indivíduos sobre seus dados pessoais, padronizar as normas de proteção de dados entre os Estados-membros e criar um ambiente seguro para o livre fluxo de informações dentro da União Europeia. Sua aprovação representou um marco global, pois além de regular empresas e entidades europeias, a GDPR se aplica também a organizações fora da União Europeia que tratam dados de cidadãos europeus, estabelecendo um padrão internacional que influenciou a criação de leis similares ao redor do mundo.

No Brasil, a influência do GDPR foi fundamental para a criação da LGPD (Lei Geral de Proteção de Dados Pessoais), sancionada em 14 de agosto de 2018, e em vigor desde setembro de 2020. Até então, o país não contava com uma legislação ampla para a proteção de dados, embora a vida privada, a intimidade, a honra e imagem já fossem garantidas pela Constituição Federal de 1988 e reforçada pelo Marco Civil da Internet (2014). Mais recentemente, os dados pessoais passaram a ser um Direito Fundamental previsto pela Emenda Constitucional nº 115 de 2023 na Constituição Brasileira. No entanto, a ausência de uma regulação específica para dados pessoais limitava a proteção dos cidadãos brasileiros e criava incertezas para as empresas que operavam com dados pessoais sensíveis.

A LGPD surgiu como uma resposta à necessidade de modernização e alinhamento com padrões internacionais, com base no GDPR,

para assegurar os direitos dos titulares de dados e criar uma estrutura de governança de dados mais sólida. O processo de criação da LGPD envolveu consultas públicas, debates legislativos e pressão de setores da sociedade que buscavam fortalecer o controle dos cidadãos sobre suas informações pessoais e garantir a segurança e a transparência no tratamento de dados. A LGPD, assim como o GDPR, trouxe princípios e direitos fundamentais aos titulares de dados, além de criar a Autoridade Nacional de Proteção de Dados (ANPD), responsável por regulamentar e fiscalizar o cumprimento da lei no Brasil.

A implementação do GDPR e da LGPD representa uma mudança significativa na forma como dados pessoais são tratados, estabelecendo uma cultura de proteção de dados e redefinindo os direitos de privacidade em um mundo digital. Ambas as legislações refletem a crescente preocupação com o uso ético e seguro dos dados, buscando equilibrar o avanço tecnológico com a proteção dos direitos individuais.

2.2. Impactos na percepção de riscos e no comportamento das organizações

Com a introdução do GDPR e da LGPD, a percepção de riscos relacionados ao tratamento de dados pessoais se tornou um tema central tanto para as empresas quanto para os indivíduos. Anteriormente, muitas organizações encaravam a segurança de dados como um assunto técnico restrito ao setor de TI. Com a imposição de sanções severas e a responsabilidade compartilhada entre diferentes departamentos, essas regulamentações fizeram com que a proteção de dados passasse a ser uma prioridade estratégica.

Para as empresas, o GDPR e a LGPD criaram uma consciência sobre os riscos de vazamento de dados, violações de privacidade e possíveis prejuízos reputacionais e financeiros. A implementação de avaliações de impacto (*Data Protection Impact Assessments* - DPIAs) e auditorias internas e externas, identificam e mitigam os riscos associados ao tratamento de dados e contribuem no processo de conformidade das organizações. Além disso, a possibilidade de multas elevadas – que no

GDPR podem chegar a até 4% do faturamento anual global da empresa, e no Brasil, pode refletir a uma sanção de até 2% do faturamento global da empresa – mudaram o comportamento organizacional, promovendo uma cultura de proteção que reduz significativamente a vulnerabilidade a falhas de segurança e riscos cibernéticos.

Para os indivíduos, essas regulamentações contribuíram para uma maior compreensão sobre o valor e os riscos associados aos seus dados pessoais. Com o direito à transparência e à informação, os titulares passaram a ter maior controle e consciência sobre como suas informações são tratadas, o que fomenta uma visão mais crítica sobre as práticas das organizações e uma exigência maior por segurança e privacidade.

2.3. Responsabilidades legais e bases de tratamento de dados pessoais

Ambas as regulamentações estabelecem bases legais e responsabilidades claras para o tratamento de dados pessoais, impondo requisitos de transparência, segurança e responsabilidade que reduzem o risco de abusos, violações de dados pessoais e incidentes de segurança.

No contexto da GDPR, as bases legais incluem o consentimento explícito, o cumprimento de obrigações contratuais, o interesse legítimo e a execução de políticas públicas, entre outras. A LGPD adota uma abordagem similar, com dez bases legais para o tratamento de dados, que vão desde o consentimento e a execução de contratos até a proteção da vida e a garantia de um legítimo interesse.

Essas bases oferecem flexibilidade para o tratamento de dados, desde que as organizações respeitem o princípio da minimização (coletar apenas os dados necessários) e o princípio da finalidade (usar os dados apenas para os fins específicos). Além disso, ambas as leis impõem a responsabilidade de segurança e integridade dos dados, demandando que as empresas adotem medidas técnicas e administrativas adequadas para prevenir vazamentos, acessos não autorizados, manipulações indevidas e monetização de dados.

Para garantir o cumprimento, tanto o GDPR quanto a LGPD, exigem que as organizações designem um Encarregado pelo Tratamento de Dados, como já mencionado anteriormente, como o responsável por assegurar que as políticas de proteção de dados estejam alinhadas com a regulamentação vigente. O encarregado atua como um ponto de contato entre a empresa, os titulares dos dados e a autoridade responsável pela proteção de dados no país, promovendo práticas organizacionais seguras e educando os funcionários sobre a importância da privacidade no âmbito organizacional.

2.4. O papel das autoridades de proteção de dados

As autoridades de proteção de dados, como a ICO (*Information Commissioner's Office*) no Reino Unido e a ANPD (Autoridade Nacional de Proteção de Dados) no Brasil, desempenham um papel fundamental na supervisão e na aplicação do GDPR e da LGPD, respectivamente. Essas entidades têm a responsabilidade de monitorar o cumprimento das regulamentações, investigar incidentes de violação de dados e aplicar sanções por meio de processo disciplinar sancionatório, quando necessário.

A ICO, uma das autoridades de proteção de dados mais respeitadas no cenário europeu, atua de forma proativa na promoção da conformidade, orientando as empresas e os indivíduos sobre as melhores práticas e aplicando multas substanciais em casos de não conformidade. Desde a implementação do GDPR, a ICO tem se destacado pelo rigor nas fiscalizações e pela imposição de sanções significativas, que servem de exemplo para outras nações.

A ANPD, no Brasil, atua como o órgão regulador responsável por implementar a LGPD e garantir que as práticas de proteção de dados sejam adotadas de forma eficaz. Embora esteja em fase de consolidação, a ANPD tem trabalhado na promoção da conscientização e na orientação das empresas sobre as práticas adequadas, além de estabelecer diretrizes para a aplicação de sanções. O papel da ANPD é crucial para a construção de uma cultura de privacidade e proteção de

dados no Brasil, e sua atuação será determinante para o fortalecimento das práticas de segurança e para a conscientização das organizações e da população.

3. PERCEPÇÃO DE RISCOS POR EMPRESAS E ORGANIZAÇÕES

A percepção de riscos relacionados à proteção de dados tem se tornado central para empresas e instituições públicas devido ao aumento da aplicação da regulamentação, aumento crescente de ataques cibernéticos, golpes por técnicas de Engenharia Social e das percepções e expectativas dos consumidores por ações de segurança e garantia de privacidade.

Grandes corporações e pequenas empresas possuem abordagens distintas, em razão das diferenças em capacidade de investimento e complexidade organizacional. Esta seção explora como diferentes tipos de empresas percebem e gerenciam os riscos de dados, analisando setores com exposição elevada, como Tecnologia da Informação (TI), financeiro e saúde, além de boas práticas de segurança e conformidade, casos práticos de violações e o uso de tecnologias de mitigação.

3.1. Diferenças na percepção de riscos entre grandes corporações e pequenas empresas

A percepção de riscos entre grandes corporações e pequenas empresas no contexto de proteção de dados pessoais e privacidade apresenta diferenças significativas, especialmente em termos de recursos, prioridades e entendimento das consequências regulatórias e reputacionais.

Grandes corporações geralmente possuem recursos mais robustos, incluindo equipes dedicadas exclusivamente à segurança da informação e ao cumprimento regulatório, como um encarregado de proteção de dados e departamentos jurídicos especializados.

Além de possuírem maior conhecimento dos impactos regulatórios devido à sua exposição e ao risco elevado de sanções, seja pela LGPD no Brasil, seja pelo GDPR na Europa. O descumprimento da legislação pode levar a multas consideráveis e impacto na reputação institucional, o que torna a adequação à lei uma prioridade.

Empresas de médio e grande portes têm uma reputação consolidada a proteger e estão sujeitas a um escrutínio público e de mídia muito mais intenso, o que as leva a adotar medidas proativas e, por vezes, preventivas de proteção de dados. Além disso as grandes corporações tendem a considerar o risco de incidentes de dados como uma questão estratégica e operacional de longo prazo.

Para grandes corporações, como as *Big Techs* (Google, Meta, Amazon), a percepção de risco em relação à proteção de dados envolve uma gama complexa de preocupações legais, financeiras e reputacionais. Estas empresas lidam com vastas quantidades de dados pessoais em escala global, enfrentando pressões para implementar robustas políticas de governança de dados e investir em tecnologias avançadas de segurança. A complexidade do risco aumenta devido à visibilidade pública e ao volume de dados processados, expondo essas empresas a repercussões mais significativas em caso de falhas de conformidade ou violações de dados, como também, medidas legais mais severas e impugnantes.

Em contraste, pequenas e médias empresas (PMEs) muitas vezes enfrentam dificuldades para implementar práticas de proteção de dados no mesmo nível das grandes corporações, devido a recursos limitados para investir em tecnologias avançadas e na contratação de especialistas em segurança e privacidade. Enfrentam também desafios financeiros e operacionais para implementar mecanismos de proteção de dados, o que leva a uma menor percepção de risco, muitas vezes por falta de conhecimento técnico ou financeiro para investir em medidas de proteção eficazes. Pequenas empresas, ao contrário das grandes corporações, frequentemente não percebem o risco regulatório de forma tão intensa. Isso se dá tanto pela ausência de fiscalização constante quanto pela falsa impressão de que a legislação aplicável só abrange organizações de maior porte.

Já as pequenas empresas, com menor visibilidade, tendem a priorizar a mitigação de riscos diretos e imediatos e podem não entender o impacto que uma falha de segurança e violação de dados pode ter em sua reputação, que, embora menor em alcance, pode ser devastador para a continuidade do negócio. O risco econômico imediato tende a dominar as decisões, o que pode resultar em menos prioridade para a proteção de dados, especialmente em um cenário de recursos limitados.

Isso não significa, entretanto, que a percepção de risco seja negligenciada. Para muitas PMEs, a proteção de dados é vista como um diferencial competitivo, capaz de aumentar a confiança e credibilidade dos clientes e garantir conformidade com a LGPD e, quando necessário, ao GDPR. A gestão do risco tende a priorizar medidas mais acessíveis, como treinamentos de conscientização e o uso de soluções terceirizadas de segurança da informação, que se concentram na proteção básica dos dados. Daí a importância de garantir a educação continuada de funcionários e colaboradores para o estabelecimento da conduta adequada e em consonância com a legislação vigente.

Essas diferenças ressaltam a necessidade de abordagens específicas de conscientização e regulação para pequenas e médias empresas, permitindo um nível básico de conformidade e proteção, ao mesmo tempo em que alivia os custos que poderiam inviabilizar pequenos negócios.

3.2. Riscos percebidos em setores de TI, financeiro e saúde

A percepção de risco e as estratégias de proteção de dados variam significativamente entre setores, com alguns segmentos enfrentando riscos e exigências mais elevadas devido ao tipo e ao volume de dados sensíveis processados.

Sabemos que empresas do setor de TI processam grandes volumes de dados pessoais e comerciais, e lidam constantemente com riscos relacionados a ataques cibernéticos, vazamentos de dados e falhas de segurança. A percepção de risco neste setor é fortemente marcada

pela necessidade de proteção contra invasões e pelo cumprimento de normas de privacidade. As empresas de TI frequentemente adotam políticas de segurança de dados rígidas, com destaque para práticas como o monitoramento de redes, a criptografia de dados e a realização de testes de invasão para identificar vulnerabilidades.

Instituições financeiras, como bancos e *fintechs*, lidam com informações altamente sensíveis, como dados bancários e de crédito. Para este setor, a percepção de risco é influenciada pela possibilidade de fraudes, perda de dados e ataques de *ransomware* e de *phishing*, que representam prejuízos significativos tanto para os clientes quanto para a instituição. Como resposta, as instituições financeiras implementam medidas robustas de segurança, incluindo criptografia, autenticação multifatorial e detecção de anomalias para prevenir transações fraudulentas. Além disso, regulamentações específicas, como o PCI-DSS (*Payment Card Industry Data Security Standard*), reforçam a necessidade de segurança e conformidade legal.

No setor de saúde, a privacidade e a proteção dos dados dos pacientes são fundamentais. Vazamentos de dados podem expor informações médicas confidenciais, o que representa um risco elevado para a privacidade dos pacientes e pode resultar em penalidades rigorosas. A percepção de risco neste setor se traduz em práticas rigorosas, protocolos consistentes, como o uso de sistemas de registros eletrônicos de saúde (EHR) seguros, garantindo integridade, autenticidade e controles de acesso baseados em função e criptografia de dados. No Brasil, as diretrizes da LGPD e normas específicas para o setor, como a Resolução RDC 36/2013 da Agência Nacional de Vigilância Sanitária (Anvisa), promovem uma abordagem cautelosa, reforçando a importância da segurança dos dados sensíveis.

3.3. Boas práticas de segurança e conformidade

Para gerenciar os riscos de proteção de dados, organizações públicas e privadas independentes do porte, estão gradativamente, buscando adotar boas práticas de segurança e conformidade legal que vão

além das exigências regulamentares. A implementação de políticas de governança de dados é uma prática essencial que estabelece diretrizes claras para o tratamento e a segurança das informações. Essas políticas incluem a definição de papéis e responsabilidades, a realização de auditorias (internas e externas) e a documentação dos procedimentos de segurança são medidas eficazes. Treinamentos de conscientização para funcionários e colaboradores também são fundamentais, pois minimizam os riscos relacionados ao fator humano, educando a equipe sobre boas práticas e a importância da proteção de dados.

Outra prática recomendada é o uso de avaliações de impacto à proteção de dados (DPIAs), que permite às organizações anteciparem e mitigarem riscos associados ao tratamento de dados pessoais, especialmente em novos projetos ou em alterações significativas nas operações de dados. As avaliações ajudam a identificar pontos vulneráveis e implementar as medidas adequadas para garantir a conformidade com regulamentos como a LGPD e o GDPR.

3.4. Relatos de casos práticos: violações de dados e suas repercussões

A crescente preocupação com a proteção de dados foi impulsionada por grandes violações de dados em empresas renomadas, que evidenciaram a importância de práticas adequadas de segurança e conformidade legal.

Em 2018, o caso do vazamento de dados do *Facebook - Cambridge Analytica* trouxe grande repercussão ao demonstrar como o uso inadequado de dados de usuários poderia impactar não apenas a privacidade, mas também a confiança pública. Este incidente resultou em uma multa de mais de 5 bilhões de dólares para a empresa, imposta pela *Federal Trade Commission* (FTC) dos Estados Unidos, ocasionando na falência da empresa e reforçou a necessidade de políticas de proteção de dados rigorosas.

Outro caso marcante ocorreu em 2017, quando a Equifax, uma das maiores empresas de crédito dos Estados Unidos, sofreu uma

violação de dados que expôs informações financeiras de cerca de 147 milhões de pessoas. Este incidente foi agravado pela falta de medidas preventivas adequadas e gerou uma multa de 700 milhões de dólares, além de impactos profundos na reputação da empresa.

No Brasil, o megavazamento de dados do Sistema Único de Saúde (SUS) em 2019 foi um caso de grande repercussão. O vazamento ocorreu em abril de 2019, quando um banco de dados com informações pessoais de 2,4 milhões de usuários do SUS foi exposto na internet. Os dados vazados incluíam nomes, endereços, números de CPF, nome da mãe e data de nascimento. O vazamento foi resultado de um ataque *hacker* que criou um algoritmo que permitia o *download* dos dados pessoais dos usuários

Esses casos servem de alerta para a importância de uma abordagem proativa em segurança de dados e inspiraram a adoção de melhores práticas, mesmo em empresas menores, que passaram a enxergar a proteção de dados como uma medida essencial para evitar prejuízos financeiros e danos à confiança do consumidor.

3.5. Adoção de tecnologias de mitigação

Para mitigar os riscos de violações, muitas empresas têm investido em tecnologias de segurança da informação, que auxiliam na proteção e no controle do acesso aos dados pessoais. Entre as tecnologias mais comuns estão:

(i) Criptografia: Amplamente adotada em setores como financeiro, saúde e nos últimos anos por instituições públicas. A criptografia protege os dados transformando-os em códigos ilegíveis para acessos não autorizados. Esta tecnologia é essencial para prevenir vazamentos em caso de acessos indevidos ou ciberataques, garantindo que os dados permaneçam protegidos.

(ii) *Data Loss Prevention* (DLP): Ferramentas de DLP são implementadas para monitorar e proteger dados sensíveis, identificando e bloqueando o compartilhamento não autori-

zado de informações. Esta tecnologia é especialmente útil para evitar a perda de dados acidental ou intencional por funcionários.

(iii) Autenticação Multifatorial (MFA): O uso de MFA reduz significativamente o risco de acessos não autorizados ao exigir múltiplos fatores de autenticação antes de conceder o acesso. Esse método é eficaz em setores onde a segurança é primordial, como o financeiro e o de TI.

(iv) Soluções de *Backup* e Recuperação de Dados: Para mitigar o impacto de ataques de *ransomware* e outros incidentes que possam causar perda de dados, as empresas também adotam soluções de *backup* e recuperação. Esses sistemas garantem que os dados possam ser restaurados rapidamente, minimizando o impacto de possíveis interrupções.

Para mitigar esses riscos, é essencial adotar estratégias robustas de gestão, que combinem políticas claras de segurança da informação, programas de compliance e auditorias regulares para identificar e corrigir fragilidades. Implementar treinamentos contínuos e atualizados para os colaboradores é fundamental para reduzir a vulnerabilidade a ataques baseados em engenharia social e melhorar a resposta a incidentes.

Além disso, o investimento em tecnologias avançadas, como inteligência artificial para monitoramento proativo, *blockchain* para assegurar a integridade dos dados e criptografia de ponta para proteger informações sensíveis, potencializa a capacidade de defesa das organizações contra ameaças digitais.

Contudo, a tecnologia, por si só, não é suficiente sem o suporte de uma cultura organizacional sólida voltada à percepção e gestão de riscos. Uma cultura de segurança promove a conscientização de todos os níveis hierárquicos sobre a importância da proteção de dados e fomenta comportamentos que minimizam vulnerabilidades.

Líderes organizacionais desempenham um papel crucial, demonstrando compromisso com a segurança e incentivando práticas responsáveis, desde a adoção de senhas fortes até a adesão irrestrita às po-

líticas de privacidade. Assim, a combinação de tecnologias avançadas, estratégias bem delineadas e uma cultura organizacional madura forma o tripé indispensável para uma gestão eficaz de riscos em proteção de dados.

4. A PERCEPÇÃO DOS INDIVÍDUOS SOBRE OS RISCOS À PRIVACIDADE E PROTEÇÃO DE DADOS

Na era digital, os indivíduos estão cada vez mais conscientes dos riscos associados à exposição de seus dados pessoais, especialmente em plataformas online e aplicativos. Com o crescimento das regulamentações de privacidade, como o GDPR e a LGPD, a proteção de dados ganhou mais visibilidade e importância, alterando a percepção pública e os comportamentos em relação ao compartilhamento de informações pessoais.

Este capítulo explora a visão dos cidadãos sobre a privacidade, discutindo pesquisas sobre a conscientização pública, o modo como os indivíduos veem o compartilhamento de dados, fatores que influenciam a confiança no tratamento de dados e exemplos de como a percepção de riscos impacta o comportamento do consumidor.

4.1. Conscientização pública sobre privacidade e dados

Pesquisas realizadas por órgãos internacionais e instituições acadêmicas apontam que, embora os indivíduos estejam cada vez mais conscientes da importância da privacidade, muitos ainda possuem uma compreensão limitada sobre como suas informações pessoais são tratadas e protegidas.

Um estudo realizado pela *Pew Research Center* em 2019, por exemplo, revelou que 79% dos adultos norte-americanos afirmam estar preocupados com a forma como empresas e governos utilizam seus dados. No Brasil, uma pesquisa da *Data Privacy Brasil* indicou que 65% dos brasileiros acreditam que a privacidade é um direito essencial, mas

muitos admitem que não entendem plenamente os mecanismos de proteção e as práticas de uso de dados adotadas pelas empresas.

Esses dados refletem um paradoxo comum na percepção dos indivíduos: enquanto há um crescente interesse por privacidade e proteção de dados, existe também uma lacuna de conhecimento técnico sobre como essas informações são armazenadas, processadas e utilizadas. Isso faz com que muitos usuários estejam conscientes dos riscos, mas não saibam exatamente como minimizar essas exposições ou interpretar políticas de privacidade. A conscientização pública, então, é fragmentada e, em geral, superficial, com um entendimento básico dos riscos, mas sem uma compreensão detalhada dos direitos e dos mecanismos de proteção.

4.2. Percepção dos riscos ao compartilhar dados em plataformas digitais

A crescente dependência de plataformas digitais para atividades cotidianas – desde o uso de redes sociais até serviços de *streaming* e compras *online* – trouxe um novo nível de exposição dos dados pessoais. Muitos indivíduos percebem o ato de compartilhar informações nessas plataformas como um risco inevitável, o que gera uma relação ambígua: por um lado, os indivíduos reconhecem a conveniência e as vantagens dos serviços digitais, mas, por outro, sentem-se vulneráveis ao disponibilizar informações pessoais e sensíveis.

Um dos aspectos mais preocupantes para os usuários é a falta de controle sobre quem pode acessar seus dados e de que forma eles são utilizados. Esse sentimento é particularmente forte em plataformas de redes sociais, onde as informações publicadas podem ser utilizadas para fins publicitários e de monitoramento. No contexto de grandes vazamentos de dados, como o caso do *Facebook-Cambridge Analytica*, a percepção de riscos se intensifica, pois evidencia como dados aparentemente inofensivos, como curtidas e preferências, podem ser usados para manipulação comportamental e política. O uso indiscriminado de dados para direcionamento de anúncios e para análises preditivas tor-

na-se uma fonte de preocupação, com muitos indivíduos temendo que suas informações sejam exploradas para fins que desconhecem.

A pesquisa sobre a percepção pública revela que muitos indivíduos sentem que perderam o controle sobre sua privacidade no ambiente digital, o que gera desconfiança e resistência ao compartilhamento de informações, especialmente entre usuários mais conscientes sobre o impacto dos dados em seus perfis comportamentais.

4.3. Fatores que influenciam a confiança do usuário em relação à proteção de seus dados

A confiança dos usuários em relação à proteção de seus dados é influenciada por uma série de fatores, incluindo a transparência das empresas, o histórico de vazamentos e a regulamentação que se coloca como complexa aos mesmos.

Empresas que adotam políticas de privacidade claras, que comunicam de forma compreensível como os dados serão usados e que permitem maior controle sobre as informações, tendem a gerar mais confiança entre os usuários.

Outro fator crucial é o histórico de incidentes de segurança. Casos de violações de dados têm um impacto significativo na confiança dos consumidores, que passam a considerar a segurança da empresa como um dos critérios para continuar ou não utilizando determinado serviço. Por exemplo, após o vazamento de dados da Equifax em 2017, a percepção dos consumidores em relação à segurança de dados na empresa despencou, afetando não só a sua reputação, mas também a fidelidade dos clientes.

A regulamentação também desempenha um papel importante na confiança dos consumidores, especialmente após a implementação de leis como o GDPR e a LGPD. Essas regulamentações impõem normas rigorosas para o tratamento de dados, o que oferece aos usuários uma segurança maior quanto ao controle e à proteção de suas informações pessoais. Pesquisas indicam que a simples existência de uma

regulamentação fortalece a confiança dos consumidores, pois cria uma rede de proteção e um meio de responsabilização das empresas.

4.4. A percepção de riscos mudando o comportamento do titular de dados

A percepção dos riscos de privacidade e proteção de dados tem um efeito direto sobre o comportamento do titular de dados, que se torna mais seletivo e cauteloso ao compartilhar informações. Muitos usuários, por exemplo, evitam fornecer dados excessivos em cadastros, preferem logins anônimos ou temporários em aplicativos e até desinstalam programas que consideram invasivos.

Um estudo conduzido pela Cisco em 2020, revelou que, 32% dos titulares de dados desinstalaram aplicativos por preocupações com a privacidade e 44% afirmam que não usam produtos ou serviços que exijam compartilhamento excessivo de dados pessoais.

A pesquisa indica que, quando a percepção de riscos é alta, os consumidores estão dispostos a abdicarem a praticidade, conveniência e funcionalidades para preservar sua privacidade.

Outro comportamento comum é a adesão a medidas de proteção como o uso de ferramentas de navegação privada, aplicativos de bloqueio de rastreamento e de segurança digital. Esses titulares, ao perceberem os riscos inerentes ao compartilhamento de dados, adotam soluções que limitam a exposição de suas informações. Isso é especialmente visível entre usuários mais jovens, que apesar de estarem fortemente presentes em plataformas digitais, demonstram uma preocupação crescente com a proteção de seus dados e têm se mostrado mais criteriosos no uso de redes sociais.

Em suma, a percepção de riscos faz com que os titulares de dados estejam cada vez mais dispostos a exigir transparência, a escolher com cautela as plataformas que utilizam e a evitar serviços que considerem excessivamente invasivos. A conscientização sobre a privacidade dos dados, ainda que incompleta, tem sido um fator importante para

que os indivíduos tomem decisões mais informadas e para que empresas se adaptem a novas demandas de segurança e transparência.

5. CONCLUSÃO

A crescente digitalização e a evolução das tecnologias disruptivas têm transformado profundamente o ambiente corporativo, os modelos de negócios e o cotidiano das pessoas. Soluções como a Web 3.0, o *blockchain* e a inteligência artificial trazem promessas de maior controle, privacidade e eficiência, redesenhando a forma como interagimos com o mundo digital e físico.

No entanto, junto com essas oportunidades, surgem desafios significativos para a proteção de dados, com a expansão de ameaças como ataques cibernéticos, vazamentos de informações e vulnerabilidades humanas. Essas ameaças reforçam a percepção de risco, tanto para indivíduos quanto para organizações, que precisam lidar com a responsabilidade de proteger dados pessoais e sensíveis e preservar a confiança em suas operações.

Nesse cenário, a adoção de tecnologias avançadas, como IA e dispositivos IoT integrados por meio da conectividade 5G, abre portas para a criação de ecossistemas mais inteligentes e interconectados, capazes de automatizar processos e impulsionar a inovação. Entretanto, a maior conectividade e complexidade tecnológica aumentam o potencial de exploração de vulnerabilidades, exigindo que organizações e indivíduos direcionem esforços para a conformidade com legislações como o GDPR (Regulamento Geral de Proteção de Dados) e a LGPD (Lei Geral de Proteção de Dados Pessoais). Essas regulamentações estabelecem diretrizes claras sobre a coleta, armazenamento e uso de dados pessoais, sendo fundamentais para mitigar riscos e garantir a segurança em um ambiente digital em constante transformação.

A definição e a classificação de riscos são fundamentais para a proteção de dados, permitindo que as organizações previnam e mitiguem incidentes de segurança. Regulamentações como o GDPR e a

LGPD destacam a importância de identificar e gerenciar esses riscos, exigindo medidas que garantam a segurança e a integridade dos dados pessoais.

Ferramentas como a *Data Protection Impact Assessment* (DPIA) desempenham um papel crucial na gestão de riscos, avaliando impactos potenciais e orientando a implementação de controles antes do início de novos projetos ou tratamentos de dados sensíveis. A gestão de riscos, integrada à política de segurança da informação e às normas legais, deve ser documentada e justificada, priorizando recursos para as áreas mais vulneráveis e assegurando que as decisões tomadas sejam baseadas em evidências sólidas e critérios alinhados aos objetivos estratégicos da organização.

Embora a avaliação de riscos dificilmente cubra todos os fatores envolvidos, é papel do controlador identificar os mais relevantes, estimando sua probabilidade e impacto. Esses impactos devem considerar os danos potenciais aos titulares, especialmente no que diz respeito a seus direitos e liberdades. Assim, uma gestão de riscos bem estruturada é essencial para garantir conformidade, proteger dados pessoais e fortalecer a confiança nos processos organizacionais.

Para isso, a adoção de políticas robustas, projeto de conformidade à LGPD efetivo, investimento em tecnologias de segurança, treinamentos contínuos e a construção de uma cultura organizacional voltada à proteção de dados são fundamentais. Indivíduos e organizações poderão navegar de forma segura no cenário digital, aproveitando as oportunidades da transformação tecnológica enquanto atendem às exigências regulatórias e preservam a confiança e os direitos dos titulares.

REFERÊNCIAS

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CERT.br. **Cartilha de Segurança para Internet.** São Paulo: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, 2024. Disponível em: <https://cartilha.cert.br>. Acesso em: 18 nov. 2024.

CERT.br. **Cartilha de Segurança para Internet**. São Paulo: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, 2024. Disponível em: <https://cartilha.cert.br>. Acesso em: 18 nov. 2024.

GDPR – General Data Protection Regulation. **Regulation (EU) 2016/679 of the European Parliament and of the Council**. Official Journal of the European Union, 27 abr. 2016.

NISSENBAUM, Helen. **Privacy as Contextual Integrity**. Washington Law Review, v. 79, p. 119-158, 2004.

SOLOVE, Daniel J. **The FTC Zoom Case: Does the FTC Need a New Approach?** LinkedIn, 2020. Disponível em: <https://www.linkedin.com/pulse/ftc-zoom-case-does-need-new-approach-daniel-j-solove/>. Acesso em: 18 nov. 2024.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890.

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

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019.

PRINCÍPIOS-BASE DA LGPD: REFLEXOS CONSTITUCIONAIS NA SOCIEDADE DIGITAL

Adriana da Costa Fernandes¹

INTRODUÇÃO

A dicotomia entre os limites do Direito Público e do Direito Privado, um dos conhecidos debates jurídicos atuais, vem sofrendo mutação em face de um importante fenômeno convergente. O Direito Privado vem se publicizando, da mesma forma que o Direito Público tem se privatizado. Isto ocorre em razão da crescente centralidade do Direito Constitucional Contemporâneo, sob uma ótica matricial e da defesa precípua dos Direitos e Garantias Fundamentais. Da mesma forma, em face de um crescente debate sobre o que supostamente consistirá, em efetivo, um Direito Constitucional Global, suas competências e abrangências.

Nesse contexto, no Brasil, desde a promulgação da Constituição Federal de 1988, o Direito Civil, entre outras áreas, tem passado por profundas e aceleradas transformações conceituais para melhor refletir os princípios e diretrizes constitucionais. Considere-se, até mesmo, o que ensina o Jurista Gustavo Tepedino em sua obra Fundamentos de Direito Civil, no tomo de Responsabilidade Civil², na apresentação do Volume 4:

“Responsabilidade Civil é dos temas mais suscetíveis aos influxos das mudanças sociais. (...) O desenvol-

1 Advogada experiente em Direito Público e em Direito Privado. Pesquisadora de importantes grupos: UFPE, CEUB, IDP e UNB. Mestranda em Constitucional, Pós-graduada em Civil, com MBA em marketing e diversas especializações.

2 TEPEDINO, Gustavo. TERRA, Aline de Miranda Valverde. GUEDES, Gisela Sampaio da Cruz. Fundamentos de Direito Civil: Volume 4, Responsabilidade Civil. 2ª. Edição Revisada e Ampliada. Editora Forense / GEN – Grupo Editorial Nacional. 2020. Rio de Janeiro – RJ.

vimento de novas tecnologias e de modelos de negócios inovadores, o estabelecimento de diferentes práticas sociais e formas de relacionamento humano provocam, não raro, danos injustos à esfera jurídica de diversos sujeitos, a requerer resposta rápida e eficaz tanto do Poder Judiciário, inexorável porta de entrada dos conflitos interpessoais, como do Poder Legislativo, chamado a disciplinar, e quiçá prevenir, referidas contendas. Por essa razão, torna-se imprescindível revisitar, constantemente, os institutos e categorias da Responsabilidade Civil, relendo seus tradicionais elementos à luz de perspectiva renovada, comprometida com sua ontológica função, consistente no integral ressarcimento da vítima.”

Na abordagem de Tepedino está claramente indicado como os influxos e práticas sociais interferem na esfera dos relacionamentos humanos, o que, não raro, exigem a criação e a aplicabilidade de novas e eficazes regras, em especial, em tempos de forte e ágil transformação como atualmente.

Em resposta aos anseios da sociedade da informação e à necessidade de resguardo de alguns de seus direitos, quando os *dados* são considerados o novo elemento essencial da vida e dos negócios, e com a mesma relevância passada do petróleo, nasceu, no Brasil, a Lei Geral de Proteção de Dados – LGPD, a Lei Federal 13.709, de 14 de agosto de 2018.

Após complexa tramitação legislativa, a LGPD foi alterada pela Lei Federal 13.853, de 8 de julho de 2019 e pela Medida Provisória 959, de abril de 2020, passando a vigorar integralmente apenas em 3 de maio de 2021, introduzindo conceitos inovadores ao ordenamento jurídico nacional e criando a Autoridade Nacional de Proteção de Dados – ANPD.

A LGPD brasileira adotou uma formatação mais ampla do que o previsto no *General Data Protection Regulation* – GDPR europeu. E mesmo que a opção tenha sido pela adoção de regulamentações específicas posteriores à sua promulgação, a serem editadas pela ANPD, essa abordagem possibilitou uma adaptação mais dinâmica às necessidades do mercado e da sociedade, garantindo que a proteção dos direitos dos

titulares acompanhe o ritmo da evolução tecnológica e dos desafios da economia digital.

Ainda que, contrariamente a outros Estados Constitucionais³ e até em face do fenômeno convergente anteriormente mencionado, fruto da já citada crescente constitucionalização do Direito nacional, a LGPD chegou procurando proteger, da mesma forma, em essência, os Direitos Fundamentais.

A proteção de dados pessoais adquiriu efetivo *status* constitucional nacionalmente por força da Emenda - EC 115, de 10 de fevereiro de 2022, que inseriu o tema entre os tutelados Direitos e Garantias Fundamentais, por meio do inciso LXXIX⁴, do art. 5º da Carta Magna. Da mesma forma que, por meio da alteração do caput dos arts. 21 e 22 da

3 SARLET, Ingo Wolfgang. Proteção de Dados Pessoais Como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo Para a Construção de Uma Dogmática Constitucionalmente Adequada. Revista Direito Fundamentais à Justiça. Páginas 179 – 218 Belo Horizonte. Ano 14. Nº 42. Jan/Jun 2020. (...) “Neste sentido, note-se que mesmo já no limiar da terceira década do século XXI, ainda existem Estados constitucionais nos quais um direito fundamental à proteção de dados não é reconhecido, pelo menos na condição de direito expressamente positivado na Constituição, muito embora tal direito seja, em vários casos, tido como implicitamente positivado, sem prejuízo de uma mais ou menos ampla regulação legislativa e administrativa, ademais de significativo desenvolvimento na esfera jurisprudencial.” (...) “No nível do direito internacional público, tanto no âmbito do sistema universal de proteção da ONU, quanto na esfera do direito europeu, um direito à proteção de dados tem sido deduzido em especial no direito à privacidade, embora com este não se confunda. Nesse sentido, a orientação adotada pela Comissão da ONU para Direitos Humanos, interceptando o alcance do art. 17 do Pacto Internacional de Direitos Civis e Políticos, assim a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE), forte no art. 8º da Convenção Europeia. Foi somente na Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (1981), comumente intitulada de Convenção de Estrasburgo, bem como, quase vinte anos mais tarde, no art. 8º da Carta de Direitos Fundamentais da União Europeia (doravante CD-FUE), do ano 2000 que o direito à proteção de dados finalmente alçou à condição de direito fundamental de natureza autônoma, mas vinculando, como tal, apenas os estados integrantes da União Europeia, o que se deu apenas com a entrada em vigor do Tratado de Lisboa, em 2009.”

4 CONSTITUIÇÃO FEDERAL BRASILEIRA. 1988. www.planalto.gov.br Acessado em 01/12/2024 às 22h05min. “Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).”

CARTA MAGNA 1988, restou estabelecida a competência privativa da União para legislar sobre a matéria, tendo sido assegurado, nos termos da Lei, o direito à proteção, inclusive em meios digitais.

É premente lembrar, em se destacando o mencionado momento digital atual e a liberdade dos seres, acerca da premente e fundamental pulverização da internet em todo o território nacional com cada vez mais ampla conectividade. Uma meta definida e uma garantia basililar pela qual se luta fortemente, embora, para muitos, ainda represente um sonho distante, por múltiplas razões estruturais e sociais.

A árdua escalada da vida contemporânea, a crescente digitalização das atividades e os *dados*, em intenso crescimento exponencial, desafiam a todos. Impondo aos operadores do Direito, às instituições, aos Poderes da República e, em especial, à ANPD, a constante avaliação das previsões e dos limites iniciais da LGPD. Isto, com vistas, até mesmo, a estabelecer, ou não, uma regulamentação mais intensiva, definindo em quais pontos em efetivo maior intervenção possa vir a ser necessária. Esse cenário deve ser entendido não apenas em relação a situações específicas já conhecidas, mas, ainda, diante de novas condutas que emergem e dos impactos identificados, seja em negócios tradicionais, seja em outros absolutamente inovadores.

Do que se compreende, ainda, é que a legislação não há de ser rígida, mas, em verdade, acompanhar seu contexto de aplicação, refletindo as transformações sociais e tecnológicas em evolução. Nesta linha, inclusive nos de e considerando-se a defesa pela constante observação do ordenamento e de sua eventual readequação, tanto por via legislativa originária, quanto judicialmente, no escopo de casos concretos, foi finalizado recentemente, no âmbito do Supremo Tribunal Federal – STF⁵, relevante julgamento acerca, especialmente, da aplicabilidade atualizada, mais específica e eficaz, do disposto nos arts. 19 e 21 do Marco Civil da Internet, a Lei Federal 12.965, de 23 de abril de 2014, precursora da proteção de dados em ambiente digital e a responsabili-

5 SUPREMO TRIBUNAL FEDERAL – STF. www.portal.stf.jus.br Acessado em 05/07/2025. 20h. RE 1.037.396, de Relatoria do Ministro Dias Toffoli e o RE 1.057.258 de Relatoria do Ministro Luiz Fux.

dade de Plataformas Digitais na divulgação de conteúdo de terceiros. Tratou-se, em realidade, do julgamento de 2 (dois) temas de Repercussão Geral, um de Relatoria do Ministro Luiz Fux (Tema 533 – sobre hospedagem de site e responsabilidades vinculadas) e outro de Relatoria do Ministro Dias Toffoli (Tema 987 – sobre a constitucionalidade dos artigos do marco civil), em sendo abordada a chamada objetivação do controle de constitucionalidade. Foi considerado, em primeiro aspecto, do conceito de (em inglês) “*notice and takedown*”, procedimento já adotado na Europa e nos Estados Unidos da América, e em segundo, dos limites da Responsabilidade Civil destas Plataformas Digitais, dos dados por elas veiculados e dos contornos desta veiculação.

De forma resumida, portanto, o STF definiu que: (i) no caso de crimes contra a honra segue mantida a regra originalmente prevista no art. 19 do Marco Civil da Internet, a não ser em caso de entendida replicação (já ocorrido julgamento anterior sobre o assunto); (ii) no caso de conteúdos impulsionados (por robôs e cia.), restou definida a responsabilização do provedor a fim de demonstrar que atuou preventivamente para evitar a consumação da lesão questionada; (iii) quanto a conteúdos de circulação massiva, considerados crimes gravíssimos, em rol taxativo, como os envolvendo atos democráticos, terrorismo, incitação ao suicídio, discurso de ódio, racial, religioso, crimes contra mulheres, pornografia infantil, crimes sexuais contra vulneráveis e tráfico de pessoas, quando a plataforma tem o dever imediato de remover o conteúdo considerado ilícito e mesmo sem ordem judicial; (iv) provedores de serviços de e-mail, de aplicações cuja finalidade primordial seja a realização de reuniões fechadas por vídeo ou voz, de serviços de mensageria instantânea (também chamadas de provedores de serviços de mensageria privada), exclusivamente no que diz respeito às comunicações interpessoais, foram resguardadas pelo sigilo das comunicações (art. 5º, inciso XII, da CARTA MAGNA 1988) e, enfim, (v) nos casos afetos a Marketplaces seguem respondendo civilmente com base no Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro 1990. Merece, por fim, destaque, que a matéria eleitoral ficou excluída do julgado, ressalvadas disposições específicas da legislação eleitoral e

os atos normativos expedidos pelo TSE, bem como tendo sido apresentado o pleito, do STF ao Legislativo, para que venha a ser promulgada lei específica apta a sanar quaisquer supostas deficiências do atual regime quanto a Direitos Fundamentais, considerando a inconstitucionalidade progressiva do art. 19 em razão de sua necessária adaptação ao tempo.

1. DESENVOLVIMENTO

1.1. Princípios fundamentais constitucionais e sua influência na LGPD

Ainda que a Constituição Federal Brasileira de 1988 tenha adotado um sistema constitucional analítico, o qual aborda amplamente diversas matérias e que, assim, acabe por ocasionar algum grau de conflito e questionamento acerca da constitucionalidade e da aplicação da legislação infraconstitucional, sua ótica inquestionavelmente humanista e paritária define, em seu Preâmbulo, os valores supremos e democráticos nacionais que devem nortear o agir:

“Nós, representantes do povo brasileiro, reunidos em Assembleia Nacional Constituinte para instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.”

Desde o nascedouro, portanto, da CARTA MAGNA 1988, ressaltou chancelada a premissa legal de necessário respeito aos corolários Princípios da liberdade, segurança, bem-estar, desenvolvimento, igualdade e justiça, em todo o território nacional, a serem espalhados por todo o ordenamento pátrio, sob pena da configuração de dada inconstitucionalidade.

Em aderência, o art. 1º da CARTA MAGNA 1988 consigna os Fundamentos da Nação: (I) a soberania; (II) a cidadania; (III) a dignidade da pessoa humana; (IV) os valores sociais do trabalho e da livre iniciativa (sobre isto, inclusive, vide a Lei nº 13.874, de 20 de setembro de 2019, a saber, a Declaração de Direitos de Liberdade Econômica); e (V) o pluralismo político.

Conforme inserção, da mesma forma, em diversos outros dispositivos, é perceptível a constante preocupação constitucional com os Direitos e Garantias Individuais e Coletivos previstos nos arts. 3º, 4º e 5º da CARTA MAGNA 1988.

Inicialmente, no art. 3º da CARTA MAGNA 1988 foram traçados os Objetivos Fundamentais da República e no art. 4º restaram dispostos os princípios que regem as Relações Internacionais. Estes, inclusive, aptos a orientar tratativas de convencionalidade face outros regulamentos paritários como o próprio GDPR europeu, vigente desde 25 de maio de 2018 e, ainda, o *California Consumer Privacy Act* – CCPA norte-americano, aprovado em 28 de junho de 2018 (AB 375).

Diante dos princípios basilares constitucionalmente definidos e como não poderia ser diferente, seja por força normativa atribuída ou pelo conceito de supremacia da Carta da República, a LGPD traz refletido em si, de plano, em seu art. 1º, caput, o objetivo de proteção aos Direitos Fundamentais de liberdade, de privacidade e do livre desenvolvimento da pessoa natural.

6 CONSTITUIÇÃO FEDERAL BRASILEIRA. 1988. www.planalto.gov.br Acessado em 01/12/2024 às 22h05min. “Art. 3º - Constituem objetivos fundamentais da República Federativa do Brasil: (I) construir uma sociedade livre, justa e solidária; (II) garantir o desenvolvimento nacional; (III) erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; (IV) promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.”

7 CONSTITUIÇÃO FEDERAL BRASILEIRA. 1988. www.planalto.gov.br Acessado em 01/12/2024 às 22h05min. “Art. 4º - A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: (I) independência nacional; (II) prevalência dos direitos humanos; (III) autodeterminação dos povos; (IV) não-intervenção; (V) igualdade entre os Estados; (VI) defesa da paz; (VII) solução pacífica dos conflitos; (VIII) repúdio ao terrorismo e ao racismo; (IX) cooperação entre os povos para o progresso da humanidade; (X) concessão de asilo político. Parágrafo único. A República Federativa do Brasil buscará a integração econômica, política, social e cultural dos povos da América Latina, visando à formação de uma comunidade latino-americana de nações.”

Em seu art. 2º foram dispostos os Fundamentos específicos da proteção de dados pessoais no País: (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.

Da análise legal, apenas até este ponto, e em concomitância com o já apresentado sobre os preceitos constitucionais afetos à matéria, é possível identificar os conceitos sociais e os direitos coletivos abrangentes que o legislador pretendeu tutelar.

Em cenários locais, regionais e globais cada vez mais díspares, onde o capitalismo de vigilância se mostra exacerbado e, não raro, até vinculado ao Populismo, bem como diante de crescentes ataques cibernéticos a expor vidas, projetos e a intimidar pessoas vulneráveis, o ponto de oclusão há de ser, sem dúvida, a busca pelo bem social, cada vez mais fortalecida na legislação e em políticas públicas definidas por órgãos governamentais.

Diante disso, a proteção de dados pessoais torna-se não meramente uma exigência social ou uma obrigação legal, mas passa a adotar contornos de uma poderosa ferramenta de apoio aos atores institucionais e às diversas áreas do Direito, a fim de permitir a consecução do foco de defesa e proteção dos Direitos e Garantias Individuais e Coletivos.

Dados são gerados em todos os contextos, inclusive nos ambientes de exercício do poder público. Assim como são passíveis a sofrer ciberataques e vazamentos A circulação de dados ocorre em velocidade crescente, alcançando proporções até então inimagináveis, especialmente diante de novos momentos tecnológicos globais que se avizinham, como o fortalecimento e a massificação da Internet das Coisas – IoT. Por essa razão, inclusive, o tratamento de dados prescinde cada vez mais de responsabilidade, regulamentação e, provavelmente, de maior e mais efetivo sancionamento.

1.2. A dignidade da pessoa humana e da proteção de dados

Desde 1789, após a Revolução Francesa, o conceito da *Dignidade da Pessoa Humana* norteia constituições mundiais, por meio da Declaração de Direitos do Homem e do Cidadão. Entretanto, foi apenas com o fim da Segunda Guerra Mundial e com a promulgação da Declaração Universal dos Direitos Humanos, em 1948, bem como a partir de uma maior conscientização mundial sobre os pavores do Holocausto, do Fascismo e do Nazismo que surgiu, no plano internacional, um movimento de fortalecimento hermenêutico conhecido como a *Volta de Valores*. Movimento este que marcou a crise moral do positivismo jurídico excessivo e a superação da, até então, extrema supremacia legal.⁸

Foi por meio do surgimento da declaração de 1948, consensual à época entre os Povos, que critérios e conceitos mais humanistas passaram a ser adotados nos ambientes internos das Nações signatárias, servindo de base para reconstruções constitucionais e permitindo que fossem repensadas questões vinculadas à dignidade dos seres e à garantia dos Direitos Fundamentais a serem protegidos pelos Tribunais Constitucionais.

Esse foi, historicamente, um dos períodos mais abundantes quanto ao surgimento de grandes pensadores, culminando com o surgimento de diversos trabalhos brilhantes de Karl Larenz, Konrad Hesse, John Rawls, Ronald Dworkin, Jürgen Habermas, Friedrich Muller, Luigi Ferrajoli, Robert Alexy e de vários outros.

O surgimento do conceito de *Dignidade* ocorreu por volta do período filosófico-político clássico, onde *dignitas* estava vinculada ao *status* social do indivíduo e ao seu reconhecimento pelos demais membros da comunidade. Foi, entretanto, no período Estoico (com Marco Túlio Cícero) que começaram a ser concebidos, mais claramente, os parâmetros de igualdade entre as pessoas e o reconhecimento da liberdade pessoal de cada indivíduo. Porém, apenas durante o Cristianismo, é que foi fortalecida efetivamente a noção de Dignidade: a partir da crença da

8 BARROSO, Luís Roberto. Direito Constitucional: Os Conceitos Fundamentais e a Construção do Novo Modelo. Página 269. 9ª Edição. Editora Saraiva Jur. 2019. São Paulo – SP.

relação do homem com Deus. E, em especial, em virtude da retomada, por São Tomás de Aquino, da noção de Livre Arbítrio na *dignitas humana*⁹. Isto ocorreu já nos primeiros tempos da Idade Moderna, onde o tema passaria por uma de suas fases de maior racionalidade, por meio do pensamento de Immanuel Kant.

Interagindo com a tradição anterior, Kant passou a considerar o, então, conceito de Dignidade como *Autonomia de Vontade*. Foi quando o homem passou a ser reconhecido enquanto fim em si mesmo, não devendo e não podendo ser tratado como mero objeto. Este embasamento transmitiu importantes raízes para o Constitucionalismo Contemporâneo. Sendo que, a partir deste ponto, foram deixados importantes legados, como o de Hegel, com seu conceito de *Qualidade* a ser conquistada e, até de Miguel Reale, com o *Valor-fonte*¹⁰, a partir de quando o conceito passa a ser tutelado internacionalmente.

A Constituição Federal Brasileira de 1988, ao consagrar a Dignidade da Pessoa Humana enquanto um dos fundamentos do Estado Democrático e Social de Direito, em seu art. 1º, inciso III, reconhece que o Estado existe em função da pessoa humana, e não ao contrário. Do mesmo modo, o Direito Constitucional reconhece a Dignidade da Pessoa Humana como princípio supremo, situado no ápice da hierarquia normativa. Ainda, a mesma Carta trata, de forma derivada, do Princípio da Dignidade Humana, por exemplo, no art. 170 (da ordem econômica, com vistas a assegurar a existência digna); no art. 226, §7º (do planejamento familiar e da paternidade); no art. 227, caput (da criança e do adolescente); no art. 230, caput (da proteção à pessoa idosa) e no art. 79 do ADCT (do Fundo de Erradicação da Pobreza), assuntos passíveis, ao certo, de grande aprofundamento e de sinergia com a proteção de dados.

Sobre esta relação, inclusive, vale destacar o ensinamento do, então, Presidente do STF e do Conselho Nacional de Justiça - CNJ, Mi-

9 TOMÁS DE AQUINO, Santo. Suma Teológica. V. I. Primeira Parte. Questões 1-49. Página 276 e s. Tradução de Alexandre Corrêa. Livraria Sulina. Porto Alegre – RS. 1980.

10 CANOTILHO, J. J. Gomes. MENDES, Gilmar Ferreira. SARLET, Ingo Wolfgang. STRECK, Lenio Luiz. Comentários à Constituição Federal do Brasil. 3ª Edição. Páginas 70 – 77. Editora Saraiva Jur. Editora Almedina. Série IDP. 2023. São Paulo – SP.

nistro Luiz Fux¹¹, em palestra concedida no ano de 2021, onde indicou que o Princípio Constitucional da Dignidade da Pessoa Humana está na origem da autodeterminação informativa prevista na LGPD, em seu art. 2º, inciso II da lei. Isto uma vez que atua na base da promessa de uma sociedade justa e equitativa.

1.3. Outros princípios constitucionais aplicáveis à proteção de dados

É possível identificar, ainda, seja no texto da LGPD ou, até mesmo, em recomendações, guias, manuais de boas práticas, novas interfaces da matéria com conceitos, valores e até princípios ditos setoriais. Isto tende a ser verificado com o passar do tempo, como consequência do fortalecimento da Lei e dos Regulamentos a ela vinculados, além da maior habitualidade de sua utilização, de forma matricial, em áreas com demandas até mais específicas como o Direito do Consumidor, o Direito Econômico, o Direito Penal (até mesmo acerca dos Cibercrimes), *Utilities* (Infraestrutura), e, cada vez mais, os Direitos Humanos tutelados e a serem aprimorados.

Contornos e conceitos já mapeados, tais como, privacidade, liberdade (individual e coletiva), em específico, liberdade de expressão, informação, comunicação e opinião, intimidade, honra, imagem e desenvolvimento, tenderão a ser revisitados em novos e futuros tempos. Alguns temas poderão até ser tratados de forma latente, em primeiro plano, extrinsecamente. Outros, entretanto, haverão de se desenvolver ou de serem revistos, de forma intrínseca, no contexto de casos específicos.

Sem dúvida, ainda, haverá de ser fortalecida a vinculação da proteção de dados com temas atualmente considerados essenciais, como a defesa do meio ambiente, sustentabilidade, agronegócio, mobilidade urbana, urbanismo, crescimento de cidades digitais, saúde, educação e nova empregabilidade. Isto em virtude dos novos *inputs* que já se

11 FUX, Luiz. Portal do Conselho Nacional de Justiça – CNJ. Palestra concedida no Congresso Nacional de Registro Civil (CONARCI 2021). www.cnj.jus.br Em 22/11/2021. Acessado em 01/12/2024 às 21:30min.

verificam e que ainda se aguardam, provenientes do desenvolvimento tecnológico, da inteligência artificial e de tecnologias imersivas.

1.4. Princípios base da lei geral de proteção de dados - LGPD

O doutrinador português Jorge Miranda detalha acerca das distinções entre Princípios Axiológicos Fundamentais, Princípios Político-Constitucionais e Princípios Constitucionais Instrumentais, ao passo que o professor e atual Presidente do STF e do CNJ, Ministro Luís Roberto Barroso trata de Princípios Fundamentais, Princípios Gerais e Princípios Setoriais. Ainda que não seja possível aprofundar, no decorrer deste texto tais diferenças, o que aqui importa é compreender que os Princípios Base da LGPD se mostram incontestavelmente afetos à essência constitucional nacional, ampliando o foco de sua aplicabilidade e vinculando as informações tratadas nos projetos desenvolvidos.

A LGPD inicialmente, portanto, trouxe consigo os seguinte Princípios^{12 13}:

1.4.1. Princípio da Boa-Fé

Fundamental para a obtenção do devido consentimento, do acesso e do tratamento de dados propriamente. Norteador do objetivo do tratamento, das escolhas principais, da definição sobre a utilização do volume informacional, da avaliação de eventuais danos causados e de suposta situação discriminatória. Impacta diretamente a Dignidade da Pessoa Humana e diz respeito à ética. *Em uma linha analógica vinculada a aplicabilidade legal multinível, diz respeito ao Princípio Processual Civil da Boa-Fé e, até mesmo, a outros dispostos no Código de Processo Civil Brasileiro de 2015.*¹⁴

12 CARLA, Adriana Silva de Oliveira. FERNANDES, Dianna Rosa Garcia. Guia Prático LGPD. 2018. Editora Motres. Natal – RN.

13 GOV.BR. Princípios da LGPD. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Pobreza. Acesso à Informação > LGPD. Publicado em 30/04/2021 às 17h45 min. Acessado em 03/01/2024 às 03h20min.

14 CÓDIGO DE PROCESSO CIVIL BRASILEIRO DE 2015. Lei Federal 13.105, de 16 de março de 2015. www.planalto.gov.br Acessado em 01/12/2024 às 21h03min. (i) art. 5º - dever do sujeito do processo; (ii) – sobre art. 322, §2º princípio norteador da interpretação do pedido formulado; e (iii) artigo 489, §3º - princípio norteador da interpretação das decisões judiciais.

1.4.2. Princípio da Finalidade

Setorialmente, diz respeito à utilização de fins e propósitos específicos e pré-determinados, informados previamente aos Titulares, sem possibilidade de utilização posterior incompatível ou derivada com o que fora acordado ou estabelecido. *Igualmente, em linha analógica, se vincula ao Princípio de mesma nomenclatura no Direito Administrativo, oriundo do Princípio da Impessoalidade.*¹⁵

1.4.3. Princípio da Adequação

Enseja que as finalidades informadas e avençadas com os Titulares estejam aderentes ao contexto do tratamento realizado. *Em linha analógica, vinculado ao Princípio da Finalidade.*

1.4.4. Princípio da Necessidade

Indica que o tratamento deve transcorrer de forma aderente às finalidades acordadas, respeitando a abrangência de dados definida, sua proporcionalidade e sem que ocorra excessividade em seu desenrolar. *Assim, em linha analógica, vinculado ao Princípio da Proporcionalidade.*

1.4.5. Princípio do Livre Acesso

Garante aos Titulares a consulta livre à integralidade de seus dados durante a realização do tratamento, de forma gratuita e fácil. *Em linha analógica, vinculado aos Princípios da Publicidade, Moralidade e Eficiência.*

1.4.6. Princípio da Qualidade dos Dados

Garantia concedida aos Titulares para que o trabalho realizado possa ocorrer com exatidão, clareza, relevância e atualização.

15 CONSTITUIÇÃO FEDERAL BRASILEIRA DE 1988 - art. 37, caput. www.planalto.gov.br Acessado em 01/12/2024 22h05min.

Em linha analógica, vincula-se aos Princípios da Necessidade e da Finalidade, com foco no atingimento do bom termo e, ainda, aos Princípios da Eficácia e da Eficiência.

1.4.7. Princípio da Transparência

Inerente à concessão de informações claras, precisas e de fácil acesso aos Titulares, devendo ser respeitados o sigilo e a confidencialidade firmados, tanto em âmbito comercial, como industrial. *Em linha analógica, vinculado aos Princípios da Motivação, Moralidade e Eficácia.*

1.4.8. Princípio da Segurança

Adoção de medidas e práticas qualificadas, com vistas a proteger os dados tratados e evitar acessos não autorizados. Procura precaver situações acidentais, ilícitas, perdas, adulterações e cibercrimes em geral. Princípio amplo. *Em linha analógica, vinculado aos Princípios da Eficácia, Isonomia e Liberdade.*

1.4.9. Princípio da Prevenção

Abordagem de medidas preventivas à ocorrência de danos, sejam quais forem, em face do tratamento realizado. Fundamental que se estabeleça visão de negócios, ampla e estratégica quanto a este aspecto. *Em linha analógica, vinculado aos Princípios da Eficácia e da Eficiência.*

1.4.10. Princípio da Não Discriminação

Indica a não realização do tratamento de dados de forma discriminatória, ilícita ou abusiva. *Em linha analógica, vinculado aos Princípios da Isonomia e da Impessoalidade.*

1.4.11. Princípio da Responsabilização e Prestação de Contas

Diz respeito à demonstração e à comprovação do cumprimento de todos os preceitos legais e de eficácia das medidas apli-

cadastros, pelo Controlador e pelo Operador. *Em linha analógica, vinculado ao Princípio da Eficácia e ao art. 34, inciso VII, do Princípio Constitucional Sensível da Prestação de Contas.*

2. CONSIDERAÇÕES FINAIS

A sociedade brasileira chega agora a seu primeiro ponto de ebulição digital na etapa onde *dados e tecnologia* já se tornaram essenciais à vida cotidiana.

Ao menos desde a promulgação da Lei de Acesso à Informação (Lei Federal 12.527, de 18 de novembro de 2011), a transparência se tornou não apenas uma opção, mas uma obrigação. A questão toda, nesta etapa digital, é como isso deve ser feito, quais são as regras claras e seus limites.

Ademais, com o avanço da Revolução Digital, novas áreas tendem a surgir, profissões serão extintas ou se modificarão completamente e, como consequência, a exigência da preparação humana tenderá a se acirrar ainda mais, seja no dia a dia, seja comercialmente. A informação nunca foi tão acessível, levando os cidadãos a uma maior conscientização sobre seus direitos e deveres. Da mesma forma, as inovações continuarão, mais e mais, a impactar fortemente os Direitos Individuais e Coletivos, além de, em muitos casos, a própria Dignidade do ser humano.

Assim, nesse cenário, o suporte há de vir do aprimoramento do ordenamento jurídico - mais constitucionalizado, é verdade, porém, mais focado. Leis específicas, como a LGPD, até mesmo dotadas de boa metodologia aplicável, desde suas fases iniciais, como o planejamento, até o monitoramento final detalhado, tendem a melhor esclarecer essas novas situações que surgem, regulando relações e responsabilidades.

Caberá, em próximo momento, portanto, aos atores institucionais envolvidos e criados, um ainda maior fortalecimento, com o intuito de regulamentar os comandos legais setoriais, de forma eficaz e pragmática. Aos cidadãos, por sua vez, tanto em sua esfera pessoal, quanto

de negócios, se torna mais premente a compreensão de riscos e ameaças às quais se encontram suscetíveis, mas igualmente, das reservas e da proteção que a legislação estabelece, desde a mais básica conceituação até a constitucional espelhada na lei aplicável.

REFERÊNCIAS

Em ordem alfabética

Livros:

BARROSO, Luís Roberto. Direito Constitucional: Os Conceitos Fundamentais e a Construção do Novo Modelo. Página 269. 9ª Edição. Editora Saraiva Jur. 2019. São Paulo – SP.

CANOTILHO, J. J. Gomes. MENDES, Gilmar Ferreira. SARLET, Ingo Wolfgang. STRECK, Lenio Luiz. Comentários à Constituição Federal do Brasil. 3ª Edição. Editora Saraiva Jur. Editora Almedina. Série IDP. 2023. São Paulo – SP.

TEPEDINO, Gustavo. TERRA, Aline de Miranda Valverde. GUEDES, Gisela Sampaio da Cruz. Fundamentos de Direito Civil: Volume 4, Responsabilidade Civil. 2ª. Edição Revisada e Ampliada. Editora Forense / GEN – Grupo Editorial Nacional. 2020. Rio de Janeiro – RJ.

TOMÁS DE AQUINO, Santo. Suma Teológica. V. 1. Primeira Parte. Questões 1-49. Página 276 e s. Tradução de Alexandre Corrêa. Livraria Sulina. Porto Alegre – RS. 1980.

E-Book:

CARLA, Adriana Silva de Oliveira. FERNANDES, Dianna Rosa Garcia. Guia Prático LGPD. 2018. Editora Motres. Natal – RN.

Artigos:

DA SILVA, Virgílio Afonso. Princípios e Regras: Mitos e Equívocos Acerca de Uma Distinção. Revista Latino-Americana de Estudos Constitucionais. Páginas 607-630. 2003.

SARLET, Ingo Wolfgang. Proteção de Dados Pessoais Como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo Para a Construção de Uma Dogmática Constitucionalmente Adequada. Revista Direito Fundamentais à Justiça. Páginas 179-218. Belo Horizonte. Ano 14. Nº 42. Jan/Jun 2020.

Sites:

CÓDIGO DE PROCESSO CIVIL, 2015. Lei Federal 13.105, de 16 de março de 2015. www.planalto.gov.br Acessado em 01/12/2024 às 21h03min.

CONSTITUIÇÃO FEDERAL BRASILEIRA. www.planalto.gov.br Acessado em 01/12/2024 às 22h05min.

GOV.BR. Princípios da LGPD. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Pobreza. Acesso à Informação > LGPD. Publicado em 30/04/2021 às 17h45 min. Acessado em 03/01/2024 às 03h20min.

FUX, Luiz. Portal do Conselho Nacional de Justiça – CNJ. Palestra concedida no Congresso Nacional de Registro Civil (CONARCI 2021). www.cnj.jus.br Em 22/11/2024. Acessado em 01/12/2024 às 21h30min.

SUPREMO TRIBUNAL FEDERAL – STF. www.portal.stf.jus.br Acessado em 05/07/2025. 20h. RE 1.037.396, de Relatoria do Ministro Dias Toffoli e o RE 1.057.258 de Relatoria do Ministro Luiz Fux.

Em ordem de apresentação no texto, com referência de localização

TEPEDINO, Gustavo. TERRA, Aline de Miranda Valverde. GUEDES, Gisela Sampaio da Cruz. Fundamentos de Direito Civil: Volume 4, Responsabilidade Civil. 2ª. Edição Revisada e Ampliada. Editora Forense / GEN – Grupo Editorial Nacional. 2020. Rio de Janeiro – RJ.

SARLET, Ingo Wolfgang. Proteção de Dados Pessoais Como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo Para a Construção de Uma Dogmática Constitucionalmente Adequada. Revista Direito Fundamentais à Justiça. Páginas 179-218 Belo Horizonte. Ano 14. Nº 42. Jan/Jun 2020.

CONSTITUIÇÃO FEDERAL BRASILEIRA. www.planalto.gov.br Acessado em 01/12/2024 às 22h05min.

SUPREMO TRIBUNAL FEDERAL – STF. www.portal.stf.jus.br Acessado em 05/07/2025. 20h. RE 1.037.396, de Relatoria do Ministro Dias Toffoli e o RE 1.057.258 de Relatoria do Ministro Luiz Fux.

CONSTITUIÇÃO FEDERAL BRASILEIRA. www.planalto.gov.br

Acessado em 01/12/2024 às 22h05min.

CONSTITUIÇÃO FEDERAL BRASILEIRA. www.planalto.gov.br
Acessado em 01/12/2024 às 22h05min.

BARROSO, Luís Roberto. Direito Constitucional: Os Conceitos Fundamentais e a Construção do Novo Modelo. Página 269. 9ª Edição. Editora Saraiva Jur. 2019. São Paulo – SP.

TOMÁS DE AQUINO, Santo. Suma Teológica. V. 1. Primeira Parte. Questões 1- 49. Página 276 e s. Tradução de Alexandre Corrêa. Livraria Sulina. Porto Alegre – RS. 1980.

CANOTILHO, J. J. Gomes. MENDES, Gilmar Ferreira. SARLET, Ingo Wolfgang. STRECK, Lenio Luiz. Comentários à Constituição Federal do Brasil. 3ª Edição. Páginas 70-77. Editora Saraiva Jur. Editora Almedina. Série IDP. 2023. São Paulo – SP.

FUX, Luiz. Portal do Conselho Nacional de Justiça – CNJ. Palestra concedida no Congresso Nacional de Registro Civil (CONARCI 2021). www.cnj.jus.br Em 22/11/2024. Acessado em 01/12/2024 às 21h30min.

CARLA, Adriana Silva de Oliveira. FERNANDES, Dianna Rosa Garcia. Guia Prático LGPD. 2018. Editora Motres. Natal – RN.

GOV.BR. Princípios da LGPD. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Pobreza. Acesso à Informação > LGPD. Publicado em 30/04/2021 às 17h45 min. Acessado em 03/01/2024 às 03h20min.

CÓDIGO DE PROCESSO CIVIL, 2015. Lei Federal 13.105, de 16 de março de 2015. www.planalto.gov.br Acessado em 01/12/2024 às 21h03min.

CONSTITUIÇÃO FEDERAL BRASILEIRA. www.planalto.gov.br
Acessado em 01/12/2024 às 22h05min.

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO BRASIL E SEU COMPARATIVO INTERNACIONAL

Adriana Giuntini Viana¹

Henriette Groenwold Monteiro²

INTRODUÇÃO

A proteção de dados pessoais se tornou uma preocupação global à medida que a tecnologia avançou e as informações pessoais se tornaram mais valiosas e vulneráveis a abusos. Em razão disso, o direito tem buscado acompanhar as transformações sociais e culturais que envolvem a noção de privacidade, o fluxo das informações e até mesmo o desenvolvimento da tecnologia, pois essas variáveis podem influenciar significativamente as esferas individual e privada.

A proteção dos dados é de extrema importância para a construção da dignidade da pessoa humana, que é um que consomem dos fundamentos basilares da Constituição Federal de 1988 (art. 1º, inciso III) e é garantida por ela (art. 5º, incisos X, XII, LXXII e LXXIX), não podendo ser abolida (art. 60, §4º). Outrossim, esses direitos também são

1 Advogada. Consultora em Proteção de Dados. Professora. Pós-graduada em Compliance e Proteção de Dados pela Universidad Católica de San Antonio de Murcia/Espanha (UCAM) – Espanha. Delegada de Protección de Datos (DPD/DPO) en General Data Protection Regulation (GDPR) pela Escuela de Negócios (EDEU) – Madri/Espanha. Pós-graduada em Gestão de Negócios pela Fundação Dom Cabral. Membro da Comissão de Privacidade e Proteção de Dados da OAB/DF.

2 Advogada. Bacharel em Direito pelo Centro Universitário do Distrito Federal (UnidF). Tecnóloga em Análise e Desenvolvimento de Sistemas pela Universidade Cruzeiro do Sul. MBA em Segurança da Informação pela Universidade Cruzeiro do Sul. Pós-Graduada em LGPD pela UniBTA Digital. Membro da Comissão de Privacidade e Proteção de Dados Pessoais da Ordem dos Advogados Seccional do Distrito Federal e da Comissão Temática de Proteção de Dados (LGPD) da Subseção do Guará/DF.

características do direito da personalidade³ – que se refere aos atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais.⁴

Isto é, o ordenamento jurídico reconhece que a tutela pela vida, a integridade física, a intimidade e a honra são direitos inerentes aos seres humanos, e são necessários para seu desenvolvimento e são absolutos, individuais, indisponíveis, intransmissíveis, irrenunciáveis, imprescritíveis, inalienáveis e impenhoráveis.⁵

E por que é necessário ter essa atenção com a proteção dos dados pessoais e com a privacidade? Em decorrência do fluxo avanço tecnológico, as informações pessoais dos sujeitos, enquanto titulares de dados, estão sendo coletadas de forma muito rápida, fácil e, de alguma forma, até mesmo barata.

Inúmeras empresas desenvolveram estratégias e modelos de negócios considerando as ações, comportamentos e padrões de consumo das pessoas, e, para tanto, observavam todos os dados que os próprios indivíduos forneciam – mesmo que esses não tivessem pleno conhecimento da “autorização” que concederam.

Infelizmente, os resultados obtidos dessas análises afetaram diretamente os direitos de privacidade e de personalidade de cada indivíduo, influenciando indevidamente a autonomia, a individualidade e a liberdade.

Hoje existem, por exemplo, roupas com sensores capazes de identificar se determinado indivíduo está com algum sintoma de hipoglicemia ou de hipertensão; os smartphones conseguem identificar as rotas, rastrear os locais frequentados e as atividades diárias de seus usuários; alguns aplicativos são capazes de influenciar o comportamento, o consumo, as decisões de compra e, até mesmo, opiniões políticas; há também a possibilidade de os dados serem utilizados em fraudes ou roubos de identidade, o que pode acarretar sérias consequências financeiras e legais.

3 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

4 PAMPLONA Filho, Rodolfo; GAGLIANO, Pablo Stolze. **Manual de Direito Civil - Volume Único** [livro eletrônico]. 5ª Ed. São Paulo: Saraiva Educação, 2021.

5 Ibid.

Além disso, existem os dados em papel, que exigem o mesmo cuidado, pois, da mesma forma que os dados digitais, podem ser perdidos, roubados ou descartados de maneira inadequada, pessoas não autorizadas podem acessá-los e compartilhá-los, o que pode gerar prejuízos aos titulares.

Diante deste cenário, eis que surgem perguntas retóricas: quem tem acesso a essas informações? Com quem essas informações são compartilhadas? Antigamente, o titular não sabia – hoje, graças às novas legislações e regulamentos que tratam da privacidade e proteção de dados, ele pode saber.

Portanto, é imprescindível que existam regulamentações rigorosas para proteger os dados pessoais: garantias quanto à coleta, à forma e ao tempo de armazenamento e informações sobre compartilhamento e utilização. O tratamento dos dados deve ocorrer de forma ética e segura e, principalmente, os titulares devem ser devidamente informados sobre como suas informações estão sendo usadas.

No Brasil, a aprovação da LGPD, em 2018, representou um marco importante na regulamentação da proteção de dados pessoais. No entanto, essa legislação não está sozinha, pois outros países em todo o mundo também implementaram dispositivos semelhantes.

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24.10.1995, que foi substituída pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, influenciaram, e continuam influenciando, as legislações de outros países que buscam proteger os dados pessoais de seus cidadãos.

Assim, o presente artigo fará uma breve análise histórica sobre a privacidade e proteção dos dados no Brasil; abordará as principais disposições constantes na LGPD; trará breves considerações acerca da criação da ANPD; fará uma abordagem histórica do GDPR; apontará os princípios fundamentais e estrutura do GDPR; fará um comparativo entre o GDPR e a LGPD; e, por fim, apontará o impacto global do GDPR.

1. A LGPD NO BRASIL

1.1. Evolução histórica

Na Constituição Federal de 1988, conforme mencionado anteriormente, é explícito o valor supremo de todos os direitos fundamentais do homem (dignidade da pessoa humana)⁶, em seu sentido mais amplo, e a privacidade, por sua vez, é um verdadeiro direito fundamental, sendo-lhe garantida a intimidade, a inviolabilidade, a liberdade e a proteção aos dados pessoais.⁷

Em relação ao direito expresso, “a proteção dos dados pessoais, inclusive nos meios digitais” é um acréscimo recente à Carta Magna, introduzido no art. 5º, inciso LXXIX, pela Emenda Constitucional nº 115, de 10.02.2022.⁸

Promulgado em 1990, o Código de Defesa do Consumidor (CDC) já garantia aos consumidores (titulares dos dados) o “acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (*caput* do art. 43); apontava o período máximo de armazenamento de informações negativas (5 anos, segundo o §1º do mesmo artigo) e previa possibilidade de retificação dos dados e o respectivo prazo para atendimento da solicitação (5 dias, segundo o §3º do mesmo dispositivo). Inclusive, caracterizava como infração penal, suscetível à pena de detenção, o impedimento ou embaraço de o consumidor acessar suas informações, bem como deixar de corrigi-las imediatamente.

Em novembro de 2012, dada a notória necessidade de coibir e punir condutas que violem a privacidade, a segurança e a dignidade das

6 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24ª Ed. São Paulo: Malheiros Editores LTDA, 2005. p. 105.

7 BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10.12.2023.

8 BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em 10.12.2023.

pessoas que utilizam a internet, na esfera penal, foi sancionada a Lei nº 12.737, conhecida como Lei Carolina Dieckmann.

A Lei nº 12.965, de 23.04.2014, denominada como Marco Civil da Internet, é outro dispositivo relevante que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Nela, é evidente a preocupação inequívoca com a proteção da privacidade e dos dados pessoais (art. 3º), com especial destaque ao art. 7º e seus incisos, que já asseguravam aos usuários a exigência de fornecimento informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, mediante finalidades devidamente justificadas, permitidas e constantes em contrato (inciso VIII).

De mais a mais, a proteção da privacidade pode ser observada em outros ramos do direito, como o processual civil⁹, o comercial¹⁰ e o tributário¹¹.¹²

No entanto, em se tratando de legislação específica do tema, foi o deputado federal Milton Monti (PR-SP), por meio do Projeto de Lei (PL) 4.060/2012,¹³ quem iniciou as discussões acerca da matéria da proteção de dados, cuja análise ocorreu nas seguintes comissões: de Ciência e Tecnologia, de Comunicação e Informática (CCTCI); de Constituição e Justiça e de Cidadania (CCJC); de Trabalho, de Administração e Serviço Público (CTASP) e de Desenvolvimento Econômico, Indústria, Comércio e Serviços (CDEICS). Assim, em razão da distribuição a mais de três comissões de mérito, foi criada uma comissão especial (em 2016) e, após apreciação e aprovação em Plenário, a matéria foi ao Senado Federal (em 2018).¹⁴

9 Nas situações em que são admitidas a tramitação em segredo de justiça.

10 Artigos 17 a 19 do Código Comercial.

11 Artigo 198 do Código Tributário Nacional.

12 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

13 BRASIL. Câmara dos Deputados. **Projeto de Lei 4.060/2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL%204060/2012. Acesso em 10.12.2023.

14 BRASIL. Câmara dos Deputados. **Ficha de Tramitação do PL 4.060/2012**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em 10.12.2023.

Desde o início, o objetivo era regular o tratamento de dados pessoais por parte de entidades públicas e privadas, alinhadas às principais legislações sobre privacidade e tratamento em vigência em outros países, em especial a Diretiva 95/46/CE do Parlamento Europeu e do Conselho (que tratava da proteção de dados), conforme constou no parecer do relator nº 1 da CCTCI, o deputado Sóstenes Cavalcante (DEM-RJ).¹⁵

Posteriormente, o projeto foi influenciado pelo GDPR, que entrou em vigor em 25.05.2018, sendo este relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e, como outrora mencionado, substituiu a Diretiva 95/46/CE.

O PL 4.060/2012, após regular trâmite no Congresso Nacional, foi sancionado pelo presidente Michel Temer em 14.08.2018, recebeu o número de Lei nº 13.709 e tinha como ementa: “Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)”.¹⁶ Não obstante, em 08.07.2019, o presidente Jair Messias Bolsonaro realizou algumas alterações e ela passou a vigorar com o nome de Lei Geral de Proteção de Dados Pessoais (LGPD)¹⁷.

Apesar da promulgação em 2018, a LGPD não entrou em vigor imediatamente após sua publicação. O período de vacância, inicialmente, era de 18 meses, mas foi alterado por outras leis e medidas provisórias, de forma que ocorreu escalonada.

Os artigos que tratavam da criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão vinculado à Presidência da Repúli-

15 BRASIL. Câmara dos Deputados. **Parecer do Relator n.1 CCTCI**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1454623&filename=Tramitacao-PL%204060/2012. Acesso em 10.12.2023.

16 BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 10.12.2023.

17 BRASIL. **Lei nº 13.853**, de 08 de julho de 2019. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em 10.12.2023.

ca e responsável por fiscalizar e orientar a aplicação da lei, entraram em vigor em 28.12.2018.

Os artigos que previam as sanções administrativas que podem ser aplicadas pela ANPD em caso de violação, tais como advertência, multa, bloqueio ou eliminação dos dados pessoais, entraram em vigor no dia 01.08.2021.

Os demais artigos – que definiram os conceitos, os princípios, os direitos e os deveres relacionados à proteção de dados pessoais no Brasil – entraram em vigor no dia 03.05.2021.

Destarte, a LGPD entrou em vigor de forma complexa e sujeita a mudanças legislativas, o que exigiu atenção e adaptação dos agentes envolvidos no tratamento de dados pessoais. Entretanto, esse fato não a tornou menos relevante, conforme elucidado a seguir.

1.2. Principais disposições

A LGPD é aplicável a qualquer pessoa física ou jurídica, pública ou privada, que realize tratamento de dados pessoais no Brasil, ou que tenha como finalidade oferecer bens ou serviços ou tratar dados de pessoas localizadas no país; ou, ainda, que tenha coletado os dados em território nacional.

No entanto, a lei não é aplicável a alguns tipos de tratamento de dados, tais como: aqueles realizados com fins exclusivamente jornalísticos, artísticos e acadêmicos, ou os que se referem à segurança pública, à defesa nacional, à segurança do Estado e às atividades de investigação e repressão de crimes.

A lei apresenta conceitos que são essenciais para sua correta compreensão. Veja alguns deles:

Dados pessoais: informações relativas à pessoa física identificada ou identificável. Exemplos: RG, CPF, gênero, data de nascimento, número de telefone, e-mail, endereço residencial, fotografia, entre tantos outros.

Dados pessoais sensíveis: são as informações da pessoa física sobre etnia, religião, estado civil, escolaridade, orientação sexual, material genético e biometria, entre outros.

Dado anonimizado: é o dado cujo titular não pode ser identificado, sendo necessária a utilização de técnicas seguras que não permitam associação a um indivíduo.

Tratamento de dados: toda operação realizada com algum tipo de dado pessoal, seja coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Titular: pessoa natural sobre quem se referem os dados que serão tratados.

Consentimento: manifestação livre, explícita e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade clara e específica.

Operador: pessoa física ou jurídica que realiza o tratamento dos dados pessoais em nome do controlador.

Controlador: pessoa física ou jurídica que toma decisões referentes ao tratamento dos dados pessoais.

Encarregado: pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

Agentes de tratamento: controlador e operador.

A lei define que as atividades de tratamento também devem observar os seguintes princípios norteadores: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, sem deixar de observar o da boa-fé.

Traz, ainda, as hipóteses taxativas para o tratamento dos dados, sendo elas: consentimento pelo titular; para o cumprimento de

obrigação legal ou regulatória pelo controlador; 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 da lei; para a realização de estudos por órgão de pesquisa – garantida, sempre que possível, a anonimização dos dados pessoais; para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, quando necessário, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiros; para a tutela da saúde, exclusivamente, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária; para atender aos interesses legítimos do controlador ou de terceiros, quando necessário, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; para a proteção do crédito.

No que diz respeito ao tratamento de dados pelas pessoas jurídicas de direito público, estas também devem observar a finalidade e o interesse comum. Todavia, são proibidas de transferir às entidades privadas, sendo-lhes admitidas algumas exceções definidas na própria na lei.

É interessante destacar que, em relação às crianças e adolescentes, a LGPD é categórica ao definir que o tratamento deve ser sempre realizado em seu melhor interesse e com o consentimento específico e destacado de pelo menos um dos genitores ou responsável legal.

Adicionalmente, a LGPD prevê que o titular tem o direito de saber como seus dados pessoais são tratados. O controlador deve fornecer informações claras e adequadas sobre a finalidade, a identificação, as responsabilidades e os direitos do titular. É garantido ao titular solicitar ao controlador informações como a confirmação do tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a eliminação dos dados pessoais tratados com o consentimento do titular, entre outros.

Certamente, a legislação traz muitos outros dispositivos que merecem análise aprofundada, de maneira que as considerações aqui feitas tecem apenas alguns de seus aspectos mais relevantes.

1.3. Criação da ANPD

Anteriormente, foi mencionado que a Lei nº 13.853 trouxe algumas modificações para a Lei 13.709/2018 (LGPD): além da nova ementa, criou a ANPD – que é uma autarquia de natureza especial, dotada de autonomia técnica e decisória.

A ANPD é composta por: conselho diretor; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; corregedoria; ouvidoria; procuradoria; unidades administrativas e unidades especializadas.

Entre as atribuições da ANPD, merece destaque que o dever de zelar pela proteção dos dados pessoais; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar as sanções quando do descumprimento da LGPD, mediante processo administrativo – assegurados o contraditório, a ampla defesa e o direito de recurso; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, entre tantas outras.

Desde a sua implementação, a ANPD enfrenta desafios, como a necessidade de estabelecer-se como uma autoridade respeitada, equipar-se com recursos suficientes e lidar com um grande volume de demandas e questões complexas de privacidade. Apesar dos desafios, sua existência é um marco para a proteção de dados no Brasil, impactando operações de empresas, a segurança e a privacidade dos cidadãos e o posicionamento do país no cenário internacional de proteção de dados.

Na página oficial da ANPD na internet, é possível encontrar o repositório de publicações, guias e documentos técnicos.¹⁸

¹⁸ Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em 12.12.2023.

2. COMPARATIVO INTERNACIONAL

2.1. Introdução histórica do Regulamento Geral de Proteção de Dados (GDPR)

A história do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UE) é uma jornada que se alinha estreitamente com a evolução da era digital e o crescente reconhecimento da importância da privacidade de dados. Antes do advento do GDPR, a Diretiva de Proteção de Dados da União Europeia de 1995 atuava como a principal legislação regulamentadora do tratamento de dados pessoais. No entanto, com os avanços tecnológicos e a crescente digitalização da sociedade, tornou-se evidente que a diretiva estava se tornando inadequada para enfrentar os novos desafios da era da informação e que havia a necessidade de uma abordagem mais unificada na UE.

A Diretiva 95/46/CE foi um marco importante, que determinou padrões fundamentais para o processamento de dados pessoais e a livre circulação desses dados dentro da UE. Ela focava, principalmente, em estabelecer um equilíbrio entre a proteção de dados pessoais e a livre circulação de informações. Contudo, a diretiva deixou muita flexibilidade para os Estados-membros da UE na implementação de suas próprias leis de proteção de dados, resultando em um mosaico de regulamentações em toda a Europa.

Em resposta a esses desafios, a UE iniciou o processo de revisão e atualização da sua legislação de proteção de dados. Este processo foi marcado por extensas deliberações, consultas públicas e negociações entre os Estados-membros e outras partes interessadas.

Como Kuner¹⁹ ressalta, esse processo foi orientado pela necessidade de modernizar as leis de proteção de dados para refletir as novas realidades da era digital, enquanto se reafirmava o compromisso com a proteção dos direitos fundamentais à privacidade.

19 KUNER, Christopher. **The European Union's General Data Protection Regulation (GDPR): Implications for international data protection law**. Review of European Data Protection Law, 2017.

O GDPR foi adotado em abril de 2016 e entrou em vigor em 25.05.2018. Este regulamento introduziu mudanças significativas e necessárias, como o conceito de “privacidade desde a concepção”, a responsabilidade e a prestação de contas por parte das organizações que processam dados e o fortalecimento dos direitos dos indivíduos em relação aos seus dados pessoais. O regulamento europeu representou não apenas uma atualização da legislação existente, mas um salto significativo na abordagem da proteção de dados, estabelecendo um novo padrão global para a privacidade e segurança dos dados na era digital.

A história do GDPR é uma narrativa sobre adaptação e resposta às necessidades emergentes de proteção de dados na sociedade moderna, refletindo o equilíbrio entre o avanço tecnológico e o direito fundamental à privacidade.

2.2. Princípios fundamentais e estrutura do GDPR

Os princípios fundamentais do GDPR da União Europeia estabelecem uma base sólida para a proteção de dados e a privacidade dos indivíduos, enfatizando a necessidade de uma abordagem proativa e centrada no usuário. Dois desses princípios, “privacidade desde a concepção” e “privacidade por padrão”, são cruciais para entender sua abordagem.

Privacidade desde a concepção (privacy by design)

O princípio da privacidade desde a concepção, como explicado por Voigt e Von dem Bussche²⁰, representa uma mudança significativa na forma como a proteção de dados é abordada nas organizações. Esse conceito enfatiza a necessidade de considerar a privacidade desde as primeiras fases de design de qualquer sistema ou processo de negócios. A ideia é que a proteção de dados não deve ser um elemento adicional ou um complemento, mas um aspecto integrado e fundamental de todo o desenvolvimento de produtos e serviços.

20 VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR)**. Springer International Publishing, 2017.

Este princípio implica a adoção de medidas técnicas e organizacionais que garantam a proteção de dados, incluindo a minimização (a coleta de dados estritamente necessários), garantindo a segurança desde o início do processamento de dados. Essa abordagem proativa é um desvio das práticas reativas anteriores, em que a proteção de dados, muitas vezes, só era considerada após o desenvolvimento de um produto ou serviço.

Privacidade por padrão (privacy by default)

O princípio da privacidade por padrão estabelece que, via de regra, somente os dados pessoais necessários para a realização de um determinado propósito devem ser coletados e processados. Isso significa que as organizações devem garantir que configurações de privacidade mais restritivas sejam aplicadas automaticamente a todos os sistemas e serviços, sem exigir que os usuários necessitem ajustar essas configurações para proteger sua privacidade.

Esse princípio implica que os dados pessoais não devem ser acessíveis a um número indefinido de pessoas por padrão, e que as organizações devem garantir que apenas os dados necessários para cada tarefa específica sejam processados. Essa abordagem minimiza a exposição de dados pessoais e reduz o risco de violações de dados e abusos de privacidade.

2.3. Estrutura e disposições principais do GDPR

O GDPR da União Europeia é uma legislação abrangente, que redefine a abordagem da proteção de dados pessoais e privacidade. Este regulamento é notável pelo seu alcance global, afetando não apenas as organizações dentro da UE, mas também aquelas fora dela que processam dados de indivíduos europeus, seja oferecendo bens ou serviços, seja monitorando seu comportamento. Essa extensão do escopo do GDPR estabelece um padrão internacional de proteção de dados,

exigindo que organizações ao redor do mundo adotem práticas de privacidade em conformidade com suas normas.

Além do amplo escopo de aplicação, o GDPR fortalece significativamente os direitos dos indivíduos, conferindo-lhes um controle sem precedentes sobre seus dados pessoais. Isso inclui o direito de acessar suas informações, de retificar dados incorretos, de apagar dados pessoais (conhecido como o direito ao esquecimento), à portabilidade de dados (permitindo que os indivíduos transfiram seus dados de uma organização para outra) e de se opor ao processamento de seus dados. Esses direitos asseguram que os indivíduos possam dispor de mais autonomia e proteção no ambiente digital, refletindo a crescente importância da privacidade de dados na era moderna.

As organizações, por sua vez, são obrigadas a adotar uma abordagem proativa para garantir a conformidade com o GDPR. Isso envolve a manutenção de registros detalhados de todas as atividades de processamento de dados, realização de avaliações de impacto sobre a proteção de dados (DPIAs) para identificar e mitigar riscos em processos que possam impactar significativamente os direitos e liberdades dos indivíduos e, por fim, a obrigação de notificar tanto as autoridades de proteção de dados quanto os indivíduos afetados em caso de violações. Essas medidas são fundamentais para garantir que as organizações não apenas protejam os dados que processam, mas também sejam transparentes em suas práticas de processamento de dados.

Um dos aspectos mais inovadores do GDPR é a introdução do princípio da responsabilidade. As organizações devem demonstrar ativamente sua conformidade com o GDPR, o que pode incluir a implementação de políticas de proteção de dados, a realização de auditorias internas para verificar a adesão às normas, o treinamento regular de pessoal sobre questões de proteção de dados e privacidade e a nomeação de um encarregado de proteção de dados (*data protection officer*, ou DPO) para supervisionar as práticas de proteção de dados e atuar como um ponto de contato com as autoridades reguladoras.

Em resumo, o GDPR não é apenas um conjunto de regras e regulamentos, é uma mudança fundamental na maneira como as orga-

nizações, independentemente de sua localização, devem tratar os dados pessoais. Estabelece um novo padrão global, promovendo uma cultura de privacidade e segurança de dados em todo o mundo.

2.4. A Lei Geral de Proteção De Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR)

A LGPD do Brasil foi influenciada significativamente pelo GDPR, refletindo uma tendência global a fortalecer a legislação de proteção de dados. O Brasil, reconhecendo a necessidade de atualizar suas leis para abordar os desafios da era digital, voltou-se para o GDPR como um modelo para sua própria legislação, adaptando muitos de seus conceitos e estruturas para o contexto brasileiro.

2.4.1. Comparativo entre o GDPR e a LGPD

O GDPR e a LGPD refletem um compromisso crescente com a proteção de dados pessoais na era digital. Apesar de suas diferenças, ambas as legislações compartilham o objetivo comum de proteger a privacidade dos indivíduos e impor obrigações rigorosas às organizações que processam dados pessoais. A compreensão dessas semelhanças e diferenças é crucial para as organizações que operam tanto na União Europeia quanto no Brasil, garantindo conformidade e proteção efetiva dos dados pessoais.

A estrutura da LGPD reflete muitos dos princípios e disposições do GDPR, adaptando-os ao contexto brasileiro. Isso inclui o foco na transparência do processamento das informações, a necessidade de consentimento para a coleta e o uso de dados pessoais e os direitos dos titulares, como acesso e exclusão.

Ambos os regulamentos possuem ênfase em consentimento informado, direitos extensivos concedidos aos titulares de dados e obrigações rigorosas para organizações que processam dados pessoais. Os dispositivos também estabelecem a figura do encarregado de proteção de dados, embora com algumas variações em suas funções e requisitos.

Embora tenha se inspirado no GDPR, a LGPD também realizou adaptações significativas ao cenário nacional. O dispositivo brasileiro, por exemplo, tem um escopo mais amplo em relação à base legal para o processamento de dados e oferece uma abordagem ligeiramente diferente em relação às transferências internacionais de dados e às penalidades por não conformidade.

2.5. Impacto global do GDPR

O GDPR serviu como um catalisador para a reforma da proteção de dados em muitos países fora da União Europeia. Jurisdições em todo o mundo, incluindo Ásia, África e Américas, têm examinado ou reformulado suas próprias leis de proteção de dados à luz do GDPR. Este movimento global em direção a padrões mais rígidos reflete uma crescente conscientização sobre a importância da privacidade de dados na era digital.

A título de ilustração, merecem destaque as seguintes legislações ao redor do mundo: a Ley nº 25.326 (PDPA), na Argentina²¹; a *Act on the Protection of Personal Information* (APPI), no Japão²²; a *The California Consumer Privacy Act of 2018* (CCPA), vigente na Califórnia, nos Estados Unidos²³; a *Personal Information Protection and Electronic Documents Act* (PIPEDA), no Canadá²⁴ e a *Digital Personal Data Protection Act* (DPDPA), na Índia²⁵.

A legislação de proteção de dados provavelmente continuará evoluindo, especialmente com o surgimento de novas tecnologias. De

21 Disponível em: <https://servicios.infoleg.gob.ar/infolegInternet/anejos/60000-64999/64790/norma.htm>. Acesso em 18.12.2023.

22 Disponível em <https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en>. Acesso em 18.12.2023.

23 Disponível em: https://coppa.ca.gov/regulations/pdf/coppa_act.pdf. Acesso em 18.12.2023.

24 Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>. Acesso em 18.12.2023.

25 Disponível em: <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>. Acesso em 18.12.2023.

acordo com Bygrave (2017), tecnologias como a inteligência artificial e o *big data* apresentam novos desafios para a privacidade e a proteção de dados, exigindo atualizações legislativas constantes.²⁶

O mundo digital atual apresenta desafios únicos para a proteção de dados. Questões de segurança cibernética, consentimento em ambientes digitais e transferências internacionais de dados requerem atenção contínua. Além disso, como Schwartz e Solove²⁷ argumentam, o equilíbrio entre a proteção de dados e outras liberdades fundamentais, como a liberdade de expressão, permanece um tópico de debate intenso.

A cooperação internacional em padrões e práticas de proteção de dados será cada vez mais crucial. A definição de normas que possam ser adotadas globalmente será um papel-chave desempenhado por organizações e países, conforme destacado por Bennett e Raab.²⁸

3. CONCLUSÃO

Como demonstrado, são de extrema relevância a privacidade e a proteção dos dados pessoais, tanto na forma digital quanto física, principalmente quando observamos o crescente avanço da tecnologia, a velocidade dos fluxos das informações, as exposições indesejadas e os abusos na obtenção e no tratamento dos dados.

De igual modo, a conscientização e a educação também são elementos fundamentais, seja pelas pessoas físicas ou jurídicas que tratam dados, seja pelos próprios titulares. Todos precisam entender sobre os direitos e responsabilidades inerentes à proteção dos dados e essas concepções devem ser adotadas em todas as etapas, da concepção ao desenvolvimento de determinado produto ou serviço.

A própria tecnologia pode ser utilizada em prol dessa cons-

26 BYGRAVE, Lee. A. **Data Privacy Law: An International Perspective**. Oxford University Press, 2017.

27 SCHWARTZ, Paul M.; SOLOVE, Daniel J. **Reconciling Personal Information in the United States and European Union**. California Law Review, 2014.

28 BENNETT, Colin J.; RAAB, Charles D. **The Governance of Privacy: Policy Instruments in Global Perspective**. MIT Press, 2006.

trução consciente, uma vez que ela permite anonimização dos dados, gerenciamento do consentimento e detecção de violações.

Quando um titular autoriza que determinada empresa utilize os seus dados, ele não transfere os seus direitos de personalidade para ela – o que existe é apenas uma permissão de utilização. Uma gama de preocupações surge a partir dessa coleta, desde a quantidade de dados até sua eliminação. Por longo período, infelizmente, essa não foi uma preocupação das empresas ou daqueles que tratavam dos dados.

No passado, as empresas acreditavam que os dados que colhiam lhes pertenciam – uma interpretação absolutamente equivocada. Felizmente, os regulamentos que tratam da privacidade e da proteção de dados pessoais estão corrigindo tal equívoco.

Atualmente, as legislações no Brasil e em outros países deixam claro que as empresas são apenas detentoras dos dados, nos termos autorizados pelo titular, e que precisam estar em conformidade com várias leis de proteção para que possam operar local e internacionalmente. A ética e a segurança também são elementos primordiais e sua ausência acarreta prejuízos consideráveis à reputação das empresas e à confiança dos clientes e da sociedade.

Assim, resta evidente que o GDPR e a LGPD são mais que legislações: representam indicativos de um movimento global em direção à conscientização e à proteção da privacidade de dados no século XXI. A evolução dessas leis – conforme refletido nas análises de autores consagrados – e sua adaptação a novas tecnologias e desafios serão fundamentais para a proteção de dados pessoais em um mundo cada vez mais *data-driven*.

REFERÊNCIAS

BENNETT, Colin. J.; RAAB, Charles. D. **The Governance of Privacy: Policy Instruments in Global Perspective**. MIT Press, 2006.

BRASIL. Câmara dos Deputados. **Projeto de Lei 4.060/2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL%204060/2012.

BRASIL. Câmara dos Deputados. **Ficha de Tramitação do PL 4.060/2012**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>.

BRASIL. Câmara dos Deputados. **Parecer do Relator n.1 CCTCI**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1454623&filename=Tramitacao-PL%204060/2012.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1.

BRASIL. **Lei nº 8.078**, de 11 de setembro de 1990. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/12737.htm.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1.

BRASIL. **Lei nº 13.853**, de 08 de julho de 2019. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm.

BRASIL. **Medida Provisória nº 869**, de 27 de dezembro de 2018. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm#art1.

BRASIL. **Medida Provisória nº 959**, de 29 de abril de 2019. Brasília,

DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv959.htm#art4.

BYGRAVE, Lee. A. **Data Privacy Law: An International Perspective**. Oxford University Press, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: A proteção de dados no Brasil**. Rio de Janeiro: Renovar, 2006.

FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (coord.). **A Lei Geral de Proteção de Dados Pessoais - LGPD: aspectos práticos e teóricos relevantes no setor público e privado**. São Paulo: Thomson Reuters Brasil, 2021.

GREENLEAF, G. **Global Data Privacy Laws: 89 Countries and Accelerating**. Privacy Laws & Business International Report, 2017.

KUNER, Christopher. **The European Union's General Data Protection Regulation (GDPR): Implications for international data protection law**. Review of European Data Protection Law, 2017.

LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford University Press, 2017.

PAMPLONA Filho, Rodolfo; GAGLIANO, Pablo Stolze. **Manual de Direito Civil - Volume Único** [livro eletrônico]. 5ª Ed. São Paulo: Saraiva Educação, 2021.

PARLAMENTO EUROPEU. **DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. **Reconciling Personal Information in the United States and European Union**. California Law Review, 2014.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24ª Ed. São Paulo: Malheiros Editores LTDA, 2005.

VOIGT, Paul; BUSSCHE, Axel von dem. **The EU General Data Protection Regulation (GDPR)**. Springer International Publishing, 2017.

DESAFIOS E SOLUÇÕES PARA A ADEQUAÇÃO DE EMPRESAS À LGPD

Arlene Pereira da Silva Sacco¹

Bibianna Valadares Versiani de Paula Peres²

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), ou Lei nº 13.709/2018, foi introduzida no ordenamento jurídico brasileiro com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Desse modo, com a LGPD, passam a integrar o ordenamento jurídico brasileiro institutos próprios da proteção de dados, com conceitos, princípios, tutela dos direitos do titular, regras de demonstração e prestação de contas, considerando o risco em atividades de tratamento de dados pessoais.³

A LGPD impõe, portanto, uma série de cuidados e restrições ao tratamento de dados pessoais, criando a necessidade de uma transformação cultural tanto no nível estratégico, quanto no nível operacional de uma empresa, tornando-se essencial o processo de adequação à Lei – o que leva a uma série de medidas necessárias que visam à proteção dos dados pessoais de clientes, empregados, colaboradores, fornecedores e terceiros.

1 Advogada, Mestranda em Direitos Sociais e Processos Reivindicatórios e especialista em Direito Digital, Proteção de Dados e Cibersegurança pela Universidade Católica do Paraná (PUC/PR).

2 Advogada com forte atuação em privacidade e proteção de dados, certificada em Direito Internacional pela The Hague Academy of International Law e especialista (MBA) em Relações Internacionais pela Fundação Getúlio Vargas (FGV).

3 DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [et al]. Rio de Janeiro: Forense, 2021. p. 4.

Tal conformidade visa mitigar o risco de aplicação das sanções administrativas previstas na Lei nº 13.709/2018, passíveis de imposição pela Autoridade Nacional de Proteção de Dados (ANPD), as quais incluem desde advertência até a suspensão parcial ou total do funcionamento do banco de dados ou da atividade de tratamento de dados pessoais. As regras sobre a proteção de dados trouxeram vários desafios para as empresas brasileiras. E, portanto, propõe-se uma breve revisão de literatura, mediante análise de publicações de estudos, de modo a trazer reflexões e contribuições que possam esclarecer melhor este tema.

1. A TIMELINE DA LGPD: A CRIAÇÃO DA ANPD E OS SEUS IMPACTOS NA ADEQUAÇÃO DA EMPRESAS

Pode-se dizer que a discussão sobre a proteção de dados pessoais surgiu com relativo atraso no Brasil, se considerarmos o fato de que essa temática já vinha sendo construída nas décadas de 60, 70 e 80 nos Estados Unidos e Europa, a exemplo da Lei de Proteção de Dados do *land* alemão Hesse, de 30 de setembro de 1970 e da Convenção 108 do Conselho da Europa em 1981.⁴

No Brasil, somente nos anos 80 testemunhou-se a promulgação das primeiras leis estaduais que asseguravam o direito de obtenção de informações pessoais contidas em banco de dados do Estado. Normas que abriram o terreno para a previsão na Constituição Federal de 1988 do *habeas data* (art. 5º, LXXII), remédio constitucional para acesso de informações relativas à pessoa constante em banco de dados governamentais.⁵

Nos anos seguintes, o tema da proteção de dados foi ganhando espaço no debate político, com especial força em 2010, quando o

4 DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [et al]. Rio de Janeiro: Forense, 2021. p. 4.

5 FRAZÃO, Ana. **Curso de proteção de dados pessoais: fundamentos da LGPD**/ Ana Frazão, Angelo Prata de Carvalho, Giovanna Milanez. 1.ed. Rio de Janeiro: Forense, 2022. p.21.

Ministério da Justiça tornou pública a primeira versão do texto que se tornou a base para a elaboração da Lei Geral de Proteção de Dados.⁶

Nesse período, diplomas normativos ingressam no ordenamento jurídico brasileiro: a Lei do Cadastro Positivo (Lei nº 12.414/2011), a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014), consolidando o ambiente para a sistematização de uma lei geral em matéria de proteção de dados pessoais.

Após oito anos de discussões, a LGPD foi aprovada em agosto de 2018, mas o início de sua vigência foi postergado para setembro de 2020. A *vacatio legis* da LGPD contribuiu para o atraso da adequação das empresas às novas regras de proteção de dados pessoais.

Não obstante a isso, o início da vigência da LGPD coincidiu com a emergência de saúde pública da COVID-19, cenário em que as empresas concentravam esforços em sobreviver, e questões relacionadas à adequação e à conformidade com regulamentações ficaram em segundo plano. Noutro aspecto, houve considerável aumento da circulação de dados pessoais pelas organizações e segmentos da sociedade.⁷

Ainda no contexto de pandemia, é relevante mencionar que a vigência da lei ocorreu sem a efetiva instauração da ANPD, que foi instituída somente em novembro de 2020, com a nomeação de seus membros – fato que contribuiu para insegurança jurídica quanto à aplicação dos dispositivos da LGPD, quanto à fiscalização e quanto à responsabilização das empresas pelo descumprimento da legislação.

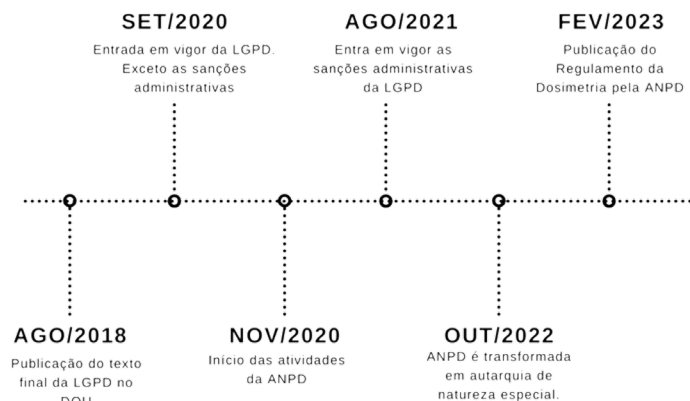
As sanções administrativas entraram em vigor em agosto de 2021, mas a ANPD só veio a editar regulamento sobre a dosimetria e

6 Ibid. p.23.

7 A despeito do cenário da pandemia, muitas empresas acreditavam que a LGPD poderia ser um óbice ao progresso econômico e um entrave para os negócios; pouco se enxergava as vantagens advindas do melhoramento dos seus processos de tratamento de dados pessoais; fato que trouxe à tona a necessidade do estabelecimento de uma cultura de proteção de dados no Brasil.

aplicação de sanções administrativas em fevereiro de 2023⁸.

Para melhor visualização do encadeamento dos fatos, segue representação gráfica da *timeline* da LGPD e da ANPD:



Fonte: elaboração das autoras.

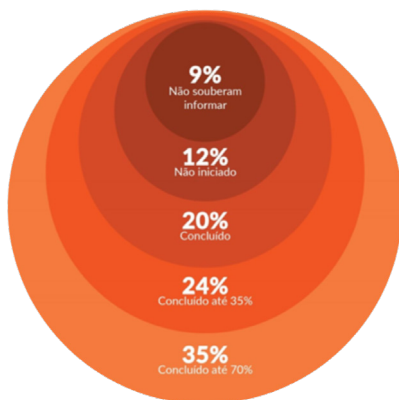
Dito isto, é possível concluir que o início da vigência da LGPD em desconhecimento com o período de criação da ANPD, somado ao contexto da pandemia, pode ter desestimulado algumas empresas a se adequarem à LGPD.

⁸ A ANPD sempre buscou o compartilhamento com o público em geral para construção de seus normativos/regulamentos. Assim, no quesito relacionado à aplicação das penalidades pela ANPD, para a devida efetivação do uso do Regulamento de Dosimetria, sempre serão levadas em consideração atenuantes que demonstrem a boa-fé e cooperação do “infrator”: a não reincidência da infração, a adoção de política de boas práticas e governança adotadas pela empresa, a adoção de medidas corretivas de maneira rápida e a adoção de mecanismos e procedimentos capazes de minimizar eventual dano. Ainda a despeito da ANPD, é importante consignar que existem lacunas a serem regulamentadas. No entanto, resta claro o objetivo do órgão a partir da similaridade com os padrões europeus, buscando o efetivo cumprimento dos objetivos da LGPD, com o estabelecimento de regras claras para empresas e pessoas físicas que tratam dados pessoais com finalidade econômica, a promoção do desenvolvimento econômico, tecnológico e da inovação, além do aumento da segurança jurídica das relações que envolvem dados pessoais.

2. A IMPORTÂNCIA DA IMPLEMENTAÇÃO DA LGPD NAS EMPRESAS

Com o advento da LGPD, os termos “proteção de dados pessoais” passaram a fazer parte do glossário jurídico brasileiro.⁹ Apesar disso, ainda hoje uma parcela significativa das empresas brasileiras não está adequada à LGPD. De acordo com pesquisa realizada pelo Instituto Daryus de Ensino Superior Paulista (IDESP), 80% das organizações no Brasil ainda não concluíram seus projetos de adequação.

Da amostra apresentada pelo Instituto, apenas 35% das organizações conseguiram avançar em até 70% nos seus projetos de adequação à LGPD. Segue abaixo a representação gráfica do resultado da pesquisa Daryus 2022-2023.¹⁰



Fonte: Daryus, 2022.

O recorte feito pelo Instituto Daryus traz o retrato da dificuldade no acultramento das empresas acerca da proteção de dados e da

9 DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: **Tratado de Proteção de Dados Pessoais**. Coord. Danilo Doneda [et al]. Rio de Janeiro: Forense, 2021. p. 10.

10 DAYRUS. Pesquisa Nacional 2022-2023. Maturidade de Privacidade e Proteção de Dados Pessoais no Brasil. Disponível em: <https://materiais.idesp.com.br/pesquisa-protecao-e-privacidade-de-dados>. Acesso em: 10 dez. 2023.

crença do valor intangível que a proteção de dados pessoais proporciona aos negócios.

Apesar disso, não se podem desconsiderar as consequências advindas pelo não cumprimento da LGPD. Como já mencionado, as sanções administrativas podem variar de advertência e suspensão das atividades de tratamento com dados pessoais à multa limitada a cinquenta milhões de reais por infração. Portanto, esse pode ser considerado o primeiro ponto de atenção para as empresas que estão em desconformidade com a lei.

A importância da LGPD para as empresas, entretanto, vai muito além de penalidades e multas; a devida adequação pode trazer aumento de produtividade, decisões mais assertivas, segurança jurídica, credibilidade da marca, entre várias outras vantagens que diferenciam os negócios.

Assim, é de extrema importância que não se utilizem políticas e termos baseados em empresas com atividades similares, cláusulas contratuais genéricas ou que não reflitam a realidade do contrato e, no que tange ao consentimento, que não seja coletado sem a devida transparência e clareza sobre o que está sendo aceito, sem a indicação da finalidade e da possibilidade de revogação, com a exclusão dos dados dos titulares que não desejem seguir com o consentido.

Para tanto, é essencial agir com transparência, garantindo informações claras, precisas e facilmente acessíveis sobre a coleta dos dados, sobre os dados armazenados, o compartilhamento e o resultado.

3. PRINCIPAIS DESAFIOS DA JORNADA DE ADEQUAÇÃO À LGPD

A proteção de dados pessoais consiste em um dos mais sensíveis desafios que o direito contemporâneo enfrenta em decorrência do extraordinário avanço tecnológico verificado nas últimas décadas.

Nessa esteira, a LGPD entra no ordenamento jurídico com uma grande amplitude de atuação, protegendo dos dados pessoais vei-

culados tanto no meio físico quanto no digital e, consequentemente, exigindo das organizações que ajustem seus processos e tecnologias para atender às demandas previstas na lei.

Desta feita, é possível dizer que o desafio é proporcional ao porte da empresa, à quantidade de dados pessoais manipulados e à quantidade de processos a serem mapeados.

Entretanto, todas as mudanças necessárias para adequar uma empresa às boas práticas de proteção de dados demandam tempo e recursos financeiros. Dependendo do porte da empresa, os investimentos incluem consultorias especializadas, implantação de sistemas e treinamento constante de colaboradores.

Somado a isso, pesquisa do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae) apontou que o porte das empresas seria um fator a acentuar a despreocupação com a LGPD, aparentemente alicerçada na crença de que determinadas atividades ou empresas menores não seriam penalizadas.¹¹

Contudo, independente do porte ou do tipo de negócio de uma empresa, os principais desafios para um projeto de adequação efetivo se concentram em três pilares: pessoas, processos e tecnologia.

Esses pilares formam a base que guiará a empresa a construir suas práticas operacionais em conformidade às normas de privacidade e proteção de dados pessoais, segundo as diretrizes da LGPD.

3.1. Pilar pessoas: a mudança cultural no tratamento de dados pessoais

A construção de uma cultura de proteção de dados é, sem dúvida, o grande desafio enfrentado pelas empresas brasileiras. Isso se deve ao fato de que a LGPD trouxe para o cenário da proteção de dados um ecossistema de direitos e obrigações e, mesmo após cinco anos de sua

11 SEBRAE. Pesquisa qualitativa LGPD. nov. 2021. Disponível em: https://datasebrae.com.br/wp-content/uploads/2020/10/091_1121_LGPD_vf.pdf. Acesso em: 22 dez. 2023.

publicação, ainda gera muitas dúvidas em decorrência da ausência de uma cultura nacional de proteção de dados pessoais.

Para uma mudança efetiva na forma como as empresas pensam sobre a proteção de dados pessoais, alguns paradigmas precisam ser superados, e o primeiro deles é que a LGPD veio para atrapalhar os negócios.

Nessa perspectiva, Maldonado¹² destaca os três principais obstáculos a serem superados para uma que haja uma mudança cultural nas empresas: falta de uma visão clara do que é a LGPD e o seu impacto para as áreas de negócio e clientes; o pensamento de que a LGPD veio para atrapalhar o alcance de metas pelas empresas; e colaboradores com baixo nível de conscientização no que tange a boas práticas de segurança e privacidade de dados.

O posicionamento da autora traz a ideia de que sem as pessoas que fazem parte da empresa não há como se falar em uma mudança cultural efetiva. Além disso, a mudança deve ser iniciada com a conscientização da alta gestão, que precisa estar diretamente envolvida no processo de aculturação, introduzindo uma mensagem positiva para as áreas de negócio sobre o uso responsável dos dados pessoais.

A cultura da proteção de dados precisa atingir todos os integrantes da empresa e, para que isso aconteça, são necessários investimentos em ações de conscientização e treinamento para que a proteção de dados seja pensada em todas as ações dos membros do time.¹³

Em suma, não há como se pensar em adequar uma empresa à LGPD sem pensar num componente essencial: as pessoas. Por isso, é crucial que a conscientização e o treinamento façam parte do dia a dia das organizações, a fim de educar os colaboradores a respeito das boas práticas de proteção de dados e da importância de respeitar os direitos dos titulares.

Nessa perspectiva, ganha destaque a figura do encarregado de proteção de dados pessoais, responsável por orientar o controlador e

12 MALDONADO, Viviane. LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Thomson Reuters Brasil, 2019, p. 45.

13 LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. *Revista de Direito*, [S. l.], v. 14, n. 01, p. 15.

os colaboradores a respeito das práticas relativas à proteção de dados pessoais.

3.2. Pilar processo

Esta ação é responsável por descrever os processos e atividades que realizam o tratamento de dados pessoais, sendo a base para a análise de adequação e conformidade das práticas operacionais relativas à privacidade e a proteção de dados pessoais, conforme a LGPD.¹⁴

3.2.1. Criação de um Plano de Adequação à LGPD

A LGPD, sozinha, não pode garantir que o tratamento de dados pessoais no Brasil seja realizado dentro dos propósitos, regras e princípios nela estabelecidos. Fato que reforça o importante papel das empresas, enquanto agentes de tratamento, no auxílio da proteção de dados no país.

Contudo, muitas empresas não sabem por onde começar a jornada de adequação à LGPD. O art. 50 estabelece os requisitos mínimos de boas práticas e de governança que devem ser cumpridos pelas empresas:

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Brasil, 2018).

14 MARTINS, Jaqueline. Adequação à LGPD: confira os 3 pilares importante. BL CONSULTORIA. 28 de abr. 2021. Disponível em: <https://blconsultoriadigital.com.br/adequacao-a-lgpd/> Acesso em: 20 dez. 2023.

Da análise do artigo supracitado, pode-se apresentar um plano estruturado em fases para a jornada de adequação à lei, conforme fluxograma a seguir:



Fonte: Elaboração da autora.

De tudo até aqui exposto, é importante ressaltar que os desafios enfrentados pelas empresas no processo de adequação não estão relacionados apenas com a falta de compreensão dos dispositivos da lei, embora a LGPD seja uma norma muito técnica.

A falta de preparo na condução do processo de adequação também pode ser atribuída a fatores como a falta de comprometimento com a conformidade, a crença na ausência de punibilidade por parte da ANPD e o descrédito no impacto positivo que a adequação terá ao negócio.

3.2.2. Mapeamento de Dados Pessoais

O mapeamento de dados pessoais é um dos maiores desafios enfrentados pelas empresas, pois a maioria das organizações não consegue diferenciar os dados pessoais das demais informações armazenadas – já que não realizam o mapeamento de processos de tratamento de dados.

O mapeamento de dados pessoais, ou *data mapping*, é uma avaliação interna dos dados pessoais tratados por uma organização, feita a partir do levantamento de informações em entrevistas ou formulários respondidos pelos colaboradores.

A apuração do mapeamento possibilita à organização um diagnóstico sobre seus processos de tratamento de dados pessoais e quais medidas de segurança devem ser aplicadas para mitigar os riscos e garantir a conformidade com as regras estabelecidas na LGPD.

Nessa fase, são atribuídas bases legais ao tratamento dos dados e realizadas adaptações nos documentos jurídicos, tais como políticas, avisos e contratos, além da avaliação da aderência dos sistemas internos à LGPD.

Trata-se, portanto, de uma etapa preliminar no planejamento para a instauração de um sistema de tratamento de dados pessoais com base nas novas diretrizes impostas pela LGPD, possibilitando uma visão detalhada de todo o fluxo de dados que transitam na organização.¹⁵ Esse é o momento em que as organizações entendem o porquê e para que tratam dados pessoais.

3.3. Pilar tecnologia: segurança da informação

As empresas que tratam dados pessoais precisam adotar medidas técnicas e administrativas aptas a protegê-las de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Em suma, precisam investir em segurança da informação.¹⁶

A necessidade de se criar medidas capazes de garantir a segurança dos dados está atrelada ao avanço da tecnologia e da transfor-

15 MUSTAFÁ, Rennan Herbert; BENFATTI, Fábio Fernandes Neves. Data mapping: adequação de escritórios de contabilidade à lei geral de proteção de dados. *Scientia Iuris*, Londrina, v. 26, n. 2, p. 103-116, jul. 2022. p. 106.

16 De acordo com a ABNT NBR ISO/IEC 27002:2013 segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança. (Item 0.1, 2013).

mação digital que, de um lado, beneficiou negócios e, de outro, tornou o ambiente digital mais vulnerável a ataques cibernéticos. Nesse viés:

As organizações e seus sistemas de informação e redes enfrentam ameaças de segurança provenientes de um amplo leque de fontes, incluindo fraudes assistidas por computador (...). As causas de dados, como códigos maliciosos, atividades de *hacking* em computadores e ataques de negação de serviço se tornaram mais comuns, mais ambiciosas e cada vez mais sofisticadas (Hintzbergen; Smulders; Baars, 2018).

Não é sem motivo que a LGPD alude à segurança da informação como conceito central para a própria proteção de dados, tendo dedicado um capítulo específico ao assunto – em que atribui aos agentes de tratamento o dever de segurança das informações sob sua tutela. Segue, abaixo, a transcrição de trechos do art. 46 da LGPD:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. [...] (BRASIL, 2018)

Desta forma, é possível inferir que a segurança da informação é importante para proteger a infraestrutura de uma empresa, evitando ou reduzindo riscos relevantes para os negócios, sendo necessária a implementação de uma série de mudanças organizacionais que requerem

investimento financeiro, mudança cultural e, por consequência, o envolvimento de todos numa organização.

Em suma, a segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Uma vez estabelecidos, os controles precisam ser monitorados, analisados e melhorados ao longo do tempo, para que seja possível assegurar os objetivos da segurança da informação.¹⁷

Nesse sentido, a gestão da segurança da informação inclui: compreender seus requisitos e estabelecer políticas e objetivos; implementar controles para gerenciar os riscos; monitorar e revisar o desempenho e eficácia do sistema de gerenciamento de segurança da informação e aprimoramento contínuo baseado em métricas.¹⁸

A relação da LGPD com a cibersegurança se dá em razão da busca pela privacidade e proteção de dados pessoais.¹⁹ Assim, enquanto a LGPD estabelece diretrizes para o tratamento de dados pessoais, a cibersegurança visa, por meio de ações concretas, mitigar riscos e evitar violações de segurança que possam comprometer os dados das pessoas.

Em resumo, para a implementação do pilar tecnologia é necessário existir uma perfeita simbiose entre a proteção de dados e a cibersegurança. Assim, torna-se possível proporcionar as condições adequadas para garantir a manutenção e desenvolvimento da privacidade e a proteção dos dados pessoais do cidadão.²⁰

17 HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans Fundamentos da segurança da informação: com base na ISO 27001 e na ISO 27002; tradução Alan de Sá. Rio de Janeiro: Brasport, 2018. p. 19.

18 Ibid. p.19.

19 Cibersegurança é a forma de proteção de sistemas de informação com recursos para a prevenção de ataques cibernéticos. Ela deve ser trabalhada em vários níveis, desde a segurança das redes físicas, dos sites, aplicativos, políticas internas, até a educação do usuário final. E, por isso, a importância de uma boa assessoria em proteção de dados quando se trata do amplo aspecto que permeia a adequação aos termos da LGPD.

20 BARRETO, G.G; ANTONIO, A. L. S; LIMA, A. L. B; GOVERNANÇA em privacidade e proteção de dados: uma visão integrada aos negócios empresariais. Realização de Serviço Federal de Processamento de Dados. Curitiba: Editorial Casa, 2022. p. 226.

4. SOLUÇÕES PARA ADEQUAR EMPRESAS À LGPD

O objetivo, aqui, não é apresentar um padrão único a ser seguido pelas empresas para a implementação de um programa de privacidade e proteção de dados, mas demonstrar que não há uma receita a ser seguida. Fundamental é dispor de uma abordagem flexível e adaptável, de modo a ajudar na tomada de decisões estratégicas para a organização.²¹

Densmore (2022) afirma que os programas de privacidade devem acompanhar as mudanças culturais, tecnológicas e legais, caso contrário, haverá lacunas entre as práticas internas de gestão de privacidade e as expectativas da sociedade.

Nesse sentido, torna-se indispensável um instrumento que permita governar todo o ambiente onde haja tratamento de dados pessoais, para que as organizações tenham um ecossistema saudável e em conformidade com as determinações da LGPD, de modo a garantir a continuidade do negócio, como bem explanado em doutrinas.

Diante desse contexto, questiona-se: quais são as etapas para implementar a governança em privacidade e proteção de dados pessoais?

O art. 50, §2º da LGPD estabelece que:

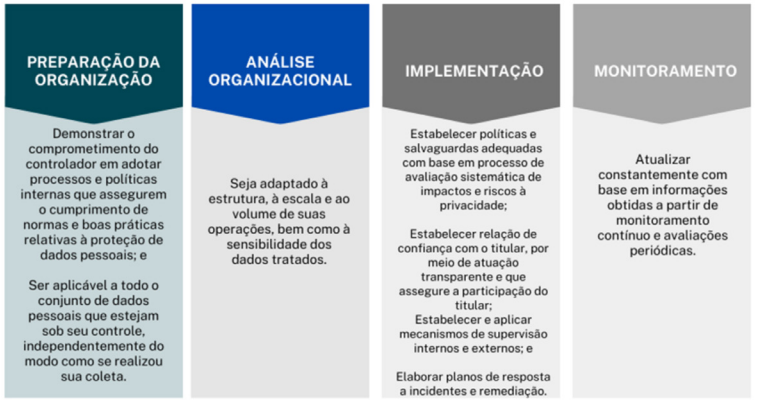
[...] as empresas poderão formular suas regras de boas práticas e de governança, e que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos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

O dispositivo citado apresenta aos agentes de tratamento os requisitos mínimos para organizarem processos e adotarem medidas de modo a comprovar sua conformidade às normas de privacidade e

21 DENSMORE, Russel. Gestão do programa de privacidade: Ferramentas para gerenciar a privacidade na sua organização. 3. Ed. Portsmouth. IAPP, 2022. p.74.

proteção de dados, dividindo-os em quatro etapas: preparação, análise da organização, implementação e monitoramento.

Seguindo a estrutura proposta no art. 50 da LGPD, segue sugestão de etapas a serem cumpridas para a implementação de um programa de governança em privacidade de proteção de dados:



Fonte: elaboração da autora.

É importante destacar que a LGPD traz um conjunto de requisitos mínimos para a sistematização de um programa de governança em privacidade e proteção de dados, sendo uma boa prática a utilização de outros *frameworks* como referencial teórico para a definição do modelo de governança a ser adotado, por exemplo a NBR ISO/IEC 27701 (ABNT, 2019) e o National Institute of Standards and Technology (NIST, 2020).

Nesse viés, um conjunto de fases para um Sistema de Gestão em Privacidade e Proteção de Dados (SGPPD), tendo como referencial teórico a LGPD (2018), a NBR ISO/IEC 27701 (ABNT, 2019), o NIST (2020) e Kyriazoglou (2019), é de extrema importância, conforme exposto a seguir:²²

22 BARRETO, G.G; ANTONIO, A. L. S; LIMA, A. L. B; GOVERNANÇA em privacidade e proteção de dados: uma visão integrada aos negócios empresariais. Realização de Serviço Federal de Processamento de Dados. Curitiba: Editorial Casa, 2022. p. 20-24.

Diagnóstico: envolve o conhecimento do contexto organizacional, o diagnóstico de nível corporativo da privacidade e proteção de dados, a estruturação dos mecanismos de governança e a criação de um plano corporativo de privacidade e proteção de dados, para tratar as lacunas globais encontradas no diagnóstico;

Mapeamento: compreende a identificação e priorização dos processos e sistemas corporativos que tratam dados pessoais, além da realização do inventário das respectivas atividades de tratamento de dados pessoais;

Análise: identificação e avaliação de riscos e não conformidades das atividades de tratamento mapeadas na etapa anterior. A avaliação de impacto à proteção de dados poderá ser realizada, a depender do resultado da avaliação de pertinência;

Planejamento: consiste na construção de um plano de ação para implementar os controles necessários ao tratamento dos riscos e não conformidades encontradas. Adiciona-se, também, correções e melhorias que podem surgir da fase de acompanhamento;

Execução: refere-se à implementação do plano corporativo, elaborado na primeira fase, além do plano de ação para implementação dos controles, correções e melhorias definidas na fase imediatamente anterior; e

Acompanhamento: envolve o monitoramento da execução, a avaliação dos resultados e retrospectiva do processo para prestar contas do SGPPD e identificar melhorias e correções (Lima; Fagundes, 2023, p. 39-40).

Diante do exposto, um programa de governança em privacidade e proteção de dados é essencial para a compreensão do tratamento de dados pessoais na organização e para a adequada implementação das diretrizes estabelecidas na LGPD.²³

23 MUSTAFÁ, Rennan Herbert; BENFATTI, Fábio Fernandes Neves. Data mapping: adequação de escritórios de contabilidade à lei geral de proteção de dados. *Scientia Iuris*, Londrina, v. 26, n. 2, 2022. p. 114.

Além disso, o não cumprimento das obrigações estabelecidas pela lei apresenta riscos às empresas, como o de violação da integridade do banco de dados, podendo afetar suas atividades por períodos indeterminados e incorrer em multas e demais sanções aplicadas pela ANPD – além de ações judiciais propostas pelos titulares, danos reputacionais, perda de confiança dos seus consumidores e custos operacionais não previstos.

5. CONSIDERAÇÕES FINAIS

É possível concluir que a adequação à LGPD requer o comprometimento de todos em uma organização, a começar pela alta gestão, que deve compreender o papel e a importância da proteção dos dados pessoais em seu modelo de negócio. Ou seja, exige das empresas uma transformação na maneira como tratam os dados sob sua tutela.

Portanto, o ponto de partida é aceitar que a adequação à LGPD é um processo necessário, inevitável e independente do porte ou do ramo de negócio de uma empresa; e os principais desafios para um projeto de adequação efetivo se concentram em três pilares: pessoas, processos e tecnologia.

A partir disso, com base nos requisitos mínimos estabelecidos na Lei, é possível construir um projeto de governança em privacidade e proteção de dados com o estabelecimento de regras internas de forma clara e transparente, promovendo mudança de cultura relacionada à segurança da informação e atendimento aos direitos dos titulares, bem como implementação de tecnologias adequadas à realidade da empresa.

Na prática, as empresas precisam compreender o fluxo dos dados pessoais, as finalidades do tratamento, conscientizar e treinar os colaboradores, revisar contratos e normativos internos e criar um sistema de segurança da informação – tudo para reduzir as possibilidades de ameaças aos dados pessoais tratados.

Em suma, para o sucesso de um projeto de adequação é fundamental a colaboração da organização como um todo. Só assim os

riscos serão mitigados e uma nova cultura de observância da proteção de dados será criada na organização.²⁴

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: **Tecnologia da informação: Técnicas de segurança: Código de prática para controles de segurança da informação**. Rio de Janeiro, 2013.

BARRETO, G.G; ANTONIO, A. L. S; LIMA, A. L. B; **GOVERNANÇA em privacidade e proteção de dados: uma visão integrada aos negócios empresariais**. Realização de Serviço Federal de Processamento de Dados. Curitiba: Editorial Casa, 2022. 374 p., il. Inclui notas explicativas. ISBN 978-65-5399-159-0. Disponível em: <https://biblioteca.aneel.gov.br/acervo/detalhe/232286>. Acesso em: 26 dez. 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Planalto, 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 3 dezembro 2023.

CRESPO, Marcelo. **Roadmap de conformidade: como deve ser um projeto de adequação para a proteção de dados**. In CRESPO, Marcelo (coord.). *Compliance no direito digital*. São Paulo: Thomson Reuters Brasil, 2020.

DAYRUS. Pesquisa Nacional 2022-2023. **Maturidade de Privacidade e Proteção de Dados Pessoais no Brasil**. Disponível em: <https://materiais.idesp.com.br/pesquisa-protecao-e-privacidade-de-dados>. Acesso em: 10 dez. 2023.

DENSMORE, Russel. **Gestão do programa de privacidade: Ferramentas para gerenciar a privacidade na sua organização**. 3. ed. Portsmouth. IAPP, 2022.

DONEDA, Danilo. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André;

24 CRESPO, Marcelo. *Roadmap de conformidade: como deve ser um projeto de adequação para a proteção de dados*. In CRESPO, Marcelo (coord.). *Compliance no direito digital*. São Paulo: Thomson Reuters Brasil, 2020. p. 152-153.

BAARS, Hans **Fundamentos da segurança da informação**: com base na ISO 27001 e na ISO 27002; tradução Alan de Sá. Rio de Janeiro: Brasport, 2018.

FLOWTI. **Como a segurança da informação é afetada pela Lei Geral de Proteção de Dados**, 16 dez. 2021. Disponível em: <https://flowti.com.br/blog/como-a-seguranca-da-informacao-e-afetada-pela-nova-lei-geral-de-protecao-de-dados>. Acesso em: 15 dez. 2023.

FRAZÃO, Ana. **Curso de proteção de dados pessoais: fundamentos da LGPD**/Ana Frazão, Angelo Prata de Carvalho, Giovanna Milanez. 1.ed. Rio de Janeiro: Forense, 2022.

INFOMONAY. **69% das empresas ativas no Brasil são MEIs, SAs são apenas 0.9% do total**. 7 jun. 2022. Disponível em: <https://www.infomoney.com.br/negocios/69-das-empresas-ativas-no-brasil-sao-meis-sas-sao-apenas-09-do-total/>. Acesso em: 22 dez. 2023.

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito, [S. l.]**, v. 14, n. 01, p. 01–20, 2022. DOI: 10.32361/2022140113764. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/13764>. Acesso em: 7 jan. 2024.

MARTINS, Jaqueline. **Adequação à LGPD: confira 3 pilares importantes**. BL CONSULTORIA. 28 de abr. 2021. Disponível em: <https://blconsultoriadigital.com.br/adequacao-a-lgpd/> Acesso em: 20 dez. 2023.

MUSTAFÁ, Rennan Herbert; BENFATTI, Fábio Fernandes Neves. **Data mapping: adequação de escritórios de contabilidade à lei geral de proteção de dados**. Scientia Iuris, Londrina, v. 26, n. 2, p. 103-116, jul. 2022. DOI 10.5433/21788189.2022v26n2p103. ISSN: 2178-8189. Acesso em: 15 dez. 2023.

OPICE BLUM, Renato; VAINZOF, Rony; MORAES, Henrique Fabretti. Data Protection Officer (Encarregado): **Teoria e Prática de acordo com a LGPD e GDPR**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2021.

PIURCOSKY, Fabrício Peloso; COSTA, Marcelo Aparecido; FROGERI, Rodrigo Franklin; CALEGARIO, Cristina Lelis Leal. **A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de**

múltiplos casos. Suma de Negócios, v. 10, n. 23, jul./dic. 2019. DOI: <https://doi.org/10.14349/sumneg/2019.v10.n23.a2>. Disponível em: <http://www.scielo.org.co/pdf/sdn/v10n23/2215-910X-sdn-10-23-89.pdf>. Acesso em 19 dez. 2023.

MALDONADO, Viviane. LGPD: **Lei Geral de Proteção de Dados Pessoais: manual de implementação**. São Paulo: Thomson Reuters Brasil, 2019.

CONTRATAÇÃO DO ENCARREGADO DE DADOS (DPO) – DESAFIOS E RESPONSABILIDADES

Daniela Lourenço de Oliveira¹

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) também conhecida como Lei nº 13.709/2018, sancionada em 2018 com vigência a partir de agosto de 2020, é um marco regulatório fundamental que define diretrizes gerais para o tratamento de dados pessoais no Brasil. Ao estabelecer princípios como transparência, finalidade, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização, a LGPD visa garantir que o tratamento de informações pessoais seja conduzido de maneira ética e responsável. Esses princípios norteadores fornecem às organizações um guia sólido para o desenvolvimento de práticas que asseguram a privacidade dos titulares dos dados.

Ao adotar uma abordagem flexível e principiológica, a LGPD incentiva as organizações a se adaptarem de acordo com suas especificidades, estimulando, ao mesmo tempo, inovação por referenciais de proteção de dados. Esse contexto de adaptação contínua vem gerando implicações significativas para o planejamento estratégico das empresas brasileiras, que precisam estar preparadas para enfrentar desafios constantes e incorporar novas práticas que assegurem a conformidade às exigências legais.

¹ Advogada graduada pela Faculdade de Direito de Franca (1994); Atuação em Direito Empresarial e Lei Geral de Proteção de Dados; Pós-graduada - Direito Digital e LGPD – NOVOESTE; Vice-Presidente da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/DF (2024); Presidente da Associação de Proteção aos Direitos do Cidadão – PRODEC; Conselheira da OAB/DF (2019 - 2021); Membro da Comissão de Compliance OAB/DF (2019 – 2020); Membro da Comissão de Direito Digital, Tecnologias Disruptivas e Startups OAB/DF (2021).

Ademais, o contexto regulatório, em constante evolução — impulsionado por decisões judiciais recentes e por atualizações normativas da Autoridade Nacional de Proteção de Dados (ANPD) — exige das organizações permanente atenção e vigilância quanto à conformidade de suas práticas de tratamento de dados pessoais. A preparação adequada e o alinhamento estratégico com a LGPD são fundamentais para mitigar riscos legais e garantir a confiança dos titulares de dados.

Nesse contexto, o papel do Encarregado de Dados, também conhecido como *Data Protection Officer* (DPO), surge como um dos elementos cruciais para a conformidade e governança em privacidade de dados dentro das organizações. Este capítulo aborda a dinâmica das questões ainda não completamente consolidadas na legislação e no ordenamento jurídico, com foco nas funções, qualificações e formas de contratação do Encarregado de Dados, explorando seus desafios e responsabilidades, e a importância de sua atuação estratégica para o sucesso na implementação das diretrizes da LGPD.

Essa perspectiva também proporciona flexibilidade para que as organizações se adaptem a diferentes contextos e situações, incentivando a inovação e o desenvolvimento de práticas de privacidade que se alinhem com os valores fundamentais da proteção de dados.

Referidas adaptações e aprimoramentos de todo contexto relacionado à Lei Geral de Proteção de Dados (LGPD) vêm gerando e continuarão gerando implicações significativas no planejamento estratégico das empresas. À medida que diversos setores da sociedade também se ajustam a essas mudanças, bem como recentes decisões emergem do Judiciário, torna-se crucial que as empresas estejam preparadas para lidar com novos critérios e desafios.

Portanto, é fundamental que as organizações fiquem atentas às mudanças e decisões emergentes relacionadas à LGPD, incorporando-as ao seu planejamento estratégico, impedindo, assim, riscos legais.

O presente capítulo abordará a figura do Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer* – DPO), examinando suas atribuições legais, requisitos de qualificação e modalidades de vinculação jurídica, à luz do ordenamento jurídico vigente.

1. FUNÇÕES E RESPONSABILIDADES DO ENCARGADO DE DADOS

A figura do Encarregado de Dados ou *Data Protection Officer* (DPO) tem suas atividades previstas nos incisos do artigo 41, § 2º, da LGPD, e consistem em: I - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - Receber comunicações da autoridade nacional e adotar providências; III - Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Resolução CD/ANPD nº 18 aprofunda essas responsabilidades ao estabelecer a importância do papel consultivo e preventivo do Encarregado. Ele deve coordenar a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD), supervisionar auditorias internas e garantir que a organização atue em conformidade com as normas.

Além das responsabilidades estabelecidas em lei, o Encarregado de Dados tem um papel estratégico na promoção de uma cultura organizacional de privacidade e proteção de dados. Algumas de suas funções adicionais incluem:

- **Conscientização e Treinamento:** O DPO é responsável por desenvolver programas de treinamento e conscientização contínua para todos os níveis da organização. Isso ajuda a garantir que todos os colaboradores compreendam a importância da proteção de dados e sigam as melhores práticas.
- **Monitoramento e Avaliação Contínua:** O Encarregado deve implementar mecanismos para monitorar o cumprimento das normas de proteção de dados, conduzindo avaliações periódicas dos processos e sistemas para assegurar que estejam de acordo com a LGPD e outras regulamentações aplicáveis.
- **Gestão de Incidentes de Segurança:** Em situações de vazamento ou comprometimento de dados, o DPO deve atuar

prontamente, coordenando a resposta ao incidente, notificando a autoridade competente (ANPD) e comunicando os titulares dos dados afetados, quando necessário. A resposta ágil e bem coordenada pode minimizar danos e reduzir a exposição da organização a sanções.

- **Assessoramento Estratégico:** O DPO também atua como conselheiro da alta administração em questões relacionadas à privacidade e à proteção de dados, fornecendo orientações que ajudam a alinhar as práticas de tratamento de dados aos objetivos estratégicos da organização, mitigando riscos e garantindo a conformidade.
- **Mediação de Conflitos:** O Encarregado de Dados desempenha um papel importante na mediação de conflitos entre os titulares de dados e a organização, lidando com reclamações e garantindo que os direitos dos titulares sejam respeitados de acordo com a legislação.
- **Auditorias Internas e Externas:** Supervisionar auditorias internas regulares e preparar a organização para auditorias externas é uma função essencial para garantir a conformidade contínua. O DPO deve garantir que todas as práticas de tratamento de dados sejam transparentes e auditáveis.
- **Manutenção de Registro de Operações:** O Encarregado é responsável por manter registros detalhados das operações de tratamento de dados, o que facilita a identificação de potenciais riscos e a implementação de medidas corretivas. Esse registro é essencial para demonstrar a conformidade da organização perante as autoridades regulatórias.

Essas funções ampliadas, indicam a complexidade e a importância do papel do Encarregado de Dados em um cenário cada vez mais orientado pela proteção e privacidade das informações. Não se trata apenas de cumprir obrigações legais, mas de integrar a proteção de dados ao cotidiano organizacional, promovendo confiança entre os titulares dos dados e agregando valor ao negócio.

2. FORMAÇÃO, QUALIFICAÇÃO E CERTIFICAÇÃO DO DPO

Não há exigências na lei referente à formação acadêmica e certificações do DPO, porém, a função de Encarregado de Dados geralmente exige uma combinação de habilidades técnicas, conhecimento jurídico e experiência em proteção de dados e privacidade, quais sejam:

1. Conhecimento jurídico em leis de privacidade e proteção de dados, tanto nacionais (LGPD) quanto internacionais (GDPR).

2. Experiência prática na gestão de programas de conformidade, com foco na aplicação de políticas de privacidade e conformidade regulatória.

3. Entendimento técnico de segurança da informação, incluindo criptografia, controle de acesso e medidas de proteção para garantir a integridade dos dados pessoais.

4. Habilidades de comunicação para lidar com diferentes públicos, desde a alta administração até os titulares dos dados, sendo capaz de explicar conceitos complexos de forma acessível.

5. Gestão de riscos: Capacidade de identificar, avaliar e mitigar riscos relacionados ao tratamento de dados pessoais, garantindo a conformidade com as exigências regulatórias.

6. Habilidades de resolução de problemas: Competência para abordar incidentes de privacidade e segurança, propondo soluções eficazes e rápidas.

7. Educação continuada: Demonstração de um compromisso contínuo com a atualização profissional, acompanhando mudanças nas leis, regulamentações e práticas de privacidade.

8. Integridade e ética: Postura ética exemplar, visto que o DPO lida diretamente com o cumprimento das obrigações legais da organização e a garantia dos direitos dos titulares de dados.

9. Conhecimento sobre a operação da organização: Compreensão profunda sobre o setor em que a organização atua e como os dados pessoais são utilizados nas operações diárias, o que facilita a implementação de práticas personalizadas de proteção de dados.

10. Habilidades interpessoais: Competência em trabalhar de forma colaborativa com diferentes equipes, como jurídico, TI, compliance, e outras áreas envolvidas no tratamento de dados.

Como dito acima, embora a LGPD e a Resolução CD/ANPD nº 18 não exijam certificações formais para o DPO, certas formações acadêmicas e certificações são amplamente reconhecidas no mercado e agregam valor ao desempenho do profissional. É importante que o DPO possua uma sólida formação acadêmica, preferencialmente em áreas relacionadas ao Direito, Tecnologia da Informação, Segurança da Informação, ou Administração, além de experiência prática em proteção de dados.

Além da formação acadêmica, certificações profissionais são altamente valorizadas por oferecerem um padrão de conhecimento e prática reconhecido internacionalmente. Algumas das certificações mais recomendadas são:

- ***Certified Information Privacy Professional (CIPP):*** Emitida pela International Association of Privacy Professionals (IAPP), esta certificação abrange legislações internacionais e práticas de privacidade de dados, sendo dividida em subcertificações regionais, como CIPP/E (Europa), CIPP/US (Estados Unidos), entre outras.
- ***Certified Information Privacy Manager (CIPM):*** Também da IAPP, esta certificação é focada na gestão e implementação de programas de privacidade. Ela é útil para um DPO que atua na supervisão e coordenação de esforços de conformidade dentro de uma organização.
- ***Certified Information Systems Security Professional (CISSP):*** Certificação oferecida pelo ISC², que é amplamente

reconhecida na área de segurança da informação. Embora não seja específica para proteção de dados, proporciona ao DPO um conhecimento aprofundado sobre como implementar medidas técnicas de proteção a dados pessoais.

- ***Data Protection Officer (DPO) Certificate***: Certificações específicas para DPO, oferecidas por instituições como EXIN e PECB, são uma opção focada na função específica de Encarregado de Proteção de Dados. Essas certificações abordam os aspectos práticos da função, incluindo o entendimento da legislação, práticas de governança de dados e a execução de relatórios de impacto.
- ***ISO/IEC 27701 Lead Implementer***: A norma ISO/IEC 27701 é um padrão internacional para gestão da privacidade, e esta certificação capacita o profissional a implementar sistemas de gestão da privacidade dentro de uma organização. Isso é particularmente útil para garantir que a empresa esteja alinhada com as melhores práticas de governança de dados.
- ***LGPD Foundation e Practitioner***: Certificações específicas para a legislação brasileira, oferecidas por empresas de treinamento em conformidade e governança. Essas certificações demonstram que o DPO possui conhecimento aprofundado sobre os detalhes da LGPD e sua aplicação prática.

A **formação contínua** é fundamental, pois as leis e as práticas de privacidade estão em constante evolução. O DPO deve buscar capacitações e participar de seminários, conferências, e workshops na área de privacidade e proteção de dados para se manter atualizado. Alguns eventos internacionais, como a conferência anual da IAPP, são altamente recomendados para networking e atualizações sobre as melhores práticas globais de proteção de dados.

Além disso, o DPO pode se beneficiar de cursos em áreas correlatas, como **Gestão de Riscos, Auditoria de TI, e Governança Corporativa**, que agregam ao papel do DPO uma perspectiva mais ampla sobre como a privacidade dos dados se relaciona com os demais aspectos da organização.

A formação acadêmica e a obtenção de certificações reconhecidas são fatores que ajudam a garantir que o DPO esteja bem preparado para lidar com os desafios da proteção de dados, trazendo um nível de confiança e profissionalismo que beneficia tanto a organização quanto os titulares dos dados. Essas credenciais não são obrigatórias pela LGPD, mas são fundamentais para proporcionar ao DPO um diferencial competitivo no mercado, além de garantir maior segurança jurídica às organizações que o contratarem.

No Brasil, a oferta de cursos especializados em proteção de dados ainda está se desenvolvendo. Muitas certificações e cursos de renome são oferecidos por instituições internacionais, o que pode ser um desafio para o DPO em termos de acesso e custos. As empresas devem, portanto, estar dispostas a investir em treinamentos específicos para que seus DPOs tenham acesso ao que há de mais moderno e atualizado em termos de capacitação profissional.

É essencial que o DPO adote a postura de um aprendiz constante, dedicando-se ao aprimoramento contínuo através de cursos, seminários e eventos especializados. A própria organização deve apoiar e incentivar essa educação continuada, alocando recursos financeiros e tempo para a capacitação do DPO. Certificações como CIPP, CIPM, DPO Certification (EXIN, PECB) e outras relacionadas à segurança da informação (como CISSP) são instrumentos que ajudam o DPO a desenvolver suas habilidades de forma estruturada e reconhecida no mercado.

3. O DPO EM DIFERENTES SETORES ORGANIZACIONAIS

O perfil do DPO pode variar de acordo com o setor de atuação da organização, já que cada setor apresenta suas peculiaridades e desafios específicos no tratamento de dados pessoais. A seguir, apresentamos exemplos práticos do papel do DPO em diferentes setores:

Setor de Saúde: No setor da saúde, que trata extensivamente dados pessoais sensíveis, é imprescindível que o Encarregado pelo Trata-

mento de Dados Pessoais (DPO) detenha conhecimento técnico especializado, inclusive sobre normativos setoriais, como a Lei nº 13.787/2018, que dispõe sobre o tratamento de prontuários e dados pessoais na área da saúde. É igualmente necessário que o DPO detenha conhecimento sobre protocolos de confidencialidade e segurança da informação, a fim de assegurar a proteção de dados relativos a prontuários médicos, exames e diagnósticos. Nesse contexto, o Encarregado deve atuar de forma diligente na gestão do compartilhamento de dados pessoais sensíveis entre hospitais, clínicas, laboratórios e demais entes da cadeia assistencial, assegurando a conformidade com as normas legais e regulamentares aplicáveis, bem como a preservação da integridade e confidencialidade das informações dos pacientes. O desafio reside em garantir que o tratamento dos dados pessoais ocorra de forma adequada às finalidades legítimas, observando-se, quando exigido, o consentimento expresso dos titulares, em conformidade com os preceitos da Lei Geral de Proteção de Dados Pessoais (LGPD), de modo a mitigar os riscos de infrações e responsabilizações decorrentes de eventuais violações.

Sector Financeiro: No setor financeiro, que é altamente regulado e manipula informações financeiras e também dados pessoais sensíveis, o DPO deve ser hábil na gestão de riscos, pois ataques cibernéticos e vazamentos de dados podem ter graves consequências econômicas e legais. O DPO precisa atuar em conformidade com normas como as do Banco Central do Brasil e da Comissão de Valores Mobiliários (CVM), além de garantir que as transações sejam seguras e que os dados dos clientes estejam protegidos contra fraudes. O desafio está em lidar com o volume de dados financeiros, garantindo a proteção dos mesmos em todas as etapas de processamento, especialmente em relação às transferências eletrônicas e à prevenção de lavagem de dinheiro.

Sector de Tecnologia e Startups: Empresas de tecnologia, particularmente startups, têm um ambiente muito dinâmico e, muitas vezes, estão em processo constante de crescimento e inovação. Aqui, o DPO precisa ser flexível e ter um bom entendimento dos processos ágeis que regem essas empresas. Frequentemente, o DPO precisará as-

essorar em questões de consentimento de usuários e anonimização de dados, além de garantir a conformidade com as normas ao mesmo tempo que possibilita a inovação. O principal desafio neste setor é equilibrar o desenvolvimento de novos produtos e serviços com as exigências legais de proteção de dados, assegurando que a privacidade do usuário seja considerada desde a concepção dos produtos (privacy by design).

Setor de Educação: Instituições de ensino, como escolas e universidades, coletam e tratam uma vasta gama de dados de alunos, professores e funcionários. Esses dados incluem informações pessoais, registros acadêmicos e dados financeiros. O DPO deve garantir que todas as práticas de coleta e armazenamento estejam em conformidade com a LGPD, além de supervisionar a transparência das informações e a garantia dos direitos dos titulares, como acesso e correção de dados. O desafio envolve a gestão de consentimento dos pais para o tratamento de dados de menores de idade, além de assegurar que terceiros, como plataformas de ensino online, estejam igualmente em conformidade com as exigências da LGPD.

Setor Público: No setor público, o DPO deve lidar com uma enorme quantidade de dados pessoais coletados em diferentes esferas governamentais. Além da conformidade com a LGPD, o DPO precisa considerar outras legislações que regem a transparência e o acesso à informação, como a Lei de Acesso à Informação (Lei nº 12.527/2011). O papel do DPO é fundamental para garantir que o uso de dados pelo governo seja responsável, seguro e transparente, respeitando os direitos dos cidadãos e minimizando riscos de exposição indevida dos dados.

Setor de Varejo: No varejo, o DPO deve gerenciar dados relacionados a clientes, incluindo informações de compras, preferências e, muitas vezes, dados financeiros. O uso de programas de fidelidade e o marketing digital são áreas de risco para a privacidade dos consumidores, especialmente no que se refere à coleta e uso de dados pessoais para estratégias de vendas. O desafio é garantir que todas as campanhas de marketing sejam conduzidas de forma transparente e que o consentimento seja obtido de forma adequada, minimizando riscos de reclamações e penalidades.

4. COMPETÊNCIAS TÉCNICAS VS. COMPETÊNCIAS COMPORTAMENTAIS

O papel do Encarregado de Dados exige uma combinação única de competências técnicas e competências comportamentais. Cada uma dessas competências é crucial para que o DPO possa desempenhar suas funções de maneira eficaz e garantir a conformidade com as legislações de proteção de dados, como a LGPD.

4.1. Competências técnicas

As competências técnicas referem-se ao conjunto de habilidades específicas que envolvem o conhecimento profundo da legislação de proteção de dados e a capacidade de aplicar essas normas no contexto da organização. Estas incluem:

- **Conhecimento das Legislações de Proteção de Dados:** O DPO deve ser bem versado na LGPD, no GDPR e em outras legislações relevantes, compreendendo como cada uma se aplica ao contexto organizacional.
- **Segurança da Informação:** Inclui o entendimento dos princípios de segurança da informação, criptografia, controle de acesso, e as melhores práticas de cibersegurança para proteger os dados pessoais.
- **Gestão de Riscos:** A habilidade de identificar, analisar e mitigar riscos associados ao tratamento de dados pessoais. Isso implica avaliar continuamente os processos de tratamento de dados e identificar possíveis vulnerabilidades.
- **Auditorias e Relatórios de Impacto:** Realização de auditorias periódicas para verificar a conformidade e elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) sempre que necessário, principalmente em situações que envolvam tratamento de dados sensíveis ou em larga escala.
- **Conhecimento de TI e Sistemas de Informação:** O DPO deve ter um entendimento técnico das infraestruturas de

TI, sistemas de gestão de dados e práticas de monitoramento. Isso garante que ele consiga avaliar a adequação dos sistemas para a proteção de dados.

- **Processos de Conformidade:** Habilidade em implementar e supervisionar políticas de conformidade, garantindo que todas as áreas da organização estejam aderentes aos requisitos da LGPD.

4.2. Competências comportamentais

As competências comportamentais estão relacionadas às habilidades sociais e de gestão do DPO, essenciais para o cumprimento de suas responsabilidades e para a interação com diferentes stakeholders da organização. As principais competências comportamentais incluem:

- **Comunicação Eficaz:** O DPO deve ser capaz de comunicar de forma clara e acessível informações sobre a privacidade e proteção de dados a diferentes públicos, que podem não ter o mesmo nível de entendimento técnico. Isso inclui funcionários, alta administração, clientes e titulares dos dados.
- **Negociação e Mediação:** O DPO frequentemente lida com conflitos de interesse entre a necessidade de coleta de dados pela organização e o direito à privacidade dos titulares. A capacidade de mediar e negociar soluções é essencial para balancear essas necessidades de maneira adequada e em conformidade com a lei.
- **Liderança e Influência:** Embora o DPO não seja necessariamente um líder formal na hierarquia da empresa, ele deve ser capaz de influenciar a cultura organizacional em direção à privacidade e à conformidade. Para isso, é importante exercer liderança e inspirar confiança nas práticas de proteção de dados.
- **Tomada de Decisão Ética:** O DPO deve possuir um forte senso de ética, uma vez que lida com decisões que impactam diretamente os direitos dos titulares de dados. Isso inclui avaliar a legitimidade do tratamento de dados e fazer recomen-

dações que priorizem a proteção dos direitos dos indivíduos.

- **Empatia:** Compreender o ponto de vista dos titulares de dados e reconhecer a importância da privacidade e da segurança de suas informações pessoais ajuda o DPO a desenvolver políticas mais centradas no ser humano e a criar um ambiente de confiança entre a empresa e seus clientes.
- **Gestão de Conflitos:** Assegurar que as questões e reclamações dos titulares sejam tratadas de maneira justa e eficaz exige que o DPO tenha uma abordagem equilibrada na gestão de conflitos, garantindo que todos os lados sejam ouvidos e que a resolução seja transparente.

4.3. Equilíbrio entre as competências

O equilíbrio entre competências técnicas e comportamentais é fundamental para o sucesso do DPO. Um profissional com forte base técnica, mas sem habilidades de comunicação, pode ter dificuldades em explicar a importância das políticas de proteção de dados para a alta administração ou em engajar os funcionários na conformidade. Da mesma forma, um DPO com excelentes habilidades comportamentais, mas sem conhecimento técnico adequado, terá dificuldades em implementar medidas efetivas de proteção e segurança dos dados.

O DPO deve ser visto como uma ponte entre o setor técnico, a gestão estratégica e o público em geral. As competências técnicas permitem que ele compreenda e implemente as normas e práticas de proteção de dados, enquanto as competências comportamentais garantem que ele seja capaz de comunicar, liderar e envolver todas as partes interessadas no cumprimento das exigências legais e na promoção de uma cultura de privacidade dentro da organização.

A combinação dessas competências é o que faz do DPO um profissional indispensável, capaz de garantir que a empresa não apenas atenda aos requisitos regulatórios, mas também crie valor através de uma abordagem ética e responsável no tratamento de dados pessoais.

5. CONTRATAÇÃO – TERCERIZAÇÃO OU INTERNO

A LGPD e a Resolução CD/ANPD nº 18 permitem flexibilidade na designação do DPO, seja por meio de contratação interna ou terceirização.

- **Terceirização:** É viável e comum, especialmente para organizações que não necessitam de um DPO em tempo integral. Contudo, o contrato deve assegurar autonomia ao profissional.
- **Interno:** É importante garantir que o colaborador designado tenha tempo e recursos para desempenhar suas funções, evitando conflitos de interesse ou acúmulo de funções.

A nomeação do Encarregado de Dados (DPO) é uma obrigação legal estabelecida pela LGPD, salvo exceções previamente definidas. Cabe ao empresário ou à organização decidir como atender a essa exigência. Caso a nomeação de um DPO seja obrigatória, o empresário pode optar por contratar um profissional externo especializado em proteção de dados ou designar um colaborador interno para assumir essa função. A escolha dependerá das necessidades, recursos e estrutura organizacional da empresa.

A LGPD não estabelece uma forma específica de contratação do DPO. Ela menciona apenas a necessidade de designar um encarregado pelo tratamento de dados pessoais, sem impor uma exigência específica de conhecimento ou formação para o profissional, mas atribuindo a ele determinadas responsabilidades relacionadas à proteção de dados.

Isso proporciona às empresas certa flexibilidade na forma de cumprir com essa obrigação, seja designando um funcionário interno para a função, ou contratando um especialista externo em proteção de dados. Em organizações menores, onde não é necessária a designação de um DPO em tempo integral, é possível que um colaborador desempenhe o papel de DPO em conjunto com outras funções, desde que sua independência e eficácia sejam mantidas.

Se um colaborador interno for designado como DPO, é essencial garantir que ele tenha a formação adequada e o tempo necessário para cumprir as responsabilidades do cargo, sem acumular funções que possam comprometer sua independência. Um dos principais desafios é evitar conflitos de interesses, que são comuns quando o colaborador acumula responsabilidades adicionais que podem impactar sua capacidade de ser imparcial. Os potenciais conflitos de interesse incluem:

1. Interesses Pessoais ou Financeiros: Se o Encarregado de Dados tiver interesses financeiros ou pessoais que possam ser afetados pelas decisões relacionadas à proteção de dados, isso poderá criar um conflito.

2. Relacionamento Próximo com a Administração: Relações estreitas com a administração ou partes interessadas podem comprometer a capacidade do DPO de agir de forma independente.

3. Posição em Departamentos de Marketing ou Vendas: Caso o DPO atue também em áreas como marketing ou vendas, pode haver conflito de interesse entre os objetivos comerciais e a proteção de dados.

4. Emprego Simultâneo em Funções Incompatíveis: Caso o DPO possua outro emprego ou responsabilidades que entrem em conflito com suas obrigações como Encarregado de proteção de dados.

5. Participação em Decisões que Afetam a Privacidade: Se o DPO estiver envolvido diretamente em decisões que afetam a privacidade dos dados, ele pode perder a capacidade de auditar essas mesmas decisões com imparcialidade.

Para evitar esses conflitos, é fundamental que o DPO opere com independência e imparcialidade, tomando decisões que considerem exclusivamente o melhor interesse dos titulares dos dados. Um exemplo disso pode ser visto em um caso ocorrido na Bélgica, onde a Autoridade de Proteção de Dados multou uma operadora de telefonia em 50 mil euros, após identificar um conflito de interesse do DPO que também exercia atividades na área de compliance.

Além disso, para muitas empresas, contratar um DPO interno em tempo integral pode ser financeiramente desafiador. Da mesma forma, designar um colaborador que já faça parte do quadro de funcionários pode trazer problemas trabalhistas, como acúmulo de função ou desvio de função.

Por outro lado, a terceirização do papel de DPO pode ser uma solução vantajosa, especialmente para organizações que não necessitam de um encarregado em tempo integral ou que desejam evitar potenciais conflitos de interesse. Ao terceirizar o DPO, a empresa pode se beneficiar de:

1. Expertise: Empresas de terceirização de serviços de DPO geralmente possuem profissionais altamente especializados e experientes em questões de privacidade de dados, trazendo um alto nível de conhecimento e expertise.

2. Redução de Conflitos de Interesse: Um DPO externo não está diretamente envolvido nas operações diárias da organização, o que reduz as chances de conflitos de interesse.

3. Flexibilidade: A terceirização oferece flexibilidade, permitindo que a empresa ajuste os serviços de acordo com suas necessidades específicas. Isso é especialmente útil em empresas que enfrentam flutuações na carga de trabalho relacionada à privacidade de dados.

Porém, mesmo ao terceirizar o papel do DPO, a empresa ainda é plenamente responsável pelo cumprimento de todas as obrigações legais e regulatórias relacionadas à proteção de dados. A escolha entre terceirizar ou designar um colaborador interno como DPO dependerá das necessidades específicas da empresa, sua estrutura organizacional e o escopo de suas operações.

Em resumo, a nomeação do DPO é uma consideração importante no contexto da conformidade com a privacidade de dados. A escolha entre contratar externamente ou designar um colaborador interno depende das circunstâncias específicas da organização, mas deve sempre garantir que o DPO tenha as qualificações e os recursos necessários para cumprir suas responsabilidades de maneira eficaz e independente.

6. DIFERENÇA ENTRE ACÚMULO E DESVIO DE FUNÇÃO DO ENCARREGADO DE DADOS CONFORME A CLT

De acordo com a Consolidação das Leis do Trabalho (CLT), o acúmulo de funções é uma situação em que um empregado é obrigado a desempenhar atividades para as quais não foi contratado originalmente, sem receber a devida contraprestação financeira por essas responsabilidades adicionais.

No sistema legal trabalhista brasileiro, não se adota a contraprestação por cada serviço específico. O parágrafo único do artigo 456 da CLT menciona que todas as tarefas desempenhadas pelo empregado, desde que dentro de sua jornada de trabalho e sem exigir maior capacitação técnica ou intelectual, são consideradas parte das atribuições do colaborador. Assim, a inexistência de cláusula expressa no contrato de trabalho pode obrigar o empregado a atuar em todo e qualquer serviço compatível com sua condição pessoal, desde que conciliável com a natureza da atividade contratada.

De acordo com o princípio do “jus variandi”, previsto no artigo 2º da CLT, o empregador tem o direito de modificar as condições de trabalho, desde que essas mudanças não resultem em prejuízo direto ao empregado e não configurem alterações substanciais no contrato de trabalho. O “jus variandi” permite ao empregador fazer ajustes razoáveis nas condições de trabalho para atender às necessidades do empreendimento, incluindo a atribuição de novas tarefas, desde que essas não impliquem em uma mudança significativa no escopo do trabalho acordado inicialmente.

Entretanto, é importante notar que há limites para o exercício do “jus variandi”. O empregador não pode agir de maneira arbitrária ou abusiva ao fazer alterações nas condições de trabalho, e tais mudanças devem respeitar os limites estabelecidos pela legislação trabalhista. Mudanças que resultem em prejuízos significativos para o empregado podem ser consideradas como desrespeito ao contrato de trabalho.

Vale transcrever as palavras do Ministro do Tribunal Superior do Trabalho Maurício Godinho Delgado:

“Haverá acúmulo de funções quando o empregado, originalmente contratado para o exercício de uma determinada função, passa a exercer, conjuntamente com esta, atribuições que não são compatíveis com a função contratada, que se referem a uma outra função, ou seja, não é o simples acréscimo de atribuições que demonstra o acúmulo de funções, pois estas atribuições novas podem se referir à função originalmente contratada. Ou seja, caso não haja prova da função exercida ou não exista cláusula contratual expressa a esse respeito, entender-se-á que o empregado se obrigou a todo e qualquer serviço compatível com a sua condição pessoal.” (2011, p. 968)

Resta claro, portanto, que no acúmulo de funções, o empregado realiza a atividade para a qual foi contratado juntamente com outra análoga. Diferente disso, o desvio de função ocorre quando o empregado é obrigado a realizar atividades substancialmente diversas daquelas para as quais foi inicialmente contratado, existindo uma demonstração clara de que as funções cumuladas são independentes e distintas.

A caracterização do desvio de função não depende necessariamente da independência e diversidade absoluta das funções cumuladas, mas sim da discrepância significativa entre as atribuições originais para as quais o empregado foi contratado e as tarefas efetivamente desempenhadas. Em outras palavras, o desvio de função ocorre quando o trabalhador é obrigado a realizar atividades que não guardam relação direta com aquelas definidas em seu contrato inicial, impactando sua remuneração e seus direitos trabalhistas.

Levando em consideração as questões trabalhistas acima mencionadas, é importante que o controlador, ao designar um colaborador interno como DPO, analise as possíveis consequências dos direitos laborais relativos ao vínculo empregatício, tendo em vista que este tema ainda não está consolidado no ordenamento jurídico brasileiro. Um DPO designado internamente pode enfrentar situações de acúmulo ou desvio de funções, caso não sejam tomadas as devidas precauções.

Para que haja maior segurança na indicação de um colaborador interno para o exercício da função de Encarregado de Dados, o controlador deve observar dois importantes quesitos:

1. Ausência de Conflito de Interesse: É essencial que não haja conflito de interesse entre a função de DPO e outras atribuídas ao colaborador. Isso garante que o DPO possa tomar decisões de forma imparcial e focada no cumprimento das obrigações relativas à proteção de dados.

2. Conexão e Compatibilidade das Funções: Deve existir uma compatibilidade e conciliação entre as funções de DPO e a função original do colaborador. Isso evita que as tarefas adicionais atribuídas resultem em desvio de função, garantindo que as atividades sejam adequadas à natureza do contrato original do trabalhador.

Considerando que a designação de um colaborador interno como DPO pode implicar em riscos trabalhistas significativos, o controlador deve avaliar cuidadosamente a distribuição de tarefas e responsabilidades para evitar problemas legais futuros e assegurar a integridade da função de DPO no contexto da proteção de dados e das relações de trabalho.

7. CONSIDERAÇÕES FINAIS

A contratação do Encarregado de Dados (DPO) é uma tarefa fundamental para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) e assegurar boas práticas de privacidade dentro das organizações. O texto discute de forma abrangente as responsabilidades, qualificações e formas de contratação do DPO, bem como as peculiaridades de sua atuação em diferentes setores. O DPO não é apenas uma exigência regulatória; é um agente estratégico na promoção de uma cultura de privacidade e na minimização dos riscos legais e reputacionais para as empresas.

A LGPD estabelece um papel dinâmico para o DPO, que envolve não apenas o cumprimento de obrigações legais, mas também

a mediação de conflitos, a conscientização interna e o assessoramento estratégico à alta administração. Esse profissional precisa ter uma combinação única de competências técnicas e comportamentais, balanceando um conhecimento profundo da legislação com habilidades de comunicação e liderança.

Outro ponto fundamental é a discussão sobre a terceirização versus a indicação interna de um colaborador como DPO. Cada opção traz desafios específicos, como potenciais conflitos de interesse ou riscos trabalhistas decorrentes do acúmulo ou desvio de funções. Assim, é essencial que as empresas escolham o modelo que melhor se adapta às suas necessidades e garantam a independência e a eficácia do DPO, mantendo uma gestão proativa da privacidade.

A capacitação contínua também se mostra crucial devido à evolução constante da legislação e das tecnologias, especialmente em setores que lidam com grandes volumes de dados sensíveis. Portanto, investir no desenvolvimento profissional do DPO e assegurar uma infraestrutura de governança em privacidade são estratégias indispensáveis para garantir a conformidade e o diferencial competitivo das organizações no mercado atual.

REFERÊNCIAS

Autoridade Nacional de Proteção de Dados (ANPD) Resoluções e orientações sobre a LGPD. Disponível em: <https://www.gov.br/anpd>.

BRASIL. Consolidação das Leis do Trabalho (CLT) Disponível em: <https://www.planalto.gov.br>.

EXIN Certification for DPOs Certificação específica para encarregados de proteção de dados. Disponível em: <https://www.exin.com>.

General Data Protection Regulation (GDPR) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu>.

IAPP (International Association of Privacy Professionals) Informações sobre certificações como CIPP e CIPM. Disponível em: <https://iapp.org>.

ISO/IEC 27701:2019 Padrão internacional para sistemas de gestão de privacidade. Disponível em: <https://www.iso.org>.

Lei Geral de Proteção de Dados (LGPD) Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <https://www.planalto.gov.br>.

MENDES, Laura Schertel; DONEDA, Danilo. *Lei Geral de Proteção de Dados Pessoais Comentada*. 2ª edição. São Paulo: Thomson Reuters, 2021.

REZENDE, Lilian Matsuura; CAPUTO, Luciano Augusto de Faria. *LGPD: Teoria e Prática*. São Paulo: Saraiva Educação, 2020.

SOARES, Patricia Peck Pinheiro. *Direito Digital Aplicado 5.0*. São Paulo: Saraiva Educação, 2021.

EDUCAÇÃO DIGITAL E CONSCIENTIZAÇÃO: FORMANDO UMA SOCIEDADE PRONTA PARA A LGPD

Dayane Karine de Sousa Mendonça¹

Daphne Kalyva de Almeida Rosa²

INTRODUÇÃO

A Lei Geral de Proteção de Dados trouxe à sociedade brasileira o debate mais aprofundado sobre temas diretamente conectados com a proteção dos direitos fundamentais de liberdade e de privacidade, assim como também sobre o livre desenvolvimento da personalidade, dentro e fora dos meios digitais.

O fenômeno da inclusão digital foi acelerado diante do cenário da pandemia de COVID-19 e inúmeros incidentes, violações de dados e à privacidade também tornaram-se evidentes e problemáticos, principalmente por romperem limites geográficos, etários e de classes sociais.

Embora digitalmente conectados, diversos titulares de dados pessoais não possuem acesso à educação digital, o que os coloca em situação de vulnerabilidade frente aos riscos da sociedade da informação, dificultando sua atuação preventiva contra incidentes e violações. No Brasil, o aumento de incidentes e violações de dados e à privacidade demandou leis próprias. A Lei dos Crimes Cibernéticos, n.º 12.737/2012, dispôs sobre a tipificação criminal de delitos informáticos e incluiu arti-

1 Pós-graduada com MBA para Data Protection Officer - DPO (LGPD & GDPR) pelo IESB, graduada em Direito pela UNIP, advogada atuante em privacidade e proteção de dados pessoais. Brasília/DF - Brasil.

2 Pós graduada em Direito Digital e proteção de dados pelo EBRADI, graduada em Direito pelo IESB, advogada atuante em privacidade e proteção de dados pessoais, pesquisadora em criptoeconomia, voluntária da cidadania na Defensoria Pública do Distrito Federal.

gos ao Código Penal. Posteriormente, surgiu o Marco Civil da Internet - Lei n.º 12.965/ 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. E após, veio a Lei Geral de Proteção de Dados – Lei n.º 13.709/2018, que dispôs sobre a Proteção de Dados Pessoais.

A Lei Geral de Proteção de Dados protege direitos considerados fundamentais. Reflete-se para a maximização do objetivo que pode ser alcançado, quando se inclui o fomento à educação digital na sociedade de risco.³ A Lei fomenta, em teoria, o debate sobre todos os atores envolvidos para mitigar os riscos à privacidade e à proteção de dados. A aplicabilidade da lei não deve ser limitada à fiscalização das pessoas jurídicas de direito público ou privado, mas integrativa na educação digital aos titulares de dados pessoais.

A educação digital deve acompanhar o desenvolvimento da inclusão digital, como forma de prevenção à insegurança dos dados pessoais, colocando o titular de dados pessoais em papel ativo na sociedade de risco. O titular de dados pessoais deve ser consciente da sua responsabilidade e de sua possibilidade de prevenção aos incidentes e violações envolvendo seus dados pessoais.

A educação digital possibilita a inclusão dos limites legais e éticos na conduta digital, além da conscientização do papel do titular de dados no combate a incidentes e violações de dados pessoais e à privacidade.

O estudo de caso demonstra que a inclusão digital, sem a devida educação digital, deixa titulares de dados pessoais em posição de vulnerabilidade frente às ameaças maliciosas que podem ser encontradas nas adjacências das tecnologias que se desenvolvem na sociedade da informação.

3 Sociedade de risco para Ulrich Beck é “marcada fundamentalmente por uma característica: pela impossibilidade de imputar externamente as situações de perigo.” Livro: Sociedade de Risco. Rumo a uma outra modernidade. Tradução: Sebastião Nascimento. Editora 34. São Paulo. p. 274. Disponível em <https://edisciplinas.usp.br/pluginfile.php/5299999/mod_resource/content/1/Ulrich%20Beck%20-%20Sociedade%20de%20risco_%20Rumo%20a%20uma%20Outra%20Modernidade.pdf>

1. OS DESAFIOS DA PRIVACIDADE DIGITAL NA SOCIEDADE MODERNA

Na Era Digital, a privacidade é constantemente antagonizada. Informações pessoais são ativos altamente cobiçados e lucrativos, tanto no mercado lícito e ilícito. Diante desse paradigma, batalhas criptográficas são impulsionadas, assim como o debate sobre a regulação ao tema.

A tecnologia tem possibilitado o desenvolvimento social e econômico, além de processos de comunicação mais ágeis e eficientes. Isso porque a informação possui um papel preponderante na sociedade atual, criando o “conhecimento”.

A tendência é que as tecnologias envolvidas na segurança de dados pessoais se desenvolvam de forma acelerada na sociedade da informação. Observa-se a característica da existência crescente de dados, sendo transmitidos de forma cada vez mais rápida.

A Emenda Constitucional nº 115, de 2022, acrescentou o inciso LXXIX ao artigo 5º da Constituição Federal, reconhecendo expressamente a proteção de dados pessoais — inclusive nos meios digitais — como um direito fundamental.

Conjuntamente às mudanças trazidas pelas tecnologias, desenvolve-se o sistema de engenharia social, que paralelamente atua na sociedade de risco onde as estratégias utilizadas por criminosos contra as vítimas para obter vantagens em sistemas eletrônicos ficam cada vez mais sofisticadas.

No 16º Relatório Anual da Verizon Business de Investigações de Violação de Dados (DBIR 2023)⁴ extrai-se que 74% do total de violações ocorrem pelo elemento humano e por meio de engenharia social, mesmo com as empresas aumentando a formação em protocolos de cibersegurança.

4 16º Relatório Anual da Verizon Business de Investigações de Violação de Dados (DBIR 2023) disponível em <<https://www.verizon.com/business/resources/T423/reports/2023-data-breach-investigations-report-dbir.pdf>>

2. EDUCAÇÃO DIGITAL COMO FERRAMENTA PARA A CONSCIENTIZAÇÃO

Considerando que grande parte das violações de dados decorre de falhas humanas, a inclusão digital, enquanto fenômeno progressivo, deve ser acompanhada de educação digital voltada para o desenvolvimento ético diante da tecnologia — e não se limitar apenas à capacidade de uso e interação com essas ferramentas.

A pandemia da COVID 19 reduziu inúmeros serviços, negócios e relações sociais que ocorriam de forma presencial a aplicativos com funcionalidades atrativas. Inúmeras agências bancárias fecharam e as pessoas passaram a utilizar os aplicativos dos bancos, que inclusive dispunham de mais funcionalidades que os terminais de autoatendimento. Muitas profissões migraram para trabalhos remotos; a telemedicina tornou-se acessível; o mercado na internet se desenvolveu aceleradamente para atender ávidos consumidores que viam na internet a possibilidade de um bom preço e uma boa variedade à sua disposição. Inúmeras pessoas durante a quarentena viram no mundo digital uma forma de se reinventar. O uso dos meios digitais ofereceu inúmeras possibilidades à sociedade, além da informação e também do (des)serviço da desinformação.

“A atração que as novas tecnologias exercem sobre todos — de formuladores de políticas e implementadores de infraestrutura e aplicações de tecnologias de informação e comunicação até usuários de todas as classes e idades — pode levar a uma visão perigosamente reducionista acerca do papel da educação na sociedade da informação, enfatizando a capacitação tecnológica em detrimento de aspectos mais relevantes.”⁵

A educação digital constitui um instrumento essencial para a formação de condutas éticas no ambiente virtual, ao mesmo tempo em que contribui para o fortalecimento da segurança da informação. O desenvolvimento de uma postura digital segura pressupõe a incorporação

5 TAKAHASHI, Tadao (org.). Sociedade da informação no Brasil: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000, p. 45.

de conteúdos voltados à análise crítica e à compreensão das técnicas de engenharia social, frequentemente utilizadas como vetor de ataques cibernéticos por meio da exploração de fragilidades comportamentais.

“A engenharia social é frequentemente classificada como um truque de confiança, e os truques de confiança dependem de ganhar a sua confiança e depois abusar dela. Enfatizamos sobre o quão importante é não confiar cegamente nas pessoas no meio virtual (e-mails, mensagens, perfis falsos nas redes sociais ou até mesmo por chamadas telefônica).”⁶

A criptografia, embora essencial, não é suficiente por si só para garantir a proteção da privacidade dos dados pessoais. É igualmente necessário conscientizar o titular sobre sua própria atuação, especialmente diante de técnicas de engenharia social que exploram o fator humano. A lei assegura direitos fundamentais como liberdade, intimidade e privacidade, mas sua efetividade depende da participação ativa e informada do titular.

3. DEVER DE PROTEÇÃO DE CRIANÇAS E ADOLESCENTES NA WEB

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação⁷ produz pesquisas que servem de indicadores sobre a Internet no Brasil e contribuem para a elaboração de políticas públicas sobre tecnologias. Em pesquisa recente, no ano de 2023, identificou que 68% das crianças entre 9 e 10 anos possuem perfil em plataforma digital, e 36% dos usuários de internet de 9 a 17 anos utilizam o Instagram. E, ainda, 78% dos usuários de internet de 9 a 17 anos possuem perfil no WhatsApp.

Os dados revelam muito sobre a atual sociedade, e sobre como lidamos com a informação. Extrai-se da pesquisa que 40% dos usuários

6 O Que você precisa saber sobre engenharia social para sua proteção virtual Disponível em < <https://www.security.ufrj.br/dicas/engenhariasocial/>> Acesso em 25/12/2024.

7 https://www.cetic.br/media/analises/tic_kids_online_brasil_2023_principais_resultados.pdf

de Internet de 11 a 17 anos concordam que o primeiro resultado de uma pesquisa na Internet é sempre a melhor fonte de informação. Revelam ainda que 73% concordam que quando pessoas jovens veem propagandas na Internet ficam chateadas por não poderem comprar um produto.

A conclusão do estudo serve de alerta ao revelar que 7% das crianças entre 11 e 12 anos já receberam mensagens de conteúdo sexual pela internet, enquanto 9% dos adolescentes entre 13 e 14 anos relataram ter sido solicitados a enviar fotos ou vídeos nus. Entre os adolescentes de 15 a 17 anos, esse índice sobe para 26%.

No recorte etário de 9 a 14 anos, a pesquisa aponta preferência pelas plataformas YouTube e, em seguida, TikTok. A partir dos 13 anos, observa-se um aumento significativo no uso do Instagram, alcançando 62% dos adolescentes de 15 a 17 anos.

Diante dos dados extraídos, revela-se crescente a participação de crianças e adolescentes na internet, e inúmeras são as inseguranças que emergem junto aos pais ou responsáveis. O Marco Civil da Internet possibilitou o incentivo para as boas práticas do uso da rede, de forma que os pais podem e devem fiscalizar e exercer o controle parental sobre o conteúdo que seus filhos acessam.

“Os diferentes estágios da vida exigem cuidados diferenciados quanto à educação e restrição de exposição aos riscos. De tal monta, ao entrar para a adolescência, um indivíduo já busca maior independência e autonomia quanto às tarefas do dia a dia, ficando, assim, mais sujeito a influências externas. Certamente no estágio da adolescência as alterações metabólicas levam ao afloramento da sexualidade e à curiosidade quanto às práticas neste sentido. O que se quer, desta forma, é chamar a atenção para o fato de que crianças e adolescentes são vítimas diferentes, expostas a riscos diversos e de modos diversos, na rede mundial de computadores, especialmente no que concerne à suscetibilidade quanto à criminalidade.”⁸

Embora crianças e adolescentes tenham mais facilidade do que os adultos para lidar com a tecnologia, essa habilidade não deve ser

8 Alice Bianchini, Ivan Luis Marques Da Silva, Luiz Flavio Gomes, Spencer Toth Sydow. Col. Saberes Monográficos: Crimes Informáticos E Suas Vítimas (locais do kindle 3689-3695). Saraiva. Edição do Kindle. p. 14

confundida com educação digital ou senso de responsabilidade no uso dessas ferramentas. Decorre que, tanto a população mais jovem quanto a população com mais idade estão na condição de hipervulnerabilidade. Eis que a educação digital transcende a capacidade de manuseio da tecnologia.

A educação digital promove o debate sobre limites éticos, comportamentais e os riscos associados ao uso da internet. Embora muitos jovens demonstrem habilidade no uso de tecnologias, frequentemente carecem de consciência digital, o que os torna plenamente inseridos, porém mais expostos e hipervulneráveis a ataques de engenharia social. Já os adultos mais velhos, por sua vez, enfrentam vulnerabilidades decorrentes da baixa familiaridade com as ferramentas digitais, o que também os coloca em condição de hipervulnerabilidade frente a essas ameaças.

“Muitos incidentes de segurança têm origem em uma “engenharia social” que explora vulnerabilidades do comportamento humano.”⁹

Conclui-se que a educação digital deve ser universal, inclusiva, começar dentro de casa, ser desenvolvida nas escolas, comunidades e também nos ambientes profissionais. A criança e o adolescente não possuem plena capacidade de compreensão, discernimento e entendimento necessário acerca dos dados que porventura estejam compartilhando, razão pela qual a lei exige a ação dos pais ou responsáveis. O dispositivo legal enseja como regra geral que a coleta, tratamento e compartilhamento de dados pessoais de crianças e de adolescentes deve ser a favor do seu melhor interesse e com o consentimento específico e em destaque dado por pelo menos um dos pais ou do responsável legal, salvo exceções legalmente previstas.

9 SEGURANÇA DIGITAL: uma análise de gestão de risco em empresas brasileiras disponível em <https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf>

Ainda que a Lei Geral de Proteção de Dados deixe claro que o acesso de crianças e adolescentes a jogos não deva ser condicionado ao fornecimento de seus dados pessoais, não é incomum ainda observarmos que continuam condicionando, exigindo de crianças e adolescentes o fornecimento de seus dados.

É inadmissível que ainda exista a utilização de técnicas de incentivos para que crianças e adolescentes forneçam seus dados pessoais. Principalmente quando as informações referentes à coleta e tratamento de dados ainda não estão disponibilizadas de maneira simples, clara e acessível - embora deversem, por previsão legal. Devem ser consideradas ainda as características sensoriais, intelectuais, mentais, físico-motoras, perceptivas, do público alvo.

“A internet permitiu o maior acesso à informação por parte da sociedade. Recentemente, a ONU (Organização das Nações Unidas) declarou que o acesso à internet é um direito humano, uma vez que ela permite uma troca de informações de forma colaborativa, isto é, o indivíduo não só mais recebe informações, ele é parte na disseminação de conteúdo, sendo a internet um veículo de expressão de suas opiniões sobre os mais variados assuntos.”¹⁰

A Lei Geral de Proteção de Dados também promove ações educativas aos controladores e operadores, pelo tratamento de dados pessoais, como regras de boas práticas e de governança. Sua aplicabilidade não deve distanciar titulares propriamente ditos, das ações educativas, que os possibilitem à segurança de seus dados pessoais. A educação digital é fundamental para o desenvolvimento dos limites éticos e da consciência sobre os dados pessoais pelo titular.

10 Martins, Murilo. A Proteção Integral da Criança e do Adolescente No Marco Civil da Internet: A Tutela nos Espaços Virtuais <<https://www.migalhas.com.br/arquivos/2015/6/art20150602-07.pdf>> Acesso em 1/7/2025.

4. DEVER DE EDUCAÇÃO EXPRESSO NO MARCO CIVIL DA INTERNET

O marco civil da internet expressa com clareza que o Estado possui o dever constitucional de prestação da educação e capacitação, para o uso seguro, consciente e responsável da internet.¹¹

A lei dispõe que as iniciativas públicas de fomento à cultura digital devem promover a inclusão digital e ainda buscar reduzir as desigualdades no acesso às tecnologias da informação e comunicação, assim como no seu uso.¹²

Cabe ao Estado e à sociedade, na totalidade, a promoção da educação digital para o desenvolvimento da consciência no ambiente online, para a definição de boas práticas no fenômeno da inclusão digital.

Algumas pesquisas, novamente, são alarmantes: “Quase metade (46%) dos adolescentes entre os 13 e os 17 anos foram intimidados ou assediados online, sendo a aparência física vista como uma razão relativamente comum. (Pew Research, 15 de dezembro de 2022). Ainda:

- Os jovens (10-16 anos) que acederam ou compartilharam conteúdos sexuais ou imagens de cyberbullying ou violência tiveram um risco até 50% maior de pensamentos suicidas. (Rede JAMA aberta, 20 de setembro de 2021).
- Um inquérito realizado com mais de 6.000 jovens entre os 10 e os 18 anos, entre Junho e Agosto do ano passado, concluiu que cerca de 50% das crianças tinham sofrido pelo menos um tipo de cyberbullying durante a sua vida, de acordo

11 Lei Nº 12.965/2014 “Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.”

12 Lei Nº 12.965/2014 “Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem: I - promover a inclusão digital; II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e III - fomentar a produção e circulação de conteúdo nacional.”

com um relatório publicado em fevereiro pelo Grupo Conjunto da Comissão Europeia. Nos 11 países europeus incluídos no relatório, 44% das crianças que foram vítimas de cyberbullying antes do confinamento afirmaram que isso aconteceu ainda mais durante o confinamento. (fevereiro de 2021)

- Houve um aumento de 70% na quantidade de bullying/ discurso de ódio entre adolescentes e crianças no mês desde o início do bloqueio da Covid. (DigitalTrends.com , 8 de abril de 2020)
- Os professores relatam que o cyberbullying é a principal preocupação de segurança nas salas de aula, de acordo com uma pesquisa realizada pelo Google em janeiro de 2019.
- Um em cada três jovens em 30 países disse ter sido vítima de bullying online, com um em cada cinco relatando ter faltado à escola devido ao cyberbullying e à violência, numa nova sondagem divulgada pela UNICEF e pelo Representante Especial do Secretário-Geral da ONU (RESG) sobre Violência contra Crianças. Disponível em “<https://enough.org/stats_cyberbullying>” Acesso em 3/7/2025.

5. A LEI 14.533/2023 E O ESTABELECIMENTO DA POLÍTICA NACIONAL DE EDUCAÇÃO DIGITAL NO BRASIL

A Educação Digital emerge como uma necessidade presente no contexto contemporâneo, onde a sociedade está cada vez mais interconectada e dependente da tecnologia. A Lei 14.533/2023, ao instituir a Política Nacional de Educação Digital, visa a proporcionar diretrizes claras para a integração efetiva da educação digital no sistema educacional brasileiro.

A legislação busca garantir que a Educação Digital seja acessível a todos, independentemente de idade, classe social ou localização geográfica. Isso implica na criação de programas inclusivos, promovendo o acesso equitativo a recursos digitais e eliminando barreiras que possam marginalizar grupos específicos.

Os principais objetivos e princípios da Política Nacional de Educação Digital trazidos na lei são o fomento da inclusão digital, o desenvolvimento de habilidades críticas no ambiente digital e a promoção da cidadania digital responsável, visto que esta legislação busca garantir que todos os segmentos da sociedade tenham acesso igualitário às ferramentas digitais, reduzindo, assim, a chamada “lacuna digital”. Isso implica em iniciativas que promovam o acesso a dispositivos e conectividade, assegurando a participação de todos na sociedade digital.

Acontece que a Educação Digital não se limita, por exemplo, ao uso técnico de dispositivos, mas inclui o desenvolvimento de habilidades críticas, como pensamento analítico, discernimento digital, avaliação de fontes, e princípios éticos, morais e de segurança. Essas competências são essenciais para formar cidadãos capazes de tomar decisões informadas no ambiente digital.

A lei marca um passo significativo na resposta do Estado aos desafios impostos pela era digital. No entanto, uma análise crítica revela uma potencial fragilidade: a lei parece privilegiar a inclusão digital em detrimento de uma abordagem mais robusta e abrangente da educação digital.

O recente dispositivo legal, ao enfatizar fortemente a inclusão digital, pode inadvertidamente relegar a educação digital a um segundo plano. Incluir o acesso à tecnologia não é o mesmo que fornecer as ferramentas cognitivas necessárias para que os indivíduos compreendam e naveguem no ciberespaço de maneira ética e segura.

A verdadeira educação digital vai além do simples acesso e uso de tecnologia. Ela deve abranger questões éticas, morais e de segurança digital. É imperativo que a sociedade como um todo, o que inclui os estudantes, compreendam não apenas como usar dispositivos e aplicativos, mas também os impactos de suas ações no ambiente digital, incluindo a responsabilidade por conteúdo, respeito à privacidade e reconhecimento de limites éticos.

A separação entre inclusão digital e educação digital pode resultar em uma superficialidade na formação dos jovens em idade esco-

lar. É crucial que a educação digital seja integrada de maneira abrangente, proporcionando uma compreensão aprofundada das implicações éticas e sociais da tecnologia.

Embora a inclusão digital seja, sem dúvida, uma meta digna, é fundamental reconhecer que ela não é suficiente para moldar cidadãos digitais responsáveis. A educação digital não deve ser eclipsada pela necessidade de fornecer acesso às tecnologias digitais. Em vez disso, ambas as abordagens devem ser integradas de maneira equilibrada, garantindo que os estudantes não apenas saibam como usar a tecnologia, mas compreendam plenamente seu impacto na sociedade e estejam equipados com as ferramentas éticas necessárias para navegar no ambiente digital de maneira responsável, entendendo as implicações legais de seus atos no ambiente online bem como os limites de privacidade e proteção de dados e a segurança cibernética, para que o indivíduo reconheça seu papel como agente de bem estar social mesmo que no ambiente digital.

Sendo assim, Patrícia Peck acrescenta:

“Acreditamos, portanto, que a educação digital deve ser promovida simultaneamente à inclusão digital dos usuários, seja dos indivíduos que estão tendo o primeiro contato com as máquinas somente no ambiente de trabalho, seja da nova geração que já nasceu dentro de uma sociedade totalmente informatizada. Este último grupo necessita de orientação especial, já que crianças e adolescentes estão passando pelo amadurecimento de seus conceitos éticos, morais e de cidadania. É extremamente necessário que pais e escolas invistam na educação digital de seus filhos. Já não basta apenas orientá-los a não abrir a porta de casa para estranhos. Eles precisam saber também que não é seguro abrir e-mails de estranhos”¹³

13 Garrido, Patricia Peck. Direito Digital (p. 553). Saraiva Jur. Edição do Kindle.

6. CIBERCRIMES NA ERA DIGITAL: DESAFIOS EMERGENTES E SUA RELEVÂNCIA PARA A SALVAGUARDA DE DADOS PESSOAIS

A estabilidade da Sociedade da informação, com seus tecnológicos sistemas de segurança, é frequentemente abalada por suas vulnerabilidades, compostos de tecnologias, má intenção humana e complexas estratégias de engenharia social.

É notável que a evolução tecnológica tenha transformado o modo como a sociedade passou a interagir. E, dentro desse contexto, a educação digital possibilita o preparo à consciência digital, criando uma participação consciente e responsável no ambiente digital.

A educação digital é capaz de conscientizar o usuário - e titular de dados pessoais - para as políticas públicas, para a formação da cidadania digital diante das vulnerabilidades digitais, tornando-se preventiva para ciberataques, cyberbullying, phishing, sequestro de servidor, ameaça, calúnia, difamação, injúria, falsa identidade, pornografia de vingança e incidentes envolvendo violações de privacidade e dados.

A engenharia social utilizada pelo agente mal-intencionado pode implicar em múltiplas táticas. O *phishing*, por exemplo, faz parte de um problema muito comum. A engenharia social manipula as emoções da vítima pelo medo, pela urgência ou ainda por uma possibilidade de recompensa para obtenção e acesso de dados sigilosos, como senhas, informações bancárias, números de cartão de crédito, fornecimento de dados pessoais em sites falsos e muitos outros.

Phishing é uma técnica de fraude baseada em engano e manipulação, utilizada para induzir a vítima a fornecer informações ou executar ações prejudiciais. Uma de suas variações é o *scam*, que consiste no envio massivo de e-mails sem um alvo específico. O agente malicioso aguarda que algum destinatário clique em um link ou abra um anexo contaminado, o que resulta na instalação de malwares no dispositivo da vítima. Diferentemente do *scam*, o *spear phishing* é direcionado a alvos específicos e busca enganar a vítima ao se disfarçar como um remetente aparentemente conhecido ou confiável.

Outra forma de *phishing* é o *vishing*, feito por meio de chamada de voz; ou, ainda, o *smishing*, que é feito por meio de texto SMS ou aplicativos de mensagens. A principal diferença entre os dois é o método de contato utilizado com a vítima.

“Os golpes de phishing usam e-mails e sites falsificados como iscas para levar as pessoas a entregar voluntariamente informações confidenciais. Não é surpreendente, portanto, que o termo “phishing” seja comumente usado para descrever essas manobras. Há também uma boa razão para o uso de “ph” no lugar de “f” na grafia do termo. Alguns dos primeiros hackers eram conhecidos como phreaks. Phreaking refere-se à exploração, experimentação e estudo de sistemas de telecomunicações. Phreaks e hackers sempre estiveram intimamente ligados. A grafia “ph” foi usada para vincular golpes de phishing a essas comunidades clandestinas.”¹⁴

A engenharia social pode ser facilmente descrita como um truque de confiança, mas dependem do ganho da confiança do titular de dados pessoais, para depois chegar ao resultado pretendido pelo agente malicioso.

Extraí-se que a educação digital é um instrumento capaz de tornar ativo o usuário titular para contribuir na mitigação dos riscos e prevenir crimes cibernéticos. Muitas vítimas poderiam ter evitado essa condição se tivessem recebido educação digital, e não apenas acesso às tecnologias. A consciência digital as teria protegido contra vulnerabilidades comuns no ambiente online.

A sociedade é capaz de mitigar os riscos, já que a conduta do usuário e titular consciente, quando no papel de “vítima”, pode impedir a concretização do delito. Não raro, observa-se que o perfil das vítimas dos crimes cibernéticos, são crianças e adolescentes, pessoas idosas, pessoas curiosas, ignorantes e sem o discernimento oferecido e necessário pela educação digital.

“Uma vez que os delitos informáticos podem ser tidos como uma nova forma de se praticar velhos delitos – uma nova ferramenta

14 <PHISHING.ORG, History of phishing, disponível em <https://www.phishing.org/history-of-phishing>>

– (delitos informáticos impróprios) ou como ações novas que violam bens jurídicos antigos (delitos informáticos próprios impuros) e/ou valores e bens jurídicos novos (delitos informáticos próprios puros), é fundamental que se aceite que, no meio informático, certas características particulares das vítimas influenciam em sua potencialidade vitimal e na própria criminogênese.”¹⁵

Mundialmente, o tema ganhou destaque com a publicação do ‘Manual sobre prevenção e controle de crimes relacionados com computadores’ das Nações Unidas. No Brasil, a legislação de combate a cibercrimes, embora tenha sofrido recentes atualizações, ainda enfrenta desafios para acompanhar a rápida evolução das condutas ilícitas no ambiente digital. Ainda, com a publicação do Decreto nº 11.856, de 26 de dezembro de 2023, o ordenamento jurídico nacional avançou na tipificação das diversas modalidades de cibercrime. Nesse contexto, reforça-se que a educação digital é um elemento essencial que deve caminhar junto à inclusão digital, atuando de forma decisiva na prevenção, ao reduzir a exposição dos indivíduos e dificultar sua exploração por agentes maliciosos.

7. ESTUDO DE CASO: UM RELATO PESSOAL DE CIBERCRIME - UMA ENTREVISTA REVELADORA NA BUSCA POR CONSCIENTIZAÇÃO E PROTEÇÃO DE DADOS SOB A LGPD.

O relato a seguir detalha a experiência de uma pessoa que vivenciou pessoalmente as ramificações de um cibercrime. Ao mergulhar nas nuances deste incidente, buscamos compreender não apenas os aspectos técnicos do ocorrido, mas também as implicações emocionais, psicológicas e as reflexões geradas em relação à proteção de dados pessoais no contexto da LGPD.

15 Alice Bianchini, Ivan Luis Marques da Silva, Luiz Flavio Gomes, Spencer Toth Sydow. Col. Saberes monográficos: crimes informáticos e suas vítimas (Locais do Kindle 3440-3444). Saraiva. Edição do Kindle.

O depoimento desta vítima (identificada como Bruna a fim de preservar sua identidade) proporciona uma perspectiva íntima dos desafios enfrentados por indivíduos que se tornam alvo de atividades ciber-criminosas. Destaca-se a relevância crucial da conscientização digital e da adoção de medidas preventivas diante dessa realidade. A narrativa é enriquecida com insights detalhados sobre as ações empreendidas durante e após o incidente, as valiosas lições extraídas e o impacto substancial dessa experiência na interpretação da legislação de proteção de dados.

Esta entrevista não apenas ilustra a vulnerabilidade presente na era digital, mas também destaca a resiliência necessária para enfrentar as consequências de um cibercrime. Por meio dessa narrativa, buscamos promover uma compreensão mais profunda das implicações práticas da LGPD e da necessidade contínua de educação digital em nossa sociedade cada vez mais interconectada.

ENTREVISTA

Contextualização: Pode nos contar um pouco sobre si mesma, sua rotina online e o papel da tecnologia em sua vida?

Tenho 23 anos e como uma boa integrante da geração Z, a tecnologia é presente na minha rotina diária. Uso em demasia para o meu trabalho e outros afazeres diários também.

Descrição do Incidente: Pode relatar o incidente de cibercrime do qual foi vítima? Quando e como isso aconteceu?

Fui vítima de um golpe aplicado pelo Instagram no ano de 2022. Eu estava em casa e encontrei a possibilidade do ganho financeiro através de compartilhamento nos stories de uma colega. Entrei em contato com ela e a mesma afirmava que aquilo era certo. Entrei em contato com os bandidos e adquiri uma dívida de R\$ 25.000,00 (vinte e cinco mil reais).

Percepção Inicial: Como você percebeu que estava sendo alvo de um cibercrime? Houve algum sinal de alerta?

Quando entrei nas minhas contas bancárias e estava com o

saldo totalmente zerado e nenhum dinheiro entrou após o período que eles estipularam.

Consequências Pessoais: Quais foram as repercussões imediatas do incidente em sua vida pessoal?

Crises de ansiedade e fiquei me culpando por meses, evitando de até comprar lanche na rua por vergonha, fiquei apática e tive insônia por um tempo também.

Medidas Iniciais: Quais foram as primeiras ações que você tomou ao perceber o cibercrime?

Chamei uma pessoa que pudesse me ajudar e logo depois fui à delegacia, em seguida por meio de uma advogada busquei a reparação via justiça.

Impacto Emocional: como o incidente afetou você emocionalmente? Houve momentos de estresse, ansiedade ou medo?

Sim, os 3. Precisei tomar medicação por algum tempo para conseguir voltar a minha rotina.

Contato com Autoridades: procurou as autoridades ou especialistas em segurança digital? Como foi essa interação?

Sim, procurei a polícia e registrei um boletim de ocorrência. Foi bem ruim, eu estava muito nervosa e sentia que o agente me julgava. Em seguida, busquei reparação da justiça e aguardo decisão.

Recuperação Psicológica: quais estratégias adotou para lidar com o impacto psicológico do cibercrime?

Muito apoio da família e medicação.

Preparo Prévio: Antes do incidente, você se considerava bem informado(a) sobre práticas de segurança online?

Não.

Aprendizados: Quais lições você tirou dessa experiência em termos de conscientização digital?

Não confiar em ninguém e nem em promessas que pareçam muito promissoras sobre dinheiro.

Conselhos para Outros: Com base em sua experiência, que conselhos daria a outras pessoas para evitar ou lidar com cibercrimes?

Não confiar em nenhuma forma de ganho de dinheiro fácil.

A entrevista com uma vítima de cibercrime oferece importantes reflexões sobre os impactos concretos desse tipo de incidente, evidenciando a vulnerabilidade dos indivíduos no ambiente digital — especialmente entre os integrantes da geração Z, cuja rotina é fortemente mediada pela tecnologia. Ela relata ter caído em um golpe aplicado pelo Instagram em 2022, ao buscar oportunidades de ganho financeiro. Este incidente destaca a sofisticação das estratégias utilizadas pelos criminosos, que exploram fortemente a confiança mútua entre usuários.

A identificação tardia do cibercrime é uma característica recorrente, conforme a vítima percebeu a fraude apenas quando seu saldo bancário estava zerado. Isso ressalta a importância de sinais de alerta e educação digital para reconhecimento precoce.

As repercussões imediatas incluem crises de ansiedade, autodepreciação e impactos psicológicos significativos. Esses aspectos evidenciam as implicações emocionais profundas que acompanham as vítimas de cibercrimes. As ações tomadas pela vítima, como buscar ajuda profissional e registrar o boletim de ocorrência, demonstram a necessidade de uma resposta rápida e coordenada diante de tais situações.

O abalo emocional — marcado por estresse, ansiedade e medo — evidencia a urgência de oferecer suporte psicológico adequado e reforça a importância de uma atuação sensível e empática por parte das autoridades. O relato da vítima sobre a interação com a polícia destaca a importância da empatia e compreensão por parte das autoridades ao lidar com vítimas de cibercrimes, minimizando o estigma associado a essas situações. O suporte familiar e o uso de medicação como estratégias para a recuperação psicológica ressaltam a complexidade do trauma emocional pós-cibercrime, demandando uma abordagem multidisciplinar. O reconhecimento da falta de informação prévia sobre práticas de segurança online destaca a importância da educação digital preventiva para mitigar riscos.

A principal lição extraída da experiência é a desconfiança em promessas de ganhos fáceis, revelando a necessidade de uma abordagem crítica diante de propostas online. O conselho central da vítima enfatiza a importância de não confiar em formas de ganho fácil, consolidando a necessidade de conscientização e ceticismo no ambiente digital.

8. CONSIDERAÇÕES FINAIS

A educação digital promove a consciência digital, e maximiza a conduta do titular de dados pessoais como ferramenta de segurança. A segurança dos dados pessoais não deve estar amparada unicamente pela cibersegurança e por modernos sistemas de criptografia. A segurança dos dados pessoais deve começar pelo próprio titular desses dados, que só estará apto a exercê-la plenamente quando existir consciência digital desenvolvida pela adequada educação digital. A partir disso, é possível vislumbrar uma diminuição no número de vítimas. É fundamental que autoridades públicas e empresas compreendam que a inclusão digital, quando não acompanhada de educação digital, contribui para o aumento de crimes cibernéticos, incidentes de segurança e violações de dados pessoais. Todos são titulares de dados pessoais, independentemente de classe social, cor, profissão, nacionalidade, crença ou cultura.

HERANÇA DIGITAL, PRIVACIDADE E PROTEÇÃO DE DADOS

Fellipe Fernandes Duarte¹

INTRODUÇÃO

O avanço da internet e toda a sua ramificação de bens e serviços é evidente. Os postos de trabalho, os meios de aquisição de produtos e contratação de mão-de-obra foram completamente afetados. Por consequência, as transações comerciais também cresceram exponencialmente – não apenas bens físicos, mas também os denominados bens virtuais, gerados e adquiridos por meios digitais.

Como exemplos de bens virtuais, podemos citar contas pessoais em plataformas e aplicativos, mensagens, vídeos, itens oriundos de games, criptomoedas, NFTs (*non-fungible tokens*, ou tokens não fungíveis, em tradução livre), entre muitos outros. Por síntese, são bens não-físicos e intangíveis, adquiridos ou gerados com o principal intuito de utilização em ambiente on-line.

O direito tem o objetivo de acompanhar as tendências da sociedade, gerar proteção e adequar-se às demandas sociais. Com o advento da internet, diversas possibilidades surgiram, entre as quais, a necessidade de regulação dos bens virtuais.

Quando um indivíduo falece sem especificar a destinação de seus bens, seus sucessores podem ser prejudicados, especialmente na

1 Advogado Pós-graduado em Direito Digital e Direito Penal e Processo Penal. Latin Legum Magister (*LL.M*) em curso em Direito Empresarial. Certificado pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC/RS) & Escola Nacional de Magistratura (ENM) em Lei Geral de Proteção de Dados (LGPD). Foi Residente Jurídico da OAB/DF 1/2023 e monitor da Residência Jurídica 1/2024. Certificado pela Data Privacy Brasil e pela Universidade Corporativa UNIEDUCAR em Lei Geral de Proteção de Dados. Certificado pela OneTrust em Data Discovery & Governance: IT Infrastructure. Membro das Comissões de Privacidade e Proteção de Dados e Compliance da OAB/DF.

ausência de procedimentos como testamento e codicilo. Nessa mesma linha, diante da ausência de disposição expressa de seus titulares, resta um interessante questionamento: para onde vão os bens digitais quando não se está mais vivo?

A relevância da temática se demonstra pela quantidade de usuários ativos diariamente nas redes sociais, sites, e-mails, aplicativos de entrega, vestuário, transportes, compras e tantos outros, gerando milhões de dados que podem possuir relevante valor comercial e até sentimental.

Por outro lado, a despeito dos diversos projetos de lei sobre herança digital em curso, nada está efetivamente definido. Não há, no Brasil, legislação específica vigente sobre a temática. Sob a ótica da Lei Geral de Proteção de Dados (LGPD), ainda há uma série de questões que precisam ser postas à mesa. É esse o tema que será abordado aqui.

1. ASPECTOS DOS BENS DIGITAIS

1.1. Definição de Bens Digitais

Inicialmente, não há como se falar em bens digitais sem que seja dada a definição de um bem. O Código Civil de 1916, no tratamento do objeto do direito, não fazia distinção entre bem e coisa, usando os termos como sinônimos. Já o Código Civil de 2002, atualmente em uso, dispõe dos bens nos artigos 79 a 103, mas utiliza apenas a expressão ‘bem’, e não ‘coisa’. Flávio Tartuce² os diferencia da seguinte maneira:

Coisa constitui gênero, e bem a espécie – coisa que proporciona ao homem uma utilidade sendo suscetível de apropriação. Todos os bens são coisas; porém nem todas as coisas são bens. Coisas são tudo o que não é humano. Bens são coisas com interesse econômico e/ou jurídico.

2 TARTUCE, Flávio Manual de direito civil: Vol. Único – 10. ed: Forense; São Paulo, 2020. P.308

Portanto, a legislação brasileira assegura ao proprietário de um bem, seja este qual for, desde que lícito e em conformidade da lei, o direito à propriedade. Este, embasado no art. 5º, XXII da Carta Magna, possibilita a apropriação privada dos bens e meios de produção e impõe aos indivíduos o respeito à propriedade alheia.³

Paulo Roberto Gaiger⁴, no XXIV Congresso Internacional do Notariado Latino, dispôs que bens podem ser classificados como bens físicos, mas também se pode conceituar um documento eletrônico, que nada mais é que uma sequência de bits representativos de um texto acadêmico ou mesmo de uma ordem de compra de milhões de reais, como um bem móvel. A definição é similar, mas não se confunde com a empregada no art. 83, I do Código Civil, que institui que as energias com valor econômico são bens móveis.

Os ativos digitais, bens virtuais ou documentos eletrônicos são registros virtuais nos quais os indivíduos têm direito ou interesse, que vão desde itens de jogos on-line e redes sociais, fotos e músicas, listas de contatos e dados de clientes até os domínios de hospedagem de sítios virtuais.

De acordo com Edwards e Harbinja⁵, os bens digitais são divididos em duas grandes categorias: bens com valor econômico e bens sem valor econômico. Os primeiros podem ser tudo aquilo que possui atributo financeiro, que pode ser comercializado ou negociado, por exemplo, livros digitais e aplicativos de software, que, notadamente, são possuidores de valor pecuniário.

Já os bens digitais sem valor econômico, também de acordo com os referidos autores, são dispostos como fotos e vídeos pessoais, documentos particulares, e-mails, mensagens, páginas da web, arqui-

3 BARCELLOS, Ana Paula de. Curso de direito constitucional / Ana Paula de Barcellos. – Rio de Janeiro: Forense, 2018 p. 154.

4 NOTORIAL. Colégio. XXIV Congresso Internacional do Notariado Latino, Bahia. 2019. Disponível em: <http://www.notariado.org.br/index.php?pG=X19leGliZV9ub3R-pY2lhcw=> Acesso em: 22 jun. 2020.

5 EDWARDS, Lilian; HARBINJA, Edina. Protecting Post-mortem Privacy: reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal*, Vol. 32, No. 1, 2013. p.106

vos, entre outros. Estes, teoricamente, não possuem preço e não são objeto de comercialização.

Todavia, os bens digitais pessoais e sem valoração econômica podem eventualmente possuir demanda comercial, a depender da relevância e da demanda social das informações ali atreladas.

A tecnologia tem se demonstrado cada vez mais usual na vida dos indivíduos e da sociedade, atraindo uma gama de novas possibilidades e, à medida que o número de bens digitais das pessoas aumenta, as questões que envolvem a disposição desses bens quando da morte ou incapacidade do indivíduo se tornam mais comuns.⁶

1.2. Qualificação e Tipificação

Dados os conceitos iniciais, convém ressaltar suas inúmeras versatilidades. Por serem acessíveis a qualquer indivíduo que tenha uma conexão simples com a internet, os itens virtuais podem ser objeto de criação e alteração por meio de aplicativos virtuais.

Os pesquisadores Carroll e Romano⁷, especialistas na comunidade digital pós-morte, definem os cinco tipos de bens digitais importantes para se atentar *post mortem*:

1. Dispositivos e dados – que englobam os dispositivos eletrônicos e os documentos ali contidos; 2. E-mails – que englobam as mensagens e a possibilidade de acesso à conta de e-mail; 3. Contas on-line – quaisquer serviços que dependam de uma conta com senha e contenham além de mensagens de texto, fotos e/ou vídeos; 4. Contas financeiras – contas que estão ligadas a uma conta bancária ou financeira; 5. Negócios Online – que incluem lojas virtuais com potencial para fluxo de receita.

6 UFADAA. The Uniform Fiduciary Access to Digital Assets Act. Disponível em: [<http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20\(2015\)>](http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015)) Acesso em: 08 jun. 2020

7 CARROLL, Evan. ROMANO, John. Your Digital Afterlife. Berkeley: New Riders, 2011. p.66

Há, ainda, as conhecidas criptomoedas, que podem ser traduzidas em ativos virtuais com finalidade financeira-comercial. Apesar de não haver regulação para a disposição desses ativos, nem de estarem presentes na Lei 12.865/2013, que rege o sistema de transações financeiras brasileiro, o interesse e a usabilidade desse tipo de artefato virtual gera cada vez mais a atenção da sociedade.

De modo semelhante às criptomoedas, encontram-se os NFTs – itens únicos, protegidos por criptografia e sistemas como o *block-chain*, que impedem que o mesmo item seja copiado ou possua mais de um proprietário nominal ao mesmo tempo, salvo em casos excepcionais.

No mesmo norte, as pontuações de cartões de crédito e milhas de viagens, cedidas por empresas que as utilizam com intuito de atrair clientes e os fidelizar, oferecem pontos que podem ser trocados por bens e serviços. Apesar de amplamente negociadas, as milhas aéreas não possuem legislação própria, mas são também parte do sistema de bens digitais. Não obstante a demanda e a valoração econômica, empresas renomadas como o Santander⁸ e a Latam⁹, nos seus respectivos programas de milhas, afirmam que as pontuações obtidas são pessoais e intransferíveis, vedando a transmissão a terceiros, seja por doação, seja por negociação, e, por consequência, impedem a sucessão desses bens em caso de falecimento do titular.

Outrossim, inclusos no universo digital e classificados como bens virtuais, têm-se os jogos eletrônicos e aplicativos de software, comuns na rotina de crianças e adolescentes, movimentando cifras bilionárias em suas transações. Estudos apontam que o mercado de jogos movimenta US\$1,5 bilhão por ano só no Brasil¹⁰ e, de maneira global, o

8 SANTANDER esfera. Banco Santander. Disponível em: < <http://respostas.bonus-esfera.com.br/regulamento.html>> Acesso em 08 de jun. 2020.

9 LATAM. Fidelidade Latam. Disponível em: < https://www.latam.com/content/dam/LATAM/latam-marca-unica/Brasil/PDF/Fidelidade/REGULAMENTO_DO_PROGRAMA_LATAM_FIDELIDADE_1_janeiro_2017.pdf> Acesso em 08 de jun. 2020

10 MENDES. Jaqueline. Indústria de games cresce e se profissionaliza cada vez mais. 2019. Disponível em: <https://www.em.com.br/app/noticia/economia/2019/10/16/inter-nas_economia,1093076/industria-de-games-cresce-e-se-profissionaliza-cada-vez-mais.shtml> Acesso: 22 jun 2020.

mercado de aplicativos para aparelhos eletrônicos estima movimentar US\$ 6 trilhões em 2021.¹¹

Sabe-se que, por meio dos jogos eletrônicos, diversos artefatos exclusivamente virtuais são negociados na plataforma fornecedora do sistema. Em alguns casos, a valoração econômica de itens virtuais é tão elevada que se torna necessária a criação de um meio exclusivo para administrar as negociações, a exemplo do software *Diablo III*¹² – que dispõe de plataforma gerenciada pela própria fabricante do *game* para que os jogadores da interface negociem entre si, com dinheiro “real”.

Observa-se a quantidade de informações transmitidas entre cada um desses bens: dados pessoais, profissionais ou metadados. Grande parte deles, muitas vezes, sequer é objeto de deliberação consciente por parte de seus titulares, que tão somente aceitam termos e condições genéricos fornecidos pelas plataformas de conteúdo. Apesar disso, nada é regulamentado na lei brasileira ante a possibilidade de transmissão dos itens virtuais no universo dos *games*. Demonstrada a relevância desta temática, embasa-se a discussão sobre a possibilidade de transmissão sucessória desses bens, seja legítima ou testamentária, a fim de evitar violações aos direitos dos sucessores.

1.3. Moedas Virtuais

É oportuno diferenciar moeda digital e moeda virtual. Moeda digital é gênero, enquanto moeda virtual é espécie. Pode-se dizer que ambos são artifícios criados para efetuar transações dentro de ambientes eletrônicos. Toda moeda digital pode ser considerada uma moeda virtual, mas nem todas as moedas virtuais podem ser digitais.¹³

11 DEMARTINI, Felipe. 2019. Mercado de apps deve movimentar US\$ 6,3 trilhões até 2021. Disponível em: <<https://br.financas.yahoo.com/noticias/mercado-apps-deve-movimentar-us-234000589.html>> Acesso: 22 jun 2020

12 G1, Globo. Casa de Leilões de 'Diablo III' com dinheiro real é aberta no game. 2012. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2012/06/casa-de-leiloes-de-diablo-iii-com-dinheiro-real-e-aberta-no-game.html>> acesso em 01.nov.2020.

13 FOXBIT. Educação Financeira. Quais as diferenças entre criptomoedas e moeda digital. 2019. São Paulo. Disponível em: <https://foxbit.com.br/blog/quais-sao-as-diferencas-entre-criptomoeda-e-moeda-digital/> Acesso 14.Nov.2020.

Por conceito, moedas virtuais são entendidas como economias dentro de um aplicativo ou software específico. Por exemplo, em um jogo eletrônico, suas moedas correspondentes, pelas quais se transacionam itens e bens dentro da interface, são consideradas moedas virtuais.

Por sua vez, as moedas digitais, como criptomoedas ou dinheiro em um aplicativo bancário, são formas de dinheiro virtual, que transitam pela internet – sejam regulamentadas ou não.

As moedas cambiais dos países são reguladas através de seus bancos centrais, que controlam a emissão e a flutuação de preço, de acordo com as necessidades do mercado.

Já as criptomoedas, diferentemente das moedas oficiais, de modo típico, são desenvolvidas por internautas e/ou empresas, não necessariamente com finalidades econômicas. Em certos casos, como o da famosa *Bitcoin*, não se sabe ao certo quem é o responsável por sua inserção e criação no universo virtual.¹⁴

Uma das principais características das criptomoedas é a não interferência governamental, ou seja, ausência de controle de determinado estado ou país sobre quaisquer de suas atribuições, sobre oscilações de preço e emissão da moeda.

Outra característica específica é sua existência apenas no mundo virtual. Diferentemente do que acontece com as moedas regulamentadas, como o real e o dólar, as moedas digitais possuem existência apenas no universo eletrônico, e, portanto, não há o que se falar em cédulas físicas.

No Brasil, o Banco Central,¹⁵ em seu comunicado nº: 25.306/2014, afirma que as moedas virtuais não possuem garantia de conversão para a moeda oficial brasileira, tampouco são respaldadas por quaisquer ativos reais ou mecanismos governamentais. A institui-

14 POLITIZE! O. CUSTÓDIO, Ana Carolina. SCHIOCHETTI, Rafaela. Criptomoe-das: O que são e como funcionam? São Paulo. 2019. Disponível em: < <https://www.politize.com.br/criptomoedas-o-que-sao-e-como-funcionam/> > Acesso 10.Nov.2020

15 BRASIL. Banco Central. Comunicado nº 25.306, 19 de Fevereiro de 2014. 2014. Disponível em: <http://www.lex.com.br/legis_25308829_comunicado_n_25306_de_19_de_fevereiro_de_2014_> acesso em 22 jun. 2020.

ção demonstra cautela com este tipo de tecnologia e afirma que o risco de uso está exclusivamente sob a responsabilidade de seus usuários.

Apesar disso, a Receita Federal¹⁶ as equipara aos ativos financeiros, e orienta aos usuários que as declarem no imposto de renda pelo seu valor de aquisição. Desse modo, percebe-se que o órgão reconhece que as moedas possuem, de fato, importância econômica, caso contrário, não solicitaria sua declaração nos tributos nacionais.

Finalmente, ainda que não regulamentadas, as criptomoedas, NFTs e milhas percebem valoração econômica no mundo atual e diversos países já até transacionam bens e serviços em moedas digitais, por intermédio de sites e até mesmo lojas físicas. Estima-se que, no futuro próximo, essa tendência se tornará cada vez mais usual à população.

1.4. Política de Privacidade, Termos de Uso e Licença

Ao contrário do que se pensa, ao comprar um bem virtual, o usuário não obtém, necessariamente, a sua posse. É comum que empresas fabricantes e fornecedoras dos bens celebrem contratos de adesão, com cláusulas de licença de uso não exclusivo e intransferível, para que assim, estes não sejam objetos de terceiros e adentrem na seara sucessória.¹⁷

As transações de compra deste tipo de bens ocorrem mediante os contratos eletrônicos. Conforme Lorenzetti, os contratos eletrônicos dividem-se em telemáticos, que usam de meio digital para sua realização, e informáticos, que tem por conteúdos os bens e serviços digitais, sendo a despersonalização, transnacionalidade e a virtualidade suas principais características, além de, em grande parte, serem também contratos de adesão.¹⁸

16 ECONOMIA, Ministério. Imposto Sobre a Renda – Pessoa Física. 2019. Disponível em: <<http://receita.economia.gov.br/interface/cidadao/irpf/2019/perguntao/perguntas-e-respostas-irpf-2019.pdf>> Acesso: 22 jun 2020.

17 LÔBO, Paulo. Direito civil: Vol. 4: coisas – 4. ed. – São Paulo : Saraiva Educação, 2019. p.139

18 LORENZETTI, Ricardo L. Comércio eletrônico. Tradução de Fabiano Menke; com notas de Cláudia Lima Marques. São Paulo: Revista dos Tribunais, 2004. P.163

Como exemplo, a Blizzard Entertainment,¹⁹ empresa mundialmente conhecida, provedora do jogo World of Warcraft, em seus termos de uso, não possibilita aos usuários a propriedade dos bens digitais criados e negociados no jogo, além de proibir a transferência de bens virtuais e a negociação entre jogadores fora de sua plataforma e com dinheiro real. O usuário deve apenas usufruir do jogo, mas jamais dispor deste como se fosse seu.

Contrariados, diversos jogadores ingressaram judicialmente contra a empresa,²⁰ reclamando indenizações; mas, curiosamente, não debatiam a respeito da propriedade dos bens virtuais, e sim da análise dos contratos de adesão celebrados momentos antes de iniciar a partida virtual, que não permitiam alternativa ao consumidor senão aceitar os termos ali dispostos.

Todavia, não apenas os jogos e aplicativos virtuais possuem cláusulas de adesão em seus termos de uso e contratos. Diversas páginas da web utilizam-se deste modo de reprodução de contratos,²¹ como a rede social Facebook e o buscador de conteúdo Google.

Os bens digitais fornecidos pela Microsoft,²² através da Xbox Life, que disponibilizam pontuações e moedas em jogos virtuais, não podem ser considerados bens pessoais e têm sua transmissibilidade cerceada – pois, segundo a empresa, aos bens é aplicável apenas uma licença pessoal, revogável, não transferível e não sub licenciável, disposta pela companhia conforme critérios próprios e exclusivos.

Semelhante modo ocorre em compras de e-books, softwares, músicas, imagens ou vídeos. Ao usuário é assegurada, via “termos de

19 WARCRAFT. World Of. Terms of Use. Blizzard. 2020. Disponível em: < http://eu.blizzard.com/en-gb/company/legal/wow_tou.html > Acesso: 08 jun. 2020.

20 RIO DE JANEIRO. Tribunal de Justiça. Apelação nº 0011124-91.2008.8.19.0002, da 12ª Câmara Cível da Comarca de Niterói. Apelante: Level UP Interactive S.A. Apelado: Vinicius Silva De Souza. Relator: Des.^a Antonio Iloizio Barros Bastos. Rio de Janeiro, 10 de agosto de 2010. Disponível em: . <<http://www4.tjrj.jus.br/ejud/ConsultaProcesso.aspx?N=201000153679>> Acesso em: 7 de junho de 2020.

21 GOOGLE. Ink. Termos de Serviços. 2020 Disponível em: <<https://policies.google.com/terms?hl=pt-BR>> Acesso: 22 jun 2020.

22 SERVICES Microsoft. Agreement. 15 jul. 2015. Disponível em: < <https://www.microsoft.com/en-us/servicesagreement/> > Acesso em: 08 jun. 2020.

uso”, apenas a licença para uso individual. Os termos são uma série de condições que regem a utilização dos programas de computadores, como a inalienabilidade e a impossibilidade de sucessão dos bens digitais, com as quais o usuário deve concordar para obter acesso ao bem virtual adquirido.²³

Em muitos casos, as cláusulas que tratam dessas questões são unilaterais. A única escolha do usuário é aceitar os termos para fazer uso da plataforma. Não há qualquer discussão ou afastamento de cláusulas que possam ser consideradas inadequadas ou prejudiciais ao consumidor, sendo apenas disponibilizado um botão na interface eletrônica onde se diz “eu aceito”.²⁴

Todavia, o dispositivo do art. 54 do CDC exige que os termos de adesão de consumo sejam redigidos em formato claro, de fácil compreensão ao consumidor e sem excesso de terminologias técnicas. Entretanto, percebe-se que, na prática, nem sempre os fornecedores atentam-se ao que diz a lei.

Um caso didático é o da empresa GameStation,²⁵ do Reino Unido. Sarcasticamente, a organização inseriu em seus documentos uma cláusula contratual que dizia que, caso o usuário aceitasse os termos, concordaria em conceder de forma irrestrita a sua alma para a companhia. Sem perceber o dispositivo inusitado, centenas de usuários assinaram o termo, aceitando a condição imposta e, teoricamente, “cedendo a alma para a empresa”.

A ideia da GameStation era demonstrar a total ineficiência dos termos de uso dos aplicativos e softwares. O resultado demonstrou uma interessante perspectiva: os usuários, de fato, não se ocupam em ler os documentos atrelados ao programa eletrônico; e, ainda que o fizessem,

23 BARBOSA, Murilo Oliveira. A Importância do Direito à Privacidade Digital, Redes Sociais e Extensão Universitária. v. 24, Goiânia, Fragmentos de Cultura 2014. p.89-97.

24 ALMEIDA, Juliana Evangelista de. Testamento Digital: como se dá a sucessão dos bens digitais / Juliana Evangelista de Almeida - Porto Alegre, RS: Editora Fi, 2019

25 LAFOUFA, Jaqueline. Empresa de venda de videogames do Reino Unido pedia 'a alma'... Disponível em: <<https://tecnologia.ig.com.br/noticia/2010/04/16/empresa+de+venda+de+videogames+do+reino+unido+pedia+a+alma+dos+consumidores+em+contrato+9460333.html>> Acesso em 20 jun. 2020

de nada poderiam discordar, pois, nesse caso, seriam impossibilitados de utilizar a plataforma desejada.

Contra essa tendência de atuação dos fornecedores, o art. 46 da Lei nº 8.078/1990, conhecida como Código de Defesa do Consumidor, esclarece que os contratos que regulam as relações de consumo não podem obrigar os consumidores, se não lhes for dada a oportunidade de ciência prévia de seu conteúdo e se forem escritos de modo a dificultar a compreensão e o seu sentido.

O referido código dispõe, no art. 54, que o contrato de adesão é aquele cujas cláusulas tenham sido estabelecidas unilateralmente pelo fornecedor. De modo complementar, há o Decreto nº 7.962/13, que trata do CDC e da contratação de bens e serviços no comércio eletrônico, sem prejuízo às normas gerais contratuais. O doutrinador Carlos Roberto Gonçalves²⁶ trata o assunto da seguinte maneira:

As partes discutem livremente as condições, porque se encontram em pé de igualdade (par a par). Contratos de adesão são os que não permitem essa liberdade, devido à preponderância da vontade de um dos contratantes, que elabora todas as cláusulas. O outro adere ao modelo de contrato previamente confeccionado, não podendo modificá-las: aceita-as ou rejeita-as, de forma pura e simples, e em bloco, afastada qualquer alternativa de discussão.

Como forma de amparo às partes desfavorecidas na relação contratual, principalmente nos contratos de adesão, preceitua o art. 423 do Código Civil que há necessidade de se interpretar de forma favorável o contrato ao aderente e, no dispositivo seguinte, o art. 424 afirma que são nulas as cláusulas que importem em renúncia antecipada de direitos.

Ainda assim, contratos como estes impossibilitam a sucessão dos bens virtuais e, por não haver legislação para tratar do tema, não há uma definição clara de como os bens poderiam ser cuidados no que tange à sucessão.

26 GONÇALVES, Carlos Roberto. Direito civil : direito das obrigações – Vol. 6 - tomo I : parte especial: contratos – 20. ed. – São Paulo : Saraiva Educação, 2018. – (Coleção sinopses jurídicas; v. 6, t. 1), p. 32

A inalienabilidade dos negócios jurídicos, característico dos negócios gratuitos, não se compartilha com os negócios onerosos. Os contratos virtuais celebrados com onerosidade não se sucederiam, em tese, como inalienáveis, pois, se assim fosse, seriam considerados nulos, conforme preceituado no art. 424 do Código Civil.

Esse tipo de cláusula, comumente encontrada nos contratos de adesão, implica em renúncia de direitos provenientes da própria natureza contratual, violando diretamente o disposto no art. 51 do Código de Defesa do Consumidor. Quando configurada a violação ao disposto na lei, as cláusulas são consideradas nulas de pleno direito.

Portanto, de modo final, é necessário observar e salvaguardar, mediante a lei específica, diretrizes a fim de coibir e regulamentar a prática de infrações contratuais no universo virtual, resguardando os dados dos consumidores e instruindo os provedores e fornecedores de bens e serviços, a fim de assegurar às partes o efetivo amparo e tutela do direito.

2. PRIVACIDADE E PROTEÇÃO DE DADOS

2.1. Dados Como Patrimônio e a Visão da LGPD

A legislação brasileira busca abarcar as novas demandas da sociedade contemporânea, em especial, no que se refere à internet e a todas as suas possibilidades. A Lei Geral de Proteção de Dados regula o uso e tratamento dos dados pessoais, virtuais ou físicos.

A LGPD traz importantes diretrizes para lidar com os dados no Brasil, zelando pela intimidade do indivíduo. Tartuce²⁷ demonstra a relevância deste regulamento com os seguintes termos:

Em termos gerais, existe uma ampla preocupação com os dados e informações comercializáveis das pessoas naturais, inclusive nos meios digitais, e objetiva-se proteger os direitos fundamentais de liberdade

27 Tartuce, Flávio. Manual de direito civil: volume único – 10. ed: Forense; São Paulo: MÉTODO, 2020. P.215

e de privacidade, bem como o livre desenvolvimento da personalidade.

Nos termos do preceito seguinte da norma específica, a disciplina da proteção de dados pessoais tem como fundamentos:

- a) o respeito à privacidade;
- b) a autodeterminação informativa, com amparo na autonomia privada;
- c) a liberdade de expressão, de informação, de comunicação e de opinião;
- d) a inviolabilidade da intimidade, da honra e da imagem;
- e) o desenvolvimento econômico e tecnológico e a inovação;
- f) a livre-iniciativa, a livre concorrência e a defesa do consumidor; e
- g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O diploma tem incidência em 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. Isso desde que a operação de tratamento seja realizada no território nacional, a sua atividade tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Estão excluídos do âmbito da norma os tratamentos de dados feitos para fins acadêmicos, jornalísticos, artísticos ou relacionados à investigação de ilícitos em geral, entre outros (art. 4.º da Lei 13.709/2018).

A LGPD busca abarcar uma série de diretrizes, orientando e organizando o modo como as instituições devem tratar os dados dos seus usuários. A lei também estabelece regras claras e transparentes sobre o tratamento de dados pessoais, fomenta o desenvolvimento econômico e tecnológico e, principalmente, garante proteção à privacidade de dados pessoais dos usuários.

A Associação Internacional de Privacidade Profissional (IAPP) define dados pessoais como todos aqueles relacionados à pessoa natural identificada ou identificável. Este conceito contempla a definição exposta no art. 5º, I, da Lei 13.709/2018. A associação definiu, também, os considerados “dados sensíveis”: informações que podem ser utilizadas de forma discriminatória e, por conta disso, carecem de especial proteção.²⁸

O art. 5º, II, da LGPD conceitua como dados sensíveis as informações que dizem respeito à convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, origem racial ou étnica, dados referentes a ideias filosóficas, políticas, à saúde, vida sexual, dados genéticos ou biométricos, quando vinculados à uma pessoa natural.

O tratamento de dados pessoais de crianças e adolescentes, segundo a legislação, deve ocorrer após consentimento específico de pelo menos um dos pais ou do responsável legal, de acordo com o art. 14, I, da LGPD; e o gerenciador desses dados deve depreender esforços para verificar que o consentimento foi realmente cedido pelo responsável do menor.

Em que pese a legislação acentue preceitos de tratamento no que tange ao uso e gestão de dados pessoais, não há, explicitamente, disposições nela que versem sobre a possibilidade de transmissão e sucessão desses dados para terceiros, legitimados ou testamentados. A lei, nesse quesito, carece de uma abordagem clara e específica sobre o assunto.

Apesar de toda a proteção e segurança que a LGPD busca assegurar aos usuários ante aqueles que gerenciam e manuseiam suas in-

28 O QUE MUDA. LGPD Brasil, São Paulo, Disponível em: <https://www.lgpdbrasil.com.br/o-que-muda-com-a-lei/> Acesso em 21. Outubro. 2020

formações pessoais, nada fora abordado no que se refere à possibilidade de transmissão sucessória dos dados.

Ainda que, por se tratar de dados pessoais, estes não possuam exata valoração econômica, diversos institutos já os consideram “o novo petróleo”, conforme afirmado pelo então CEO da Mastercard, Ajay Banga, durante evento em São Paulo.²⁹ A grande questão acerca da afirmação do multimilionário árabe é saber como se pode mensurar o preço de um dado pessoal.

De maneira ilustrativa, o livro “O Poder do Hábito”, best seller mundial, do autor Charles Duhigg, traz à tona o caso da rede varejista americana Target, quando a empresa soube, antes mesmo de suas próprias clientes, quando elas estariam grávidas.

Por meio do cruzamento de milhares de informações coletadas, a empresa detectou padrões de comportamento de compra e, com o auxílio da inteligência artificial, previu com maestria a possibilidade de os clientes que compravam determinados tipos de produtos, futuramente, terem filhos. O resultado: um faturamento de US\$ 70 bilhões, somados, em suas 1.800 unidades físicas nos EUA.³⁰

Desta feita, é nítido o valor inestimável dos dados pessoais, que mostram-se capazes de construir lucros significativos às empresas. Apesar disso, a legislação brasileira ainda não se mostra hábil a tratar dos dados pessoais como bens, a fim de inseri-los e transmiti-los por intermédio do direito sucessório.

2.2. O Direito Sucessório e o Direito à Privacidade

A sucessão de bens virtuais no Brasil ainda não possui definições claras. Nos tempos recentes, em especial, devido às mudanças decorrentes da pandemia do novo coronavírus (covid-19), a demanda por esse dispositivo tem crescido substancialmente. Todavia, há de se

29 NEGÓCIOS. Época. Dados são o novo petróleo diz Ceo da Mastercard. 2019. Disponível em: <<https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html>> Acesso em 21. Out. 2020

30 EXAME. Revista. A nova indústria da espionagem. Disponível em: <<https://exame.com/revista-exame/a-nova-industria-da-espionagem/>> Acesso em 21. Out. 2020

perceber que, sem legislação específica, os cuidados relativos aos bens digitais pessoais se submetem aos interesses das empresas privadas de tecnologia. Karppi³¹ afirma que:

Para uma empresa, o que torna os dados “dignos de preservar” é, em última análise, sua capacidade de contribuir direta ou indiretamente para o lucro da empresa. Os dados pertencentes a usuários falecidos podem ser valiosos para esses fins. Por exemplo, os perfis memorializados ainda podem servir para atrair usuários vivos que visitam o perfil para lamentar.

Apesar dos conflitos de interesse, em que pese não haja na lei a possibilidade de transmissão de bens virtuais de modo *ab intestato*, ou seja, por legítima, nada impede que um indivíduo disponha destes bens via testamento, seguindo pressupostos do *favor testamenti*.

O art. 1.916 do Código Civil regula o testamento como ato revogável pelo qual alguém dispõe do seu patrimônio, total ou em partes, para depois da sua morte. Entre seus tipos, encontram-se os testamentos públicos, cerrados, particulares, também chamados de hológrafos e, sob forma especial, os testamentos marítimos, aeronáuticos e militares.³²

Ao contrário do que ocorre no Brasil, existe, nos Estados Unidos, uma lei federal que padroniza diretrizes de tratamento dos bens virtuais, chamada UFADAA (*The Uniform Fiduciary Access to Digital Assets Act*)³³. A lei engloba testamenteiros, curadores, inventariantes e mandatários, ampliando seus poderes, com o intuito de permitir gerenciar os bens digitais.

A legislação americana também autoriza o gerenciamento de domínios da web, de moedas virtuais e arquivos de computador. Entretanto, restringe o acesso a e-mails e mensagens pessoais, contas e

31 KARPPI T (2013). Noopolítica de memória de usuários mortos do Facebook. *Máquina de cultura* 14: 1–20. Disponível em: <www.culturemachine.net> Acesso em 20. Setembro. 2020

32 STOLZE, Pablo; Pamplona Filho, Rodolfo. Manual de direito civil – Vol. Único – 4. ed. – São Paulo: Saraiva Educação, 2020. P.2318

33 FIDUCIARY ACCESS to. Digital Assets Act, Revised. ULC. 2015. Disponível em:< [http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access %20to%20Digital%20Assets%20Act,%20Revised%20\(2015\)](http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015))> Acesso: 08 jun. 2020

mídias sociais, salvo quando o interessado possui procuração especial para requerer tal acesso.

O estado americano de Indiana, de acordo com o item nº 32.3.2.4 do Código Interno, também autoriza o acesso do herdeiro a qualquer um dos bens digitais, desde que o falecido tenha autorizado previamente. Em casos judiciais, a lei também autoriza o acesso, disponibilizando uma cópia de todo o conteúdo das contas pessoais ao sucessor.³⁴

Contudo, nem todos os bens digitais podem ser transferidos após a morte. Se forem bens de caráter personalíssimo, ou mesmo inerentes à pessoa daquele que faleceu,³⁵ não há que se falar em sucessão. Se não dispostos, continuam no provedor de internet até que seja feita a exclusão.

Assim, se não forem objeto de sucessão *causa mortis* ou de tutela por meio do direito autoral, a destinação desses bens não possui regulamentação própria.³⁶ Mesmo que o Código Civil brasileiro assegure, no art. 1.857, que toda pessoa capaz pode dispor de seus bens por testamento, há conflitos de direitos tutelados entre as partes, a exemplo dos termos de uso pactuados por contratos eletrônicos de adesão, conforme citado anteriormente. Por diversas vezes, o direito sucessório esbarra no direito à privacidade. Ambos mantêm uma relação de respeito e proximidade, mas não podem, de modo algum, ser sobrepostos um ao outro. É relevante observar suas limitações e maneiras de solucionar possíveis conflitos entre estes institutos.

Originada na Alemanha, a teoria das esferas busca evidenciar a finalidade e a importância do direito à privacidade, demonstrando, em diferentes níveis, a necessidade de resguardá-la na vida dos indivíduos.

34 INDIANA. Indiana Code. 2007. Disponível em: < <http://iga.in.gov/legislative/laws/2016/ic/titles/032/> > Acesso em: 08 jun. 2020.

35 DINIZ, Maria Helena. Curso de Direito Civil Brasileiro. Volume 6 – direito das sucessões, 26ª edição, São Paulo: Saraiva, 2012, P. 77

36 ALMEIDA, Juliana Evangelista de. Testamento Digital: como se dá a sucessão dos bens digitais [recurso eletrônico] / Juliana Evangelista de Almeida -- Porto Alegre, RS: Editora Fi, 2019

Oliveira, em seu livro “Direitos da Personalidade”,³⁷ dispõe desta teoria e a correlaciona com a personalidade e privacidade do morto, com os dizeres:

A situação do morto é explicada por fundamentos que podem ser reunidos em quatro categorias:

a) Não há um direito da personalidade do morto, mas um direito da família, atingida pela ofensa à memória de seu falecido membro;

b) Há, tão somente, reflexos post mortem dos direitos da personalidade, embora personalidade não exista de fato;

c) Os direitos da personalidade, em razão de interesse público, passam à titularidade coletiva com a morte da pessoa;

d) Com a morte, transmite-se a legitimação processual, de medidas de proteção e preservação para a família do defunto.

Convém destacar que o direito de sucessão não se confunde com o direito autoral nem com os bens virtuais. Os direitos autorais são transmissíveis mediante a sucessão, conforme preceito do art. 5º, XXVII, da Constituição Federal, onde a lei assegura que “aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar.”.

Por isso, os direitos do autor são considerados de natureza dúplice, e a sucessão, nesse caso, ocorre de modo distinto, tendo em vista seus aspectos materiais e pessoais. O direito moral do autor possui natureza extrapatrimonial e está relacionado ao vínculo personalíssimo entre o criador e sua obra, sendo intransferível. Já o direito patrimonial autoral diz respeito ao direito do proprietário de explorar financeiramente

37 NAVES, Bruno Torquato de Oliveira. SÁ, Maria de Fátima Freire de. Direitos da Personalidade. Belo Horizonte: Arraes, 2017.

a criação e usufruto deste bem, tornando-se um direito disponível.³⁸

Assim, uma das questões levantadas sobre os direitos dos autores que utilizam plataformas eletrônicas e virtuais para criar, fornecer ou disponibilizar suas obras e trabalhos é: seriam elas detentoras de uma parcela dos frutos concebidos por aquela arte?

Nota-se que os conceitos de autor e titularidade da obra não são capazes de abarcar por completo as inovações tecnológicas advindas da internet. No caso hipotético de um autor que auferir renda na internet: caso ele não utilizasse o serviço online disponibilizado pelo provedor, a criação e a divulgação do seu conteúdo artístico seriam extremamente difíceis.

Todavia, os bens virtuais regulados por contratos possuem caráter *intuitu personae*, ou seja, personalíssimos – como imagens, mensagens, nomes de domínio, páginas pessoais em redes sociais, dentre outros. Desta forma, a transmissibilidade desses bens encontra-se limitada.

Quando não há um contrato firmado e os bens possuem aspecto patrimonial, como criptomoedas e direitos autorais, caso o falecido não tenha deixado disposição de vontade, a transmissão poderá ser feita sem prejuízo da legitimação processual dos herdeiros.

Contudo, há de se observar que a Constituição Federal tornou inviolável o sigilo das comunicações telegráficas, das correspondências e de dados, como disposto no art. 5º, inciso XII. De forma análoga, pode-se assegurar a inviolabilidade de e-mails e outras mensagens enviadas por meio de sistemas eletrônicos e virtuais.

Mas esta condição não é absoluta. A título informativo, uma das maiores fornecedoras de serviços de internet no mundo, a multinacional Google³⁹, em seus termos de uso, certifica o direito à propriedade

38 POLI, Leonardo Macedo. Direito Autoral: parte geral. Belo Horizonte: Del Rey, 2008.

39 GOOGLE. Termos de Serviços. 2020. Disponível em: <<https://policies.google.com/terms?hl=pt-BR>> Acesso: 22 jun 2020.

intelectual do indivíduo e administra os dados do usuário via licença – que, de acordo com a empresa, não interfere na em sua privacidade.

Nos casos de falecimento, quanto aos objetos deixados, a empresa deixa explícito o seguinte parecer:⁴⁰

Reconhecemos que muitas pessoas falecem sem deixar instruções claras sobre como gerenciar suas contas on-line. Podemos trabalhar com membros imediatos da família e com representantes para fechar a conta de uma pessoa falecida, quando apropriado. Em certas circunstâncias, podemos fornecer o conteúdo da conta de um usuário falecido. Em todos esses casos, nossa principal responsabilidade é manter as informações das pessoas seguras, protegidas e particulares. Não podemos fornecer senhas ou outros detalhes de login. Qualquer decisão de atender a uma solicitação sobre um usuário falecido será feita somente após uma cuidadosa análise.

Já a empresa Apple, em suas políticas de privacidade,⁴¹ afirma rigidez no que tange à possibilidade de acesso da conta do usuário por terceiros. A companhia não autoriza que ninguém, além do titular, tenha acesso aos dados custodiados pela empresa, salvo em caso de determinação legal ou por requerimento de uma autoridade governamental.

Caso o *de cujus* tenha deixado um dispositivo eletrônico dessa fabricante, é assegurado ao herdeiro o direito à sucessão do aparelho físico, e apenas deste. Não é permitido, pela empresa, o acesso aos arquivos armazenados na conta, salvo exceções que envolvam a segurança e interesses relevantes, sempre a critério do provedor.

Por sua vez, a rede social Facebook⁴² informa que não compartilha perfis deixados pós-morte, por se tratarem de páginas pessoais, sem possibilidade de transmissão sucessória. Faz parte da sua política, porém, a conversão das contas dos usuários falecidos em memoriais virtuais, mediante requerimento.

40 GOOGLE. Central de Ajuda de conta do Google. [S.I.] Disponível em: <<https://support.google.com/accounts/troubleshooter/6357590?hl=pt-BR>> Acesso: 22 jun 2020.

41 APPLE. Central de Privacidade. Disponível em: <https://www.apple.com/br/privacy/>

42 FACEBOOK. Contas transformadas em memorial. [S.I.] Disponível em: <<https://www.facebook.com/help/1506822589577997>> Acesso: 22 jun 2020.

Nessa hipótese, a expressão “em memória de” será apresentada ao lado do nome do falecido na página da rede social, os amigos poderão ter acesso ao conteúdo por ele compartilhado, como fotos e vídeos, e é possibilitado ao herdeiro habilitado acesso parcial a dados da página e a uma quantidade limitada de recursos. Todavia, é vedado o acesso às mensagens pessoais.

Convém ressaltar que, mesmo que caracterizados pelas empresas como um “herdeiro”, segundo o art. 1.805, parágrafos 1º e 2º do Código Civil, não se exprime em aceitação de herança os atos oficiais conservatórios ou os de administração e guarda provisória. A prática desses atos pode configurar simples respeito e apreço pela memória daquele que faleceu, não significando, entretanto, a necessária aceitação da herança deixada.

Já na esfera autoral, os direitos patrimoniais do autor podem, de fato, ser transmitidos, pois possuem natureza dúplice: abrangem aspectos materiais e pessoais. Os aspectos morais e pessoais são considerados extrapatrimoniais, intransmissíveis, de caráter personalíssimo. Já os aspectos materiais estão relacionados à possibilidade de exploração econômica pelo autor, configurando-se como um direito disponível.

Em argumentação final, a questão é notavelmente controversa. Se, por um lado, os bens digitais ou físicos devem ser resguardados, ainda que na ausência de seus titulares, por outro lado, há vedação legal quanto à privacidade e a proteção de dados diretamente relacionados aos bens e aos próprios titulares. Tal controvérsia finda por gerar insegurança jurídica aos consumidores, às empresas e aos investidores estrangeiros, que buscam um ambiente seguro e estável para proliferação de projetos que envolvam tratamento de bens e dados virtuais.

3. CONSIDERAÇÕES FINAIS

Mesmo após a morte, certos direitos permanecem, permitindo que terceiros indiretamente lesados ingressem com ações por violação à honra ou à imagem do falecido, com fundamento nos artigos 12 e 20 do Código Civil. O morto tem resquícios de personalidade civil, não se

aplicando o art. 6.º da Codificação Material (Código Civil) aos direitos da personalidade, conforme preceitua Tartuce.⁴³

Assim, é prudente observar a transmissão dos bens virtuais, em especial, dos perfis de redes sociais, de mensagens e de e-mails, sob o olhar do direito sucessório, mas também em respeito aos princípios constitucionais da intimidade, personalidade e vida privada das partes envolvidas nas mensagens enviadas e recebidas.

Como fundamentação, preceitua o inciso X do art. 5º da Carta Magna a inviolabilidade da intimidade, da honra, da imagem e da vida privada, assegurando o direito de indenização por danos decorrentes de sua violação. Ainda assim, contra a hipótese de transmissão de mensagens e e-mails deixados pelo *de cujus*, tem-se a inviolabilidade das comunicações telegráficas, de correspondência e dados, preceituados no art. 5º, XX, da Constituição – que, de modo análogo, pode-se levantar em prol da proteção dos direitos individuais e adversos à sucessão deste tipo de bens.

Ressalta-se que, assim como em diversos países, a legislação pátria aborda somente o direito à privacidade das pessoas vivas. É o caso, por exemplo, do Reino Unido,⁴⁴ que discorre sobre os “dados pessoais de um indivíduo vivo que pode ser identificado” em sua lei de proteção de dados pessoais.

Como dito anteriormente, a teoria das esferas⁴⁵ é essencial para a compreensão e o respeito à vida privada, destacando a importância da privacidade. Segundo essa teoria, a privacidade é dividida em níveis, abrangendo a vida privada, a vida íntima e a vida secreta. A tutela jurídica deve acompanhar cada uma dessas esferas com diferentes graus de intensidade, conforme sua relevância.

43 TARTUCE, Flávio. Manual de direito civil: Vol. Único – 10. ed: Forense; São Paulo, 2020. P.223

44 UNITED KINGDOM, 1998. Data protection act. 1998. Disponível em: <<http://www.legislation.gov.uk/ukpga/1998/29/part/I>> Acesso em 08 de jun. 2020.

45 GÖTTING Horst-Peter, SCHERTZ Christian, SEITZ Walter. Handbuch des Persönlichkeitsrechts.

A Enciclopédia Jurídica da Pontifícia Universidade Católica de São Paulo (PUC-SP) complementa tal entendimento da seguinte forma:

A teoria das esferas divide, desse modo, a noção de privacidade em três esferas concêntricas chamadas de *Privatsphäre*, *Intimsphäre* e *Geheimsphäre* (esferas privada, íntima e secreta).

Na primeira, a esfera privada, estão contidas as outras duas esferas.

Nela se encontram aspectos da vida da pessoa excluídos do conhecimento de terceiros. Aproxima-se, de certa forma, da noção de privacidade ou *privacy*. A esfera íntima é a segunda, intermediária às outras duas, contendo os valores do âmbito da intimidade, com acesso restrito a determinados indivíduos com os quais a pessoa se relaciona de forma mais intensa. Por fim, a menor e mais interna esfera, a do segredo, referindo-se ao sigilo. Desse modo, quanto mais interna for a esfera, mais intensiva deve ser a proteção jurídica da mesma.

Portanto, o motivo de atenção ante a possibilidade de transmissão dos bens virtuais é a limitação dos direitos de privacidade individual. Pois, se por um lado, a sucessão desses bens é fator relevante e assegura a efetividade do direito sucessório; por outro, o respeito à intimidade pode ser diretamente confrontado, especialmente no que diz respeito à transmissão de bens personalíssimos, tais quais as mensagens instantâneas, imagens e e-mails.

Outro fator preponderante na questão é o custo do armazenamento destes bens, que, atualmente, após a morte, são excluídos pelas empresas. Karppi⁴⁶ observa que “para uma empresa, o que torna os dados “dignos de preservar” é, em última análise, sua capacidade de contribuir direta ou indiretamente para o lucro”.

46 KARPPI T (2013) Noopolítica de memória de usuários mortos do Facebook. *Máquina de cultura* 14: 1–20. Disponível em: <www.culturemachine.net> Acesso em 20. Setembro. 2020

Segundo Palm,⁴⁷ o real custo do armazenamento é o gerenciamento, pois “para manter a utilidade dos dados, as empresas devem atualizar rotineiramente os sistemas e cuidar de seu conteúdo, um empreendimento caro e tedioso para o qual o atual modelo de curadoria do Facebook (e outras empresas) não foi projetado para suportar”.

Em caso levantado pelo jornal britânico The Guardian, o ator Bruce Willis supostamente desejaria processar a Apple pelo direito de deixar toda a sua biblioteca do *iTunes* em testamento. Segundo o jornal,⁴⁸ o ator afirmou possuir milhares de horas de música em vários aparelhos *iPods* em sua propriedade.

O jornal também informou que os representantes do astro avaliavam a possibilidade de criar um fundo familiar para deter legalmente as músicas baixadas ou apoiar uma ação judicial já em andamento em cinco estados dos EUA, com o objetivo de garantir a transmissão das músicas adquiridas digitalmente.

Assim, cabe ao legislador, em colaboração com entidades civis especializadas e com o Congresso como um todo ou o Senado, zelar pelos conflitos entre os institutos garantidos pela Constituição Federal, tais como o direito à sucessão, a privacidade, a proteção de dados, a intimidade e o respeito às instituições de tecnologia, garantindo, ao mesmo tempo, o avanço da ordem econômica.

Finalmente, com a mais respeitosa licença à Lei Geral de Proteção de Dados e, parafraseando palavras de Watson,⁴⁹ pesquisador da Universidade Oxford, em Londres, a herança digital deve ser observada não apenas pelo seu valor financeiro e/ou pessoal, mas sim para que as gerações futuras consigam compreender nossa história.

47 PALM, J. O Buraco Negro Digital, Estocolmo : Riksarkivet / Arquivos Nacionais . 2016. Disponível em: <<https://journals.sagepub.com/doi/10.1177/2053951719842540>>; acesso em 26. Julho. 2020.

48 GUARDIAN. The. News e Media Limited. Bruce Willis to fight Apple over right to leave iTunes library in will... Disponível em: <<https://www.theguardian.com/film/2012/sep/03/bruce-willis-apple-itunes-library>> Acesso: 21. Outubro. 2020

49 OXFORD Internet Institute, University of Oxford, UK; Alan Turing Institute, London, UK. 2019 Disponível em: <https://journals.sagepub.com/doi/10.1177/2053951719842540> Acesso em 26 maio 2020.

REFERÊNCIAS

ALMEIDA, Juliana Evangelista de. **Testamento Digital: como se dá a sucessão dos bens digitais** [recurso eletrônico] / Juliana Evangelista de Almeida -- Porto Alegre, RS: Editora Fi, 2019.

ALMEIDA, Juliana Evangelista de. **Testamento Digital: como se dá a sucessão dos bens digitais** / Juliana Evangelista de Almeida - Porto Alegre, RS: Editora Fi, 2019.

APPLE. **Central de Privacidade**. Disponível em: <https://www.apple.com/br/privacy/>.

BARBOSA, Murilo Oliveira. **A Importância do Direito à Privacidade Digital, Redes Sociais e Extensão Universitária**. v. 24, Goiânia, Fragmentos de Cultura 2014. p. 89-97.

BARCELLOS, Ana Paula de. **Curso de direito constitucional** / Ana Paula de Barcellos. – Rio de Janeiro: Forense, 2018, p. 154.

BRASIL. Banco Central. **Comunicado nº 25.306, 19 de Fevereiro de 2014**. 2014. Disponível em: http://www.lex.com.br/legis_25308829_comunicado_n_25306_de_19_de_fevereiro_de_2014.

CARROLL, Evan; ROMANO, John. **Your Digital Afterlife**. Berkeley: New Riders, 2011, p. 66.

DEMARTINI, Felipe. **Mercado de apps deve movimentar US\$ 6,3 trilhões até 2021**. 2019. Disponível em: <https://br.financas.yahoo.com/noticias/mercado-apps-deve-movimentar-us-234000589.html>.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. Volume 6 – direito das sucessões, 26ª edição, São Paulo: Saraiva, 2012, P. 77.

ECONOMIA, Ministério. **Imposto Sobre a Renda – Pessoa Física**. 2019. Disponível em: <http://receita.economia.gov.br/interface/cidadao/irpf/2019/perguntao/perguntas-e-respostas-irpf-2019.pdf>.

EDWARDS, Lilian; HARBINJA, Edina. **Protecting Post-mortem Privacy: reconsidering the privacy interests of the deceased in a digital world**. Cardozo Arts & Entertainment Law Journal, Vol. 32, No. 1, 2013, p. 106.

EXAME. Revista. **A nova indústria da espionagem**. Disponível em:

<https://exame.com/revista-exame/a-nova-industria-da-espionagem/>.

FACEBOOK. **Contas transformadas em memorial**. [S.I.] Disponível em: <https://www.facebook.com/help/1506822589577997>.

FIDUCIARY ACCESS to. **Digital Assets Act, Revised**. ULC. 2015. Disponível em: [http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20\(2015\)](http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015)).

FOXBIT. **Educação Financeira. Quais as diferenças entre criptomoedas e moda digital**. 2019. São Paulo. Disponível em: <https://foxbit.com.br/blog/quais-sao-as-diferencas-entre-criptomoeda-e-moeda-digital/>.

G1, Globo. **Casa de Leilões de ‘Diablo III’ com dinheiro real é aberta no game**. 2012. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/06/casa-de-leiloes-de-diablo-iii-com-dinheiro-real-e-aberta-no-game.html>.

GOOGLE. **Central de Ajuda de conta do Google**. [S.I.] Disponível em: <https://support.google.com/accounts/troubleshooter/6357590?hl=pt-BR>.

GOOGLE. Ink. **Termos de Serviços**. 2020. Disponível em: <https://policies.google.com/terms?hl=pt-BR>.

GONÇALVES, Carlos Roberto. **Direito civil: direito das obrigações – Vol. 6 - tomo I: parte especial: contratos – 20. ed. – São Paulo: Saraiva Educação, 2018. – (Coleção sinopses jurídicas; v. 6, t. 1), p. 32.**

GÖTTING, Horst-Peter; SCHERTZ, Christian; SEITZ, Walter. **Handbuch des Persönlichkeitsrechts**.

GUARDIAN, The. News e Media Limited. **Bruce Willis to fight Apple over right to leave iTunes library in will...** Disponível em: <https://www.theguardian.com/film/2012/sep/03/bruce-willis-apple-itunes-library>.

INDIANA. **Indiana Code**. 2007. Disponível em: <http://iga.in.gov/legislative/laws/2016/ic/titles/032/>.

KARPPI, T. **Noopolítica de memória de usuários mortos do Face-**

book. Máquina de cultura 14: 1–20. 2013. Disponível em: www.cultu-remachine.net.

LAFOUFA, Jaqueline. **Empresa de venda de videogames do Reino Unido pedia ‘a alma’...** Disponível em: <https://tecnologia.ig.com.br/noticia/2010/04/16/empresa+de+venda+de+videogames+do+reino+unido+pedia+a+alma+dos+consumidores+em+contrato+9460333.html>.

LATAM. **Fidelidade Latam.** Disponível em: https://www.latam.com/content/dam/LATAM/latam-marcaunica/Brasil/PDF/Fidelidade/REGULAMENTO_DO_PROGRAMA_LATAM_FIDELIDADE_1_janeiro_2017.pdf.

LÔBO, Paulo. **Direito civil.** Vol. 4: coisas – 4. ed. – São Paulo: Saraiva Educação, 2019, p. 139.

LORENZETTI, Ricardo L. **Comércio eletrônico.** Tradução de Fabiano Menke; com notas de Cláudia Lima Marques. São Paulo: Revista dos Tribunais, 2004, p. 163.

MENDES, Jaqueline. **Indústria de games cresce e se profissionaliza cada vez mais.** 2019. Disponível em: https://www.em.com.br/app/noticia/economia/2019/10/16/internas_economia,1093076/industria-de-games-cresce-e-se-profissionaliza-cada-vez-mais.shtml.

NAVES, Bruno Torquato de Oliveira; SÁ, Maria de Fátima Freire de. **Direitos da Personalidade.** Belo Horizonte: Arraes, 2017.

NEGÓCIOS, Época. **Dados são o novo petróleo diz CEO da Mastercard.** 2019. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html>.

NOTORIAL, Colégio. **XXIV Congresso Internacional do Notariado Latino, Bahia.** 2019. Disponível em: <http://www.notariado.org.br/index.php?pG=X19leGliZV9ub3RpY2lhc>.

PALM, J. **O Buraco Negro Digital,** Estocolmo: Riksarkivet / Arquivos Nacionais. 2016. Disponível em: <https://journals.sagepub.com/doi/10.1177/2053951719842540>.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia O. A. **Crise da Informação: A quem pertence?** Revista de Direito, governança e novas

tecnologias, v. 2, p. 23-38, 2016.

POLI, Leonardo Macedo. **Direito Autoral: parte geral**. Belo Horizonte: Del Rey, 2008.

SERVICES, Microsoft. **Agreement**. 15 jul. 2015. Disponível em: <https://www.microsoft.com/en-us/servicesagreement/>.

TARTUCE, Flávio. **Manual de direito civil**: Vol. Único – 10. ed: Forense; São Paulo, 2020, p. 223 e 308.

UNITED KINGDOM. **Data Protection Act**. 1998. Disponível em: <http://www.legislation.gov.uk/ukpga/1998/29/part/I>.

WARCRAFT, World of. **Terms of Use**. Blizzard. 2020. Disponível em: http://eu.blizzard.com/en-gb/company/legal/wow_tou.html.

PROTEÇÃO DE DADOS COMO DIREITO CONSTITUCIONAL: A EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO CONSTITUCIONAL NO BRASIL

Graziella Angela Tinari Dell'Osa¹

INTRODUÇÃO

Nos tempos atuais, a proteção dos dados pessoais tem recebido grande destaque, seja por conta dos recorrentes escândalos de ataques cibernéticos que estão sendo divulgados pela mídia, seja porque está havendo uma conscientização da população sobre a importância do tema.

Isso decorre do fato de que muitos indivíduos tiveram seus dados pessoais expostos de forma indevida ou tomaram conhecimento dos riscos a que estão sujeitos, especialmente por conta da crescente participação em mídias sociais, compras on-line e outras atividades que usualmente demandam a disponibilização dos seus dados pessoais em meios digitais.

Nesse contexto, surge a necessidade de os titulares dos dados pessoais terem conhecimento da proteção que lhes é assegurada pela Constituição Federal (CF) de 1988, antes e após a promulgação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022 – que instituiu, de forma expressa, a proteção aos dados pessoais como um direito constitucional autônomo assegurado a todos os brasileiros e estrangeiros residentes no País.

¹ Sócia de Gonsales e Cho Advogados Associados (GCAA). Advogada com Certificação Profissional em Proteção de Dados (CPPD) – LEC/FGV Projetos.

Antes da publicação da EC nº 115/2022 e da vigência da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709, de 14 de agosto de 2018, existiam interpretações controversas sobre a extensão da proteção constitucional aos dados pessoais. Havia quem entendesse que os direitos pessoais não estariam totalmente contemplados em outros direitos já previstos constitucionalmente, tais como o direito à privacidade, ao sigilo e à dignidade da pessoa humana. Por outro lado, havia quem entendesse que os dados pessoais estariam protegidos como direito fundamental justamente por estarem incorporados em outros direitos.

Em 2020, o Supremo Tribunal Federal (STF) proferiu importante decisão sobre o tema ao julgar ações diretas de inconstitucionalidade² versando sobre o compartilhamento de dados pessoais por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE). Essa decisão deixou clara a posição do STF sobre a matéria, no sentido de que os dados pessoais estavam protegidos constitucionalmente e, portanto, os seus titulares estariam sob a tutela das garantias constitucionais.

Contudo, foi com a publicação da EC nº 115/2022 que essa proteção foi explicitamente assegurada, conforme apontado neste artigo.

1. A EVOLUÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL

Conforme ensina Zulmar Antonio Fachin³, o nascimento de novos direitos fundamentais é um processo histórico. A depender das circunstâncias e necessidades, novos direitos fundamentais são gerados

2 Ações diretas de inconstitucionalidade 6.387, 6.388, 6.389, 6.390 e 6.393, propostas por diversos partidos políticos e pelo Conselho Federal da Ordem dos Advogados do Brasil.

3 FACHIN, Zulmar Antonio. O Direito Fundamental à Proteção de Dados Pessoais: Análise da Decisão Paradigmática do STF na ADI nº 6.387-DF. **VIDERE**. V. 14, nº 29, jan-abr. 2022 ISSN: 2177-7837, Páginas 298/313.

e, ao cabo de determinado espaço temporal, eles se incorporam ao acervo já existente. É por essa razão que, nas últimas décadas, tem se desenvolvido em nosso País um processo de reconhecimento gradual do direito fundamental à proteção de dados, tanto na esfera constitucional quanto nas esferas legal e infralegal.

Do ponto de vista constitucional, antes da publicação da EC nº 115/22, a CF já contemplava uma série de direitos que tratavam de questões associadas à proteção de dados pessoais, entre os quais merecem destaque: a inviolabilidade da vida privada, intimidade, honra e imagem das pessoas (art. 5º, X); a inviabilidade de interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), e a proibição da violação de correspondência (art. 5º, XII). Ainda, a CF instituiu o *habeas data* (art. 5º, LXXII) com um importante instrumento de direito de acesso e retificação de dados pessoais.⁴

Do ponto de vista legal, vários normativos já dispunham a respeito da proteção de determinados dados pessoais, de forma esparsa, antes da EC nº 115/2022.

O Código de Defesa do Consumidor (CDC) – Lei nº 8.078/90, por exemplo, estabeleceu em seu artigo 43 uma série de direitos e garantias para o consumidor em relação às suas informações pessoais constantes de “bancos de dados e cadastros”, notadamente no que se refere ao direito de ser informado sobre a abertura de cadastros em seu

4 Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...) X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação;

(...) XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

(...) LXXII – conceder-se-á *habeas data*: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou banco de dados de entidades governamentais ou de caráter público, b) para a retificação de dado, quando não se prefira fazê-lo por processo sigilosos, judicial ou administrativo.

nome e de corrigir seus dados pessoais que tenham sido registrados de forma inexata.⁵

Por sua vez, a Lei nº 12.414/2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito – o chamado cadastro positivo – atribuiu aos denominados “cadastrados” uma série de direitos. Por exemplo, é devida a comunicação ao cadastrado sobre a abertura do cadastro em seu nome no banco de dados, com a indicação dos canais disponíveis para o cancelamento do cadastro em tal banco. O cadastrado também tem o direito de acessar suas informações de forma gratuita e, independentemente de justificativa, solicitar a correção de dados, revisar decisão realizada por meios automatizados e ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual foram coletados. Essa lei consolidou a evolução do conceito de autodeterminação informativa em nosso ordenamento jurídico, na medida em que atribuiu ao titular dos dados pessoais decidir se tem interesse ou não em formar esse histórico e quando deseja cancelá-lo.

A Lei de Acesso à Informação – Lei nº 12.527/2011 dispõe, em seu artigo 31, da forma de tratamento a ser adotada para o compartilhamento das denominadas “informações pessoais”, devendo ser respeitado o direito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais.⁶

5 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. (...) §2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. §3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá solicitar a sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

6 Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

A Lei nº 12.965/2014, também conhecida como Marco Civil da Internet, assegurou aos usuários da internet, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações e dos dados armazenados (art. 7º, II e III).⁷

Do ponto de vista infralegal, vale ressaltar o Decreto nº 6.425/2008, que dispõe sobre o censo anual de educação. Ele faz uso do princípio da finalidade ao determinar que os dados do censo não podem ser utilizados para fins estranhos ao da legislação educacional aplicável e, ainda, menciona expressamente a proteção aos direitos pessoais e ao seu sigilo (art. 6º).⁸

A despeito de todo esse arcabouço constitucional, legal e infralegal existente, antes da implementação da LGPD não havia um reconhecimento claro, por parte da doutrina e jurisprudência, sobre a proteção constitucional aos dados pessoais.

Doneda⁹ expôs sua preocupação nesse sentido ao mencionar que, para parte da doutrina, ainda que a privacidade fosse encarada como um direito fundamental, os dados pessoais estariam protegidos apenas em relação à sua comunicação, conforme reza o art. 5º, XII – que trata do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. Tal interpretação geraria uma

7 Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

8 Art. 6º Ficam assegurados o sigilo e a proteção de dados pessoais apurados no censo da educação, vedada a sua utilização para fins estranhos aos previstos na legislação educacional aplicável.

9 DONEDA, Danilo. Da Privacidade à Proteção de Dados. Revista dos Tribunais, Terceira Edição, 2021, p. 269-272.

grande permissividade em relação à utilização de informações pessoais, segundo o autor.

O posicionamento expressado pelo Supremo Tribunal Federal, em 2006, em decisão relatada pelo ministro Sepúlveda Pertence¹⁰, caminhou nessa linha, eis que reconheceu a garantia da inviolabilidade da comunicação dos dados armazenados em computador com fulcro em garantias constitucionais; mas, por outro lado, não reconheceu a garantia constitucional de proteção dos dados em si mesmos. Conforme Doneda, “esta decisão foi, a partir de então, amplamente referenciada como precedente em julgados nos quais o STF identificou que a natureza fundamental da proteção aos dados estaria restrita ao momento da sua comunicação”.¹¹

Naquela época, também havia um receio de que todos os dados pessoais estariam sob a tutela constitucional, pelo fato de alguns deles não guardarem relação com informações íntimas ou privadas, protegidas pelo direito de privacidade.

Ocorre que, com o tempo, com o desenvolvimento tecnológico e o compartilhamento expressivo dos dados pessoais sob as mais diversas formas, especialmente pelas redes sociais, verificou-se uma tendência a superar esse entendimento expressado pelo STF, até mesmo para compatibilizar a legislação com os fluxos internacionais de proteção de dados pessoais.

A LGPD é um importantíssimo marco legal na proteção de dados no País, representando um diploma legal específico para tratar de

10 “3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve “quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim de apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial.”. 4. **A proteção a que se refere o art. 5º, XII da Constituição, é da comunicação “de dados” e não dos “dados em si mesmos”, ainda quando armazenados em computador**”. ST, Plenário. RE 418.416/sc. Re. Min. Sepúlveda Pertence, 10/5/2006. Publicado no Diário da Justiça em 19.12.2006.

11 DONEDA, Danilo. **Da Privacidade à Proteção de Dados**. Revista dos Tribunais, Terceira Edição, 2021, p. 270-271.

um tema que já vinha sendo objeto de diversos normativos esparsos e que demandavam uniformização em âmbito federal.

1.1. O reconhecimento da proteção dos dados pessoais como direito constitucional pelo STF

Pouco tempo após a publicação da LGPD, em 2020, o Supremo Tribunal Federal proferiu uma importante decisão para o desenvolvimento da proteção de dados no País, ao julgar as Ações Diretas de Inconstitucionalidade (ADIs) 6.387, 6.388, 6.389, 6.390 e 6.393, propostas por diversos partidos políticos e pelo Conselho Federal da Ordem do Advogados do Brasil.

Essas ADIs questionaram a Medida Provisória nº 954/2020, que, entre outros assuntos, determinava que empresas de telecomunicações compartilhassem com o IBGE nome, número de telefone e endereço dos seus consumidores de telefonia móvel e fixa. No entendimento dos requerentes das ADIs, tal prática violaria os seguintes direitos fundamentais insculpidos na CF: dignidade da pessoa humana, inviolabilidade da intimidade e da vida privada e até mesmo à autodeterminação informativa (arts. 1º, III¹² e 5º, X e XII¹³ da CF).

Ao proferir seu voto, a relatora, ministra Rosa Weber, expressou seu entendimento no sentido de que informações relacionadas à identificação de pessoa natural tais como nome, número de telefone e

12 Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como **fundamentos**: (...) III – a **dignidade da pessoa humana**”.

13 “Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X – **são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas**, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...) XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

endereço configuram dados pessoais e integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual, da privacidade e do livre desenvolvimento da personalidade. Por consequência, sua manipulação e tratamento deveriam observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.¹⁴

Ainda segundo a relatora, a aludida medida provisória não conteria interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia e não definiria apropriadamente como e para que seriam utilizados os dados coletados. Tampouco haveria mecanismo técnico ou administrativo apto a proteger de vazamentos acidentais ou da utilização indevida no compartilhamento dos dados, com garantia de sigilo, higidez e, quando fosse o caso, anonimato dos dados pessoais compartilhados. Para a ministra, era excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública (à época, a pandemia do coronavírus) para a finalidade pretendida.

Importante destacar que, na ocasião, ainda não estava em vigor a LGPD e que, conforme entendimento da relatora, situações de emergência – como a crise do coronavírus – não poderiam ser invocadas como pretexto para justificar investidas para enfraquecer direitos e excluir garantias fundamentais previstas na CF, conforme trechos do acórdão a seguir:

“8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.

9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas

14 Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.837 Distrito Federal, Ministra Rosa Weber, Decisão de 07 de maio de 2020.

que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição”.¹⁵

O ministro Luiz Fux, em seu voto, ressaltou que os dados pessoais representam uma *commodity* da economia da informação e que dados como nomes, telefones e endereços são extremamente relevantes para a identificação pessoal e potencialmente gravosos quando cruzados com outras informações compartilhadas por pessoas e por entidades. Citou como exemplos os problemas inerentes às *fake news* e o escândalo envolvendo a Cambridge Analytica, que revelou como modelos de negócios são rentabilizados por meio da análise de dados e pelo seu uso indevido, lesando valores constitucionais – como o da privacidade dos indivíduos.

Como bem salientado por Mendes e Fonseca, o significado histórico dessa decisão deve ser avaliado sob a perspectiva de uma tutela constitucional mais ampla e abstrata do que o direito à inviolabilidade da esfera íntima e da vida privada. Isso porque o conteúdo desse direito fundamental exorbita aquele protegido exclusivamente pelo direito de privacidade, pois não se limita apenas aos dados íntimos ou privados, ao revés, refere-se “a qualquer dado que identifique ou possa identificar um indivíduo”.¹⁶

Quanto aos efeitos gerados por essa proteção, Mendes e Fonseca destacam que, alinhando-se ao conceito de autodeterminação positiva, é possível pensá-los a partir de uma dupla dimensão: de um lado, essa proteção se desdobra como liberdade negativa do cidadão oponível perante o Estado (dimensão subjetiva); do outro lado, ela estabelece uma atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva).¹⁷

15 Referendo na medida cautelar na Ação Direta de Inconstitucionalidade 6.837 do Distrito Federal, ministra Rosa Weber, decisão de 07 de maio de 2020.

16 MENDES, Laura Schertel e FONSECA, Gabriel Campos Soares da. STF Reconhece Direito Fundamental à Proteção de Dados. Revista de Direito do Consumidor. RDC 130. 2020, p. 474-475.

17 MENDES, Laura Schertel e FONSECA, Gabriel Campos Soares da. STF Reconhece Direito Fundamental à Proteção de Dados. Revista de Direito do Consumidor. RDC 130. 2020, p. 475.

A ministra Rosa Weber foi acompanhada em seu voto pelos demais ministros, exceto pelo ministro Marco Aurélio Mello. A discordância do ministro foi pautada, entre outras justificativas, no fato de que a Medida Provisória nº 954/2020, que autorizou que empresas de telecomunicações compartilhassem determinados dados pessoais de seus usuários com o IBGE, foi editada para ser aplicada exclusivamente durante a situação de emergência de saúde pública decorrente do coronavírus, já que, naquele período, o IBGE estava impossibilitado de visitar domicílios e residências para colher dados. Segundo o ministro, a referida medida provisória continha uma série de medidas que deveriam ser adotadas pelo IBGE para minimizar riscos aos titulares dos dados pessoais, como a utilização exclusiva dos dados pelo instituto, para finalidade específica de levantamento estatístico; a posterior eliminação daquelas informações de sua base de dados; a possibilidade de recusa de fornecimento de informações pelos titulares e o caráter sigiloso do compartilhamento dos ditos dados.

1.2. A Emenda Constitucional Nº 115, de 10 de fevereiro de 2022 (EC nº 115/2022)

Haja vista o cenário de ampla proteção aos dados pessoais que vinha sendo desenhado no País e com vistas ao reconhecimento formal da natureza de garantia constitucional autônoma àqueles dados, foi aprovada a Proposta de Emenda à Constituição nº 17/2019 (PEC 17/2019), de iniciativa do senador Eduardo Gomes, e promulgada a EC nº 115/2022.¹⁸

¹⁸ Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:

“Art. 5º (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Art. 2º O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:

“Art. 21. (...) XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.” Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:

“Art. 22. (...) XXX - proteção e tratamento de dados pessoais. (..) (NR)

Art. 4º Esta Emenda Constitucional entra em vigor na data de sua publicação.

A EC nº 115/2022 acrescentou o inciso LXXIX ao art. 5º da Constituição Federal, atribuindo, de forma expressa, status constitucional ao direito à proteção aos dados pessoais; e, ainda, atribuiu como competência exclusiva da União legislar sobre a proteção e tratamento de dados pessoais, bem como organizar e fiscalizar o seu cumprimento.

Na justificação apresentada na PEC nº 17/2019, foram apresentadas importantes razões para as mudanças propostas: países de todo o planeta já visualizavam a importância e a imprescindibilidade de se regular juridicamente o tratamento de dados cidadãos, como era o caso dos membros da União Europeia e de alguns países da América do Sul (como Chile e Argentina); o Brasil necessitava muito mais do que uma lei ordinária sobre o tema proteção de dados, apesar da envergadura jurídica da LGPD; era necessário estabelecer uma legislação uniforme quanto à proteção dos dados, tendo em vista ser praticamente impossível aos governos e empresas de todo o mundo se adaptarem às normas específicas de cada localidade; e a existência de pluralidade normativa poderia trazer problemas de contabilidade e adequação dos dados, em especial nos serviços disponibilizados pela rede mundial de computadores, que utilizam os dados pessoais de formas cada vez mais abrangentes e inovadoras.¹⁹

A Comissão de Constituição, Justiça e Cidadania do Senado Federal, ao apreciar a PEC nº 17/2019, reforçou que a proteção dos dados pessoais se tornou um grande desafio aos legisladores de todo o mundo, especialmente em tempos de mudanças das relações sociais e avanços tecnológicos, que motivaram a necessária modificação da legislação para se adequar a essa nova realidade. Também salientou que, naquela época, doutrina e jurisprudência já reconheciam que o direito à privacidade ia além da proteção da vida íntima do indivíduo, passando também por seus dados pessoais e que, por esse motivo, o Congresso Nacional não deveria medir esforços para “solucionar o hiato existente entre a legislação e realidade”.²⁰

19 PEC nº 17/2019, disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline&_gl=1*1y7gao*_ga*MTA-xNzg4MDU5OS4xNjYzOTMwMDc5*_ga_CW3ZH25XMK*MTcwMTI3NTAzMC4yLjAuMTcwMTI3NTAzMC4wLjAuMA.

20 Parecer da CCJ do Senado Federal sobre a PEC nº 2017/201, disponível em <https://legis.senado.leg.br/sdleg-getter/documento?dm=7956536&ts=1620769236520>

2. A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

Com a promulgação da EC nº 115/2002, as discussões sobre a natureza do direito de proteção aos dados pessoais foram superadas, na medida em que lhes foi atribuído o status de um direito fundamental autônomo e explícito, previsto no art. 5º da CF. Essa natureza de direito autônomo tem por base o princípio da dignidade humana, definida por Sarlet:

“Assim sendo, temos por dignidade humana a qualidade intrínseca e distintiva reconhecida a cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos, mediante o devido respeito aos demais seres que integram a rede da vida”.²¹

Ao adquirir o status de um direito fundamental autônomo, importantes garantias constitucionais ficam asseguradas aos titulares dos dados pessoais.

Por exemplo, o direito à proteção de dados é caracterizado como uma cláusula pétrea e, por conseguinte, ele não pode ser objeto de proposta de emenda que o pretenda abolir, nos termos do art. 60, §4º, da CF.²²

21 SARLET, Ingo. Dignidade (da Pessoa) Humana e os Direitos Fundamentais na Constituição Federal de 1988. 10ª Edição. Porto Alegre. Livraria do Advogado, p. 70-71.

22 Art. 60. A Constituição poderá ser emendada mediante proposta:

(...)

§4º Não será objeto de deliberação a proposta de emenda tendente a abolir:

(...) IV – os direitos e garantias individuais”.

Ademais, nos termos do art. 5º, I, da CF²³, as normas relativas aos direitos e garantias fundamentais – neles inserida a proteção de dados – têm aplicação imediata, ou seja, não é necessária nenhuma formalidade adicional para que possam ser aplicadas, nos termos da legislação.

Outras características inerentes aos direitos fundamentais, citadas por Silva²⁴, são:

1) Complementaridade/interdependência: os princípios e garantias fundamentais são complementares entre si e devem ser analisados, exercidos e garantidos conjuntamente;

2) Historicidade: não são estanques, acompanham a evolução social;

3) Imprescritibilidade: não prescrevem, podem ser exercidos a qualquer momento;

4) Inalienabilidade: por não possuírem conteúdo econômico-patrimonial, são intransferíveis, inegociáveis e indisponíveis;

5) Inviolabilidade: devem ser observados por disposições infraconstitucionais ou por atos das autoridades públicas;

6) Irrenunciabilidade: não podem ser renunciados, observadas certas limitações;

7) Relatividade: podem ser relativizados em determinadas situações; e

8) Universalidade: são extensivos a todos os indivíduos.

3. O PAPEL DA ANPD NA PROTEÇÃO AOS DADOS PESSOAIS

A EC nº 115/2022 também conferiu mais segurança jurídica aos titulares dos dados pessoais ao atribuir à União a competência le-

23 Art. 5º (...) §1º. As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.

24 SILVA, Priscilla. Estudos Sobre Privacidade e Proteção de Dados: Capítulo 18: A proteção de dados como um direito fundamental. Revista dos Tribunais, 2021, p. 491-509.

gislativa privativa para tratar de temas afetos à proteção e tratamento de dados pessoais e para organizar e fiscalizar a proteção e o tratamento de dados, na forma da lei.

Antes da promulgação da EC nº 115/2022, existiam diversos normativos tratando do tema e várias autoridades exercendo papel fiscalizatório, o que poderia levar a entendimentos distintos por parte dessas autoridades e fiscalizações concomitantes.

Por consequência, a partir da EC nº 115/2022, a União passou a dar diretrizes necessárias sobre a proteção de dados pessoais no Brasil, por meio da Autoridade Nacional de Proteção de Dados (ANPD), na qualidade de “órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação”.²⁵

Dentre as formas de estabelecer tais diretrizes sobre a proteção de dados, a ANPD vem publicando determinados guias orientativos, previamente submetidos à consulta pública e processos de audiência pública, para que seja assegurado a todos os interessados o direito de participar da elaboração desses documentos. Até o momento da elaboração deste artigo, já foram divulgados pela ANPD os seguintes guias orientativos: Guia Orientativo de Tratamento de Dados para Fins Acadêmicos e para a Realização de Estudos e Pesquisas²⁶, Guia Orientativo de Cookies e Proteção de Dados Pessoais²⁷, Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público²⁸, Guia Orientativo de Aplicação da LGPD por Agentes de Tratamento no Contexto Eleitoral²⁹, Guia Orientativo de Segurança da Informação para Agentes de

25 De acordo com o Guia Orientativo da ANPD para tratamento de dados pessoais pelo Poder Público, “a ANPD é o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação, no que se inclui a deliberação administrativa, em caráter terminativo, sobre a interpretação da lei e sobre as suas próprias competências e casos omissos (artigo 55-K, parágrafo único; artigo 55-J, XX)”.

26 <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>

27 <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>

28 <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>

29 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf

Tratamento de Pequeno Porte³⁰, e Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.³¹

A ANPD também vem editando normas infralegais que dispõem, dentre outros temas, sobre o processo de fiscalização e o processo administrativo sancionador no âmbito da ANPD (Resolução CP/ANPD nº 1/2021), sobre o regulamento da aplicação da LGPD para agentes de tratamento de pequeno porte (Resolução CP/ANPD nº 02/2022) e sobre o regulamento de dosimetria e aplicação de sanções administrativas (Resolução CP/ANPD nº 04/2023).

4. CONSIDERAÇÕES FINAIS

Os processos de proteção aos dados pessoais começaram a ser implementados no Brasil como reflexo de uma demanda internacional decorrente da evolução dos meios digitais de comunicação e da necessidade premente dos titulares dos dados.

Assim, acompanhando um movimento mundial de atualização dos normativos até então em vigor, o Brasil passou, ao longo do tempo, pela interpretação doutrinária e jurisprudencial dos direitos e princípios existentes na Constituição Federal e atualização dos seus normativos até chegar à EC nº 115/2022, um importante marco para a proteção de dados pessoais no País, em conjunto com a LGPD.

Uma vez assegurado, de forma expressa, o direito à proteção de dados pessoais como um direito fundamental, os titulares possuem segurança jurídica suficiente para assegurar que eles não serão abolidos (por se tratar de cláusula pétrea) e que eles têm as proteções constitucionais inerentes a todos os demais direitos fundamentais, incluindo a imprescritibilidade, irrenunciabilidade e inalienabilidade.

Por óbvio, a realidade sofre sucessivas mudanças – e essas são bastante rápidas nos meios digitais – e, por essa razão, é necessário um

30 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps_defeso_eleitoral.pdf

31 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado_defeso_eleitoral.pdf

olhar atento para as novas transformações sociais defronte aos normativos aplicáveis, para que os direitos dos titulares estejam assegurados.

Nesse sentido, a ANPD tem sido um órgão de relevante importância para assegurar a efetiva participação dos indivíduos na elaboração e revisão de normativos e guias orientativos. É crucial que esses trabalhos sigam em pleno movimento, para tornar efetivos todos os princípios e garantias estabelecidos constitucionalmente aos titulares dos dados pessoais.

REFERÊNCIAS

DONEDA, Danilo. Da Privacidade à Proteção de Dados. **Revista dos Tribunais**, Terceira Edição, 2021.

FACHIN, Zulmar Antonio. O Direito Fundamental à Proteção de Dados Pessoais: Análise da Decisão Paradigmática do STF na ADI nº 6.387-DF. **VIDERE**. V. 14, nº 29, jan-abr. 2022 ISSN: 2177-7837, Páginas 298-313.

MENDES, Laura Schertel e FONSECA, Gabriel Campos Soares da. STF Reconhece Direito Fundamental à Proteção de Dados. **Revista de Direito do Consumidor**. RDC 130. 2020. Páginas 474-475.

MENDES, Laura Schertel. O Direito Fundamental à Proteção dos Dados Pessoais. **Revista de Direito do Consumidor**. RDC, v. 20, nº 79, jul./set. 2011. Páginas 45-82.

SILVA, Priscilla. Estudos Sobre Privacidade e Proteção de Dados: Capítulo 18: A proteção de dados como um direito fundamental. **Revista dos Tribunais**. Páginas 491-509, 2021.

SARLET, Ingo. Dignidade (da Pessoa) Humana e os Direitos Fundamentais na Constituição Federal de 1988. 10ª Edição. Porto Alegre. **Livraria do Advogado**, Páginas 70-71.

DIREITOS DOS TITULARES DE DADOS SOB A PERSPECTIVA DA LGPD

Ivana Avellar Nicolau de Lima e Silva¹

INTRODUÇÃO

Para abordar os direitos dos titulares de dados pessoais, necessário se faz analisar de forma resumida o desenvolvimento do conceito de privacidade no decorrer dos séculos. O conceito idealizado por Aristóteles, na Grécia Antiga, distingue a esfera pública (*polis*) da esfera privada (*oikos*).

Em sua origem, o conceito de privacidade significava a não intervenção do Estado na vida dos cidadãos. O conceito desenvolveu-se até chegar à ideia da não intromissão na vida alheia de nenhuma forma e por ninguém.

Em 1890, os juristas Warren e Brandeis, em artigo publicado em revista acadêmica, definiram a privacidade como o “direito de estar só”, criando, assim, uma nova perspectiva na definição do direito à privacidade. Eles reconheceram as premissas de Aristóteles, mas foram além: defenderam que o direito deve evoluir e se adaptar a novas realidades, em função de novas tecnologias – câmeras fotográficas instantâneas, por exemplo.

A visão clássica de privacidade já não se aplicava mais ao indivíduo dentro de uma sociedade da informação, produto do desenvolvimento tecnológico ocorrido nas últimas décadas. O conceito precisou evoluir, sendo necessário admitir que a proteção dos dados pessoais é uma das facetas do conceito maior de privacidade.

1 Advogada, especialista em Proteção de Dados Pessoais, atuando na adequação condicional à Lei Geral de Proteção de Dados. Pós-graduada em Direito ao Uso e Proteção de Dados Pessoais pela PUC Minas.

A privacidade, atualmente, deve ser entendida como controle. Controle do titular sobre suas informações pessoais, garantindo a ele o direito de acessar, alterar e excluir, em determinados contextos, as suas informações. Tal controle recebe o nome de autodeterminação informativa, um dos fundamentos da disciplina de proteção de dados, previsto no art. 2º, II, da Lei Geral de Proteção de Dados (LGPD).

A LGPD, alinhada ao Regulamento Europeu, reproduz grande parte dos mesmos princípios fundamentais, trazendo o direito à proteção de dados como elemento autônomo. Nessa vertente, o Senado Federal, em 02 de julho de 2019, aprovou proposta de emenda à Constituição que inclui no texto constitucional, de maneira expressa, a proteção de dados pessoais como um direito fundamental.

Com a aprovação da PEC 17/2020 e posterior promulgação, em fevereiro de 2022, da Emenda Constitucional 115/2022, foi acrescentado o inciso LXXIX ao art. 5º da Constituição Federal, dispondo que “é assegurado, nos termos da lei, direito à proteção dos dados pessoais, inclusive nos meios digitais”, elevando o direito à proteção de dados pessoais à categoria de direito fundamental.

Desta forma, será feita uma análise de alguns dos direitos dos titulares garantidos pela LGPD – uma vez que não é possível esgotar o assunto no presente artigo.

1. DIREITOS DOS TITULARES: PRINCÍPIOS, GARANTIAS E INSTRUMENTOS DE PROTEÇÃO

A LGPD assegura a proteção e o livre desenvolvimento da personalidade da pessoa natural. A lei possui, assim, caráter objetivo, de proteção específica dos dados pessoais. Neste sentido, os direitos nela elencados dizem respeito apenas às pessoas físicas, excluindo as pessoas jurídicas de seu escopo. O legislador, aqui, maximizou as garantias do titular dos dados pessoais, garantindo a eles especial status.

Por outro lado, a proteção de dados pessoais não se exaure na proteção dos direitos dos titulares, ou seja, os dados pessoais são tutelados independentemente da manifestação da vontade dos seus titulares.

O art. 17 da mencionada lei, considerado a base dos direitos dos titulares, garante que o preceito normativo não se limite a regular apenas as atividades de tratamento e a tutelar os dados pessoais, mas também confere direitos aos titulares para que eles possam proteger seus dados.

A LGPD estabelece ao titular os papéis de destinatário, de legitimado e de beneficiário para a proteção dos dados pessoais. O titular, por meio da lei, tem seus direitos tutelados e ele próprio pode exercê-los para a proteção de suas informações pessoais.

É imprescindível considerar, antes de abordar os direitos do titular, que o inciso X do art. 5º da LGPD define que qualquer operação realizada sobre os dados pessoais é considerada tratamento de dados pessoais.

A seguir, expõem-se alguns direitos garantidos pela lei aos titulares:

- **Direito à confirmação da existência de tratamento:**

Dentre os direitos assegurados pela LGPD, em especial no art. 18, observa-se o direito que permite ao titular a possibilidade de confirmar a existência de tratamento de seus dados pessoais sem a exigência de apresentação de justificativa – muito embora de acordo com o princípio da transparência (art. 6º, VI) o titular deva ser informado, antes de seus dados serem coletados, sobre a maneira que suas informações pessoais serão tratadas.

O art. 2º da LGPD lista a autodeterminação informativa como um dos fundamentos da lei, conferindo ao titular o direito de controlar e proteger o acesso aos seus dados pessoais. A autodeterminação informativa garante ao titular o direito ao conhecimento do tratamento realizado por determinado controlador e da forma como é feito. O titular tem o direito de controlar seus próprios dados.

Ainda há, porém, um descontrole informacional: os titulares não sabem quem coletou, com quem estão e como seus dados estão sendo tratados. Eis a importância do direito ao conhecimento da existência de tratamento na LGPD.

- **Direito de acesso aos dados:**

Para o exercício do direito de acesso aos dados, previsto no inciso II do art. 18, é necessário o conhecimento prévio da existência do tratamento de dados. O titular poderá ter acesso aos dados e suas informações, como prazo de conservação e existência de decisões automatizadas, por exemplo.

O direito de acesso não é apenas um mero direito previsto na LGPD, mas uma ferramenta para a efetivação do direito fundamental à proteção de dados, que também está relacionado a um dos fundamentos da lei: a autodeterminação informativa.

- **Direito à correção dos dados incompletos, inexatos e/ou desatualizados**

Quanto ao direito à correção de dados incompletos, inexatos ou desatualizados, previsto no inciso III do art. 18 da LGPD, a intenção do legislador foi evitar fraudes causadas pela falta de precisão dos dados, principalmente em ambiente on-line. Dados incompletos e inexatos devem ser corrigidos.

A requisição de alteração de dados deve partir do próprio titular, pois o controlador não dispõe de meios para saber se houve modificações sem que ele mesmo faça a provocação. Além disso, considerando a complexidade do tratamento e o modelo de negócio, por exemplo, poderá o controlador criar mecanismos de autenticidade para averiguar a identidade e a legitimidade do titular que está requisitando a correção de dados pessoais incompletos, inexatos ou desatualizados.

Para se efetivar este direito, as organizações devem implementar um processo de gestão voltado ao recebimento das solicitações de correção de dados pessoais. Tal processo deve ser bem estruturado, garantindo um canal de comunicação capaz de coletar a solicitação, analisar, adotar soluções em tempo hábil e fornecer resposta fundamentada ao titular. Lembrando que, em situações em que o agente de tratamento não consiga tecnicamente efetuar a correção, o controlador deverá adotar todas as medidas possíveis para realizá-la.

- **Direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade (art. 18, inciso IV, da LGPD)**

A anonimização está elencada como um dos direitos do titular, mas o exercício de tal direito não ocorre de forma absoluta, tendo em vista que, no art. 7º, IV, a LGPD prevê não ser possível exigir do controlador a adoção do processo de anonimização se este for considerado impossível.

O art. 12 da LGPD estabelece que os dados anonimizados não são considerados dados pessoais, uma vez que a própria lei define pessoas como identificadas ou identificáveis. A anonimização dos dados garante que o titular não seja identificado, portanto, não são dados pessoais. Porém, no campo da ciência da computação, pesquisadores vêm demonstrando que as técnicas de anonimização não são 100% seguras, podendo ocorrer falhas, sendo impossível de se garantir o anonimato absoluto e irreversível. Dessa forma, conclui-se que dados anonimizados podem, sim, ser identificados.

Ainda falta clareza quanto à aplicação dos processos de anonimização existentes, o que de certa forma gera insegurança jurídica. Espera-se da Autoridade Nacional de Proteção de Dados (ANPD) que elabore um guia de uso da anonimização de dados pessoais adequado à atual realidade.

Segundo Garcia², o bloqueio é a suspensão temporária de qualquer operação de tratamento mediante a guarda do dado pessoal ou do banco de dados. A temporalidade se dá até que a irregularidade seja sanada, conforme define a letra da lei. Trata-se, portanto, do direito que tem o titular de obter restrição quanto ao tratamento em situações específicas.

Sendo assim, enquanto houver bloqueio, o controlador não poderá tratar aqueles dados – ressaltando que essa restrição é temporária.

O direito ao apagamento dos dados pessoais significa o direito à eliminação dos dados a pedido do titular. A eliminação de dados pes-

2 GARCIA, Valéria Reani Rodrigues. LGPD, Direito dos Titulares. Forum, vol I, 2023, p.103.

soais também não é um direito absoluto, uma vez que a própria lei, no art. 16, autoriza a possibilidade de conservação dos dados mesmo após o esgotamento da finalidade do tratamento, havendo obrigação legal ou regulatória a ser observada pelo controlador.

Destaca-se aqui que, embora o atendimento à solicitação do titular não se dê de maneira absoluta, conforme exposto anteriormente, o titular tem o direito de solicitar a eliminação de quaisquer de seus dados pessoais que sejam desnecessários, excessivos e sem hipótese de tratamento definida pela lei.

- **Direito à portabilidade**

No contexto atual, em que as grandes empresas aglutinam a maior parte do mercado, a LGPD assegura aos titulares o direito à portabilidade, que serve como ferramenta de gestão que facilita a tomada de decisões por parte do titular. Por este direito, poderá o titular de dados obter, junto ao controlador, seus dados de forma estruturada para serem transferidos a outro controlador.

A regra da portabilidade, prevista no art. 18, V, da LGPD, é clara: visa à garantia da possibilidade de o titular contratar o controlador concorrente, exercendo, assim, sua livre escolha. O controlador só fornecerá as informações relativas ao próprio titular, pois a lei prevê a preservação dos segredos comerciais e industriais.

A portabilidade é um direito individual, pois permite ao titular-consumidor não só a gestão de seus dados, mas a possibilidade de ser protagonista no ecossistema da informação.

- **Direito à revogação do consentimento:**

Conforme prevê o art. 5º, XII, da LGPD, considera-se “consentimento” a manifestação livre, informada e inequívoca pela qual o titular de dados concorda com o tratamento de seus dados pessoais para determinada finalidade. O consentimento corrobora com os valores e princípios constitucionais, pois exerce um papel importante nas decisões de cada indivíduo, além de dialogar com os princípios da autonomia privada e da autodeterminação informativa.

Antes de assinar o termo de consentimento, o titular deverá receber todas as informações necessárias e suficientes para analisar a

situação e a forma como serão tratados seus dados, significando dizer que apenas dessa maneira seu consentimento será manifestado, conforme previsto no art. 9º da LGPD.

A lei elenca o consentimento como uma das 10 hipóteses legais que autorizam o tratamento dos dados pessoais comuns e uma das 8 hipóteses para tratamento de dados sensíveis. É importante salientar, porém, que a revogação pode se dar a qualquer tempo, não havendo nenhuma condicionante para esta revogação, podendo ocorrer até mesmo no instante seguinte ao consentimento.

O consentimento será considerado nulo quando for requerido mediante informações fornecidas ao titular com conteúdo enganoso, abusivo, sem transparência, de forma duvidosa; configurando, assim, vício de consentimento. É vedado, nesta hipótese, o tratamento dos dados, de acordo com o art. 8º, §3º, da LGPD.

A qualquer momento, o consentimento poderá ser revogado, mediante manifestação expressa do titular, sem custos. Entretanto, existe questionamento quanto à forma que a revogação poderá ser instrumentalizada. A LGPD não disciplinou essa questão, porém, a disponibilização de canais de contato (como e-mail, telefone e espaços em sites) atendem à determinação legal. O prazo de até 15 dias, contados da data do requerimento, poderá ser utilizado pelo controlador no atendimento ao direito de revogação do consentimento, em analogia ao disposto no art. 19, inciso II, da mesma Lei.

Acredita-se que, em momento oportuno, a Autoridade Nacional de Proteção de Dados regulamentará e desenvolverá orientação voltada ao atendimento dos direitos aos titulares.

2. CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados traz consigo a árdua missão de alterar paradigmas quanto à proteção de dados pessoais e privacidade. O mundo está cada vez mais conectado – o que não é novidade para mais ninguém.

No contexto atual, dados pessoais são fornecidos a todo momento, em vários contextos: para ter acesso a um aplicativo, para frequentar uma academia, para matricular os filhos em uma escola, para participar de uma festa em determinado condomínio. Os titulares agem naturalmente ao fornecerem seus dados em nome de uma cultura equivocada e incoerente, que entende que a privacidade se resume a trancar a porta de sua casa ou não aceitar a violação de uma correspondência. Não questionam a necessidade e a finalidade da coleta de seus dados por normalizarem a conduta dos agentes de tratamento. Simplesmente os fornecem, muitas vezes sob o contexto da segurança, sob a concessão de descontos ou até mesmo por entenderem que, em uma sociedade digital, fornecer seus dados pessoais é o normal.

O desequilíbrio se instaurou: a todo tempo, pessoas são vigiadas, manipuladas, têm a privacidade violada. Os novos modelos de negócios, surgidos nos anos 1990, têm uma dependência muito maior de fluxos internacionais de bases de dados, especialmente os relacionados a pessoas; e inspiraram o surgimento de regulamentações de proteção de dados.

A LGPD não é a primeira lei que regula e protege os titulares de dados pessoais, e sua vigência não revoga outros dispositivos legais — como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo — que continuam coexistindo no ordenamento jurídico e sendo aplicados de forma conjunta. Tamanha é a importância da LGPD que um de seus fundamentos é a autodeterminação informativa, prevista no art. 2º, II, cláusula aberta de proteção que confere ao titular o direito de controlar e proteger o acesso a seus dados pessoais.

A autodeterminação informativa protege a privacidade pois confere ao titular o poder de se informar e tomar decisões sobre seus dados pessoais. Assim, ele tem o conhecimento do tratamento realizado pelo controlador: quais dados são coletados e para qual finalidade. A autodeterminação confere o direito de dar o seu consentimento para o tratamento de seus dados.

A LGPD não proíbe o tratamento de dados pessoais, apenas estabelece parâmetros para sua realização, protegendo tais dados e

dando ao titular o total controle de suas informações pessoais. A lei é essencial, pois o agente de tratamento de dados tem acesso a direitos elementares de seus titulares, como saúde, privacidade e educação. Tal acesso justifica a existência de fundamentos para que terceiros tenham autorização legal, descrita nas hipóteses de realização de tratamento, caso contrário, a atividade de tratamento seria ilícita.

Do titular de dados demanda-se a necessidade de vigília contra a atividade abusiva e exploratória de informações. A LGPD coloca o titular em posição de proteção e controle, fornecendo mecanismos capazes de garantir a efetivação de direitos fundamentais – porém, para que isso possa se concretizar, a maturidade e a cultura da privacidade e proteção de dados precisam estar presentes na sociedade da informação.

REFERÊNCIAS

FRANCOSKI, Denise de Souza Luiz; TEIVE, Marcello Muller. **LGPD – Direito dos Titulares**. Belo Horizonte: Forum, 2023.

GARCIA, Valéria Reani Rodrigues. **LGPD – Direito dos Titulares**. Forum, vol I, 2023, p.103.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD – Lei Geral de Proteção de Dados Comentada**. 4ª ed. São Paulo: Revista dos Tribunais, 2022.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018 (LGPD)**. 2ª ed. São Paulo: Saraiva, 2020.

A APLICAÇÃO DO PODER SANCIONATÓRIO PELA AUTORIDADE NACIONAL DE DADOS PESSOAIS (ANPD) NA ERA DA GOVERNANÇA DIGITAL

Joelane Rodrigues Carvalho¹

Eduarda Moraes Chacon Rosas²

INTRODUÇÃO

A Agência Nacional de Proteção de Dados Pessoais, ANPD, emergiu no cenário brasileiro como instituição essencial para a normatização e supervisão do tratamento de dados pessoais, nos termos da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018. Este processo não foi rápido e nem fácil.

A Medida Provisória 869/2018, posteriormente convertida na Lei 13.853/2019, dispôs sobre a criação da ANPD, cuja estrutura regimental e quadro de cargos foram estabelecidos pelo Decreto nº 10.474/2020 (alterado pelo Decreto nº 10.975/22 e pelo Decreto 11.758/23³). Em 6 de dezembro de 2020 foram nomeados os cinco Diretores da autoridade, dentre os quais o primeiro Presidente, Sr. Waldermar Ortunho.

No dia 08 de março de 2021 foi publicado o Regimento Interno da ANPD, que trouxe consigo significativa mudança estrutural na entidade mediante a redistribuição de diversas competências às Coordenações, competências estas originalmente atribuídas por lei e

1 Graduada em Direito pela Universidade de Brasília

2 Doutoranda pela Universidade de Brasília

3 Que alterou as regras para nomeação dos membros do Conselho de Proteção de Dados (CNPd).

decreto ao Conselho Diretor. Este fato, aliás, levanta questionamentos a respeito da legalidade do regimento que distribuiu atribuições de modo diverso da lei.

Finalmente, em 13 de junho de 2022, saiu a Medida Provisória nº 1.124/22, convertida em Lei Ordinária 14.460/2022, que consagrou a ANPD, até então vinculada à Presidência da República, como autarquia de direito especial. A providência atendia aos anseios de estudiosos e profissionais da área de proteção de dados por uma instituição “independente” e “autônoma” – medida que foi um dos últimos atos do Governo do Presidente Jair Bolsonaro.

Em janeiro de 2023, o Presidente eleito Luís Inácio Lula da Silva fez publicar o Decreto nº 11.348 que aprovou a estrutura regimental, quadro de cargos e de funções do Ministério da Justiça e Segurança Pública, oportunidade na qual a ANPD foi vinculada a este Ministério por força do artigo 2º, inciso IV, alínea “b”.

Com o posterior Decreto nº 11.758/2023, o Ministério da Justiça (MJ) assumiu o controle político do Conselho de Proteção de Dados (CNPd) da ANPD: será atribuição do Ministro da pasta aprovar os nomes dos futuros membros (listas tríplexes) e encaminhar a lista final à Presidência da República para nomeação – atribuição anteriormente delegada à autoridade. O ministério indicará também o representante que presidirá o CNPD. Ainda no âmbito desta agenda “digital”, o MJ nomeou Assessora Especial para Direito Digital, posição atualmente ocupada por especialista que integra o *High-Level Advisory Board on Artificial Intelligence*, órgão consultivo da ONU, criado para debater sobre a “governança global da Inteligência Artificial”.

Como se percebe, no contexto político – passados três anos de sua criação – a ANPD enfrenta desafios significativos de estabilização e desenvolvimento de autonomia decisória e orçamentária. Tanto é que até hoje não se viabilizou a realização de concurso público para preenchimento dos quadros da instituição por profissionais que não sejam concursados provenientes da administração pública.

Os “braços” da autoridade, assim, são os funcionários públicos de carreira que ingressaram na autoridade via seleções internas e/ou cessões. E faz sentido que assim seja, aliás, considerados os valores das próprias funções disponibilizadas nos atos normativos que regem a estrutura da autarquia, modestos em relação ao nível de especialização e responsabilidade esperado dos ocupantes, principalmente nos cargos-chave.

Com efeito, o orçamento é um problema antigo na ANPD, o que tem sido relatado em notícias recentes disponibilizadas no Terra⁴ e no Carta Capital⁵. Curiosamente, ambas as matérias ventilam a possibilidade de que a autoridade se torne também órgão normatizador e fiscalizador da inteligência artificial (IA), desejo que vem publicamente manifestando os seus Diretores.

Do ponto de vista operacional, apesar de agendas bianuais arrojadas, muitos têm a impressão de que a autarquia está superestimando sua própria capacidade de entrega, envolvida em diversas iniciativas distintas e sem conseguir dar a devida atenção e a necessária vazão a questões regulatórias urgentes e pendentes, como a transferência internacional de dados e a revisão de decisões automatizadas, por exemplo.

Em dezembro de 2023, a ANPD aprovou o Mapa de Temas Prioritários para o biênio 2024-2025 (por meio da Resolução CD/ANPD nº10/23), documento na qual se propôs a dedicar 2025 a dois temas da maior importância: mapear riscos pertinentes ao uso de dados pessoais para reconhecimento facial por IA e mapear/regular o impacto da raspagem de dados.

Ato contínuo, via Resolução CD/ANPD nº 11/23, alterou a agenda regulatória para o biênio 2023-2024 que contempla importantes

4 ANPD atua por orçamento maior em meio a PLs no Congresso para regular economia digital e IA. **Terra**. Disponível em <<https://www.terra.com.br/noticias/checamos/anpd-atua-por-orcamento-maior-em-meio-a-pls-no-congresso-para-regular-economia-digital-e-ia,84fb3ca5dc8cb0668ecf7c4ca04cd236vlu12t0l.html>>. Acesso em 02 jan. 2024.

5 Sem estrutura e orçamento, ANPD ainda pode ser o regulador da Inteligência Artificial. **Capital Digital**. Disponível em <<https://capitaldigital.com.br/sem-estrutura-e-orcamento-anpd-ainda-pode-ser-o-regulador-da-inteligencia-artificial/>>. Acesso em 02 jan. 2024.

iniciativas e projetos em andamento como regulação de comunicação de incidentes de segurança; regulamentação do legítimo interesse; regulamentar direitos dos titulares, dentre os quais revisão de decisões automatizadas (art. 20 da LGPD); transferência internacional de dados pessoais; regulamentar o RIPD (Relatório de Impacto à Proteção de Dados Pessoais) e as funções do Encarregado de Dados; disciplinar compartilhamento de dados pelo Poder Público e o uso da biometria; regulamentar o art. 46 da LGPD e dispor sobre padrões técnicos mínimos de segurança; elaborar Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e dispor sobre o art. 50 e as boas práticas de Governança de que tratam o dispositivo – entre outras iniciativas.

Para se consolidar como futuro órgão de regulação e fiscalização da IA, a ANPD está tentando mostrar sua capacidade técnica e operacional na área por meio de iniciativas como a análises e notas técnicas (relativas ao Projeto de Lei nº 2338/23 – que se propõe a regulamentar a IA), tomada de subsídios para realização de *sandboxes* de IA e inclusão de temas como revisão de decisão automatizada, biometria e “inteligência artificial” na agenda bianual 23-24.

Os desafios que rodeiam a ANPD, diante do contextualizado, são robustos. Mesmo um órgão com orçamento vasto e independência política teria dificuldade em alcançar objetivos tão ambiciosos como os anunciados pela autoridade. Não bastasse, a agência precisa se projetar no cenário internacional, tanto sendo incluída nos ambientes de discussão da tecnologia, privacidade e proteção de dados, quanto sendo reconhecida como um *Data Protection Authority* forte e bem estruturado por seus pares e organizações internacionais.

Este artigo se propõe a analisar duas das diversas facetas da ANPD, em meio a este complexo ecossistema em que se encontra: a de autoridade que de um lado sabe (i) reconhecer os esforços de seus fiscalizados para recompensá-los, em termos de governança da privacidade; mas que do outro (ii) não deixará de puni-los na medida de suas falhas, com proporcionalidade e equidade.

Isso porque a governança da privacidade e da proteção de dados é iniciativa valorosa, amparada internacionalmente, e que reflete a eficiência dos esforços envidados pela iniciativa privada para a conscientização (educação) e prevenção de incidentes de segurança e de riscos. Enquanto isso, o processo sancionatório – o outro lado da mesma moeda – é o resultado das escolhas dos agentes de tratamento que os levam à não conformidade legal, possivelmente em razão da não adoção (ou adoção insuficiente) de medidas e providências adequadas. Acontece que a não correção destes comportamentos inadequados pode refletir, em alguma medida, uma falha da própria autoridade na regulação do mercado.

Isso tudo partindo da premissa de que a missão da ANPD é estabelecer uma cultura de privacidade, os processos sancionatórios – e as fases que o antecedem – pode representar uma oportunidade para a autoridade (que é a única autoridade pública tecnicamente capacidade para tanto) compreender quais as dificuldades dos agentes de tratamento de dados pessoais e de que modo aperfeiçoar seu próprio trabalho.

Pois bem. Para deixar clara a importância da relação entre governança e sanção, faz sentido remeter à metáfora sobre “*the carrot and the stick*”, suficientemente conhecida e traduzida aqui como “a cenoura e o bastão”. The Cambridge Dictionary explica, em tradução livre, que a expressão representa um sistema no qual a pessoa é recompensada por algumas ações, enquanto sofre ameaça de ser punida por outras⁶.

A Wikipedia esclarece que se trata da combinação entre recompensa e punição para fins de induzir um comportamento desejável⁷. Originalmente, cartunistas retratavam corridas de burros em que o animal que seguia uma cenoura pendurada à sua frente corria melhor do que aquele que era apossado com golpes de vara. Décadas depois, Winston Churchill utilizou a expressão em uma carta para descrever a relação entre a Áustria e o Nazismo, dizendo que os nazistas utilizavam

6 Carrot and Stick. **Cambridge Dictionary**. Disponível em <<https://dictionary.cambridge.org/pt/dicionario/ingles/carrot-and-stick>>. Acesso em 07 jan. 2024.

7 Carrot and Stick. **Wikipedia**. Disponível em <https://en.wikipedia.org/wiki/Carrot_and_stick>. Acesso em 07 jan.2024.

tanto a cenoura quanto o bastão (a vara) para “dobrar” a população austríaca. De lá para cá, a metáfora tem sido largamente incorporada no vocabulário mundial⁸.

Assim é que, em termos de atividade dualmente preventiva e sancionatória, é preciso questionar em que medida utilizar a cenoura e o bastão em relação aos fiscalizados e, em última instância, analisar de que modo a ANPD tem se posicionado neste sentido.

1. ACENOURA: GOVERNANÇA DE PRIVACIDADE E DADOS PESSOAIS

A proteção de dados pessoais é uma evolução do direito à privacidade, sendo impulsionada pela necessidade de tutela aos direitos dos titulares de dados em um ambiente de avanço tecnológico e diante da reorganização da sociedade e da economia com base no poder da informação e na monetização dos dados. Ao ser considerada uma dimensão da privacidade, compartilha dos mesmos fundamentos, centrados na tutela da personalidade e da dignidade do indivíduo⁹. No entanto, é fundamental compreender que essa disciplina não apenas herda tais fundamentos, mas também os modifica, aprofunda e atinge os pontos centrais dos interesses em questão.

Ganhando cada vez mais destaque em relação à privacidade, a proteção de dados emergiu como um direito fundamental autônomo¹⁰. Isso implica reconhecer que, embora esteja enraizada na mesma matriz conceitual da privacidade, possui características próprias que a diferenciam e a destacam como uma questão de relevância singular.

Nesse contexto, a Lei nº 13.709/2018 assumiu um relevante papel ao instituir a ANPD como o organismo responsável por supervi-

8 Carrot and Stick. **Wikipedia**. Disponível em <https://en.wikipedia.org/wiki/Carrot_and_stick>. Acesso em 07 jan. 2024.

9 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 35.

10 DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: RT, 2020. p. 165.

sionar e implementar as disposições relacionadas ao tema. No entanto, é necessário realizar uma análise crítica da eficácia dessa estrutura, considerando desafios e lacunas potenciais que podem surgir na aplicação prática da legislação.

Desde os anos 1980, o cenário de proteção de dados tem sido moldado por marcos importantes, delineando o caminho para a compreensão e consolidação do conceito de privacidade associado à proteção de dados pessoais. Um desses pontos cruciais foi o conjunto de diretrizes emitido pela Organização para o Desenvolvimento e Cooperação Econômica (OCDE), intitulado “*Guide lines on the Protection of Privacy and Transborder Flows of Personal Data*”. Estas diretrizes não apenas contribuíram para fortalecer o conceito de privacidade no contexto da proteção de dados pessoais, mas também impulsionaram o avanço do fluxo transfronteiriço de dados¹¹.

Outro passo essencial para consolidar um sistema de proteção de dados foi elaboração da Convenção nº 108/1981, conhecida como a Convenção de Estrasburgo. Além de representar o primeiro instrumento internacional vinculativo para a proteção de dados pessoais, o documento desempenhou um importante papel ao abordar a necessidade de uma autoridade independente e competente para garantir a proteção dos dados pessoais¹².

Com a promulgação da Diretiva 95/46/CE pela União Europeia, surgiu um marco relevante da proteção de dados pessoais, porquanto a iniciativa padronizou formas e normas de tratamento de dados. Ao passar por um processo de modernização e adaptação, a Diretiva 95/46/CE serviu como base para a criação do *General Data Protection Regulation* (GDPR)¹³.

O artigo 51 do Regulamento estabelece as regras para a designação de autoridades públicas independentes ou *Data Protection*

11 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 42

12 BEZERRA, Maria Ruth Borges. Autoridade Nacional de Proteção de Dados Pessoais: a importância do modelo institucional independente para a efetividade da lei. **Revista Caderno Virtual**, Brasília, v. 2, p. 177-271, 2020. p. 09-10.

13 Id. p. 11.

Authorities (DPAs) pelos estados membros da União Europeia (UE), encarregadas de supervisionar e aplicar as disposições do GDPR. O dispositivo sublinha a importância do papel desempenhado por essas autoridades na proteção dos direitos e liberdades fundamentais dos indivíduos no que se refere ao tratamento de dados, indo além da simples livre circulação desses dentro da UE. Além disso, enfatiza a necessidade de cooperação entre as DPAs para assegurar uma aplicação eficaz do GDPR em todos os estados membros¹⁴.

A gênese destas entidades, portanto, é compreendida dentro da necessidade de que elas se desenvolvam completamente independente dos poderes públicos, sobretudo porque suas funções principais são as de fiscalizar o tratamento de dados, sancionando eventuais irregularidades.

Com a significativa influência do GDPR no regime jurídico da proteção de dados em escala internacional, diversos governos passaram a dar prioridade ao desenvolvimento ou à adaptação de regulamentos nacionais, seguindo os moldes estabelecidos pelo regulamento europeu (Efeito Bruxelas). No Brasil, este processo culminou na elaboração da LGPD que prevê a criação e normatização da Autoridade Nacional de Proteção de Dados (ANPD).

Segundo a tradição Europeia, as DPAs, inclusive a ANPD, se propõe a assumir, precipuamente, o papel de educadoras. A ideia é prestigiar a prevenção de incidentes de segurança e o letramento digital de empresas e titulares de dados, tudo com vistas à concretização de uma cultura de privacidade que altere, efetivamente, o *mindset* social e mercadológico em relação aos dados pessoais.

As pessoas precisam compreender a importância e como preservar seus dados pessoais, e os controladores e operadores de dados devem intoejetar que ser *compliant* com estas regras não apenas é moralmente esperado, mas também um bom negócio. A redução e mitigação de riscos, não apenas pode poupá-los do pagamento de multas vultosas,

14 MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 227.

milionárias, como também contribuir com sua boa reputação, sendo um critério de eleição objetivo no mercado.

Deste modo, a ênfase na capacitação individual e na redução da vulnerabilidade evidencia-se como um princípio essencial na proteção de dados. Ao fomentar uma cultura de privacidade, a intenção é empoderar o titular de dados, permitindo que este exerça controle sobre suas informações pessoais. A LGPD, como marco regulatório, alinha-se a esses princípios, buscando estabelecer diretrizes claras para o tratamento de dados pessoais e fortalecer os direitos individuais. Nada obstante, embora o controle individual seja um componente significativo na criação de uma cultura de privacidade, não é suficiente por si só para garantir uma tutela adequada do direito fundamental à proteção de dados¹⁵.

A compreensão da importância desempenhada por uma autoridade na garantia da proteção de dados tem sido construída ao longo do tempo, desde a Convenção de Strasbourg e a Diretiva 95/46/CE, que introduziram de maneira abrangente o modelo de autoridade independente na União Europeia, como mencionado anteriormente. Porém, a mera existência formal de uma autoridade de fiscalização não assegura de forma ideal o cumprimento das normas de proteção de dados. É essencial que o modelo adotado reflita a importância desse órgão em sua atuação, com base em suas características fundamentais.

A ANPD, atuando como uma autoridade técnica e teoricamente independente, desempenha um papel central na efetiva implementação e fiscalização das normas de proteção de dados, contribuindo para a preservação da privacidade e dos direitos individuais no cenário digital em constante evolução¹⁶.

Feitas estas considerações, a Governança da Privacidade e dos Dados Pessoais deve ser trabalhada em duas frentes distintas: (i) no

15 DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: RT, 2020. p. 340.

16 BEZERRA, Maria Ruth Borges. Autoridade Nacional de Proteção de Dados Pessoais: a importância do modelo institucional independente para a efetividade da lei. **Revista Caderno Virtual**, Brasília, v. 2, p. 177-271, 2020. p. 16-17.

âmbito regulatório, claro, a partir da ação da DPA que pode assumir diversos modelos (regulamentos, guias orientativos, notas técnicas, campanhas educativas) e, por influência da primeira ou por pressão do mercado e dos demais *stakeholders*, (ii) no âmbito e por iniciativa dos próprios agentes de tratamento de dados pessoais (na forma do artigo 50 da LGPD e de diversos frameworks internacionais, como por exemplo, as normas ISO 37000 e em especial a ISO 37301).

Diversos fóruns e iniciativas globais discutem a importância da Governança e do Compliance. Estas pautas, que começaram a ocupar mais espaço a partir das iniciativas anticorrupção, nos últimos anos se converteram em importantes políticas internas e medidas reputacionais. Não é por outro motivo que o próprio conceito de “ESG¹⁷” traduziu em linguagem financeira a relevância de investir no ambiental, no social e na Governança.

O entendimento e a aplicabilidade de critérios ESG pelas empresas brasileiras é, cada vez mais, uma realidade. Atuar de acordo com padrões ESG amplia a competitividade do setor empresarial, seja no mercado interno ou no exterior. No mundo atual, no qual as empresas são acompanhadas de perto pelos seus diversos stakeholders, ESG é a indicação de solidez, custos mais baixos, melhor reputação e maior resiliência em meio às incertezas e vulnerabilidades¹⁸.

O Compliance, conceito muito próximo à Governança, passou a incluir, assim, medidas e campanhas para garantia da adoção de regras anticorrupção, pró sustentabilidade, de adequação às normas de proteção de dados e de adesão a princípios éticos e morais pelas organizações.

No Congresso Europeu de Proteção de Dados realizado pelo IAPP (*International Association of Privacy Professionals*), talvez a mais renomada associação de profissionais de privacidade do mundo, promovido em Bruxelas no mês de novembro em 2023, os dois tópicos

17 Que significa “Environmental, Social, Governance”, em tradução livre Ambiental (Sustentabilidade), Social e Governança.

18 ESG. **Pacto Global Rede Brasil**. Disponível em <<https://www.pactoglobal.org.br/pg/esg>>. Acesso em 07 jan. 2024.

de destaque foram a inteligência artificial e os *Ethics Officers: Data Ethics Officer, Digital Ethics Officer e Artificial Intelligence Ethics Officer*. É possível, de fato, encontrar vários profissionais no LinkedIn utilizando estas credenciais, ou as de eticista ou *chief-ethics* e *AI ethicist*.

Significa dizer que a Governança e o Compliance se tornaram exigências de mercado que hoje podem parecer opcionais para alguns, mas que nos anos vindouros tendem a ditar o que é ou não viável em termos econômicos e práticos.

No Brasil, a ANPD (e a LGPD) certamente estimulam as boas práticas e a Governança de Privacidade, na medida em que todos os guias e o regulamento fiscalizatório e sancionatório expressamente estipulam que a comprovação da boa-fé e da adoção de medidas de Governança da Privacidade e dos Dados Pessoais serão atenuantes em eventual penalização¹⁹. Consciente do poder da imagem no mercado e do custo financeiro a ela atrelado, a ANPD manifestou, inclusive no texto do regulamento e desde a primeira sanção por ela aplicada, que considera como sanção a exposição pública do infrator como agente antiético.

2. O BASTÃO: SANÇÃO

Nem só de Governança vive o homem.

É princípio da física que toda ação tem uma reação. Muitas doutrinas cristãs ensinam sobre as consequências das boas e má ações

19 A recente Resolução CD/ANPD nº 04/2023 adota uma definição para “política de boas práticas e de governança” (artigo 2º) e, no artigo 5º, determina que se considere como critério de definição da sanção a boa-fé do infrator (inciso II); sua cooperação (inciso VIII); a adoção reiterada de mecanismos internos de minimização do dano e compliance com a LGPD (inciso IX); a existência de política de boas práticas e governança (inciso IX); a pronta utilização de medidas corretivas (inciso XI) e a gravidade da sanção (inciso XII). Nacional, I. **Resolução CD/ANPD No 4, DE 24 DE FEVEREIRO DE 2023 - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077>>. Acesso em: 7 jan. 2024.

20 ROSSO, A. e CHACON ROSAS, E. Comentários à Versão 1.0 do Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. **Comentários aos regulamentos e orientações da ANPD**. Coord. Ana Paula de Canto Lima e Fabrício da Mota Alves. 1ª ed. ISBN 978-6526005866. São Paulo: Revista dos Tribunais, 2022.

e fazem analogias entre “colheita e plantio”. Esta noção guia também o Direito que responsabiliza os jurisdicionados pelos danos decorrentes de suas condutas ilícitas.

No âmbito da proteção de dados, a ANPD tem a responsabilidade de interpretar a LGPD e fiscalizar o seu cumprimento. Como tal, a autoridade não age somente por inércia, como o Judiciário que apenas pode atuar depois de provocado; é papel da dela ser proativa e instituir mecanismos fiscalizatórios que apurem ilícitos, canais para denúncias e peticionamento por titulares; assim como agir de ofício quando constata, em qualquer circunstância, violação aos direitos dos titulares de dados pessoais.

Muito se tem questionado a respeito da função sancionatória da DPA brasileira, não apenas pelo modo como conduziu seus primeiros processos do tipo, mas por uma questão cultural: as empresas costumam calcular o custo-benefício do ilícito, motivo pelo qual a ausência de sanções pode ser – e talvez esteja sendo – vista como desincentivo à adesão legal.

As críticas à atuação sancionatória da ANPD ilustram bem um aspecto cultural brasileiro pró-litígio e pró-sanção que não é aleatório, mas reflete um comportamento histórico de empresas e órgãos públicos que costumam recalitrar em relação a mudanças necessárias até que pesadas multas lhe sejam impostas. Mesmo assim, não raro, essas penalidades são levadas ao Judiciário onde passam anos em discussão. Significa dizer que está enraizada a tradição, inclusive em termos contábeis e de estratégia jurídica, de calcular o “custo do descumprimento legal”.

Este *mindset* é altamente prejudicial à missão da ANPD que é, justamente, em oposição a ele, educar, prevenir e aplicar penalidades não pecuniárias. Por isso a Governança é tão importante, porque pode servir como instrumento de adequação cultural no ambiente da proteção de dados e privacidade. No entanto, resta o dilema sobre o que fazer quando os incentivos não se traduzem na necessária mudança.

A adesão da autoridade à filosofia da cenoura e bastão pode ser compreendida de duas formas distintas, na regulamentação das sanções

e em sua efetiva aplicação. Parece, todavia, razoável afirmar que em ambas as instancias a postura do ente tem sido mais pró-cenoura do que pró-bastão e que, como antecipado no tópico sobre governança, mesmo quando opta pela punição, nem sempre se decide em favor de um castigo pecuniário.

Foram três as decisões sancionatórias tornadas públicas pela ANPD até o início de 2024: a primeira em face da Telekall Infoservice (Processo Administrativo Sancionador nº 00261.000489/2022-62²¹); a segunda contra o Instituto de Assistência ao Servidor Público Estadual de São Paulo – IAMSPE (Processo Administrativo Sancionador nº 00261.001969/2022-41²²) e a terceira em desfavor da Secretaria de Estado da Saúde de Santa Catarina - SES/SC (Processo Administrativo Sancionador nº 00261.001886/2022-51²³).

Contra a empresa privada Telekall, a autoridade fixou multa pecuniária de R\$14.400,00 (quatorze mil e quatrocentos reais); já em face de ambos os entes da administração pública, não foi imposta sanção financeira. Em contrapartida, foram fixadas obrigações de fazer face ao poder público, além de advertências em todos os casos e publicação em relação às três sancionadas²⁴.

Esta última providência reflete a convicção da ANPD de que a repercussão reputacional de incidentes de segurança serve ao triplo propósito de alertar potenciais afetados, conscientizar a população e estimular os penalizados e outros agentes de tratamento ao compliance legal.

21 Nacional, I. **Despacho Decisório - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/despacho-494550988>>. Acesso em: 7 jan. 2024.

22 Nacional, I. **Despacho Decisório - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/web/dou/-/despacho-decisorio-514655381>>. Acesso em: 7 jan. 2024.

23 Nacional, I. **Despacho Decisório - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/despacho-decisorio-517000207>>. Acesso em: 7 jan. 2024.

24 A divulgação dos despachos decisórios pela própria ANPD não se confunde com o previsto no artigo 20 da Resolução e CD/ANPD nº 04/2023, que trata como sanção de publicização a obrigação de o próprio infrator divulgar sua penalização nos termos a serem definidos pela autoridade.

A análise mesmo superficial dos três casos comprova factualmente que a DPA (Autoridade) brasileira não pretende aderir, em um primeiro momento, a uma postura tradicional de “Procon”, mas sim insistir nos postulados da regulação responsiva que adotou.

Partindo para um estudo mais profundo, institucional, desde a leitura combinada das Resoluções CD/ANPD nº01/2021 e CD/ANPD nº 04/2023, observa-se a consistência ideológica da autoridade entre “diz e o que faz”, porquanto ambos os documentos (que aprovam o regulamento do processo de fiscalização e do processo administrativo sancionador²⁵; bem como a dosimetria e aplicação de sanções administrativas²⁶, respectivamente) valorizam a cooperação do agente e a comprovação da adoção pré-incidente de medidas adequadas de prevenção ou mitigação de riscos e de danos; e a boa-fé.

Desde o artigo 15 da Resolução nº 01 está claro que a DPA pretende (i) monitorar, (ii) orientar e (iii) prevenir e, em última instância, que “poderá (iv) iniciar a atividade repressiva”. De quatro competências autoatribuídas a si mesma pela ANPD, três são não sancionatórias e visam, claramente, compreender de que maneira as coisas funcionam e que dificuldades e entraves efetivamente estão na raiz dos tratamentos irregulares de dados pessoais, de modo a atuar de modo eficiente e informado no macrossistema da proteção de dados.

Sendo, como antecipado, a única autoridade em atuação no Brasil com conhecimento técnico (*know-how*), é prerrogativa da autoridade não apenas a exegese da lei, conforme expressamente consignado no texto da LGPD, mas ainda interpretar as informações e dados relevantes para tomar decisões conscientes (art. 15, §1º da Res. 01/21); considerando, para tanto, aspectos econômicos e instrumentais para a realização da atividade de orientação (§2º). Note-se, ademais, que o §3º do dispositivo em estudo anuncia explicitamente que a atuação da DPA

25 Nacional, I. **Resolução CD/ANPD No 1, DE 28 DE OUTUBRO DE 2021 - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513>>. Acesso em 07 jan. 2024

26 Nacional, I. **Resolução CD/ANPD No 4, DE 24 DE FEVEREIRO DE 2023 - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077>>. Acesso em: 7 jan. 2024.

se pauta preferencialmente pela “construção conjunta e dialogada de soluções e medidas” de *compliance* legal dos agentes de tratamento – não pela punição dos regulados.

Resta cristalino que o *framework* desenhado pela ANPD é, conforme outorga legal que lhe é conferida pela LGPD, inerentemente *pró consenso*, orientada ao resultado via cooperação, a depender da postura dos agentes regulados (art. 17, IV, Res. 01/21), incentivando-se a adoção de mecanismo de transparência, retroalimentação e autorregulação (art. 17, VI, Res. 01/21); incentivando-se a conciliação entre as partes via reparação “espontânea” pelo agente de tratamento (art. 17, VIII, Res. 01/21); sempre com intervenção mínima pela DPA (art. 17, IX, Res. 01/21).

No paradoxo criado em relação à cultura litigiosa e sancionatória (pecuniária) estabelecida historicamente no Brasil – sobretudo a partir das regras de proteção ao consumidor – e a cultura que a ANPD se dispõe a tentar criar, de cooperação e conscientização, não parece que a resposta esteja na eleição de um ou outro *mindset*, mas na coexistência e complementariedade entre eles.

Isso porque a ANPD e a Secretaria Nacional do Consumidor (SENACON) firmaram, desde 2021, um acordo de cooperação institucional, em plena conformidade com a LGPD, que prevê a aplicação do Código de Defesa do Consumidor (CDC) nas hipóteses de violação de direitos dos titulares no contexto das relações de consumo (art. 45 da LGPD).

Em outras palavras, diante de um mesmo conjunto fático, aplica-se a LGPD quanto ao tratamento de dados pessoais e, simultaneamente, o CDC no que se refere à relação de consumo. A confusão recorrente — que por si só justificaria um artigo específico — decorre da tentativa de alguns intérpretes de tratar a questão exclusivamente sob a ótica da LGPD, mas com um viés de proteção ao consumidor, o que representa abordagens conceitualmente distintas. Por isso é perceptível, no meio da proteção de dados, a existência de um certo clamor por multas altas, que façam “doer no bolso do infrator” - como se ao não agir desse modo a ANPD estivesse sancionando um comportamento ilí-

cito. Acontece que este fornecedor, como tal, está sujeito normalmente à disciplina dos órgãos de defesa do consumidor que poderão, aí sim, alinhados com as práticas da área, impor as multas que acharem de direito.

Voltando à metáfora da cenoura e do bastão, a situação se traduz no fato de que a LGPD e o CDC possuem bastões distintos e medidas diferentes para equilibrar incentivo e punição (pecuniária), sendo prerrogativa da ANPD por medida de coerência, utilizar sanções outras (bloqueio de dados, eliminação de dados, publicização, suspensão parcial, suspensão, proibição total ou parcial) que entenda mais adequadas ao seu propósito.

3. CONSIDERAÇÕES FINAIS

Muito se tem falado na adequação à LGPD em relação aos controladores e operadores de dados. E com razão. A proteção aos dados pessoais é uma garantia constitucional e um direito legal dos titulares destes dados e precisa ser levada a sério.

O que se coloca aqui, no entanto, após as reflexões realizadas ao longo do texto, é a extensão deste processo de adequação que não deve se limitar aos agentes de tratamento, mas precisa chegar nos próprios titulares e, sobretudo, nos profissionais e estudiosos.

Sendo a proteção aos titulares de dados pessoais um “nicho” novo no direito em todo o mundo, é preciso que se desenvolva a consciência de que é a sociedade e o ordenamento jurídico que precisam se adequar ao novo direito, e não o novo direito que dever ser curvado e envergado para se ajustar a concepções e modelos preexistentes. Isso porque estes modelos, por mais que sejam adequados (ainda) em seus respectivos contextos, podem ser inapropriados ou defasados para necessidades novas.

O primeiro movimento, nesse sentido, é compreender que o que se protege não são os “dados pessoais”, mas seus titulares. Informações não são sujeitos de direito e a leitura da LGPD deve ser sistemática, não literal.

Nesse contexto, é imperativo reconhecer que a forma mais eficaz de garantir a tutela dos titulares de dados pessoais reside na indução de uma mudança estrutural e progressiva no comportamento do mercado, especialmente no cenário atual de economia baseada em dados e de sociedade orientada por algoritmos. Não se alcançarão novos resultados mediante a repetição de práticas tradicionais. Com essa premissa, a Autoridade Nacional de Proteção de Dados (ANPD) propõe-se a adotar medidas inovadoras, como o letramento digital — compreendido como a promoção da educação voltada à conscientização da sociedade, do setor privado e das entidades públicas quanto à relevância da privacidade e da proteção de dados pessoais enquanto direitos fundamentais.

Basta pensar que apesar de as ações terem consequências, são comumente condicionadas “por” ou “a” algo. As pessoas e as empresas se comportam de determinadas formas em resposta a gatilhos que podem ser certas condições, concepções ou hábitos, por exemplo. A ideia da regulação responsiva é alterar esses estímulos para modular os comportamentos que deles decorrem, despertando o interesse pela mudança comportamental, por parte dos regulados, a partir de uma abordagem adaptativa e participativa. E isso leva tempo.

Não é possível conciliar o resultado desejado pela autoridade e imediatismo. Portanto, não faz sentido julgá-la (pelo menos de forma definitiva) com apenas três anos de atuação. Isso não implica dizer que a DPA não cometeu erros, ou não se superestimou em alguns cenários; mas sim compreender que ninguém é indene a erros e que quando chegar a hora do acerto de contas, importa saber se os acertos foram mais numerosos e/ou relevantes.

A ANPD, a despeito de suas limitações e da pertinência ou não das críticas que sofreu, tem produzido conteúdo relevante e demonstrado a partir de sua atuação e de suas manifestações públicas a importância da governança e da adoção de boas práticas. Isso não é impugnável.

A governança e a adoção de boas práticas, a disseminação de conceitos como ESG e a conscientização das pessoas a respeito não apenas da importância, mas das vantagens econômicas, competitivas e reputacionais atreladas ao compliance exercerão papel essencial no

processo de adaptação e mudança cultural – sendo a proteção de dados uma faceta essencial do *compliance* e um importante *asset* corporativo.

O projeto educativo-transformador da ANPD não invalida a aplicação de sanções. Estas, aliás, podem ser instrumentais na concretização destes ideais porque os incentivos são importantes, mas não são suficientes. As sanções – e o poder sancionatório da DPA – são fundamentais tanto para a criação da cultura de Privacidade quanto para a proteção aos titulares de dados pessoais, independentemente de qualquer coisa.

Ou seja, não existe dúvida de que, sejam de natureza reputacional, obrigacional, suspensiva, proibitiva ou pecuniária, as sanções são necessárias. O que se questiona, no âmbito da regulação responsiva, é se a punição financeira é realmente a forma mais eficiente de sancionar; se é apenas quando “dói no bolso” que o regulado se ajusta à regulação.

A ANPD – e isso se observa de suas palavras (guias, notas técnicas, manifestações em geral, resoluções divulgadas) e de seus gestos (conclusões dos processos sancionatórios, tomadas de subsídios, realização de audiências, participação em eventos e seminário, disponibilidade ao público) – parece acreditar que não: as multas não “resolverão” o problema da proteção de dados.

É preciso ponderar a tendência global de valoração ética e moral e de empoderamento dos cidadãos; é importante tirar as empresas da zona de conforto e fazê-las repensar suas imagens.

Pagar multa é inconveniente, discutir astreintes e juros por anos no Judiciário é desgastante; mas nada disso é novidade. Estes custos e estratégias estão incorporados no *modus operandi* da iniciativa privada. O Judiciário costuma ser leniente em relação às multas aplicadas contra a administração pública. Mas qual seria a consequência, para um negócio ou serviço na economia de dados, da suspensão de uma plataforma? Ou da proibição de uma atividade?

Qual seria o custo, em sentido amplo, de 24 horas sem rede social? Do bloqueio do acesso a um grande buscador online? Em que resultaria a suspensão por uma semana de um chat? Como repercutiria

no cenário global a divulgação de falhas de segurança por grande fornecedor de serviços online? Estas sanções podem derrubar gigantes.

Governança e sanção coexistem - e se complementam. Especialmente na medida em que a governança é um fator de mitigação do risco de sanção – ou de uma penalidade mais severa, mais disruptiva. Neste sentido, a ANPD assumiu o papel de garantir o equilíbrio e a proporcionalidade entre cenoura e bastão, com vistas aos interesses dos titulares de dados pessoais e à construção de uma privacidade viável e realista: a pós-privacidade.

REFERÊNCIAS

ANPD atua por orçamento maior em meio a PLs no Congresso para regular economia digital e IA. **Terra**. Disponível em <<https://www.terra.com.br/noticias/checamos/anpd-atua-por-orcamento-maior-em-meio-a-pls-no-congresso-para-regular-economia-digital-e-ia,84fb3ca-5dc8cb0668ecf7c4ca04cd236vlul2t0l.html>>. Acesso em 02 jan. 2024.

ANPD e Senacon assinam acordo de cooperação técnica. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-senacon-assinam-acordo-de-cooperacao-tecnica>>. Acesso em: 7 jan. 2024.

BEZERRA, Gabrielle Sales Sarlet; RODRIGUEZ, Daniel Piñeiro. A autoridade nacional de proteção de dados (ANPD) e os desafios tecnológicos: alternativas para uma estruturação responsiva na era da governança digital. **Rev. direitos fundam. democ.**, v. 27, n. 3, p. 217–253, 2022.

BEZERRA, Maria Ruth Borges. Autoridade Nacional de Proteção de Dados Pessoais: a importância do modelo institucional independente para a efetividade da lei. **Revista Caderno Virtual**, Brasília, v. 2, p. 177-271, 2020.

BRASIL. **Lei Geral de Proteção de Dados (LGPD)**. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 27 dez. 2023.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Transforma a Autoridade Nacional

de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm. Acesso em 27 dez. 2023.

Carrot and Stick. **Cambridge Dictionary**. Disponível em <<https://dictionary.cambridge.org/pt/dicionario/ingles/carrot-and-stick>>. Acesso em 07 jan. 2024.

Carrot and Stick. **Wikipedia**. Disponível em <https://en.wikipedia.org/wiki/Carrot_and_stick>. Acesso em 07 jan.2024.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: RT, 368p, 2020.

HOFFMANN-RIEM, Wolfgang. **Teoria do direito digital**: transformação digital: desafios para o direito. Rio de Janeiro: Forense, 240p, 2021

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

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

Nacional, I. **Despacho Decisório - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/despacho-494550988>>. Acesso em: 7 jan. 2024.

Nacional, I. **Despacho Decisório - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/web/dou/-/despacho-decisorio-514655381>>. Acesso em: 7 jan. 2024.

Nacional, I. **Despacho Decisório - DOU - Imprensa Nacional**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/despacho-decisorio-517000207>>. Acesso em: 7 jan. 2024

Nacional, I. **Resolução CD/ANPD No 1, DE 28 DE OUTUBRO DE 2021 - DOU - Imprensa Nacional.** Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513>>. Acesso em 07 jan. 2024

Nacional, I. **Resolução CD/ANPD No 4, DE 24 DE FEVEREIRO DE 2023 - DOU - Imprensa Nacional.** Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077>>. Acesso em: 7 jan. 2024.

ROSSO, Ângela. e CHACON ROSAS, Eduarda. Comentários à Versão 1.0 do Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Comentários aos regulamentos e orientações da ANPD. Coord. Ana Paula de Canto Lima e Fabrício da Mota Alves. 1ª ed. ISBN 978-6526005866. São Paulo: Revista dos Tribunais, 2022.

SCHÜTZ, Philip. **Comparing Formal Independence of Data Protection Authorities in selected EU Member States.** Conference Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference 2012.

Sem estrutura e orçamento, ANPD ainda pode ser o regulador da Inteligência Artificial. Capital Digital. Disponível em <<https://capitaldigital.com.br/sem-estrutura-e-orcamento-anpd-ainda-pode-ser-o-regulador-da-inteligencia-artificial/>>. Acesso em 02 jan. 2024.

SOMBRA, Thiago Luis Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais:** pluralismo jurídico e transparências em perspectiva. São Paulo, Thomson Reuters Brasil, 2019.

ANÁLISE SOBRE A DISCRIMINAÇÃO ALGORÍTMICA NA ERA DA PROTEÇÃO DE DADOS PESSOAIS

Luanna da Costa e Silva¹

INTRODUÇÃO

A sociedade contemporânea está cada vez mais imersa na era digital. Este movimento de imersão foi detalhadamente descrito e batizado pelo economista Klaus Schwab, ao tratar do que chamou de “quarta revolução industrial”. Ele afirma em sua obra que esta quarta revolução industrial está baseada na revolução digital, um movimento que tem por marca uma internet praticamente onipresente e móvel, miniaturização de sensores e uma produtividade que subtrai custos com base na inteligência artificial (IA) e na aprendizagem de máquina. Em suas palavras, “as tecnologias digitais, fundamentadas no computador, software e redes, não são novas, mas estão causando rupturas (...) e, consequentemente, transformando a sociedade e a economia global” (Schwab, 2016).

Recentemente, esse espaço passou a ser permeado pela influência de algoritmos computacionais, que exercem papel cada vez maior na dinâmica das interações cotidianas. Cormen (2013) define algoritmos computacionais como um conjunto de passos com o objetivo de cumprir uma tarefa que são suficientemente bem descritos para que um computador possa executá-los.

Nesse contexto, tecnologias em geral, e a IA em particular, moldam, em diferentes dimensões, a maneira como as pessoas agem, vivem e se relacionam por meio dos algoritmos que norteiam sua ação (Casagrande e Vivan, 2023). Com o avanço tecnológico e a dissemina-

¹ Advogada, pós-graduanda em Direito Digital e Compliance e membro da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/DF.

ção do uso de ferramentas de IA, a questão do viés algorítmico surge e ganha relevância. Silva (2022) delimita o conceito de viés algoritmo a partir da incapacidade de máquinas corrigirem os erros decorrentes do subjetivismo humano. Além disso, o autor chama a atenção para a probabilidade de que os algoritmos repliquem e reforcem os preconceitos presentes na sociedade, levando a distinções, preferências ou exclusões que afetam a igualdade de tratamento entre indivíduos, especialmente os grupos vulneráveis (Silva, 2022).

A Lei Geral de Proteção de Dados (LGPD) - Lei 13.709, de 14 de agosto de 2018 - define o objetivo fundamental de proteger os direitos de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural², fundamentais para a preservação dos direitos constitucionais. Entretanto, a legislação deixa lacunas quanto à proteção nos casos de discriminação algorítmica ou tratamento de dados algorítmicos. Embora se possa inferir implicitamente tal determinação, esta continua insuficiente como mecanismo impeditivo do viés algorítmico discriminatório, especialmente no contexto do avanço das IA. Com base na limitação percebida da LGPD diante da constante evolução das IA, torna-se essencial incentivos para que legislações, políticas públicas, organismos governamentais e a sociedade civil possam desempenhar um papel relevante no gerenciamento de dados para enfrentar a discriminação algorítmica.

A identificação e a mensuração da discriminação em algoritmos são tarefas desafiadoras em função da complexidade técnica de suas operações. Essa dificuldade é agravada pela falta de transparência em relação ao funcionamento dos sistemas, o que torna a responsabilização por práticas discriminatórias mais complexa. Além disso, as legislações antidiscriminatórias vigentes frequentemente não estão preparadas para abordar as particularidades do ambiente digital, demonstrando a necessidade de adaptações e atualizações específicas para esse panorama (Ludgero, 2024).

Nesse viés, os debates para regulamentação das IA avançam no Brasil com o objetivo de garantir a proteção dos direitos fundamen-

2 Tais preceitos estão especialmente explícitos no caput do artigo 1º da Lei 13.709 de 14 de agosto de 2018.

tais e promover o uso de tecnologias seguras, confiáveis e alinhadas com valores éticos. A aprovação pelo Senado Federal, no dia 10 de dezembro de 2024, do substitutivo do senador Eduardo Gomes (PL-TO) que tem como base o PL 2.338/2023, apresentado pelo atual presidente do Senado, Rodrigo Pacheco, é um marco. O texto será avaliado pela Câmara dos Deputados. Chama a atenção, porém, o fato de que a proposta retirou da lista de sistemas considerados de alto risco os algoritmos das plataformas de redes sociais (Senado, 2024). Isso deverá impactar a abordagem da questão do viés algoritmo dentro das chamadas *big techs*, dificultado a adoção de soluções nessas que são atualmente as proprietárias dos grandes fóruns de diálogo social.

1. LGPD E A DISCRIMINAÇÃO ALGORITMICA RACIAL POR USO DE IA

O artigo 6º da LGPD estabelece princípios fundamentais para o tratamento de dados pessoais, incluindo livre acesso, transparência, segurança, prevenção e não discriminação. Além disso, dispõe aos titulares de dados a garantia do direito de solicitar a revisão de decisões automatizadas que afetem seus interesses³. Essas decisões podem incluir a definição de perfis pessoais, profissionais, de consumo, de crédito ou aspectos da personalidade. Entretanto, a rápida evolução tecnológica, especialmente no campo da IA, desafia a capacidade do marco legal em lidar com as complexidades emergentes.

A proliferação das IA tem se tornado mais presente na vida das pessoas e no cotidiano profissional das empresas e de seus funcionários (McKinsey, 2023), permeando plataformas sociais, assistentes pessoais e tecnologias avançadas.

Por outro lado, esse avanço tecnológico não está isento de desafios. Um deles é o viés algorítmico, que ocorre quando os dados usados por programadores para concepção de algoritmos trazem consigo conceitos pré-concebidos de origens diversas. O problema pode tam-

3 Este aspecto específico está abrangido no caput do artigo 20º

bém estar associado ao banco de dados utilizado no treinamento da IA. Este pode conter dados ou quantidades de dados que criam um viés, que por sua vez redundará em deturpações nos resultados de resposta da IA. Nesse caso, haveria uma distorção daquilo que foi inicialmente planejado pelos programadores. Esses vieses acabam, portanto, incorporados às tecnologias, determinando comportamentos e respostas a problemas diversos, perpetuando desigualdades por meio dos algoritmos e gerando impactos em várias áreas da vida (Da Rocha et al, 2020).

A LGPD estabelece mecanismos que asseguram a autodeterminação informativa, a transparência, o acesso a dados e a vedação do uso de informações para práticas discriminatórias. No entanto, ela não é capaz de eliminar ou reduzir integralmente os riscos relacionados ao uso de algoritmos em IA. Essa limitação decorre da complexidade e da falta de transparência desses sistemas, que comprometem a plena garantia de justiça nas decisões automatizadas.

Além disso, a LGPD determina a proteção aos segredos comerciais e industriais, o que torna o princípio da transparência menos rígido. Por outro lado, introduz medidas de governança importantes para assegurar a proteção de dados pessoais no Brasil. Entre essas medidas estão: auditoria de algoritmos, revisão de decisões automatizadas e Relatórios de Impacto à Proteção de Dados Pessoais (RIPDP).

A auditoria de algoritmos, por si só, pode não ser a solução mais adequada em sistemas avançados de *machine learning*. Esses algoritmos possuem a capacidade de reorganizar sua lógica interna com base nos dados que analisam, ajustando-se dinamicamente de acordo com o ambiente e as informações processadas. Essa complexidade torna difícil rastrear e compreender plenamente o funcionamento e as decisões dessas tecnologias apenas por meio de auditorias tradicionais.

O direito de revisão de decisões automatizadas, previsto na LGPD, não assegura, porém, que essa revisão seja realizada por um ser humano (Almada, 2019). Dessa forma, existe a possibilidade de que o próprio sistema automatizado, potencialmente enviesado, seja o responsável por reavaliar as decisões que tomou, o que pode resultar no fortalecimento dos mesmos erros e preconceitos embutidos no algoritmo.

A elaboração de RIPDP ocorrerá nos casos em que o tratamento de dados apresentar alto risco aos princípios gerais de proteção. Contudo, a obrigatoriedade de elaboração desses relatórios depende de solicitação específica da Autoridade Nacional de Proteção de Dados (ANPD), sendo atualmente uma faculdade dessa entidade e não uma exigência automática para os controladores.

Dessa forma, é fundamental a necessidade de utilização de novos mecanismos que sejam capazes de proteger os dados pessoais e os dados pessoais sensíveis relacionados às pessoas naturais, tendo como finalidade a gestão dos riscos provenientes a partir do manuseio de algoritmos de IA.

Atualmente, os algoritmos desempenham uma variedade de funções, desde a resolução de problemas e tomada de decisões até a classificação e ranqueamento de indivíduos, bem como a previsão de comportamentos futuros. Essas atividades tornaram-se corriqueiras no cotidiano de parte significativa da população mundial, exercendo um impacto expressivo na forma como as pessoas agem individualmente e interagem na sociedade (Da Silveira, 2019).

A opacidade⁴ e ausência de neutralidade algorítmica⁵ demonstram que o enviesamento dos algoritmos é um reflexo da sociedade, conforme afirma Silva (2022). Assim, os algoritmos perpetuam e propagam os preconceitos, desigualdades e injustiças enraizadas no subjetivismo humano construído no processo histórico e cultural da sociedade brasileira (Silva, 2022).

Sobre o tema, os autores Maurício Requião e Diego Carneiro também destacam os caminhos por onde o viés algorítmico surge ao afirmar que:

4 Uma das definições de opacidade algorítmica está relacionada com a falta de visibilidade dos processos computacionais por trás dos algoritmos que geram uma situação em que humanos não são aptos a inspecionar os funcionamentos internos para verificar por si próprios como os resultados e conclusões foram processados (Paudyal e William Wong, 2018).

5 Um sistema é considerado neutro somente se os valores externos ao objetivo do sistema forem os únicos aspectos a desempenhar um papel na forma como esse sistema produz os seus resultados. Ou seja, se o sistema pré-determinar de qualquer maneira a forma de entrega dos resultados, esse sistema não poderá ser considerado neutro (Phillips-Brown, 2023).

As discriminações algorítmicas podem ocorrer basicamente de duas maneiras: i) quando os algoritmos refletirem os preconceitos humanos (conscientes ou não) embutidos desde a programação; ii) quando entrarem em contato com bases de dados contendo vieses preconceituosos o que faz com que o algoritmo “aprenda” a discriminar (Requião e Costa, 2022).

As consequências dos vieses algorítmicos são visíveis em diversos setores, incluindo nas áreas de educação, saúde, trabalho e consumo. Um exemplo emblemático desse problema é ilustrado no caso da cientista Joy Buolamwini, estudante do MIT Media Lab, cujo rosto não foi reconhecido por um software de análise facial devido à falta de treinamento para identificar nuances de tons de pele e estruturas faciais de pessoas negras (Buolamwini, 2024).

Outro exemplo de viés algorítmico foi o caso *Chatbot Tay*, nos Estados Unidos, um lançamento da *Microsoft* em parceria com o *Twitter*, em 2016. O *Chatbot* foi implementado como um perfil do *Twitter* que aprenderia em tempo real a conversar a partir da interação com usuários da plataforma. Em poucas horas, passou a repetir e elaborar comentários racistas ao interagir com usuários da plataforma que direcionaram as conversas para esses temas (Silva, 2022).

No ano de 2021, o Colégio Nacional de Defensores Gerais (CONDEGE) conduziu uma pesquisa que revelou que 81% das pessoas que foram injustamente detidas por reconhecimento fotográfico eram negras (DPRJ, 2021). Abundam, portanto, os casos de viés algorítmico discriminatório de natureza racista contra negros⁶.

Nesse contexto, a inclusão da discriminação algorítmica no Plano Plurianual 2024-2027, aprovado pelo Congresso Nacional, destaca o reconhecimento do Executivo federal em relação à urgência em combater essa questão em sua atuação (MPOG, 2023). Trata-se de um exemplo de iniciativa de políticas públicas⁷ contra a discriminação al-

6 Outros casos envolvendo outros segmentos sociais também são fartamente noticiados, conforme será visto adiante.

7 Santana (2018) conceitua políticas públicas como um fenômeno complexo que busca colocar o governo em ação por meio da proposição de medidas. Segundo ela, o termo significa o conjunto de ações governamentais que delineiam a atuação do Estado, envolvendo a definição de metas, prioridades, alocação de recursos orçamentários e meios de implementação para cumprir os compromissos constitucionais.

gorítmica racial, que se destaca por priorizar o resgate da participação social nesse processo.

Além disso, a criação do Hub de Igualdade Racial, uma plataforma online pioneira, que centraliza informações para consulta, oferecendo dados detalhados por cor ou raça, juntamente com outras interseccionalidades, oferece acesso a informações para o público em geral e para agentes governamentais.

Outro ponto relevante é a proposição de ações legislativas, como o Projeto de Lei 2821/2022, apresentado pelo senador Fabiano Contarato (PT-ES), que busca combater a disseminação de conteúdos que promovam ódio, discriminação e preconceito nas redes sociais e plataformas de busca. Esse projeto, voltado para aprimorar o Marco Civil da Internet (Lei 12.965/2014), é parte de um movimento legislativo em resposta à discriminação algorítmica.

De toda forma, a transparência limitada das plataformas que utilizam esses algoritmos torna essencial a implementação de mecanismos robustos de controle e auditoria para que haja análise e a responsabilização por práticas discriminatórias. Além disso, a criação de processos mais claros e a supervisão mais rigorosa dos sistemas automatizados são necessárias para garantir que a discriminação, de qualquer natureza, seja identificada e corrigida, promovendo uma maior responsabilidade e equidade no uso das tecnologias.

2. ANÁLISE DE CASOS: ALGORÍTMICOS DISCRIMINATÓRIOS NAS RELAÇÕES DE TRABALHO, CONSUMO E GÊNERO

A discriminação algorítmica com base no perfil socioeconômico de clientes é um dos exemplos que demonstram como dados enviesados podem reforçar desigualdades baseadas também nesses critérios. Ou seja, o viés algorítmico tem potencial multifacetado de gerar externalidades negativas nas relações entre pessoas naturais e plataformas digitais que usam IA como ferramenta central para funcionamento de suas atividades.

O caso Decolar.com oferece uma análise relevante. A empresa do setor de turismo e hospedagem foi multada em R\$ 2,5 milhões pela Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça e Segurança Pública (MJSP). O motivo da condenação foi a prática de oferecimento de preços diferenciados para reservas em hotéis no Brasil com base na localização geográfica dos seus clientes. Além disso, a companhia estaria privilegiando seus clientes estrangeiros ao ofertar acomodações no Brasil, em detrimento do público nacional (MJSP, 2022).

Outro caso que ganhou notoriedade ocorreu em 2018, envolvendo a empresa Amazon. Foi divulgado pela grande imprensa à época que a Amazon enfrentou problemas ao utilizar um algoritmo em processo seletivo. A ferramenta adquiriu um comportamento que, na prática, penalizava candidaturas femininas na seleção de profissionais para atuarem no segmento de tecnologia da informação (TI) na empresa. O viés teria surgido a partir da base de dados usada no treinamento do algoritmo, que se alimentou dos padrões de currículos enviados para a Amazon durante um período que abrangeu 10 anos. Durante esse tempo de registro de candidaturas, a maior parte dos candidatos era composta por homens. Esses dados foram compreendidos pela máquina como uma predileção natural por esse tipo de perfil, criando o viés (FSP, 2018).

Mais um caso de repercussão internacional envolveu uma das maiores empresas de tecnologia do mundo, a Apple. Diversos veículos de imprensa de diferentes países reportaram o caso do cartão de crédito Apple Card. Segundo usuários de diversas partes do planeta, o serviço teria oferecido limites de crédito reduzido para mulheres. Os reportes davam conta de situações em que cônjuges solicitavam o cartão em pedidos separados e não diretamente vinculados quando da aplicação e recebiam limites de crédito diferentes, ainda que seu patrimônio fosse partilhado em igualdade de condições. Essa avaliação de crédito era realizada por meio de um algoritmo. A questão chegou a envolver o Departamento de Serviços Financeiros do Estado de Nova York (DFS, na sigla a partir da língua inglesa). A entidade pública faz a regulação dos serviços e produtos bancários. O DFS chegou a acionar o banco Goldman Sachs, responsável pela emissão dos cartões (BBC, 2019).

Mais recentemente, foi noticiado o uso de IA para monitorar empregados em grandes corporações. A Teleperformance, na Colômbia, teria solicitado que trabalhadores em regime de home office permitissem a instalação de câmeras em seus computadores, conectadas a uma IA que detectaria violações de regras internas e enviaria fotografias para análise. Em outro caso, a IBM desenvolveu uma tecnologia capaz de identificar sinais de desmotivação ou intenção de demissão entre empregados, com o objetivo de oferecer suporte ou alternativas. (Matias e Moraes Júnior, 2024).

Esses exemplos demonstram que, a exemplo do viés algoritmo racial, o problema, que se estende para outros segmentos e mostra dimensões sexistas, sociais e econômicas, está longe de ser mera exceção, já que os casos são cada vez mais frequentes.

No contexto da LGPD e do Código de Defesa do Consumidor (CDC) – Lei 8.078, de 11 de setembro de 1990 -, a formação de bancos de dados de usuários requer o consentimento expresso do titular, vinculado ao princípio da autodeterminação informativa (Leal e Paulo, 2023). Esse consentimento deve ser obtido por meio de manifestação livre e esclarecida, destinada a uma finalidade específica e devidamente informada. Essa exigência busca garantir transparência no tratamento de dados e assegurar que os titulares exerçam controle sobre suas informações pessoais, respeitando os direitos previstos em ambos os diplomas legais.

O modelo de consentimento enfrenta uma crise significativa. A complexidade das políticas de privacidade, aliada à rapidez do consumo digital, leva muitos usuários a aceitarem termos sem compreender plenamente seus efeitos (Medeiros et al, 2023). Essa situação reflete a vulnerabilidade dos consumidores em um ambiente de coleta intensiva de dados, onde a falta de clareza e acessibilidade das informações compromete o exercício pleno de seus direitos.

O livre acesso aos dados e informações pessoais dos titulares, por empresas ou pelo Estado, intensifica a prática de coleta de dados de forma indiscriminada ferindo a dignidade da pessoa humana e seus direitos fundamentais (Doneda, 2011). Esse gigantesco número de da-

dos agrupados e manipulados beneficia e fortalece empresas e grandes organizações, aumentando as chances de geração de uma descompensação nas relações de mercado e de consumo.

Nesse contexto, Frazão (2021) reflete como a captação de dados e sua análise é uma ferramenta bastante relevante nas relações sociais atualmente:

“os sistemas algorítmicos têm sido peça fundamental para manter uma engrenagem que tem por finalidade fazer julgamentos e predições sobre as pessoas no tocante às suas mais diversas características: seus méritos, seus perfis, suas preferências, suas inclinações, propensões e probabilidades nas mais variadas searas – desde a propensão ao consumo de determinado produto até a propensão a delinquir ou a reincidir na prática de um crime –, suas capacidades e aptidões – no campo físico, intelectual, emocional, profissional, econômico, etc –, e suas fraquezas e vulnerabilidades” (Frazão, 2021).

O problema não se limita ao mercado, embora este seja um aspecto bastante preocupante da questão. Entretanto, a captação, manipulação e análise de dados pelos algoritmos pode afetar a autonomia privada dos cidadãos, considerando que esses sistemas algorítmicos passaram a ter papel relevante em inúmeros cenários, tais como: acesso a universidades, empregos e cargos. Diante dos vários casos reportados e da experiência no dia a dia, é evidente que diferentes aspectos da vida privada das pessoas podem ser condicionados por julgamentos automatizados. Essa realidade é indício forte da necessidade de reflexão crítica sobre o impacto desses sistemas na equidade e nos direitos individuais.

Desse modo, o complexo normativo de proteção de dados enfrenta o desafio de transformar o ambiente virtual em um espaço seguro e confiável. Por isso, é fundamental prevenir e, quando tal medida falhar, minimizar os efeitos das práticas eventualmente discriminatórias e o uso indevido de dados.

3. REGULAMENTAÇÃO DE INTELIGÊNCIA ARTIFICIAL

O campo da IA emergiu entre as décadas de 1930 e 1950, com contribuições fundamentais como o artigo de Warren McCulloch e Walter Pitts, em 1943, que propôs a simulação do sistema nervoso humano por meio de redes neurais matematicamente modeladas. Em 1950, Alan Turing ampliou essa perspectiva ao publicar o artigo “Computing Machinery and Intelligence”, introduzindo o Teste de Turing, que explora a possibilidade de máquinas pensarem de forma comparável aos seres humanos. Esses estudos inauguraram o desenvolvimento científico da IA.

Atualmente, a IA é predominantemente baseada em *machine learning* (aprendizado de máquina), o que permite que os sistemas aprendam a criar modelos e soluções para problemas específicos. Essas tecnologias têm uma capacidade exponencial de processamento, oferecendo resultados rápidos e em grande escala. No entanto, o desempenho da IA está diretamente vinculado à qualidade dos dados fornecidos. Dados precisos e relevantes são essenciais para que a IA processe informações, gere resultados confiáveis e otimize processos por meio da automatização (Costa e Kremer, 2022).

O principal desafio técnico associado à IA está na utilização de redes neurais profundas (*deep learning*), que frequentemente operam como “caixas-pretas” (*black box*). Apesar de entregarem resultados precisos, esses sistemas são altamente complexos, tornando difícil compreender ou explicar o processo que levou a determinadas decisões, de onde deriva o problema da opacidade. Essa opacidade impossibilita auditorias eficazes e levanta questionamentos sobre a confiabilidade, justiça e ética dessas decisões, evidenciando a necessidade de maior transparência e controle sobre o funcionamento desses modelos (Costa e Kremer, 2022).

Por esse motivo, torna-se tão importante a explicabilidade em algoritmos de IA. Trata-se da capacidade de os sistemas fornecerem explicações claras e compreensíveis sobre suas decisões. Essa prática é fundamental em um cenário onde decisões algorítmicas impactam dire-

tamente negócios e indivíduos. A explicabilidade contrasta com o conceito de *black box*, permitindo que humanos compreendam as lógicas subjacentes aos resultados, promovendo transparência e alinhamento com princípios éticos e ideológicos.

No Brasil, o projeto que estabelece a regulamentação da IA foi aprovado pelo Senado em dezembro de 2024. Sua tramitação ainda não está concluída e o debate em torno da redação final será uma grande oportunidade. O texto atual reúne contribuições de sete outras propostas legislativas, como o PL 21/2020, já aprovado pela Câmara dos Deputados, além de integrar várias emendas de diferentes senadores. Do jeito que está, a proposta aborda pontos importantes com o intuito de atenuar os riscos provenientes do uso de IA, fortalecendo a proteção de dados pessoais e o papel da Autoridade Nacional de Proteção de Dados (ANPD). Além disso, estabelece direitos às pessoas afetadas pelo uso de IA tais como informação prévia de que está interagindo com sistemas de IA; direito à privacidade e a proteção de dados pessoais; direito à não discriminação ilícita e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; uso de linguagem simples e clara quando destinados a criança e adolescentes, idosos ou pessoas com deficiência (Senado, 2024).

A regulação de IA demonstra preocupação com os direitos autorais, relações de trabalho para que haja redução de riscos aos trabalhadores; assegurar aos cidadãos os direitos à explicação e revisão humana das decisões que tiverem impacto jurídico relevante; nos casos de identificação biométrica, garantir proteção contra discriminação; avaliar preliminarmente para classificação de riscos; avaliar impacto para riscos excessivos; e a sanção administrativa e responsabilização cível.

Sobre as sanções administrativas, o marco regulatório determina multa de até R\$ 50 milhões ou a 2% do faturamento bruto do grupo ou conglomerado por infração normativa. Além disso, prevê responsabilização civil por danos causados por sistemas de IA por meio de regras previstas no Código Civil e Código de Defesa do Consumidor.

O Brasil, ao se lançar na regulação de IA, dá um passo importante na tentativa de administrar e controlar os impactos dos efeitos da

IA. Espera-se que o texto final não frustrasse as expectativas e necessidades que claramente se apresentam diante da sociedade neste momento.

4. CONSIDERAÇÕES FINAIS

Com o crescente avanço tecnológico, o aumento da utilização de ferramentas de IA e sua pulverização por diferentes segmentos da vida cotidiana, bem como a velocidade de evolução dessas tecnologias, corre-se o risco de que a resposta legislativa não seja capaz de contemplar satisfatoriamente a todas as questões que surgem a partir da disseminação desses instrumentos. Nota-se que a LGPD, embora traga avanços bastante significativos, carece de reformas que possam lhe conferir abrangência sobre a preservação da privacidade, do direito de personalidade, da proteção de dados pessoais e da dignidade da pessoa humana no contexto digital.

A IA impulsiona mudanças profundas e certamente tem sido, e cada vez mais será, uma ferramenta protagonista para o progresso humano e a melhoria da qualidade de vida. Contudo, o desenvolvimento da IA levanta consigo questões éticas e desafios relacionados à privacidade, equidade e transparência, exigindo que seu uso seja acompanhado de regulamentações responsáveis e reflexões críticas sobre seu impacto social, econômico, ambiental e cultural.

A proteção de dados na era dos algoritmos avançados exige um equilíbrio delicado entre inovação tecnológica e a preservação dos direitos fundamentais. A LGPD representa um passo significativo ao estabelecer diretrizes como transparência, explicabilidade e vedação à discriminação, contudo, sua aplicação enfrenta limitações diante da complexidade do processamento de dados em larga escala e de decisões automatizadas no âmbito da interação com sistemas de IA.

Questões como a perpetuação de preconceitos por algoritmos e a opacidade nos processos de tomada de decisão indicam a necessidade de mecanismos mais robustos e de uma fiscalização mais efetiva para garantir que as empresas cumpram seus deveres legais e éticos.

A discriminação algorítmica é um problema global que exige uma abordagem colaborativa envolvendo governos, organizações internacionais, empresas e sociedade civil. Nesse contexto, será essencial o compartilhamento de boas práticas e a implementação de mecanismos de responsabilização que garantam que os algoritmos sejam projetados com transparência, alinhados aos princípios éticos e antidiscriminatórios.

O avanço relacionado à aprovação da Regulamentação de Inteligência Artificial no Brasil traz uma perspectiva de proteção aos direitos dos titulares de dados, mas requer atenção. A avaliação preliminar de riscos, atrelada ao monitoramento e fiscalização de empresas, revela a tentativa de prevenir e mitigar as consequências do uso indiscriminado de algoritmos de IA. A sociedade necessita de segurança jurídica, econômica, política e social no meio digital.

No entanto, não é possível afirmar se a regulamentação conseguirá resguardar efetivamente a todos os direitos dos cidadãos diante a renovação constante de tecnologias e nem se há mecanismos de fato efetivos para fiscalizar tamanha quantidade de dados produzida. Parece não restar dúvidas de que a velocidade dos avanços tecnológicos é bastante superior à do processo legislativo e dá a impressão de estar acelerando cada vez mais. Eis um enorme desafio diante desta quadra histórica.

O texto recentemente aprovado pelo Senado busca alcançar o equilíbrio entre o desenvolvimento tecnológico e os direitos fundamentais. Ao longo do tempo, a norma a ser implementada poderá ser avaliada no que se refere a aplicabilidade e efetividade.

A adoção de tecnologias que promovam a clareza e a compreensão dos critérios utilizados pelos algoritmos, fortalecendo a confiança dos usuários nos sistemas é um caminho desejável, mas que esbarra no caos criativo que permeia as iniciativas corporativas e individuais característicos na busca pela invenção e criação de novas plataformas e serviços e nas leis de mercado que balizam os investimentos mundo afora.

Além disso, o uso de instrumentos de regulação deve ser bem planejado, uma vez que é consagrada a literatura que demonstra como seu excesso pode ser altamente prejudicial para o desenvolvimento econômico que promove o bem-estar coletivo. Não se pode cair na armadilha da excessiva restrição e tão pouco parece ser funcional um paradigma baseado na ideia do “liberou geral”. O desafio será encontrar este equilíbrio enquanto as tecnologias evoluem rapidamente e desafiam inclusive os limites das fronteiras nacionais e jurisdicionais.

REFERÊNCIAS

ALMADA, Marco. Revisão humana de decisões automatizadas. Pós-Debate realizado no dia, v. 7, 2019. Disponível em: https://bit.ly/revi-sao_humana. Acesso em: 13 dez. 2024.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 1977.

BBC News Brasil. 2019. Por que o serviço de cartão de crédito da Apple está sendo acusado de sexismo. Disponível em: <https://www.bbc.com/portuguese/geral-50355369>. Acesso em: 13 dez. 2024.

BRASIL. Secretaria de Comunicação Social da Presidência da República e Ministério da Igualdade Racial. Relatório Racismo na Internet: evidências para a formulação de políticas digitais. SILVA, Ane; SOUZA, Gustavo (coord.). Brasília: Secretaria de Comunicação Social, 2023. Disponível em: <https://www.gov.br/igualdaderacial/pt-br/assuntos/gti-comunicacao-antirracista/bibliografia>. Acesso em: 1º jan. 2024.

BRASIL. **Reconhece discriminação algorítmica**. Desvelar Justiça racial, IA e tecnologias digitais. Disponível em: <https://desvelar.org/racismoalgoritmico/>. Acesso em: 6 dez. 2024.

BEZERRA, A. C.; COSTA, C. M. da. Pele negra, algoritmos brancos: informação e racismo nas redes sociotécnicas. **Liinc em Revista**, [S. l.], v. 18, n. 2, p. e6043, 2022. Disponível em: <https://revista.ibict.br/liinc/article/view/6043>. Acesso em: 6 dez. 2024.

BUOLAMWINI, Joy. Unmasking AI: My mission to protect what is human in a world of machines. Random House, 2024.

CASAGRANDE, Divaleia; VIVAN, Gefferson. A REVOLUÇÃO

COMPORTAMENTAL: A NOVA FASE DA TRANSFORMAÇÃO HUMANA. **Revista Conexão**, n. 11, p. 249-263, 2023. Disponível em: <https://revistas.uceff.edu.br/conexao/article/view/712/661>. Acesso em: 12 dez. 2024.

CONDEGE. **Relatórios indicam prisões injustas após reconhecimento fotográfico**. 2021. Disponível em: <https://www.condege.org.br/arquivos/1029>. Acesso em 06 dez. 2024.

CORMEN, T. H. *Algorithms Unlocked*. MIT Press, 2013

COSTA, Ramon; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 16, p. 145-167, out. 2022. Acesso em: 9 dez. 2024.

DA ROCHA, Cláudio Jannotti; PORTO, Lorena Vasconcelos; ABAURRE, Helena Emerick. Discriminação algorítmica no trabalho digital. *Revista de Direitos Humanos e Desenvolvimento Social*, [S. l.], v. 1, p. 1–21, 2020. DOI: 10.24220/2675-9160v1e2020a5201. Disponível em: <https://seer.sis.puc-campinas.edu.br/direitoshumanos/article/view/5201>. Acesso em: 13 dez. 2024.

DA SILVEIRA, Sergio Amadeu. **Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas**. Edições Sesc, 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico: Journal of Law*, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=4555153>. Acesso em: 13 dez. 2024.

DPRJ - Defensoria Pública do Estado do Rio de Janeiro. Relatórios apontam falhas em prisões após reconhecimento fotográfico. 2021. Disponível em: <https://www.defensoria.rj.def.br/noticia/detalhes/11088-Relatorios-apontam-falhas-em-priso-es-apos-reconhecimento-fotografico>. Acesso em: 15 dez. 2024.

FRAZÃO, Ana. Discriminação algorítmica: a relação entre homens e máquina. Disponível em: https://www.professoraanafrazao.com.br/files/publicacoes/2021-07-28-Discriminacao_algoritmica_a_rela

cao_entre_homens_e_maquinas_Os_riscos_das_interacoes_disfuncionais_e_da_irresponsabilidade_organizada_Parte_VII.pdf. Acesso na data em: 7 dez. 2024.

FSP - Folha de S.Paulo. Amazon desiste de ferramenta de recrutamento que penalizava mulheres. Disponível em: <https://www1.folha.uol.com.br/tec/2018/10/amazon-desiste-de-ferramenta-de-recrutamento-que-penalizava-mulheres.shtml>. Acesso em: 13 dez. 2024.

FRAZÃO, Ana. Discriminação algorítmica: Compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade. Disponível em: https://www.professoraanafraza.com.br/files/publicacoes/2021-06-16-Discriminacao_algoritmica_Compreendendo_o_que_sao_os_julgamentos_algoritmicos_e_o_seu_alcance_na_atualidade_Parte_I.pdf. Acesso em: 7 dez. 2024.

IBGE. Censo 2022. Disponível em: https://censo2022.ibge.gov.br/panorama/?utm_source=ibge&utm_medium=home&utm_campaign=portal. Acesso em 5 dez. 2024.

INSTITUTO DE ENGENHARIA. **A história da inteligência artificial**. Disponível em: <https://www.institutodeengenharia.org.br/2019/02/27/a-historia-da-inteligenciaartificial/>. Acesso em: 6 dez. 2024.

LEAL, Mônia Clarissa Hennig; PAULO, Lucas Moreschi. A Lei Geral de Proteção de Dados, a vulnerabilidade dos usuários da internet e a tutela dos direitos: linhas introdutórias à dinâmica dos dados, do Big Data, da economia de dados e da discriminação algorítmica. *Civilistica*. com. Rio de Janeiro, a.12,n.3,2023.Disponível em: <https://civilistica.emnuvens.com.br/redc>. Acesso em: 6 dez. 2024.

LIMA, B. **Racismo Algorítmico**: O enviesamento Tecnológico e o impacto aos direitos fundamentais no Brasil. Dissertação (Mestrado em Direito) - Universidade Federal de Sergipe. Sergipe, 2022.

LUDGERO, Paulo Ricardo. Desvendando os Desafios Legais na Prevenção da Discriminação Algorítmica: Uma Análise da Proteção Antidiscriminatória. Disponível em:<https://www.jusbrasil.com.br/artigos/desvendando-os-desafios-legais-na-prevencao-da-discriminacao-algoritmica-uma-analise-da-protecao-antidiscriminatoria/2364895551>. Data de acesso em: 6 dez. 2024.

MATIAS, João Luís Nogueira; MORAIS JÚNIOR, Ricardo Antônio Maia de. Discriminação algorítmica na relação de emprego: eficiência econômica, inteligência artificial e fragilidade do empregado. Revista do Tribunal Superior do Trabalho, Porto Alegre, v. 90, n. 2, p. 128-147, abr./jun. 2024. Data de acesso em: 6 dez. 2024.

MEDEIROS, Guilherme Tadeu Portella et al. Os impasses dos termos de uso em razão da modalidade de adesão. Conhecimento: diversidade de estudos produzidos no curso de direito, p. 597, 2023.

MIR - Ministério da Igualdade Racial (2023a). **lança HUB da Igualdade Racial para disseminar indicadores de raça/cor no governo federal**. Disponível em: <https://www.gov.br/igualdaderacial/pt-br/assuntos/copy2_of_noticias/ministerio-lancamento-do-hub-da-igualdade-racial-para-disseminar-indicadores-de-raca-cor-no-governo-federal>. Acesso em: 6 dez. 2024.

MIR - Ministério da Igualdade Racial (2023b). Ministério lança plataforma online inédita para disseminar indicadores de raça/cor no Governo Federal. **Agência gov**. Disponível em: <https://agenciagov.ebc.com.br/noticias/202309/ministerio-lancamento-do-hub-da-igualdade-racial-para-disseminar-indicadores-de-raca-cor-no-governo-federal>. Acesso em: 4 dez. 2024.

MJSP - Ministério da Justiça e Segurança Pública. 2022. Decolar é multada em R\$2,5 milhões por oferecer melhores preços a clientes que estão fora do Brasil. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/decolar-e-multada-em-r-2-5-milhoes-por-oferecer-melhores-precos-a-clientes-que-estao-fora-do-brasil>. Acesso em: 7 dez. 2024.

MCKINSEY – 2023. O estado da inteligência artificial em 2023: o ano do crescimento explosivo da IA Generativa | McKinsey. Disponível em: <<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year/pt-BR>>. Acesso em: 13 dez. 2024.

MPOG - Ministério do Planejamento e Orçamento. **PPA ciclo 2024-2027 é aprovado no Congresso Nacional**. O plano segue agora para sanção presidencial. 2023. Disponível em: <https://www.gov.br/planejamento/pt-br/assuntos/noticias/2023/dezembro/ppa-ciclo-2024-2027-e-aprovado-no-congresso-nacional>. Acesso em: 5 dez. 2024.

PAUDYAL, Pragma; WILLIAM WONG, B. L. Algorithmic opacity: making algorithmic processes transparent through abstraction hierarchy. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Sage CA: Los Angeles, CA: SAGE Publications, 2018. p. 192-196.

PHILLIPS-BROWN, Milo. Algorithmic neutrality. arXiv preprint arXiv:2303.05103, 2023. Disponível em: <https://arxiv.org/pdf/2303.05103>. Acesso em: 13 dez. 2024.

REQUIÃO, Maurício; COSTA, Diego Carneiro. Discriminação algorítmica: ações afirmativas como estratégia de combate. *Civilistica.com*. Rio de Janeiro, a.11, n.3, 2022. Disponível em: <http://civilistica.com/discriminacao-algoritmica/>. Data de acesso em: 6 dez. 2024.

SENADO - Agência Senado. Senado aprova regulamentação da inteligência artificial; texto vai à Câmara. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/12/10/senado-aprova-regulamentacao-da-inteligencia-artificial-texto-vai-a-camara>. Acesso em: 12 dez. 2024.

SCHWAB, Klaus. A quarta revolução industrial. São Paulo: Edipro, 2016

SILVA, M. A. **Racismo estrutural**: um obstáculo à eleição de parlamentares negros. Mestrado em andamento em Direito. Universidade de Brasília, UnB, Brasil, 2023. Orientador: Dra. Ana Cláudia Farranha Santana.

SILVA, T. **Racismo Algorítmico**: inteligência artificial e discriminação nas Redes Digitais. 1ª Edição. São Paulo: Edições Sesc SP, 2022.

SILVA, T. Racismo algorítmico em plataformas digitais: microagressões e discriminação em código. In: Comunidades, algoritmos e ativismos digitais. Tarcizio Silva (Org.) São Paulo: **LiteraRua**, 2020. Disponível em: <https://cee.fiocruz.br/?q=Tarcizio-Silva-O-racismo-algoritmico-e-uma-especie-de-Atualizacao-do-racismo-estrutural>. Acesso em: 6 dez. 2024.

SOARES, M. J. P. Impacto da evolução tecnológica no reconhecimento de novos direitos: proteção dos dados pessoais e uso adequado da inteligência artificial. **Revista de Direito e as Novas Tecnologias**. vol. 15. ano 5. São Paulo: Ed. RT, abr.-jun. 2022.

GOVERNANÇA EM PRIVACIDADE DE DADOS: A LGPD E SEU ARTIGO 50

Lucas Paglia¹

INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) tem por objetivo principal proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. A lei versa sobre o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica (pública ou privada), sendo ambos os documentos físicos e os digitais estão contemplados nessa proteção.²

1 Consultor em Proteção de Dados, Privacidade e Compliance do CSMV Advogados; Vice Presidente da Rede Governança Brasil; Pós-graduado em Compliance pela Fundação Getúlio Vargas – FGV, certificado pelo INSPER em Proteção de Dados & Privacidade, certificado como Especialista e como PMO (Líder de Projeto) para Governança em Privacidade pelo Data Privacy Brasil e formado pelo Colégio Brasileiro de Executivo de Saúde (CBEX) de especialização em Healthcare Compliance; Especialista em Cibersegurança pela Universidade de Harvard; Membro da Associação Brasileira de Inteligência Artificial; Especialista convidado para integrar o GT-1 - Subsídios para Elaboração da Política Nacional de Proteção de Dados do Conselho Nacional de Proteção de Dados (CNPd) - GT1/CNPd/ANPD; Presidente do Comitê de LGPD da Rede Governança Brasil – RGB; Coordenador do Livro “LGPD Boas Práticas e Governança para os Municípios Brasileiros”; DPO da Willis Towers Watson Brasil e Colômbia; DPO e Compliance Officer Global da Digibee e Líder do Comitê de Riscos da Digibee Brasil e US; DPO da QGA, ELEMAR tech, Grupo Educacional Galicia e Legale e Monest Fintech; Curador e criador da Pós-graduação da Galicia Educação em DPO – Data Protection Officer reconhecida pelo MEC: (<https://direito.galiciaeducacao.com.br/produto/pos-graduacao-em-data-protection-officer/>); Formou mais de 4.000 alunos em proteção de dados e privacidade; Professor da Puccamp, Legale, Galicia, Meu curso, SEBRAE Nacional, Universidade Corporativa CNI/IEL; Ex-Presidente do Conselho Fiscal da Associação Latino-Americana de Governança – ALAGOV; Membro do Conselho Fiscal da Associação de Ex-Alunos do Colégio Dante Alighieri.

2 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Nesse sentido, a LGPD define um importante passo para a construção da cultura de privacidade e proteção de dados pessoais dos órgãos da administração pública, sejam eles municipais, estaduais ou federais; e empresas privadas e de economia mista, obrigadas todas a cumprir o disposto em lei. Destaca-se a horizontalidade entre suas características, pois permeia todos os departamentos das organizações, nas quais o tratamento de dados pessoais pode envolver diferentes titulares – desde os próprios colaboradores até consumidores, clientes, fornecedores e usuários dos serviços públicos.³

Sendo assim, um programa de governança em privacidade deve atender a alguns requisitos, em especial aos elencados no artigo 50 da própria LGPD. Denominada “Das Boas Práticas e da Governança”, a seção tem apenas dois artigos, entre outros incisos, que elencam algumas das recomendações a ser seguidas pelas empresas durante a implementação da LGPD, com claros apontamentos de continuidade do projeto em momentos posteriores à adequação em si – “Dia 2 da LGPD” ou “Início da fase de governança e monitoramento do projeto”.

O artigo 50⁴, descrito abaixo, traz as principais diretrizes que o legislador observou no início da criação da Cultura de Privacidade e Proteção de Dados no Brasil.

- a. Demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- b. Estabelecer diretrizes e regras que possam ser aplicáveis a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

3 <https://rondonia.ro.gov.br/setic/institucional/lgpd/introducao/>

4 Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

- c. Ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- d. Estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- e. Ser um instrumento que inspira relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- f. Estar integrado à sua estrutura geral de governança e aplicar mecanismos de supervisão internos e externos;
- g. Contar com planos de resposta a incidentes e remediação; e
- h. Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

1. O QUE É GOVERNANÇA?⁵

Considerando que o ato de governar envolve funções como administrar, liderar, orientar, controlar e influenciar, a governança pública se estabelece por meio da implementação e integração de três pilares fundamentais: liderança, estratégia e mecanismos de controle. Esses componentes são operacionalizados com o propósito de avaliar, direcionar e monitorar as ações da gestão municipal, promovendo a consolidação de uma rede organizacional — interna e externa — comprometida com uma cultura de gestão orientada por resultados, transparência, participação e eficiência⁶.

Em termos operacionais, a governança contribui diretamente para a estruturação e o aprimoramento da atuação do(a) prefeito(a) e sua equipe.

5 REDE GOVERNANÇA BRASIL. Cartilha de Governança Pública Municipal. Brasília: RGB, 2021

6 IBGC – Instituto Brasileiro de Governança Corporativa. Código das Melhores Práticas de Governança Corporativa.

No setor corporativo, a definição apresentada pelo Instituto Brasileiro de Governança Corporativa (IBGC) sobre governança é: “o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas”⁷.

Em resumo, pode-se dizer que a governança, tanto no setor público quanto no privado, refere-se ao conjunto de práticas que uma organização adota para consolidar as suas estruturas e sua gestão, indicando a direção a ser seguida, demonstrando confiabilidade e fidelização.

Sendo assim, uma das definições da governança, seja ela pública ou privada, é “compreender todos os processos de governar, seja pelo estado, seja por um governo eleito ou conselhos de administração, ou até mesmo por uma rede de um sistema social, através de leis, normas, políticas, regimentos internos, poder ou até linhagem de sucessão, por exemplo. Todos podem ser considerados sociedades organizadas – sociedades que possuem regras de governança.”

O exercício da governança é composto por decisões de hierarquia e supervisão, mas, principalmente, por ciclos de liderança, estratégia e mecanismos de regulação. A figura acima, extraída da Cartilha de Governança Pública Municipal da Rede Governança Brasil, demonstra efetivamente o ciclo PDCA – *plan* (planejar), *do* (executar), *check* (verificar) e *act* (agir). Tal ciclo é capaz de retratar a constante e necessária evolução que todas as sociedades, administrações, redes ou empresas devem ter para continuar o processo de governança e de melhoria constante.

Nesse sentido, “monitorar”, “avaliar” e “direcionar” são os resultados obtidos a partir da imagem abaixo, que comprovam a eficácia do sistema de governar.

7 ed. São Paulo: IBGC, 2015.



Figura 1

Entre as várias organizações que podem exercer a governança, pode-se considerar a mais formal o governo (federal, estadual, municipal), no contexto da administração pública. No setor privado, por sua vez, isso se manifesta por meio de um conselho ou pela criação de um organograma ajustado à realidade de cada organização.

Dessa forma, a governança tem como única incumbência tomar decisões vinculantes (semelhantes às de um estado), podendo estabelecer leis ou criar regras de controle, como procedimentos e políticas. Além disso, outros tipos de organização podem envolver governança, como grupos sociopolíticos, tribos, gangues, famílias, grupos religiosos ou outros grupos informais de pessoas.

A governança é, portanto, a maneira de determinar ações, sejam elas regras, normas ou controles estruturados e regulados. Certamente, o grau de formalização das ações de uma organização, seja ela pública, que o exige por lei, ou privada, que opta pelo “caminho da governança”, é determinado pelo nível de controle que os líderes (**liderança**) devem ou precisam exercer.

Além disso, a governança pode assumir diversas formas, impulsionadas por motivações diferentes e que podem obter resultados diferentes (**estratégia**). Os resultados decorrem destas escolhas e medidas tomadas pelos governantes e líderes – sejam eles públicos ou privados. A estratégia escolhida é essencialmente vinculada ao “*tone at*

the top” (“o exemplo vem de cima”). A estratégia deve, naturalmente, ser desenhada dentro dos padrões aceitos e cabíveis dentro de cada organização.

É nesse contexto que a governança se instituiu como um dos maiores pilares de sustentabilidade e manutenção das organizações que a utilizam como meios de obter autoridade, domínio ou até mesmo governo (**controle**). A forma natural de se controlar uma organização pública ou privada é monitorar suas ações e escolher uma liderança que fiscalize as estratégias e os resultados obtidos. Assim, a necessidade de controle é facilmente compreendida como um dos fatores preponderantes para o sucesso da implementação da governança nas organizações.

Nesse contexto, a governança geralmente se refere a um nível específico de gestão associado a um tipo de organização (como governança pública, governança global, governança do setor sem fins lucrativos, governança corporativa e governança de projetos), a um “campo” particular de governança relacionado a um tipo de atividade ou resultado (como governança ambiental, governança da internet e governança de tecnologia da informação) ou a um “modelo” específico de governança, frequentemente derivado de uma teoria empírica ou normativa (como governança regulatória, governança participativa, governança multinível, metagovernança e governança colaborativa).



Fonte: LIMA, 2018.

Figura 2

A governança também pode definir agendas normativas ou práticas. Conceitos normativos de governança justa ou boa governança são comuns entre as organizações políticas, do setor público, voluntárias e do setor privado.

2. AS ETAPAS DA ADEQUAÇÃO À LGPD

A fim de obter os primeiros passos para a criação de um projeto de governança de dados pessoais ou governança em privacidade, é fundamental percorrer os artigos anteriores da LGPD, que descrevem o trajeto a ser desempenhado por organizações públicas ou privadas para entender o fluxo de dados pessoais existentes.

Como fase inicial do projeto de adequação da Lei Geral de Proteção de Dados, temos o diagnóstico preliminar/mapeamento de dados:

a. FASE DE DIAGNÓSTICO OU MAPEAMENTO DE DADOS

A etapa de diagnóstico e mapeamento compreende identificar e analisar o fluxo inicial dos dados pessoais e dados pessoais sensíveis que transitam dentro das organizações. Ou seja, mapear os três estágios principais que o dado percorre dentro “de casa”: i) entrada/origem; ii) armazenamento/retenção; iii) compartilhamento/expurgo.

Ou seja, no início do projeto de adequação à LGPD, deve-se identificar, por meio de entrevistas e/ou formulários, o fluxo de vida útil dos dados pessoais, com o objetivo de responder aos itens anteriores. Neste estágio, é fundamental entender também quais leis, regulamentos e normas se aplicam a cada organização, uma vez que o legislador determinou a necessidade de identificar finalidades claras e justificativas consistentes para o uso de cada dado pessoal coletado e tratado.

O artigo 37 da LGPD estabelece que “o controlador e o operador devem manter registro das operações de tratamento de dados pes-

soais que realizarem”. Além disso, tem como finalidade apoiar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e outras ações necessárias, como a identificação de lacunas em relação às exigências da LGPD ou de outras normas. O objetivo é realizar o levantamento das ações que o órgão desenvolve com dados pessoais, delimitando-se o escopo das operações de tratamento de dados pessoais, abrangendo, no mínimo: identificação dos agentes de tratamento; as fases do ciclo de vida do tratamento; descrição do fluxo do tratamento; hipótese legal de tratamento; finalidade e previsão legal do tratamento; quais dados são tratados; categoria dos titulares; informações sobre compartilhamento; classificação das medidas de segurança; informações sobre transferência internacional e informações sobre contratos, termos ou congêneres que estejam correlatos com o tratamento.

Ao final, as organizações deverão ter obtido os registros das operações de tratamento de dados pessoais considerando cada processo existente na organização. Importante destacar que, a partir do princípio da governança, bem como a necessidade de atualização frequente dos registros, é importante sempre manter tais registros atualizados, portanto deve-se estabelecer um ciclo de periodicidade para revisão.

A saber, dentro da etapa de mapeamento, deve ser considerado o gerenciamento de direitos individuais dos titulares de dados pessoais, a gestão de eventual consentimento e o rastreamento de preferências e a redução de responsabilidade por violação.

b. FASE DE EXECUÇÃO

Na etapa seguinte do processo de adequação à LGPD das organizações, deve-se implementar as mudanças necessárias e diagnosticadas no momento inicial do projeto. Ou seja, considerando os dados obtidos no mapeamento dos processos e fluxo de dados pessoais, são identificados os *gaps* a serem corrigidos. A construção das medidas de adequação tem início no mapeamento, mas, uma vez identificados os *gaps*, a fase de execução torna-se obrigatória – salvo contrário, o mapeamento resta infrutífero.

Essa etapa é desenvolvida com base em alguns documentos, sendo os principais descritos a seguir, de forma a amparar o caminho a ser percorrido pelas organizações que buscam definir parâmetros, regras e boas práticas.

A fase de execução é uma parte muito focada em documentação e definição de parâmetros. Por exemplo: a lei determina que todo tratamento de dados pessoais deve ser feito de forma transparente e com finalidades claras, precisas e informadas aos titulares de dados pessoais. De forma irrestrita, as organizações devem cumprir estes princípios, mas de que forma? A solução encontrada para cumprir os requisitos propostos foi criar um documento, denominado Política de Privacidade, no qual os processos são descritos de forma clara, transparente e de fácil acesso aos titulares de dados pessoais, contendo todas as finalidades para as quais os dados serão utilizados.

Por conseguinte, a fase de execução é o momento em que se elaboram as documentações e se executam as ações com o objetivo de cumprir a legislação e proporcionar clareza sobre o tratamento de dados pessoais, tanto para os titulares dos dados quanto para as autoridades responsáveis pelo controle.

Alguns documentos considerados mandatórios durante a fase de mapeamento incluem:

1. Políticas e práticas para proteção da privacidade;
2. Cultura de segurança e proteção de dados e *privacy by design*;
3. Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
4. Adequação de cláusulas contratuais;
5. Identificação de riscos por atividade de tratamento de dados pessoais;
6. Identificação de dados pessoais sensíveis.

Logo, a fase de execução tem o objetivo de trazer documentação concreta ao processo de adequação à LGPD. A necessidade de implementar procedimentos de melhoria decorre da nova regulamentação criada, que aprimora substancialmente a governança e a sucessão de processos nas organizações. Os processos que a cultura de privacidade e, certamente, a cultura da governança desejam estabelecer para desenvolver procedimentos de melhoria a curto, médio e longo prazo — com foco principal no último — são melhor compreendidos quando são concretos e efetivamente implementados.

A ideia de manutenção das execuções propostas será compreendida na etapa seguinte do projeto. No entanto, a concretização dos procedimentos e processos que anteriormente não estavam desenhados e implementados só será possível quando a fase de execução estiver totalmente concluída.

c. ETAPA DE MONITORAMENTO

A última etapa do projeto de adequação à LGPD é a de monitoramento, que inclui indicadores de performance, gestão de incidentes, análise de resultados e o reporte de resultados. Essa fase só deverá ser iniciada se concluídas as fases anteriores, principalmente a fase de execução.

O monitoramento é a primeira fase de implantação da governança das organizações, pois é a partir dele que os primeiros indicadores são coletados e analisados. Sendo assim, somente após a primeira “rodada” de resultados é que o ciclo de melhorias pode ser iniciado.

Assim, independentemente do prazo a ser concluído do projeto, a análise de resultados só tem efetividade após o primeiro ciclo de monitoramento ser finalizado, uma vez que a revisão de metas só traz novos controles se demonstrado que as conclusões iniciais não trouxeram os resultados esperados.

Conforme a doutrina, entre os indicadores de performance, podem-se destacar os índices de serviços com dados pessoais inventa-

riados, os índices de serviços com termos de uso elaborados, o índice de conscientização em segurança, entre outros.⁸

Nesse sentido, a terceira etapa do projeto determina que metas e indicadores de performance e desempenho das execuções realizadas na fase anterior tenham sido criados, tendo em vista a recomendação de comparação entre resultados desejados e resultados coletados no primeiro ciclo de indicadores.

Como já elucidado, a análise e reporte dos resultados obtidos precisa ser constante para verificar a eficácia ou a necessidade de melhorias e adaptações no processo.

É importante mencionar que, após a conclusão das três etapas estabelecidas pela legislação e que fazem parte do projeto de adequação à LGPD, uma das principais premissas do legislador na criação da lei foi a inclusão da legítima expectativa dos titulares de dados pessoais.

Certamente, um dos principais ditames da LGPD, se não o mais importante, é o “princípio lógico” presente em seus artigos. Explica-se: ao elaborar a legislação, o legislador optou por não definir todos os limites para o tratamento de dados, mas, sim, por influenciar o conceito amplo da legítima expectativa que o titular de dados pessoais tem em relação à utilização de seus dados durante seu ciclo de vida útil, conforme já explicado.

Assim, durante o tratamento dos dados pessoais, deve-se preservar a finalidade pela qual o dado foi coletado e garantir que ela tenha sido claramente comunicada ao titular. Ele deve, portanto, compreender o uso de todos os seus dados e a forma do tratamento prevista pelo controlador e pelo operador já no momento da coleta. Ou seja, o dado pessoal coletado para preenchimento de um cadastro, por exemplo, deve ser informado ao titular e mantido ao longo de toda a sua trajetória.

Mais especificamente: se o dado pessoal foi coletado com a finalidade de realizar cadastro de consumidor em uma farmácia, este mesmo dado não deveria ser utilizado para cadastro em um outro comércio não anteriormente citado, mesmo que do mesmo grupo econômico; cumprindo-se os princípios da finalidade e da transparência.

8 Boas Práticas de Governança na proteção de Dados: o Programa (direitoreal.com.br)

Reitera-se que o uso do dado pessoal pela própria farmácia para outra finalidade, como, por exemplo, o envio de um aviso sobre uma promoção para um consumidor que frequentemente compra um medicamento naquele estabelecimento, é amparado pela base legal da legítima expectativa, podendo ser realizado, mesmo que não tenha sido previsto nas primeiras coletas de processos e finalidades do uso desse dado pessoal.

Denota-se, portanto, que a irregularidade a ser evitada, sob a perspectiva do legislador na criação da LGPD, não é o uso do dado pessoal sem finalidade anteriormente prevista, mas, sim, o uso de finalidades que não remetem à legítima expectativa que o titular de dados pessoais tinha ao fornecer aquele dado pessoal.

3. GOVERNANÇA COMO PROCESSO: O PASSO SEGUINTE AO MONITORAMENTO

Em seu sentido mais amplo, a governança é um conceito teórico que se refere a ações e processos. Como um processo, deve ser observada e delineada no sentido de preservação das estruturas, independentemente de quem ocupa os cargos e postos. A preservação se dá pela manutenção fidedigna da estratégia adotada pelas organizações, e que não deve ser alterada ou substituída, salvo sob instrução da liderança a respeito de novos controles a serem implementados.

Ainda, a definição de processo, no âmbito corporativo, se dá por um “conjunto de atividades inter-relacionadas ou interativas que usam ou transformam entradas para entregar um resultado”⁹. Pode-se inferir, a partir disso, que a estrutura organizacional da governança decorre das estratégias e políticas para tomada de decisões e responsabilização das organizações. É necessário delimitar as responsabilidades de cada pessoa, departamento, órgão, entidade e terceiros e garantir o cumprimento das atribuições estabelecidas – *accountability*.

9 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO 9000:2015 – Sistemas de gestão da qualidade – Fundamentos e vocabulário*. Rio de Janeiro: ABNT, 2015

A governança, quando implementada, deve ser mantida nas estruturas da organização, visto que tem objetivos de longo prazo, não somente de curto e médio prazos. As metas são estabelecidas de acordo com os três períodos, mas com foco no último, criando o processo correto para obter os resultados desejados.

Logo, a estruturação da governança como um processo tem por objetivos:

- i) Refletir a identidade, missão ou propósito da organização em relação à sociedade e suas partes interessadas;
- ii) Aumentar a eficácia organizacional, sustentabilidade, responsabilidade e equidade;
- iii) Cumprir o propósito da organização;
- iv) Evitar grandes incidentes.

Contudo, a organização que baseia suas atividades na governança não deve acreditar que somente isso é o necessário. A revisão dos controles implementados junto aos resultados obtidos sempre deve ser analisada a partir das metas (números programados e desejáveis) e, quando necessário, deve realizar ajustes aos pontos “fora da curva”.

O ciclo PDCA, conforme demonstrado anteriormente, é a forma recomendada de trazer perspectivas hialinas e objetivas aos alvos desenhados anteriormente.

A governança deve refletir quais os resultados a organização querem atingir, aumentando a eficácia no sentido de organizar as estruturas e, principalmente, os processos internos e externos. Naturalmente, ao revisar os pontos anteriormente previstos, os processos se atualizam, devem buscar a melhoria constante, mesmo na ausência das pessoas que participaram da criação dos processos.

Nesse diapasão, nota-se, portanto, que as pessoas são os meios pelos quais os processos ocorrem, entretanto não podem ser maiores que os processos em si. A busca pelo equilíbrio entre resultado, eficácia e governança também é observada na LGPD e, conseqüentemente, na implementação do programa de governança de dados pessoais recomendado.

Sendo assim, no caso da proteção de dados, deve-se colocar o titular no centro da discussão. A partir dos modelos elucidados, denota-se uma importante definição de quem é o foco dos processos para alcançar a chamada governança. No projeto de adequação à LGPD, o titular de dados pessoais, seja ele o hóspede de um hotel ou o paciente de um hospital, deve ser respeitado como o principal foco da governança.



Figura 3

4. A GOVERNANÇA EM PRIVACIDADE DE DADOS PESSOAIS

Os agentes de tratamento de dados pessoais – controladores e operadores, no âmbito de suas competências, com relação ao tratamento de dados, podem elaborar individualmente ou por intermédio de associações regras de boas práticas e de governança que determinem as condições de organização, os padrões técnicos, as normas de segurança, entre outros, nos termos do artigo 50, caput, da LGPD.

Ao estabelecer as referidas regras, os controladores e operadores devem levar em consideração, no que se refere ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade, bem como a

gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular. Conforme mencionado anteriormente, as fases do projeto de adequação são essenciais para identificar estes pontos.

Outrossim, as regras de boas práticas e de governança devem ser atualizadas e publicadas de maneira periódica.

Vale destacar o papel central da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por determinar as principais alterações legislativas e de interpretação da letra fria da lei. Além disso, é responsável por zelar pela proteção dos dados pessoais; por elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; por fiscalizar e aplicar sanções nos casos de tratamento de dados que descumprirem a legislação, por meio de processo administrativo, que assegure o contraditório, a ampla defesa e o recurso, entre outros.

A ANPD tem como objetivo, ainda, receber e analisar as denúncias enviadas pelos titulares de dados pessoais e pode, de ofício, solicitar esclarecimentos acerca do tratamento de dados realizados pelos controladores e operadores de dados pessoais.

Assim, o programa de governança em privacidade de dados pessoais pode ser entendido como o conjunto de regras e de boas práticas que determinem as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações para os envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de diminuição de riscos e outros aspectos referentes ao tratamento de dados pessoais.

No artigo 50, § 2º, da LGPD são indicadas as características mínimas de um programa de governança em privacidade de dados pessoais, quais sejam:

- O comprometimento do controlador na adoção de processos e políticas internas que assegurem o cumprimento, de maneira abrangente, de normas e boas práticas relacionadas à proteção de dados pessoais;
- A aplicação a todo conjunto de dados pessoais que estejam sob o seu controle, independentemente da forma como

foi realizada a coleta;

- A adaptação à estrutura, à escala e ao volume de suas operações, assim como, à sensibilidade dos dados tratados;
- O estabelecimento de políticas e salvaguardas de acordo com o processo de avaliação sistemática de impactos e riscos à privacidade;
- O estabelecimento da relação de confiança com o titular, por intermédio de atuação transparente e que assegure mecanismos de participação do titular;
- A integração da estrutura geral de governança, o estabelecimento e a aplicação de mecanismos de supervisão internos e externos;
- Planos de resposta a incidentes e remediação;
- A atualização constante com base nas informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Uma vez estruturado, o programa deve ser implementado de acordo com as instruções estabelecidas nos documentos de privacidade provenientes das etapas do projeto de adequação à LGPD. Esse é o momento que comprova a importância da correta elaboração das etapas do projeto.

Um bom projeto incorre em um bom programa de governança em privacidade, sendo certo que o papel da governança, nesse momento, é determinar sua efetividade. É a governança, ainda, que identifica se os controles e metas previstos anteriormente terão os resultados obtidos.

Nesse momento, é importante que a equipe de proteção de dados pessoais, liderada pelo encarregado de dados, conduza todos os esforços para garantir que as políticas e procedimentos estabelecidos sejam corretamente aplicados pelo restante da equipe. O gerenciamento do ciclo de vida dos dados deve possuir todos os processos, padrões e funções bem definidos e registrados.

Logo, a criação da denominação do termo Governança em Privacidade decorre da necessidade da criação do próximo estágio da adequação à LGPD.

Observando de modo prático, após concluído o “dia 1 da LGPD”, que consiste em identificar os dados pessoais, mapear os fluxos internos das organizações, realizar as mudanças identificadas e mitigar os riscos apresentados, conforme trazido anteriormente, se faz necessário retomar o projeto da criação da estrutura da governança, desta vez, em privacidade e proteção dos dados pessoais.

Assim, cada política, norma e ação criada pelas organizações deve ser documentada para demonstrar a efetividade de seu programa de governança quando houver questionamento e, em especial, a pedido da ANPD. A adoção de políticas de boas práticas e governança não apenas auxilia o cumprimento das obrigações estabelecidas pela LGPD, como também demonstra os esforços nesse sentido, e todos os registros documentados das ações adotadas serão considerados em uma eventual aplicação de sanção por tratamento inadequado de dados pessoais.

Conforme já mencionado, a governança possibilita um aprimoramento da capacidade de gestão, do controle e da integridade das informações, servindo como base de sustentação dos processos internos.

Dessa forma, pode-se observar que os requisitos para um programa de governança baseado na LGPD estão alinhados com as diretrizes adotadas por grandes empresas e órgãos públicos.

A implementação de medidas de segurança e de procedimentos de retenção e eliminação de dados pessoais, restrição de acesso e compartilhamento, tratamento de dados internacionais, gerenciamento de terceiros e notificações sobre vazamento de dados são determinantes para o bom andamento e efetiva mitigação dos riscos levantados pelo mapeamento de dados.

Passando por outras etapas do programa de governança em privacidade, deve-se observar, além da revisão do próprio programa em si, algumas das lacunas apontadas pelo mapeamento de dados pessoais

realizados anteriormente. Tais ações não apenas dizem respeito à própria adequação do processo, mas também identificam-se como partes fundamentais da etapa da governança.

Em determinado momento do fluxo, são identificados os agentes de tratamento de dados, que, na maioria das vezes, são operadores que atuam em nome dos controladores. Um dos riscos mais difíceis de mensurar em caso de incidentes de segurança da informação está relacionado a terceiros, devido à falta de informações detalhadas sobre eles.

É possível, portanto, que esses terceiros apresentem falhas em suas adequações, o que, devido ao princípio da responsabilidade objetiva estabelecido pela lei, também recai sobre o controlador. Uma das formas de dirimir esse impacto e, conseqüentemente, mitigar os riscos que correm o tratamento de dados ao ser realizado por operadores é a elaboração de cláusulas contratuais de responsabilização e prestação de contas.

Essas cláusulas são responsáveis por obrigar a devida adequação de operadores e/ou terceiros que agem em nome do controlador, assegurando mais proteção e transparência no tratamento dos dados pessoais dos titulares – ou seja, reforçando o exercício da governança em privacidade.

Uma vez que os terceiros integram o sistema de tratamento de dados pessoais e representam uma extensão desse processo, eles são obrigados a participar do programa de governança dos controladores, tornando necessária a inclusão de cláusulas contratuais.

Outro ponto de suma importância, já destacado anteriormente, é a nomeação de um encarregado de dados pessoais, o DPO (sigla para *data protection officer*). Ele é a figura responsável pela manutenção da adequação à LGPD e pelo programa de privacidade de dados.

Denota-se, a partir da figura abaixo, extraída do “Guia de Como Implementar um Programa de Governança em Dados” (tradução livre) da Autoridade de Proteção de Dados de Cingapura, que o encarregado de dados é o agente condutor do programa em si.

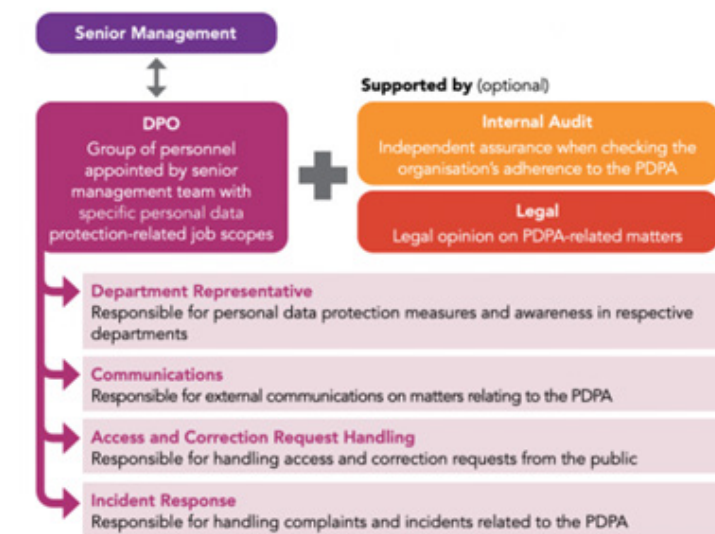


Figura 4 - A governança da proteção de dados é liderada pelo DPO, que coordena ações em várias áreas e pode contar com apoio jurídico e de auditoria para garantir conformidade com a PDPA.

Ressalta-se, entre as principais atividades da governança em privacidade, o conceito de *privacy by design*, a ideia de que medidas técnicas e administrativas de privacidade e proteção de dados devem ser implementadas desde a concepção do desenvolvimento de um sistema.

O conceito de *privacy by design* destaca ao menos três valores: (i) a proatividade, ao se incluir a privacidade como parte dos requisitos de engenharia do sistema; (ii) a incorporação de controles de privacidade, que serão auditados e avaliados continuamente; e (iii) o respeito aos titulares de dados, por meio do uso de controles transparentes, permitindo que indivíduos exerçam seus direitos.

Como exemplo, o Ministério da Economia, em documento publicado¹⁰, apresenta algumas medidas técnicas e organizacionais que o conceito de *privacy by design* abrange, incluindo:

10 BRASIL. Ministério da Economia. *Governo digital e proteção de dados pessoais: guia de boas práticas*. Brasília: Ministério da Economia, 2020.

- a. Uso de criptografia para proteção de bases de dados e meios de comunicação;
- b. Minimização e pseudonimização de bases de dados;
- c. Controle de acesso baseado em funções;
- d. Mecanismo de respostas a requisições e reclamações dos titulares de dados;
- e. Plano de respostas a incidentes e remediação de segurança e privacidade;
- f. Segurança física;
- g. Políticas de privacidade para aquisição de produtos/serviços;
- h. Políticas de gerenciamento da segurança da informação;
- i. Política de retenção e eliminação de dados pessoais.

Dos exemplos apontados, duas práticas se destacam como as mais relevantes no contexto do *privacy by design*, pois colocam o titular de dados no centro da discussão, como já mencionado anteriormente. Essas práticas envolvem os mecanismos de resposta a solicitações, dúvidas e eventuais reclamações dos titulares de dados, bem como a gestão de suspeitas de incidentes de segurança e privacidade, incluindo a condução de respostas a tais incidentes.

Tais mecanismos têm como objetivo garantir o respeito aos direitos dos titulares de dados previstos pela LGPD, além de preparar a organização para cenários indesejados, como vazamentos de dados, identificando as áreas que precisam ser envolvidas para mitigar os danos, informando as partes interessadas (como a ANPD e os próprios titulares de dados) e lidando com as possíveis responsabilizações judiciais.

A governança de dados, ou a governança em privacidade (que são estruturas diferentes, mas convergentes) passam pelo idealismo que a lei trouxe. Um incidente de segurança da informação pode ocorrer,

mas a correta condução e gestão de medidas para reduzir os impactos e riscos aos titulares, assim como a comunicação assertiva e tempestiva dos fatos, são fundamentais.

Ou seja, a governança, nesse momento, é totalmente direcionada a atingir estes objetivos, pois, mesmo que o programa de adequação tenha identificado lacunas nos processos das organizações, e que documentos e procedimentos tenham sido criados e desenvolvidos, a correta condução dos incidentes e resposta aos titulares de dados – e revisão de possíveis ajustes necessários – só terá resultados efetivos por meio da governança.

É importante ressaltar que, frequentemente, de maneira equivocada, utiliza-se o termo «governança de dados» como sinônimo da estrutura jurídico-regulatória relacionada à proteção de dados.

No entanto, de acordo com o DAMA – *Data Maturity Body of Knowledge*¹¹, a governança de dados é “o exercício de autoridade e controle (planejamento, monitoramento e execução) sobre o gerenciamento de ativos de dados”, e “fornece orientação e supervisão para o gerenciamento de dados, estabelecendo um sistema de direitos de decisão sobre dados que atenda às necessidades da empresa”. Vale ressaltar que os “dados” referidos englobam tanto os considerados “pessoais” como “não pessoais”, como dados estratégicos da empresa e dados de pessoas jurídicas.

A governança em privacidade, por sua vez, é voltada para os dados considerados “pessoais” pela LGPD — aqueles que identificam ou tornam uma pessoa natural identificável — e tem como base um direito humano fundamental: a privacidade. Embora a conformidade normativa seja essencial, as atividades de um programa de governança em privacidade não se resumem ao cumprimento do mínimo exigido pelo artigo 50, mas vão além disso.

11 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 9000:2015 – Sistemas de gestão da qualidade – Fundamentos e vocabulário. Rio de Janeiro: ABNT, 2015

Nesse sentido, a intenção do legislador não é apenas garantir o cumprimento dos requisitos legais e documentar que as organizações, sejam privadas ou públicas, estejam em conformidade com a legislação. Deve-se explorar os princípios e fundamentos da lei, com ênfase na legítima expectativa do titular de dados pessoais, além de demonstrar como a liderança adota esses princípios por meio de seus controles. Ou seja, transformar a privacidade e sua governança em um ativo estratégico para as organizações.

Quando as empresas demonstram ir além do cumprimento legal em matéria de proteção de dados e privacidade, sendo proativas no reforço à transparência, à boa-fé, à segurança e à não discriminação no uso dos dados pessoais, por exemplo, ao mesmo tempo em que promovem a inovação, a autodeterminação informativa, o livre desenvolvimento da personalidade e o respeito à privacidade, estão promovendo sua valorização sob os olhos dos titulares.

Logo, a governança em privacidade transforma-se em um ativo. Além disso, promove o compliance e auxilia de forma efetiva na prevenção a sanções administrativas e judiciais e, principalmente, gera impactos positivos na operação e agrega valor à empresa.

A governança de dados, tendo o compliance – que assegura que as atividades da organização estejam de acordo com as exigências legais e regulatórias pertinentes – como um de seus pilares, apresenta uma intersecção com a governança em privacidade. Ambas estão debaixo do guarda-chuva da governança corporativa, um sistema que dirige a organização por meio de boas práticas que contribuem para sua gestão, longevidade e bem comum.



Figura 7. Considerações Etapa de Construção e Execução

Figura 5

5. CONSIDERAÇÕES FINAIS

Considerando a vigência da lei e a sua relevância para as organizações, tanto públicas quanto privadas, é de suma importância compreender a legítima expectativa do legislador para aplicar a legítima expectativa do titular de dados como centro do debate.

Conforme exposto, o caminho mais adequado para aplicar a LGPD em sua essência é a criação de um programa de governança em privacidade de dados pessoais bem fundamentado nas fases precedentes à adequação à lei e descrito em etapas. Para relembrar, a adequação à LGPD é o “dia 1”, e a existência do programa de privacidade de dados pessoais é o “dia 2” do aculturamento das organizações.

De modo prático, o conceito clássico de governança, relacionado à organização e estruturação de sistemas e processos, também deve ser objeto de estudo nos moldes da legislação brasileira de prote-

ção de dados. Além disso, o próprio texto da lei enfatiza a relevância da governança nos artigos 50 e subsequentes.

Por outro lado, as organizações públicas e privadas que param no “dia 1” do projeto encontrarão dificuldades de conscientização e aculturação ao longo do tempo. Portanto, recomenda-se incluir treinamento dos colaboradores e garantir o real entendimento do objetivo do programa ao implementar os processos de governança.

Logo, para que a transformação exigida pela LGPD seja efetiva, deve a organização prosseguir até o “dia 2”, a fim de obter indicadores de resultados para compreender se os objetivos traçados anteriormente são precisos.

A maneira mais eficaz de realizar o monitoramento exigido pela lei, e que integra a criação da governança em privacidade, é por meio da coleta de dados e análise de números, no intuito de avaliar e orientar possíveis ajustes e alterações.

A criação de um programa de governança em privacidade de dados torna-se, portanto, um ativo organizacional, composto por estruturas de governança, compliance e metodologias de revisão de processos, com o objetivo de alcançar resultados mais efetivos, adotar condutas mais adequadas, promover o aculturação diante dos novos desafios digitais e, principalmente, atender à intenção da Lei Geral de Proteção de Dados: garantir que o titular de dados pessoais seja respeitado como centro do debate.

REFERÊNCIAS

Cartilha: Governança Pública Municipal – Transformando Sua Administração – 2ª Edição de 2021 (Rede Governança Brasil - RGB) https://www.rgb.org.br/_files/ugd/5a9d77_6e122020ad594965b75f6fcb96e22024.pdf

Guia de Elaboração de Programa de Governança em Privacidade – Lei Geral de Proteção de Dados Pessoais – Versão 1.0 de outubro de 2020 https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf

Livro: Data Protection Officer (encarregado): por Renato Opice Blum
286

(Autor), Rony Vainzof (Autor), Henrique Fabretti Moraes (Autor).

Guide to Developing a Data Protection Management Programme <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Management-Programme-14-Sep-2021.ashx?la=en>

Livro: Dama-Dmbok (2Nd Edition): Data Management Body of Knowledge

Artigo: Afinal de contas: o que é a “Governança em Privacidade” da LGPD? <https://www.migalhas.com.br/depeso/330230/afinal-de-contas--o-que-e-a--governanca-em-privacidade--da-lgpd>

IMPACTOS DA LGPD NO E-COMMERCE BRASILEIRO: DESAFIOS E BOAS PRÁTICAS PARA A PROTEÇÃO DE DADOS DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO

Mariana Landim Carneiro¹

INTRODUÇÃO

Estamos no meio de uma revolução ainda mais exponencial com a inteligência artificial e temos consumido conteúdos cada vez mais curtos e fragmentados. Por isso, é importante que o *E-commerce* acompanhe esse movimento, não só com foco nas vendas, mas em uma comunicação eficiente e de acordo com a legislação. Ademais, de acordo com a pesquisa *E-commerce Trends 2024*,² realizada pela Octadesk em parceria com o Opinion Box, 62% dos consumidores realizam de duas a cinco compras online por mês, sendo que 85% comprem pelo menos uma vez no mesmo período.

Nesse cenário, a pandemia do coronavírus acelerou ainda mais a busca por tecnologia pelos consumidores e obrigou as empresas de pequeno e médio porte a se reinventarem para atravessar a crise. De acordo com um levantamento da Mastercard,³ o número de companhias brasileiras que fizeram a migração para o ambiente digital cresceu 208% em 2020, na comparação com o volume de movimentações de

1 Advogada pós-graduanda em Direito Digital e Proteção de Dados pelo Instituto Brasileiro de Direito Público (IDP); membro da Associação Internacional de Profissionais de Privacidade (International Association of Privacy Professionals - IAPP); Certificada em Privacidade e Proteção de Dados pelo Data Privacy Brasil e Legal Designer.

2 SCHOLZ, Mahara. *E-commerce Trends*: 62% dos consumidores fazem até cinco compras online por mês. **BLOG OCTADESK**. 17 ago. 2023. Disponível em: <https://encurtador.com.br/huANT>. Acesso em: 5 dez 2023.

3 ALVES, Pedro. O número de PMEs brasileiras que migraram para o digital cresceu 208% durante a pandemia, indica a Mastercard. **MASTERCARD**. 6 out. 2021. Disponível em: <https://encurtador.com.br/nAINS>. Acesso em: 3 dez. 2023.

2019. Além disso, estudos da Associação Brasileira de Comércio Eletrônico (ABComm)⁴ preveem que o faturamento do *E-commerce* deve alcançar mais de 200 bilhões de reais por ano até 2027. Junto com esse crescimento exponencial, aumentam também as ameaças cibernéticas.

Ataques como roubo de dados, *phishing* e *ransomware* tornaram-se mais sofisticados, visando explorar vulnerabilidades e comprometer a confiança dos consumidores. Assim, as empresas precisam adotar uma postura proativa na defesa contra essas ameaças por meio de investimentos em segurança da informação, além de cumprir as exigências da Lei 13.709/18 (Lei Geral de Proteção de Dados - LGPD) e, ainda, conquistar e manter a confiança dos seus clientes, colaboradores e parceiros.

Vale lembrar que essa confiança pode ser construída por meio de ações de transparência e responsabilidade, por isso as empresas de *E-commerce* devem comunicar da forma mais clara possível as suas práticas de segurança e demonstrar comprometimento com a proteção dos dados dos titulares em uma escala maior do que o varejo tradicional “analógico”, já que as informações na internet são ainda mais vulneráveis, acessíveis e escaláveis.

A transparência é um princípio essencial da LGPD. Este princípio determina, em resumo, que as organizações precisam ser honestas com os titulares e devem informar aos titulares de dados sobre os respectivos agentes de tratamento, que são, basicamente, outras empresas envolvidas no processo de tratamento dos dados. O princípio da transparência, de acordo com o inciso VI do art. 6º desta Lei, é a “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”.

Esse princípio fica bastante visível no atendimento ao cliente, sobretudo naqueles realizados em meio digital e em ações de *marketing*. Além disso, é importante que o usuário seja sempre avisado sobre

4 ABComm. Previsão de vendas no *E-commerce* para os próximos 5 anos. 1 dez. 2023. Disponível em: <https://dados.abcomm.org/previsao-de-vendas-online>. Acesso em: 3 dez. 2023.

como é feita a utilização dos seus dados, mesmo que este tratamento não dependa do consentimento. Trata-se de uma boa prática que pode melhorar, entre outros pontos, a gestão de relacionamento com o cliente (CRM - Customer Relationship Management).

Resta claro, portanto, que o comércio eletrônico oferece conveniência e acessibilidade aos consumidores, mas traz consigo desafios significativos, especialmente no que diz respeito à segurança dos dados que ali circulam. Em um cenário onde informações pessoais são trocadas a cada transação, a proteção desses dados torna-se um compromisso inegociável e um desafio para organizações de qualquer porte.

1. A AMPLITUDE DO CONCEITO DE *E-COMMERCE*

Também chamado de comércio eletrônico ou comércio online, o *E-commerce* é muito mais que apenas vender na internet. É “toda e qualquer relação realizada virtualmente, por meio da transmissão eletrônica de dados, por computador ou outro veículo de comunicação em que não há contato físico entre as partes”.⁵ Logo, o *E-commerce* não se refere apenas às vendas por meio de uma loja online. As vendas por aplicativos de mensagem (como o WhatsApp ou Telegram), por telefone e *marketplaces* também são variações desse conceito.

O *marketplace* é um tipo de *E-commerce*, uma variação na qual a loja virtual não é própria. Ou seja, oferece uma plataforma comum para que várias empresas vendam os seus produtos. Essa plataforma faz a intermediação do processo de cobrança e, em muitos casos, também assume uma certa parcela da responsabilidade sobre a garantia da entrega e da qualidade do produto vendido.⁶

Para um lojista, o *marketplace* é uma alternativa atraente, porque é bem mais simples de gerenciar, já que toda a estrutura está pronta, bastando fazer um cadastro e catalogar produtos. Por outro lado,

5 SOUZA, Sylvio Capanema de. WERNER; José Guilherme Vasi; NEVES, Thiago Ferreira Cardoso. **Direito do Consumidor**. Rio de Janeiro: Forense. 2018. p. 393.

6 SAMPAIO, Daniel. O que é *E-commerce*? Tudo o que você precisa saber para ter uma loja virtual de sucesso! **ROCK CONTENT**. 9 out. 2019. Disponível em: <https://rockcontent.com/br/blog/E-commerce-guia>. Acesso em: 26 dez. 2023.

a sua responsabilidade quanto ao tratamento de dados pessoais pode ser solidarizada. É o que diz o art. 42 da LGPD a respeito de eventual indenização ao titular:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva **indenização ao titular dos dados**:

I - o operador responde **solidariamente** pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

Já em um atendimento pelo telefone, por sua vez, a empresa tem acesso a dados pessoais básicos antes mesmo de efetuada a venda, como o número do telefone e o nome do titular (além de voz e imagem em alguns casos), isso sem falar nas vendas que são realizadas por meio das redes sociais, que abrangem uma infinidade de referências pessoais. Assim, apenas com poucas informações é possível criar um banco de dados de clientes e interessados para envio de propagandas em massa, e é isso que muitas empresas fazem até hoje.

Portanto, participar ou criar um *E-commerce* requer inúmeros cuidados, sobretudo com o crescente número de fraudes e ataques cibernéticos, e é imprescindível que as organizações que operam no digital tenham um programa de compliance geral e de proteção de dados muito bem estruturado.

2. DESAFIOS CONTEMPORÂNEOS DE PRIVACIDADE E PROTEÇÃO DE DADOS NO COMÉRCIO ELETRÔNICO BRASILEIRO

A segurança de dados no *E-commerce* é uma jornada constante e multidimensional. Empresas que investem em tecnologias avançadas e em conformidade com os padrões de segurança de normas técnicas (como aquelas da família ISO), educação do usuário e resposta eficaz a incidentes não estão apenas protegendo seus clientes, mas também fortalecendo sua posição no mercado.

E mais: em um ambiente digital cada vez mais desafiador, a existência de uma Política ou Aviso de Privacidade não é sinônimo de segurança. Ela precisa estar aliada a estratégias eficazes e ações imperativas para o sucesso sustentável de uma empresa no mercado digital, assim como em uma loja física, por exemplo. Outro desafio está na captação e fidelização de clientes, já que a publicidade deve ser direcionada a finalidades específicas e estar justificada por pelo menos uma base legal válida dentre aquelas indicadas pela LGPD nos artigos 7º e 11º.

No tocante ao site em que a loja on-line fica acessível ao público, é importantíssimo que sejam feitos alguns ajustes. Por exemplo, é indispensável que a página contenha todas as informações necessárias aos titulares e ao público em geral em local de fácil acesso, com linguagem compreensível, clara e direta.⁷ O mesmo vale para as responsabilidades inerentes aos negócios jurídicos. O titular de dados deve estar ciente de seus deveres quando acessa uma página na internet (o documento ideal para isso são os Termos de Uso do site, que funciona como um contrato entre as partes) e deve poder exercer os seus direitos, tanto aqueles previstos no Código de Defesa do Consumidor (CDC) quanto os da LGPD.

Nesse novo cenário, estratégias mais personalizadas e éticas ganham destaque, alinhando-se não apenas com as exigências legais,

7 LIMA, Ana Paula Moraes Canto de. A adequação do *E-commerce* à LGPD. In: CRESPO, Marcelo; PECK, Patrícia (coord.). **LGPD Aplicada**. São Paulo: Atlas, 2021, p. 85-101.

mas também com as expectativas crescentes dos clientes em relação à privacidade e segurança de seus dados, sobretudo em um imenso banco de dados digital com todo tipo de informações armazenadas e disponibilizadas das mais diversas formas.

2.1. Comunicação e transparência nos negócios digitais

O compartilhamento de dados pessoais na internet está literalmente a um clique de distância entre as empresas e seus consumidores diretos e indiretos. E quando o assunto é comprar online, a assimetria de informações e tratamento indevido de dados pessoais nas relações de consumo oriundas da internet amplia o estado de vulnerabilidade do consumidor.

O próprio CDC consagra o direito de acesso às informações de bancos de dados das empresas e o direito à retificação dos dados, direitos que também estão presentes também na LGPD. Vejamos:

Código de Defesa do Consumidor	Lei Geral de Proteção de Dados
Art. 43 - Caput: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.	Art. 18 - O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
Art. 43 - §3º: O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.	I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; [...]

Diante disso, as empresas de *E-commerce* precisam estar atentas ao cumprimento de determinados requisitos para se adequar não só à

legislação consumerista, mas à própria LGPD, garantindo aos titulares informações precisas sobre como os seus dados pessoais são tratados, desde a coleta até o descarte.

O primeiro passo é a criação e divulgação de um Aviso de Privacidade⁸ na página da empresa, e esse documento precisa refletir a realidade da organização com informações claras e acessíveis sobre o responsável pelo tratamento; os dados pessoais coletados e suas respectivas finalidades, inclusive aqueles não informados pelo usuário; a base legal para o tratamento; o prazo de retenção dos dados pessoais; as informações de contato do Encarregado de Proteção de Dados; entre outros.⁹

Uma dúvida recorrente no meio corporativo sobre o Aviso de Privacidade é se este documento deve ser restrito ao site da empresa ou à organização como um todo. Alguns especialistas defendem a primeira opção, no entanto, não há regra específica na legislação. Em termos práticos, o Aviso de Privacidade deve ser o mais completo possível, voltado ao meio externo (clientes, fornecedores, terceiros, etc.) e em linguagem simples.

Aliás, o termo linguagem simples - ou *plain language* - converge com o princípio da transparência e do livre acesso ao titular de dados, pois defende uma comunicação facilmente percebida pela audiência desde o primeiro contato. O *Plain Writing Act*, legislação norte-americana sobre o tema, define linguagem simples como uma “redação clara, concisa, bem organizada e que segue outras práticas recomendadas apropriadas ao assunto ou área e ao público-alvo”.¹⁰

8 Aqui o termo Aviso se refere ao documento direcionado ao público externo e que deve ser divulgado no site da empresa. A doutrina entende que o termo técnico correto para este documento seria Aviso de Privacidade. Já a Política de Privacidade seria um documento interno, direcionado aos colaboradores da organização.

9 FREITAS, Carla. Como elaborar uma política de privacidade aderente à LGPD? **SERPRO**. 11 out. 2019. Disponível em: <https://encurtador.com.br/jnAP6>. Acesso em: 28 dez. 2023.

10 THE PLAIN LANGUAGE ACTION AND INFORMATION NETWORK. What is plain language? Disponível em: www.plainlanguage.gov/about/definitions. Acesso em: 28 dez. 2023.

Na prática isso pode ser feito por meio de técnicas de *Legal Design*, como avisos multicamadas e *layouts* estruturados, afinal, as pessoas só podem concordar com algo que elas efetivamente entendam. Por exemplo, no site de uma empresa, o Aviso de Privacidade pode ser dividido em “camadas”, sendo a primeira apenas um resumo e as demais com informações detalhadas sobre o tratamento dos dados.

É importante ressaltar que no *E-commerce* as vendas não são presenciais e, portanto, o contato com os clientes se dá praticamente apenas no *online*. Ainda assim, é importante que os agentes de tratamento possuam um canal de comunicação efetivo com o consumidor, não só por meio de uma Ouvidoria, recomenda-se, ainda, um canal exclusivo de atendimento aos direitos dos titulares apenas para demandas relacionadas à privacidade e proteção de dados pessoais. Uma forma simples de resolver isso é por meio de formulários digitais e um *e-mail* exclusivo para o Encarregado de Dados (*Data Protection Officer* - DPO), que ficará responsável por estas demandas.

2.2. Publicidade responsável para captação de *leads* de acordo com a LGPD

Outro ponto de atenção que as empresas de *E-commerce* devem ter é com relação ao *marketing* digital para captação de possíveis clientes, os chamados *leads*. Pela definição do Sebrae, *lead* é uma oportunidade de negócio, uma pessoa que fornece seus dados de contato em troca de uma oferta, que pode ser um *e-book*, uma ferramenta, uma *newsletter*, entre outros. Essa pessoa demonstra interesse por um produto ou serviço quando preenche um formulário *online*, passando a ser um potencial cliente.¹¹

A captação de *leads* é muito importante para o *E-commerce*, pois esses dados e contatos de pessoas que já se interessaram por algum conteúdo ou produto da empresa podem ser convertidos em vendas quando trabalhados da forma correta.

11 SEBRAE. Você sabe o que é lead? Entenda como implementar uma estratégia de marketing digital eficaz para identificar e captar leads para o seu negócio. 29 nov. 2022. Disponível em: <https://encurtador.com.br/morU1>. Acesso em 30 dez. 2023.

Por isso é tão comum encontrarmos em qualquer tipo de site um formulário de cadastro gratuito. A famosa frase do jornalista americano, Andrew Lewis, explica bem isso: “se você não paga pelo produto, o produto é você”. A ideia desses cadastros é justamente coletar informações para propagandas direcionadas a consumidores em potencial. Mas, de acordo com a LGPD, o titular precisa ter conhecimento disso, deve saber a finalidade do tratamento e, neste caso específico, deve ter o poder de escolha em fornecer ou não os seus dados pessoais.

A melhor forma de fazer isso é deixando claro ao consumidor a finalidade da coleta por meio de avisos diretos e com acesso facilitado ao Aviso de Privacidade, e ele deve expressamente concordar com o recebimento de e-mails publicitários. Nesse sentido, ao preencher o cadastro, o cliente deve dar o seu consentimento para receber conteúdo da empresa (*opt-in*), expressando real interesse em receber as comunicações. Outrossim, deve ser dado ao cliente também o direito de oposição (*opt-out*), que é a opção de não mais receber este tipo de propaganda (no e-mail em que a empresa enviar a publicidade do produto, deverá conter a opção do titular se descadastrar da lista de contatos).

Outra estratégia de *marketing* no comércio eletrônico que está diretamente ligada à regulamentação trazida pela LGPD é a criação dos chamados *cookies* de Internet: pequenos fragmentos de dados que são desenvolvidos especificamente para que navegadores da *web* rastreiem, personalizem e salvem informações sobre a sessão de cada usuário. Ou seja, os *sites* criam *cookies* e gravam o arquivo no computador do usuário para personalizar a navegação.

No *E-commerce*, essa estratégia serve, por exemplo, para manter itens adicionados a um carrinho de compras mesmo que a pessoa mude de página ao navegar entre vários produtos. Sem os *cookies*, o site não seria capaz de manter as informações salvas no meio do caminho.¹²

Além de preservar dados durante o tráfego, os *cookies* funcionam como identificador do computador. O endereço IP, do inglês

12 ALVES, Paulo; O que são cookies? Entenda os dados que os sites guardam sobre você. **TECHTUDO**. 4 out. 2018. Disponível em: <https://encurtador.com.br/kHKQ8>. Acesso em: 15 nov. 2023.

Internet Protocol, por exemplo, é uma informação que pode identificar uma pessoa. Com base nisso, os endereços *online* podem personalizar anúncios e destaques a serem exibidos para o usuário conforme o histórico de visitas anteriores.

A Autoridade Nacional de Proteção de Dados (ANPD) publicou um Guia Orientativo¹³ a respeito desse tema e apresentou dois tipos de *banners* de cookies: *Cookies Consent* e *Cookies Notice*. O primeiro consiste em painel de gerenciamento de *cookies*, por meio do qual os usuários podem escolher (com exceção daqueles essenciais) se aceitam os *cookies* e de quais tipos. Esse é o modelo por excelência usado na Europa, em razão da necessidade de consentimento para *cookies* (não pela *General Data Protection Regulation* - GDPR, mas pela *e-Privacy Directive*). Já o segundo (muito difundido nos Estados Unidos, que não estabelecem o consentimento como base legal para *cookies*, mas prevêem deveres de transparência e informação dos titulares), consiste em um aviso mais simples sobre a utilização da ferramenta no *site*, tipos de *cookies* e outras informações relevantes que precisam ser esclarecidas.

Contudo, segundo o guia da ANPD, “os *banners* de *cookies* são mecanismos difundidos no ambiente digital, desenvolvidos como uma forma de materialização dos princípios previstos na LGPD, em especial os da transparência e do livre acesso. Ao apresentar informações essenciais sobre o uso de *cookies* de maneira resumida e simplificada, os *banners* contribuem para o processo de tomada de decisão consciente pelo titular, além de fortalecer o controle sobre seus dados pessoais e o respeito às suas legítimas expectativas. Assim, o *banner* serve como uma ferramenta para trazer transparência e aderência aos princípios de proteção de dados pessoais”.

Nessa perspectiva, o *banner* de primeiro nível deve conter opções mais amplas, como “aceitar todos os *cookies*” e “rejeitar *cookies* não necessários». E, ainda de acordo com o Guia, é essencial a disponibilização de um mecanismo simplificado e gratuito para a revogação do consentimento pelo titular.

13 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo: Cookies e proteção de dados pessoais. 18 out. 2022. Disponível em: <https://encurtador.com.br/bhrLN>. Acesso em: 27 nov. 2023.

O banner de segundo nível, por sua vez, deve possibilitar a gestão dos *cookies* de modo mais específico, com as categorias de *cookies* e de modo a garantir a obtenção de consentimento específico do titular dos dados pessoais. Deve disponibilizar também no *website* a Política de *Cookies* que, de acordo com o Guia da ANPD, pode ser apresentada “como uma seção específica do Aviso de Privacidade; em um local específico e separado; ou no próprio *banner* de *cookies*”.

Essas mudanças não apenas desafiam as práticas tradicionais de *marketing*, mas instigam as empresas digitais a repensarem suas abordagens para engajamento e fidelização de clientes, priorizando a transparência e a confiança na gestão de dados pessoais de consumidores em toda rede mundial de internet.

2.3. Segurança de dados de pagamento e potencial efeito lesivo

No *E-commerce*, os consumidores sempre devem fornecer seus dados pessoais para realizar uma compra. Mas o que muitos não sabem é que essas informações, em regra, não são consideradas sensíveis pela legislação, o que permite tratamentos um pouco mais flexíveis - em tese.

Para comprar online, normalmente são coletados dados como nome completo, CPF, endereço de cobrança, telefone, e-mail e, é claro, os dados de pagamento, como número do cartão de crédito. Ocorre que, apesar da relevância dessas informações, a LGPD não reconhece a sua sensibilidade à luz do conceito formal trazido no art. 5º. Vejamos:

Art. 5º Para os fins desta Lei, considera-se:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Logo, os dados do cartão de crédito, não são, em tese, dados sensíveis. Inclusive, a 2ª Turma do Superior Tribunal de Justiça (STJ) entendeu, em março de 2023, que o vazamento de dados pessoais não gera dano moral presumido (*in re ipsa*), “sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações”.¹⁴ A decisão foi proferida nos autos do Agravo em Recurso Especial nº 2.130.619/SP, que reformou o acórdão do Tribunal de Justiça de São Paulo que havia condenado uma empresa ao pagamento de indenização por dano moral pelo vazamento de dados pessoais não sensíveis da autora. A conclusão do STJ foi que o inciso II do art. 5º da LGPD traria “um rol taxativo daquilo que seriam dados pessoais sensíveis”.

Contudo, a professora Caitlin Mulholland entende que este rol seria exemplificativo, pois “não somente o conteúdo dos dados previsto neste inciso merecerão a qualificação como dados sensíveis, podendo abarcar outras situações não previstas”.¹⁵ Semelhante a esta ideia, Danilo Doneda defende que dados sensíveis “seriam determinados tipos de informações que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva”.¹⁶

Em resumo, um dado é categorizado como sensível de acordo com o potencial efeito discriminatório (igualdade material) e/ou lesivo à liberdade (utilizações indevidas ou abusivas) de tratamento em relação aos demais dados pessoais. Ou seja, para Doneda, o rol de dados sensíveis trazidos no inciso II do art. 5º da LGPD são opções trazidas pelo legislador motivadas pelo efeito potencialmente lesivo do seu tratamento. Logo, seguindo esta premissa, dados de cartão de crédito ou comprovantes de pagamento poderiam ser considerados sensíveis a depender do contexto.

14 SUPERIOR TRIBUNAL DE JUSTIÇA. Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma. 17 mar. 2023. Disponível em: <https://encurtador.com.br/cnPRT>. Acesso em: 30 dez. 2023.

15 MULHOLLAND, Caitlin. **Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais**. Revista do Advogado, São Paulo, n. 144, p. 47-53, nov. 2019.

16 DONEDA, Danilo. **Da privacidade à proteção de dados**. Rio de Janeiro: Renovar. 2005, p. 160-161.

No comércio eletrônico isso se potencializa. Imagine um *E-commerce* que não confirma a identidade do titular (por meio de dupla autenticação, por exemplo) ou que não possui protocolos de criptografia e, por consequência, seus dados de pagamento são facilmente vazados, inclusive na *deep web*. O potencial lesivo desse tratamento é imensurável.

Por isso, é responsabilidade das empresas que operam no comércio eletrônico garantir a segurança desses dados e cumprir com as exigências da LGPD. E, para garantir que o ambiente de uma loja virtual seja confiável, é preciso se preocupar não só com o ambiente digital, mas também com o físico, sobretudo quanto à mudança de mentalidade sobre a importância da proteção de dados pessoais. Por trás do digital existem “pessoas que movem toda a estrutura, as quais precisam compreender a importância e a necessidade das mudanças e da adequação a ser promovida”.¹⁷

É imprescindível que todas as pessoas envolvidas na cadeia de produção sejam efetivamente treinadas quanto às melhores práticas de tratamento de dados e todas as medidas de segurança precisam ser registradas. O mesmo vale para os agentes de tratamento de pequeno porte, como pequenas lojas virtuais ou criadores de conteúdo.

2.1.1. O perfil do consumidor pós-pandemia e o caráter extraterritorial da LGPD aplicado ao *E-commerce*

Podemos dizer que uma das maiores vantagens da internet é a amplitude dos limites geográficos, a globalização do consumo. Hoje é plenamente possível adquirir um produto de países do oriente ou de qualquer outro lugar do mundo, sobretudo por meio de *marketplaces* como Aliexpress e Amazon, que revendem mercadorias nacionais e internacionais. Inclusive, de acordo com a pesquisa de Intenção de Com-

17 LIMA, Ana Paula Moraes Canto de. A adequação do *E-commerce* à LGPD. In: CRESPO, Marcelo; PECK, Patrícia (coord.). **LGPD Aplicada**. São Paulo: Atlas, 2021, p. 85-101.

pra e Top Of Mind,¹⁸ da NielsenIQ Ebit Brasil, 19% dos brasileiros têm a Amazon como principal marca de *E-commerce* quando vão realizar suas compras *online*.

E quanto à proteção dos dados pessoais dos consumidores brasileiros que adquirem produtos de fornecedores internacionais? Essas empresas estariam “blindadas” pela LGPD? Este é um assunto pertinente e que merece atenção, pois, diferentemente de outras legislações brasileiras, a LGPD possui caráter extraterritorial, ou seja, ela transcende os limites territoriais de sua jurisdição.

De acordo com a professora Ana Frazão,¹⁹ “a preocupação da lei é justificável diante da globalização e de uma série de características de mercados digitais, o que possibilita que cada vez mais titulares de dados no território nacional estejam submetidos a tratamentos de dados por empresas estrangeiras que ofertam seus serviços no Brasil. Dessa maneira, é salutar que a LGPD procure assegurar sua aplicação mesmo diante de agentes estrangeiros ou de tratamentos de dados realizados no exterior, desde que preenchidos os requisitos do art. 3º da LGPD. Todavia, a depender do caso, haverá grandes dificuldades práticas para assegurar a eficácia da lei em tais situações”.

A partir da leitura da LGPD, a sua aplicação extraterritorial depende, portanto, do seguinte: que a operação de tratamento seja realizada no Brasil; ou que o objetivo do tratamento seja a oferta ou o fornecimento de bens ou serviços para indivíduos localizados no Brasil; ou que o tratamento tenha por objetivo o tratamento de dados pessoais de indivíduos localizados no Brasil; ou, por fim, que os dados pessoais sejam coletados no Brasil.

Podemos concluir então que, para qualquer empresa que opera *online* estar sujeita às normas da LGPD, ela não precisa possuir sede em território nacional, bastando cumprir um dos requisitos acima, o que

18 *E-COMMERCE BRASIL*. Amazon é o principal *E-commerce* na mente dos brasileiros, mostra relatório da NielsenIQ Ebit. 19 maio 2023. Disponível em: <https://encurtador.com.br/fors5>. Acesso em: 28 dez. 2023.

19 FRAZÃO, Ana. Aplicação Territorial da LGPD e Eficácia Extraterritorial. **GEN JURÍDICO**. 5 jul. 2022. Disponível em: <https://encurtador.com.br/kntyQ>. Acesso em: 28 dez. 2023.

faz com que praticamente todo o comércio digital esteja submetido aos princípios e regras da LGPD, mesmo aqueles que ainda não possuam legislação específica sobre este tema.

3. ENCERRAMENTO

No atual cenário do *E-commerce* brasileiro, é evidente que as empresas de pequeno, médio e grande porte precisam adotar uma abordagem estratégica para enfrentar os desafios contemporâneos relacionados à privacidade e proteção de dados, sejam dos seus clientes, colaboradores ou terceiros que com elas se relacionam.

Diante da diversidade e amplitude do conceito de *E-commerce*, fica claro que a proteção de dados deve ser uma prioridade constante. A solidariedade na responsabilidade, conforme destacado pela LGPD, ressalta a importância de uma abordagem colaborativa entre os participantes do ecossistema digital para garantir a integridade e segurança das informações pessoais dos consumidores. Nesse contexto, uma comunicação jurídica eficiente e o cumprimento das regulamentações, especialmente da LGPD, são fundamentais para manter a confiança dos consumidores e garantir uma operação segura e ética.

A segurança de dados torna-se uma jornada constante, exigindo investimentos em tecnologias avançadas, conformidade com padrões de segurança e educação contínua dos usuários. A existência de um Aviso ou Política de Privacidade não é suficiente por si só, e os agentes de tratamento devem adotar medidas rigorosas para garantir a proteção dessas informações, incluindo autenticação dupla, protocolos de criptografia e treinamento abrangente para todos os envolvidos na cadeia de produção.

Em resumo, o *E-commerce* brasileiro enfrenta desafios complexos e deve estar sempre preparado para lidar com a globalização do consumo e suas respectivas obrigações regulatórias. É um desafio, não só para as empresas, para para os agentes fiscalizadores como Ministério Público, Instituto de Defesa do Consumidor (Procon), Secretarias

e a própria Autoridade Nacional de Proteção de Dados (ANPD), por lidarem com um infinito oceano de oportunidades e carência de regulamentação específica.

O objetivo principal não deve ser apenas estar em conformidade com a lei, mas priorizar a segurança, honra e dignidade do titular de dados, tendo em vista, inclusive, que a proteção de dados foi incluída no rol de direitos fundamentais do art. 5º da Constituição Federal pela Emenda Constitucional (EC) 115/2022.

Logo, a adoção de práticas transparentes e éticas não apenas fortalece a segurança dos dados pessoais e do próprio titular de dados, mas também contribui para a construção de uma sociedade mais consciente e relacionamentos duradouros com os consumidores em um ambiente digital em constante evolução.

REFERÊNCIAS

ABCOMM. Previsão de vendas no *E-commerce* para os próximos 5 anos. 1 dez. 2023. Disponível em: <https://dados.abcomm.org/previsao-de-vendas-online>. Acesso em: 3 dez. 2023.

ALVES, Paulo; O que são cookies? Entenda os dados que os sites guardam sobre você. **TECHTUDO**. 4 out. 2018. Disponível em: <https://encurtador.com.br/kHKQ8>. Acesso em: 15 nov. 2023.

ALVES, Pedro. O número de PMEs brasileiras que migraram para o digital cresceu 208% durante a pandemia, indica a Mastercard. **MAS-TERCARD**. 6 out. 2021. Disponível em: <https://encurtador.com.br/nAINS>. Acesso em: 3 dez. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo: Cookies e proteção de dados pessoais. 18 out. 2022. Disponível em: <https://encurtador.com.br/bhrLN>. Acesso em: 27 nov. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados**. Rio de Janeiro: Renovar. 2005, p. 160-161.

E-COMMERCE BRASIL. Amazon é o principal *E-commerce* na mente dos brasileiros, mostra relatório da NielsenIQ Ebit. 19 maio 2023. Disponível em: <https://encurtador.com.br/fors5>. Acesso em: 28 dez. 2023.

FRAZÃO, Ana. Aplicação Territorial da LGPD e Eficácia Extraterritorial. **GEN JURÍDICO**. 5 jul. 2022. Disponível em: <https://encurtador.com.br/kntyQ>. Acesso em: 28 dez. 2023.

FREITAS, Carla. Como elaborar uma política de privacidade aderente à LGPD?. **SERPRO**. 11 out. 2019. Disponível em: <https://encurtador.com.br/jnAP6>. Acesso em: 28 dez. 2023.

LIMA, Ana Paula Moraes Canto de. A adequação do *E-commerce* à LGPD. In: CRESPO, Marcelo; PECK, Patrícia (coord.). **LGPD Aplicada**. São Paulo: Atlas, 2021, p. 85-101.

MULHOLLAND, Caitlin. **Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais**. Revista do Advogado, São Paulo, n. 144, p. 47-53, nov. 2019.

SAMPAIO, Daniel. O que é *E-commerce*? Tudo o que você precisa saber para ter uma loja virtual de sucesso! **ROCK CONTENT**. 9 out. 2019. Disponível em: <https://rockcontent.com/br/blog/E-commerce-guia>. Acesso em: 26 dez. 2023.

SCHOLZ, Mahara. *E-commerce* Trends: 62% dos consumidores fazem até cinco compras online por mês. **BLOG OCTADESK**. 17 ago. 2023. Disponível em: <https://encurtador.com.br/huANT>. Acesso em: 5 dez 2023.

SEBRAE. Você sabe o que é lead? Entenda como implementar uma estratégia de marketing digital eficaz para identificar e captar leads para o seu negócio. 29 nov. 2022. Disponível em: <https://encurtador.com.br/morU1>. Acesso em 30 dez. 2023.

SOUZA, Sylvio Capanema de. WERNER; José Guilherme Vasi; NEVES, Thiago Ferreira Cardoso. **Direito do Consumidor**. Rio de Janeiro: Forense. 2018. p. 393.

SUPERIOR TRIBUNAL DE JUSTIÇA. Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma. 17 mar. 2023. Disponível em: <https://encurtador.com.br/cnPRT>. Acesso em: 30 dez. 2023.

THE PLAIN LANGUAGE ACTION AND INFORMATION NETWORK. What is plain language? Disponível em: www.plainlanguage.gov/about/definitions. Acesso em: 28 dez. 2023.

MARKETING DIGITAL E PROTEÇÃO DE DADOS PESSOAIS: ANÁLISE DA PERCEPÇÃO DOS CONSUMIDORES QUANTO À PROTEÇÃO DE SEUS DADOS E A CONSTRUÇÃO DA CONFIANÇA NA MARCA

Mariani Nazaré da Silva Costa¹

Matheus Resende da Silva Costa²

INTRODUÇÃO

Na contemporaneidade da era digital e com o avanço da Internet, pode-se notar o elevado consumo de informações por parte dos consumidores, assim como a grande busca das empresas pelos dados dos titulares.

É cada vez mais difícil pensar em ações isoladas no ambiente na Internet, visto que o que é comunicado nesse ambiente pode afetar os consumidores e marcas, direta ou indiretamente.³

Nesse contexto, as empresas têm utilizado o marketing digital, em especial a publicidade direcionada, visando estabelecer um relacionamento mais próximo e individualizado com o consumidor. Para tanto, é necessário o tratamento de dados pessoais que implicam em reações positivas ou negativas, a depender da maneira pela qual se deu a utilização dos dados.

1 Analista de Privacidade e Éticas de Dados no Grupo Boticário, Bacharel em Sistemas da Informação com experiência em análise de dados, selecionada para o Programa Youth Brasil 2023 – Comitê Gestor da Internet

2 Advogado em Privacidade e Proteção de Dados, Secretário Adjunto da Comissão de Privacidade e Proteção de Dados da OAB/DF, Certificado em Privacidade e Proteção de Dados pelo Data Privacy Brasil.

3 TORRES, Claudio. **A bíblia do marketing digital: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar**. São Paulo: Novatec, 2009. p. 61-62.

O objetivo principal do presente artigo é analisar as percepções dos consumidores quanto à privacidade e proteção dos seus dados pessoais no contexto do marketing digital e como isso impacta na construção da confiança entre os consumidores e as marcas. No primeiro capítulo é feita uma análise de diferentes pesquisas realizadas através de entrevistas de usuários da internet/consumidores sobre o grau de confiança na proteção de sua privacidade por empresas das quais consomem produtos ou serviços online; a sua opinião quanto ao uso de seus dados para envio de publicidade direcionada; e as principais ações realizadas para gerenciar o acesso a seus dados pessoais.

Já no segundo capítulo apresenta-se o conceito de personalização no marketing digital e como seu uso pode aumentar a relevância do serviço e a aceitação por parte dos clientes e, paradoxalmente, aumentar a sensação de vulnerabilidade gerando uma rejeição por parte dos consumidores a depender da adoção ou não do consentimento.

No terceiro capítulo, é analisada a conexão entre os princípios da Lei Geral de Proteção de Dados Pessoais e a construção da confiança entre o consumidor e as marcas, apresentando pesquisas sobre as principais atitudes praticadas pelas empresas na construção da confiança, bem como as que têm maior potencial de quebrá-la ao mesmo tempo em que se analisa como a aplicação dos princípios da finalidade, adequação, necessidade e transparência contribuem para tanto.

No quarto capítulo, são mencionados casos reais em que marcas renomadas se posicionaram no sentido de contribuir com a garantia da autodeterminação informativa adotando práticas diretamente e indiretamente relacionadas à publicidade direcionada no contexto do marketing digital.

Por fim, são apresentadas as considerações finais.

1. PERCEPÇÕES DOS CONSUMIDORES QUANTO À SUA PRIVACIDADE E PROTEÇÃO DOS SEUS DADOS NO MARKETING DIGITAL

Na atual conjuntura da sociedade da informação, as empresas disputam a atenção dos consumidores por meio do seu principal instrumento de comunicação: o marketing. Com o desenvolvimento da internet, os meios tradicionais de comunicação cederam lugar para os meios digitais como websites, plataformas de *streaming*, redes sociais, de modo que se desenvolveu o marketing digital para alcançar o consumidor que navega pela internet com o intuito de criar um relacionamento mais próximo.

Antigamente, as empresas utilizavam a publicidade de massa por meio da TV e rádio, mas, através da internet, é possível estabelecer uma publicidade mais direcionada a um indivíduo ou grupo de pessoas por meio da identificação de seus interesses, do seu comportamento ou da maturidade do consumidor dentro do processo de compra.⁴

Nunca é demais mencionar o clássico exemplo de um usuário que navega em um site de viagens clicando em destinos que o interessam e, ao deixá-lo, visita outro site sobre esportes e recebe uma propaganda referente a uma viagem para o destino que havia pesquisado pouco tempo antes. Isso é publicidade direcionada.

Ocorre que, no processo de envio de uma publicidade direcionada, é necessário que as empresas colem dados pessoais de clientes os quais, muitas vezes, nem têm conhecimento desse processo e, inclusive, sequer autorizam essa operação (“tratamento de dados”).

Diante de tal situação surge um sentimento de insegurança nos usuários internautas ao consumir produtos e serviços online. Segundo pesquisa realizada pela Axios em 2019,⁵ após entrevistar 2.122

4 ROCKCONTENT. **Personalização de Conteúdo**. ROCKCONTENT BLOG, disponível em: <https://rockcontent.com/br/blog/personalizacao-de-conteudo/>. Acesso em: 2 jul. 2025.

5 SURVEYMONKEY. SurveyMonkey and Axios Poll: **Privacy Deep Dive**. SURVEYMONKEY, disponível em: <https://www.surveymonkey.com/curiosity/survey-monkey-axios-poll-privacy-deep-dive/>. Acesso em: 2 jul. 2025.

americanos adultos, 59% dos entrevistados afirmaram não estar confiantes quanto à proteção de sua privacidade por empresas das quais consomem produtos ou serviços online. Na mesma ocasião, 43% dos entrevistados consideraram inapropriado o uso, por parte de empresas, dos dados pessoais de forma a fornecer produtos e serviços melhores e mais individualizados, enquanto 29% o consideraram apropriado e 26% não consideram apropriado nem inapropriado.

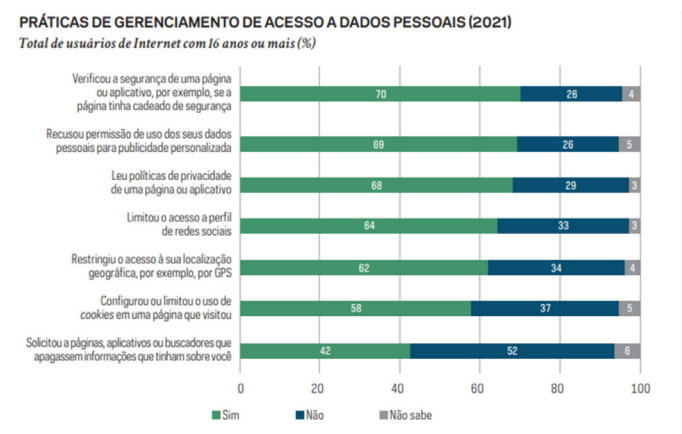
No cenário brasileiro não é diferente. Conforme estudo realizado entre graduandos em Direito na Universidade Federal de Juiz de Fora em 2020, a maioria dos estudantes (64,8%) não consideram válido ter de compartilhar seus dados pessoais como mecanismo para recebimento de ofertas, descontos em bens e serviços advindos de anúncios on-line. Além disso, 54,5% dos estudantes entendem que o recebimento de publicidade enquanto navegam pela internet, sem o seu consentimento, não os auxiliam em suas compras.⁶

A preocupação com a privacidade e proteção dos dados pessoais existe no imaginário das pessoas, mesmo que muitos cidadãos não saibam ao certo quais atitudes tomar para resguardar suas informações no ambiente online. Já quando o usuário de internet conhece certos instrumentos de proteção, verifica-se a tomada de certos cuidados no seu dia a dia.

É o que se observa da pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br) ao entrevistar usuários de internet com 16 anos ou mais, em 2021, a qual verificou que, dentre as ações realizadas para gerenciar o acesso a seus dados pessoais, a mais utilizada é a verificação de segurança de página ou aplicativo (70%) - a exemplo da verificação do cadeado de segurança do navegador -, seguida da recusa de permissão de uso de seus dados para publicidade personalizada (69%) e a leitura

6 NEGRI, S. M. C. A.; RIBEIRO, L. C.; TERRA, A. M. V.; FERES, Marcos Vinício Chein. **Percepção do Consumidor Referente à Proteção de seus Dados Pessoais no Contexto de Utilização de Publicidades On-line pelo E-commerce**. 2020. Dissertação (Mestrado em Direito e Inovação) - Universidade Federal de Juiz de Fora.

de políticas de privacidade de páginas ou aplicativos (68%).⁷ Veja o quadro a seguir:



Fonte: Comitê Gestor da Internet.⁸

Ante o exposto até aqui, percebe-se que os titulares de dados pessoais não se sentem confiantes em como seus dados pessoais têm sido tratados de um modo geral e, principalmente, quando são alvos de publicidade direcionada, comumente realizada sem transparência e sem a autorização do titular.

2. A PERSONALIZAÇÃO E O USO DOS DADOS DOS CONSUMIDORES

O conteúdo personalizado configura-se como qualquer interação da marca, seja o oferecimento de serviços online ou ofertas, criando uma experiência única e direcionada utilizando dados e informações,

7 BRASIL. Comitê Gestor da Internet no Brasil. (2022). **Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil**. São Paulo: CGI.br. <https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/>

8 *Ibid.*

previamente coletadas, específicas sobre o cliente.⁹ Os consumidores almejam uma experiência mais individualizada ao interagir com as marcas, sobretudo com as marcas com as quais eles interagem frequentemente.¹⁰

Diante da necessidade de personalização, as marcas têm se empenhado para que haja assertividade nos anúncios direcionados e que, por meio do tratamento dos dados, consigam influenciar as decisões de compras.¹¹ Dessa forma, realizam a coleta de dados sobre o comportamento online dos consumidores, para posteriormente realizar o oferecimento de serviços personalizados.

Uma maior personalização normalmente aumenta a relevância do serviço e a aceitação por parte dos clientes, porém, de forma paradoxal, também pode aumentar a sensação de vulnerabilidade e gerar uma rejeição por parte dos consumidores. Por vezes, sem o consentimento expresso, a coleta de dados é feita de forma silenciosa, e ao receber a publicidade de serviços personalizados, o que antes seria bem aceito pelo consumidor em caso de uma coleta de consentimento, se transforma em vulnerabilidade e desconforto, por parte do consumidor, ao descobrir que seus dados foram coletados sem a sua autorização.¹²

O sentimento de vulnerabilidade, uma vez instaurado, tende inicialmente a afastar o indivíduo da marca, sendo geralmente seguido por questionamentos quanto à sua segurança, confiança e transparência na coleta dos dados, por ora inquestionáveis na ausência de uma publicidade direcionada. Em vista disso, um estudo realizado entre

9 ADOBE BUSINESS. **How to Personalize Content**. ADOBE BLOG, disponível em: <https://business.adobe.com/blog/basics/how-to-personalize-content>. Acesso em: 2 jul. 2025.

10 *Ibid.*

11 HAWKINGS, Gary. **Will Big Data Kill All But the Biggest Retailers?** Harvard Business Review, September 18, 2012. Disponível em: <https://hbr.org/2012/09/will-big-data-kill-all-but-the>. Acesso em: 2 jul. 2025.

12 AGUIRRE LOPEZ, E., MAHR, F. D., GREWAL, D., DE RUYTER, J. C., & WETZELS, M. G. M. (2015). **Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness**. Journal of Retailing, v. 91, n. 1, p. 34-49, Jan. 2015. <https://doi.org/10.1016/j.jretai.2014.09.005>.

graduandos em Direito na Universidade Federal de Juiz de Fora em 2020,¹³ demonstrou que mesmo se sentindo vulneráveis com o uso dos seus dados, a maioria dos participantes não utiliza nenhum instrumento online de forma protetiva/preventiva para gerenciar o recebimento de anúncios online. Isso revela um “paradoxo da privacidade”, uma vez que, embora os consumidores demonstrem preocupações diretas em como os seus dados estão sendo tratados, os seus comportamentos não refletem essa preocupação.¹⁴

3. A INTERLOCUÇÃO DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A CONSTRUÇÃO DA CONFIANÇA DO CONSUMIDOR NA MARCA

A confiança assume papel fundamental nas relações comerciais, principalmente no ambiente online. Se de um lado a construção da confiança do consumidor em uma marca leva a um aumento de compras, recomendação a amigos e publicação de comentários positivos em redes sociais, por outro, a quebra da confiança pode levar consumidores a abandonarem completamente uma marca.¹⁵

Segundo pesquisa Future of Marketing realizada pela Adobe em 2021, entrevistando mais de 2.017 consumidores, no Reino Unido, diversas marcas têm ferido a confiança dos consumidores por meio do mau uso dos seus dados pessoais. Dentre as três principais atitudes to-

13 NEGRI, S. M. C. A.; RIBEIRO, L. C.; TERRA, A. M. V.; FERES, Marcos Vinício Chein. **Percepção do Consumidor Referente à Proteção de seus Dados Pessoais no Contexto de Utilização de Publicidades On-line pelo E-commerce**. 2020. Dissertação (Mestrado em Direito e Inovação) - Universidade Federal de Juiz de Fora.

14 TADDICKEN, Monika. **The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics and the Perceived Social Relevance on Different Forms of Self-Disclosure**. Journal of Computer-Mediated Communication, 2014. p. 249. Disponível em: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/jcc4.12052>. Acesso em 2 jul. 2025.

15 ADOBE BUSINESS. **7 in 10 Customers Will Buy More from Brands They Trust**. ADOBE BLOG, disponível em: <https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk>. Acesso em: 2 jul. 2025.

madras pelas marcas com potencial de quebrar a confiança do consumidor, destacam-se: a) o rastreamento online em dispositivos móveis sem a permissão do consumidor, o envio de e-mails/outras comunicações, sem que o consumidor se lembre de ter fornecido suas informações” (49%); b) o envio de demasiadas comunicações, sem a clareza sobre as políticas de privacidade ou o que fazem com os dados pessoais (39%); e c) a insistência do envio de anúncios ou comunicações, mesmo depois do consumidor ter feito o “opt-out” (39%).¹⁶

No que se refere à construção da confiança, vale a pena destacar o achado do mesmo estudo segundo o qual, de acordo com os consumidores entrevistados, a ação mais importante para ganhar a sua confiança é “pedir permissão para usar os seus dados” (45%) enquanto a segunda mais importante é a utilização mais “aberta e transparente” dos seus dados (40%), seguida por permitir que os consumidores tenham mais “controle sobre os seus dados” (39%).¹⁷

Percebe-se que a maior queixa dos consumidores (titulares de dados pessoais) é justamente por uma inobservância por parte das empresas (agentes de tratamento de dados) aos preceitos da Lei Geral de Proteção de Dados Pessoais (LGPD).

“Ter mais controle sobre os seus dados” nada mais é do que uma das definições da autodeterminação informativa, um dos fundamentos da LGPD previsto em seu artigo 2º, inciso II, que guia toda a interpretação da norma. A autodeterminação informativa é compreendida como o controle pessoal sobre o fluxo de dados relativos ao próprio titular durante toda a cadeia de tratamento dos dados.¹⁸

No tocante aos princípios do tratamento dos dados pessoais, destaca-se os princípios da finalidade, adequação, necessidade e transparência que constituem o núcleo da LGPD e são determinantes para a

16 ADOBE BUSINESS. **7 in 10 Customers Will Buy More from Brands They Trust**. ADOBE BLOG, disponível em: <https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk>. Acesso em: 2 jul. 2025.

17 *Ibid.*

18 MALDONADO, Viviane Nóbrega, BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 29. Bibliografia. ISBN 978-65-5065-023-0.

garantia da proteção dos direitos fundamentais de liberdade, de privacidade e do livre desenvolvimento da pessoa natural, através da tutela dos dados pessoais.¹⁹

O princípio da finalidade, previsto no inciso I, do art. 6º da lei, estabelece um vetor por meio do qual toda utilização dos dados pessoais deve obedecer à finalidade estabelecida. A partir dessa finalidade, é possível avaliar a possibilidade de uso dos dados para outra finalidade, desde que seja compatível com aquela estabelecida. A análise dessa compatibilidade é justamente a aplicação do princípio da adequação, previsto no inciso II, do art. 6º da LGPD.²⁰

Quanto ao princípio da necessidade, previsto no inciso III, do art. 6º, tem-se que os dados devem ser tratados com o mínimo necessário para a satisfação da finalidade estabelecida.²¹

Já o princípio da transparência, previsto no inciso VI, do art. 6º, visa a diminuir a assimetria informacional entre o titular e o agente de tratamento de dados, ao estabelecer o dever de garantia aos titulares de informações claras, precisas e facilmente acessíveis tanto sobre o tratamento em si quanto sobre quem são os agentes de tratamento.²²

Nesse sentido, a LGPD preceitua nos artigos 9º, 18 e 19 diversos tipos de informações que devem ser prestadas ao titular espontaneamente ou mediante requerimento dos titulares. Cita-se como exemplo a necessidade de se informar ao titular a: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; confirmação da existência de tratamento; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; dentre outros.²³

19 *Ibid.*, 128.

20 BRASIL. [Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**]. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 2 jul. 2025.

21 *Ibid.*

22 *Ibid.*

23 *Ibid.*

Ressalta-se que a informação precisa ser disponibilizada de forma clara, adequada e ostensiva de modo e na medida certa, a fim de não causar um excesso de informações que confundam o titular de dados ou dificultem sua compreensão.

Nas palavras de Bruno Bioni, a informação precisa ser adequada, pois somente assim “o cidadão estará capacitado para controlar seus dados. O fluxo dos seus dados precisa tomar forma (ser informado), sendo pressuposto para que haja qualquer tipo de processo de tomada de decisão por parte do titular dos dados”.²⁴

Conforme visto anteriormente, a pesquisa realizada pela Adobe revelou que “pedir permissão para usar os seus dados”, a “utilização mais aberta e transparente dos dados” e permitir ao consumidor “ter mais controle sobre os dados” são as principais ações praticadas pelas empresas com potencial de construir a confiança entre os consumidores e a marca.²⁵

Se as empresas (controladores) se propuserem a aplicar eficazmente os princípios da LGPD, discutidos até aqui, não apenas contribuirão para a autodeterminação informativa do titular, trazendo o controle dos dados para o titular, mas também ganhando a confiança do consumidor e gerando um diferencial competitivo, visto que os consumidores comprem mais das marcas que confiam e tendem a abandonar as que rompem sua confiança.²⁶

Por fim, apesar de não ser o objeto de estudo desse artigo, vale a pena esclarecer que a escolha da hipótese legal para tratamento de dados pessoais, dentre as opções previstas na LGPD como o consentimento, legítimo interesse e execução de contrato, varia conforme a arquitetura da operação da empresa, mas se tem observado uma preferência dos titulares pelo consentimento, tema que pode ser alvo de uma pesquisa futura.

24 BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 242. Inclui bibliografia. ISBN 978-85-309-8328-4.

25 ADOBE BUSINESS. **7 in 10 Customers Will Buy More from Brands They Trust**. ADOBE BLOG, disponível em: <https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk>. Acesso em: 2 jul. 2025.

26 *Ibid.*

4. CASOS DE SUCESSO

Na mesma linha dos princípios para o tratamento de dados pessoais estabelecidos pela LGPD, algumas marcas têm se empenhado em trilhar um percurso marcado pela transparência e confiança. Dessa forma, um movimento de protagonismo do titular de dados e a construção desse caminho têm sido cada vez mais evidenciados, a exemplo da afirmação da Apple em seu site Apple Desenvolvedores de que “nada é mais importante do que manter a confiança dos usuários”.²⁷

Tão relevante quanto afirmar o lugar de importância da confiança do cliente é construir mecanismos executáveis que condizem com esse posicionamento. Nesse sentido, vale destacar que, em 2021, a Apple lançou uma ferramenta nativa do iOS, chamada App Tracking Transparency - ATT (Transparência no Rastreamento de Aplicativos). Por meio dessa iniciativa, é preciso receber a permissão do usuário na ferramenta para só então conseguir rastreá-lo ou realizar o compartilhamento de dados dos titulares.²⁸

Ou seja, o consumidor, ao abrir o aplicativo da empresa A, recebe uma solicitação do App Tracking Transparency para autorizar ou não o rastreamento. Após a permissão ser concedida, é permitido o uso do IDFA, ou Identificador para Anunciantes (em inglês, Identifier for Advertisers), que é uma identificação única atribuída para cada dispositivo Apple. Em resumo, o identificador IDFA é utilizado para personalizar anúncios com base nas atividades do usuário. Um exemplo desse processo é a entrega de anúncios personalizados a partir da coleta de dados dos usuários, após a sua autorização.

Em um segundo cenário, o usuário abre o aplicativo da empresa B, recebe a solicitação de permissão para rastreamento do ATT, porém decide não autorizá-lo. A negativa do usuário impossibilita o acesso ao IDFA, dessa forma a empresa B enfrenta barreiras na personalização de anúncios com base nas atividades deste usuário.

Portanto, após as mudanças significativas da política de privacidade da Apple, com a decisão da marca pela implementação do ATT,

27 APPLE. **User Privacy and Data Use**. APPLE DEVELOPER, disponível em: <https://developer.apple.com/app-store/user-privacy-and-data-use/>. Acesso em: 2 jul. 2025.

28 APPLE. **User Privacy and Data Use**. APPLE DEVELOPER, disponível em: <https://developer.apple.com/app-store/user-privacy-and-data-use/>. Acesso em: 2 Jul. 2025.

trazendo maior controle dos usuários por parte dos seus dados, prevê-se impacto bilionário em receitas de vendas de anúncios da META, conforme afirma David Wehner, CFO da referida empresa, devido à mudança da coleta e rastreamento dos dados dos usuários.²⁹

A adoção dessa ferramenta trouxe dois pontos de reflexão: o controle dos consumidores quanto aos seus dados coletados e uma diminuição na visualização dos dados pessoais e não pessoais fornecidos aos anunciantes.

Conforme mencionado anteriormente na pesquisa da Adobe, 39% dos consumidores britânicos afirmam que as empresas não os escutam, pois mesmo após expressarem descontentamento no recebimento do anúncio, as empresas insistem em continuar enviando publicidade direcionada.³⁰

Por outro lado, em 2021 a C&A, empresa de vestuário, chamou a atenção de alguns consumidores ao enviar um e-mail marketing na campanha de Dia das Mães perguntando sobre sua preferência no recebimento daquele conteúdo, visto que para muitos essa data é motivo de alegria enquanto para outros é motivo de tristeza e luto, dado o contexto de muitas perdas durante a pandemia da COVID-19. Mariana Moraes, gerente sênior de marketing da C&A Brasil, à época, informou que mais de 2.000 consumidores solicitaram não receber comunicação no Dia das Mães.

Na ocasião, diversos consumidores se manifestaram nas redes sociais elogiando a empatia por parte da empresa e o acolhimento dos seus interesses em não receber esse tipo de anúncio. Sentir-se ouvido e respeitado pela marca são grandes pilares na construção da confiança do consumidor.³¹

29 NEWMAN, Daniel. **Apple, Meta, and the Ten Billion Dollar Impact of Privacy Changes**. FORBES, 10 fev. 2022. Disponível em: <https://www.forbes.com/sites/daniel-newman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/>. Acesso em: 2 Jul. 2025.

30 ADOBE BUSINESS. **7 in 10 Customers Will Buy More from Brands They Trust**. ADOBE BLOG, disponível em: <https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk>. Acesso em: 2 Jul. 2025.

31 PROPMARK. **Marcas permitem que clientes recusem comunicação sobre Dia das Mães**. PROPMARK, disponível em: <https://propmark.com.br/marcas-permitem-que-clientes-recusem-comunicacao-sobre-dia-das-maes/>. Acesso em: 2 Jul. 2025.

5. CONSIDERAÇÕES FINAIS

Analizando-se as pesquisas mencionadas ao longo desse artigo, é possível inferir que, na atual conjuntura, os consumidores externalizam uma percepção negativa da marca quando são expostos a publicidade direcionada, tendo em vista a coleta de seus dados pessoais sem sua autorização e sem transparência por parte das empresas.

As pesquisas revelaram essa percepção dentro e fora do contexto brasileiro. No entanto, vale salientar que a preocupação dos consumidores com o uso indevido dos seus dados não traz um posicionamento preventivo/protetivo, por parte dos usuários, o que levanta questionamentos para futuras pesquisas decorrentes da ausência do letramento digital e o conhecimento da importância dos dados pessoais no ambiente online.

Notou-se que as principais queixas dos consumidores quanto à insegurança no tratamento dos seus dados poderiam ser mitigadas se as empresas se propussem a aplicar eficazmente os princípios da LGPD, como os da finalidade, adequação, necessidade e transparência, que contribuem para autodeterminação informativa do titular ao mesmo tempo em que conquistam a sua confiança.

Conforme demonstrado, o ganho da confiança gera um diferencial competitivo tendo em vista que os consumidores compram mais das marcas que confiam e tendem a abandonar as que quebram a sua confiança.

Embora não seja o foco deste artigo, é pertinente esclarecer que a escolha da base legal para o tratamento de dados pessoais no marketing digital — entre as previstas na LGPD, como consentimento, legítimo interesse ou execução de contrato — depende da estrutura da operação de cada empresa. No entanto, tem-se observado uma tendência de preferência dos titulares pelo uso do consentimento, o que pode justificar uma investigação mais aprofundada em futuras pesquisas.

Desta forma, espera-se, que o trabalho aqui apresentado contribua para novas pesquisas acerca do tema em questão, que é vasto e

possui longo caminho a ser percorrido nas esferas do Direito, Marketing e Tecnologia.

REFERÊNCIAS

ADOBE BUSINESS. **7 in 10 Customers Will Buy More from Brands They Trust**. ADOBE BLOG, disponível em: <https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk>. Acesso em: 2 jul. 2025.

ADOBE BUSINESS. **How to Personalize Content**. ADOBE BLOG, disponível em: <https://business.adobe.com/blog/basics/how-to-personalize-content>. Acesso em: 2 jul. 2025.

AGUIRRE LOPEZ, E., MAHR, F. D., GREWAL, D., DE RUYTER, J. C., & WETZELS, M. G. M. (2015). **Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness**. *Journal of Retailing*, v. 91, n. 1, p. 34-49, Jan. 2015. <https://doi.org/10.1016/j.jretai.2014.09.005>

APPLE. **User Privacy and Data Use**. APPLE DEVELOPER, disponível em: <https://developer.apple.com/app-store/user-privacy-and-data-use/>. Acesso em: 2 jul. 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.p 242. Inclui bibliografia. ISBN 978-85-309-8328-4. BRASIL. [Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**]. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 2 jul. 2025.

BRASIL. Comitê Gestor da Internet no Brasil. (2022). **Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil**. São Paulo: CGI.br. <https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/>

HAWKINGS, Gary. **Will Big Data Kill All But the Biggest Retailers?** *Harvard Business Review*, September 18, 2012. Disponível em: <https://hbr.org/2012/09/will-big-data-kill-all-but-the>. Acesso em: 2 jul. 2025.

MALDONADO, Viviane Nóbrega, BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 29, 128. Bibliografia. ISBN 978-65-5065-023-0.

NEWMAN, Daniel. **Apple, Meta, and the Ten Billion Dollar Impact of Privacy Changes**. FORBES, 10 fev. 2022. Disponível em: <https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/>. Acesso em: 2 jul. 2025.

NEGRI, S. M. C. A.; RIBEIRO, L. C.; TERRA, A. M. V.; FERES, Marcos Vinício Chein. **Percepção do Consumidor Referente à Proteção de seus Dados Pessoais no Contexto de Utilização de Publicidades On-line pelo E-commerce**. 2020. Dissertação (Mestrado em Direito e Inovação) - Universidade Federal de Juiz de Fora.

PROPMARK. **Marcas permitem que clientes recusem comunicação sobre Dia das Mães**. PROPMARK, disponível em: <https://propmark.com.br/marcas-permitem-que-clientes-recusem-comunicacao-sobre-dia-das-maes/>. Acesso em: 2 jul. 2025.

ROCKCONTENT. **Personalização de Conteúdo**. ROCKCONTENT BLOG, disponível em: <https://rockcontent.com/br/blog/personalizacao-de-conteudo/>. Acesso em: 2 jul. 2025.

SURVEYMONKEY. SurveyMonkey and Axios Poll: **Privacy Deep Dive**. SURVEYMONKEY, disponível em: <https://www.surveymonkey.com/curiosity/surveymonkey-axios-poll-privacy-deep-dive/>. Acesso em: 2 jul. 2025.

TADDICKEN, Monika. **The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics and the Perceived Social Relevance on Different Forms of Self-Disclosure**. Journal of Computer-Mediated Communication, 2014. p. 249. Disponível em: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/jcc4.12052>. Acesso em 2 jul. 2025.

TORRES, Claudio. **A bíblia do marketing digital: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar**. São Paulo: Novatec, 2009. p. 61-62.

PRIVACIDADE POR PADRÃO: INTEGRANDO A LGPD AO DESENVOLVIMENTO TECNOLÓGICO

Neyanne Felipe Bezerra Araújo¹

Marcela Calazans Medeiros Silva²

INTRODUÇÃO

A revolução tecnológica contínua e a rápida expansão dos sistemas interconectados têm desencadeado uma mudança significativa na forma como os dados pessoais são tratados e protegidos. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) estabeleceu diretrizes fundamentais para garantir a privacidade e a segurança das informações pessoais dos indivíduos.

Este artigo explora os princípios orientadores da proteção de dados, unificando a essência da LGPD com os pilares do tratamento de informações pessoais em prol do desenvolvimento tecnológico. Com o rápido avanço da tecnologia e a proliferação de dispositivos conectados à internet, a privacidade dos dados pessoais tornou-se uma preocupação crucial.

Em resposta a esse desafio, os princípios de *privacy by design* (privacidade desde a concepção) e *privacy by default* (privacidade por

1 Advogada. Graduada em Direito pelo Centro Universitário UniCEUB. Pós-graduada em Direito Processual Civil pelo Instituto Brasiliense de Direito Público (IDP). Especializada em Segurança Cibernética no Centro Universitário UniCEUB e estudiosa da área de Direito Digital e LGPD, com cursos no INSPER – Instituto de Ensino e Pesquisa (SP), no Instituto Brasiliense de Direito Público (IDP) e na Next Law Academy. Membro da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/DF e do Instituto Brasileiro de Recursos e Processos nos Tribunais Superiores – IRTS.

2 Advogada. Graduada em Direito. Pós-graduada em Direito Digital e Compliance pelo Damásio Educacional. Certificada como *Data Protection Officer* e *Information Security Officer* pela EXIN. Atua como Encarregada de Proteção de Dados. Membro da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/DF.

padrão) surgiram como abordagens proativas e essenciais para garantir a proteção da privacidade desde o estágio inicial de desenvolvimento de produtos e serviços.

A implementação desses conceitos proativos não só promove o aumento da confiança dos usuários, mas também contribui para a cultura de respeito à privacidade, desde a concepção de novas tecnologias até a sua aplicação prática.

Contudo, o desafio atual reside na harmonização entre a inovação tecnológica e a responsabilidade na gestão dos dados pessoais, considerando a falta de legislação aplicável e a constante evolução das tecnologias.

1. PRINCÍPIOS NORTEADORES DA PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados (Lei 13.709/2018) estabeleceu diretrizes fundamentais para o tratamento de informações pessoais, tendo em vista garantir a privacidade e a segurança dos dados dos indivíduos como pessoas naturais (art. 1º da LGPD).³

Da leitura das normas que tratam sobre o tema, denota-se que tanto a LGPD quanto outras legislações vigentes possuem um verdadeiro “núcleo comum” de princípios que norteiam a proteção de dados, de forma que, mesmo fracionados, condensados ou adaptados, permitem a convergência das normas sobre o tema. Basan sintetiza tal ideia com os seguintes princípios:

- i) princípio da publicidade ou transparência, segundo o qual a existência de um banco de dados deve ser de conhecimento público;

3 “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.” Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Acesso em 04 dez. 2023.

ii) princípio da exatidão, exigindo que os dados armazenados sejam verídicos, encontrando fidelidade com a realidade que pretendem expressar, além da necessária e constante atualização;

iii) princípio da finalidade, pelo qual a utilização dos dados deve obedecer à finalidade conhecida pelo titular antes da coleta de seus dados, limitando a extrapolção do uso para outros fins, sob pena de ser considerada prática abusiva;

iv) princípio do livre acesso, que garante ao titular acesso ao banco de dados onde constam suas informações, além de possibilidade de controle destes dados; e

v) princípio da segurança física e lógica, segundo o qual os dados devem ser protegidos de maneira cuidadosa, evitando os riscos inerentes ao extravio, modificação ou acesso não autorizados.⁴

Dentro desse contexto, a LGPD previu princípios que são essenciais para nortear as práticas relacionadas à coleta, ao armazenamento, à utilização e ao compartilhamento dessas informações; ou seja, o tratamento de dados pessoais na concepção do art. 5º, X, da LGPD, devem se orientar pelos princípios previstos no art. 6º da referida lei, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Ainda que todos os princípios devam ser observados, verifica-se que a LGPD também aderiu à ideia do núcleo comum, em que quatro deles são percebidos como essência norteadora da lei: finalidade, adequação, necessidade e transparência.

Um dos princípios centrais é o da finalidade, pois é ele que garante que o tratamento da informação seja realizado por um motivo específico, legítimo e expresso e que seja informado ao titular, a fim de

4 MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). Comentários à lei geral de proteção de dados pessoais: lei 13.709/2018. 1. ed. Indaiatuba, SP: Foco, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 05 dez. 2023.

garantir que tenha conhecimento das razões para o tratamento e para que possa arguir seu direito em caso de tratamento posterior de forma incompatível, conforme determina o inciso I do art. 6º da LGPD.

Percebe-se que não é qualquer motivo que autoriza o tratamento de dados, uma vez que para tal a lei impõe três requisitos legais: o **propósito específico**, que é aquele indicado de forma precisa e clara para o titular, com uma relação lógica com o objetivo do tratamento, impedindo que seja realizado de forma genérica e sem contexto; o **propósito legítimo**, que pode ser entendido como a base legal do tratamento, seja ela extraída da própria lei de proteção de dados, seja de outra norma; e o **propósito expresso** e informado para garantir que o controlador exponha as razões para a realização do tratamento.⁵

Como são interligados, o princípio da finalidade apresentado atrai, por consequência, os demais. Isso porque a adequação, que deve ser analisada em conjunto com a necessidade do tratamento, refere-se à relevância dos dados coletados em relação aos propósitos estabelecidos, implicando que as informações sejam limitadas somente àquelas necessárias para atingir as finalidades específicas do tratamento, a fim de evitar a coleta excessiva de dados pessoais.⁶

Todos esses princípios objetivam, especialmente, garantir a transparência na relação entre controlador, operador e titular dos dados. Assim, exige-se que as organizações forneçam informações claras, precisas e acessíveis aos titulares sobre o tratamento de seus dados pessoais. Isso inclui a disponibilização de políticas de privacidade compreensíveis, que expliquem de forma transparente quais dados são coletados, com que finalidade, por quanto tempo serão armazenados e com quem poderão ser compartilhados.⁷

5 TAMER, Maurício. **LGPD: comentada artigo por artigo**. 1. ed. São Paulo: Rideel, 2021. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 dez. 2023.

6 MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à lei geral de proteção de dados pessoais: lei 13.709/2018**. 1. ed. Indaiatuba, SP: Foco, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 dez. 2023.

7 TAMER, Maurício. **LGPD: comentada artigo por artigo**. 1. ed. São Paulo: Rideel, 2021. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 dez. 2023.

A observância desses princípios não está relacionada apenas ao cumprimento de exigências legais, seja para tecnologias já implementadas, seja para novas tecnologias – ela contribui para o desenvolvimento de relações de confiança entre as instituições e os titulares dos dados, elevando o nível de consciência quanto à cultura de respeito à privacidade e à proteção de dados como uma configuração padrão, desde o nascimento da tecnologia.

2. ***PRIVACY BY DESIGN E PRIVACY BY DEFAULT***

Com o rápido avanço da tecnologia e a multiplicação de dispositivos conectados à internet, a privacidade dos dados pessoais tornou-se uma preocupação crucial. Em atenção a essa nova realidade, surgiram dois conceitos baseados em uma abordagem proativa e essencial por parte do desenvolvedor da nova tecnologia para garantir a privacidade dos usuários desde o estágio inicial de desenvolvimento de produtos e serviços.

Os conceitos são os de *privacy by design*, que, em português, entende-se por privacidade desde a concepção; e de *privacy by default*, que entende-se por privacidade por padrão. Tais proposições são expressamente mencionadas no artigo 25 do Regulamento Geral de Proteção de Dados Europeu (GDPR) e, de forma implícita, no art. 46, *caput* e § 2º, da LGPD:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

[...]

§ 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Denota-se o cuidado do legislador ao prever que a adoção de medidas de segurança deve ocorrer desde a concepção do produto ou serviço, ou seja, a cautela com a privacidade deve nascer junto com a ideia.

Essa noção de privacidade desde a concepção surge com a proposta de Ann Cavoukian, professora e comissária de privacidade em Ontário, Canadá, que colocou a privacidade como um componente central, com a ideia de que a garantia à privacidade do titular deve estar incorporada e assegurada durante todo o processo de criação de produto ou serviço que demande tratamento de dados pessoais.⁸

Cavoukian⁹ desenvolveu sete princípios fundamentais para o alcance dos objetivos do *privacy by design*: 1) proatividade, buscando prevenir incidentes; 2) *privacy by default*, para que seja uma configuração automática e independa do usuário; 3) incorporação da privacidade ao desenvolvimento; 4) funcionalidade total, de modo que a privacidade não seja empecilho para o bom uso; 5) segurança de ponta a ponta, presente do início ao fim; 6) transparência com o usuário; e 7) respeito à autonomia do usuário quanto ao seu poder de decisão quanto ao tratamento.

Dessa forma, o conceito de privacidade por padrão surge como consequência da privacidade desde a concepção, uma vez que, da mesma forma que a privacidade deve ser pensada durante todo o processo de desenvolvimento dos sistemas, configurações mais protetivas devem ser automaticamente aplicadas, sem a intervenção do usuário.

Isso implica que as configurações iniciais dos sistemas e serviços devem ser definidas para garantir o mais alto nível de privacidade, permitindo que os usuários façam escolhas conscientes e informadas para flexibilizar essas configurações, se desejado.

8 MARTINS, Ricardo Maffei; Martins e GUARIENTO, Daniel Bittencourt. *Privacy by design, by default e by redesign*. Migalhas, 21 maio de 2021. Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/345919/privacy-by-design-by-default-e-by-redesign>. Acesso em: 07 dez. 2023.

9 CAVOUKIAN, Ann. *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*. Portal da Privacidade. Disponível em: <https://portaldaprivacidade.com.br/wp-content/uploads/2017/11/Seven-Principles-of-Privacy-by-Design.pdf>. Acesso em: 07 dez. 2023.

Como bem destacado por Cavoukian, a privacidade deve ser observada paralelamente à funcionalidade total do produto ou serviço, para facilitar a compreensão dos usuários em relação às medidas adotadas para a segurança de seus dados pessoais.

Logo, considerando que a observância da privacidade e da proteção de dados pessoais e a adoção de boas práticas contribui para o desenvolvimento de relações de confiança entre as instituições e os titulares dos dados, esses conceitos estão intimamente ligados ao desenvolvimento tecnológico confiável e produtivo, pois aumentam a adoção e a aceitação de novas tecnologias.

3. NOVAS TECNOLOGIAS E A PROTEÇÃO DE DADOS PESSOAIS

O progresso tecnológico segue sem interrupções. O mundo clama por inovação. Inteligência artificial, *blockchain*, Internet das Coisas (IoT), metaverso, avatar e muito mais. Criam-se e recriam-se ambientes. Tecnologias são transformadas, aprimoradas e redesenhadas a todo momento. Novos dados são gerados. *Business intelligence* (BI), formação de perfil, listas, bancos de dados; informações consolidadas e armazenadas, muitas vezes, por prazo indeterminado.

Não há dúvidas de que o avanço da tecnologia impacta diretamente na forma como dados pessoais são utilizados. O grande desafio, agora, é conciliar as informações geradas pelas novas tecnologias com a proteção dos dados pessoais e resguardo à privacidade dos titulares, uma vez que o uso inadequado dos dados pode causar violações e danos irreparáveis ao titular.

O primeiro passo é capacitar a equipe que comandará o projeto, seja de desenvolvimento técnico, seja de processos; até mesmo a equipe operacional. Todos os envolvidos precisam conhecer os ditames da lei e conseguir identificar os dados pessoais que serão tratados, bem como os riscos inerentes: de privacidade, de proteção dos dados ou de segurança da informação.

O controlador deve, ainda, designar um encarregado de proteção de dados com capacitação técnica adequada para acompanhar o desenvolvimento do novo projeto e conseguir, assim, orientar sobre as melhores práticas a serem adotadas, indicando os locais em que devem constar avisos de privacidade para transparência com o titular, coleta de consentimento (quando aplicável), formulários para exercício de direitos e demais mecanismos aplicáveis ao caso.

A adoção de boas práticas de segurança da informação e da *privacy by design* são indispensáveis para o atendimento à LGPD. Contudo, outras questões também precisam ser consideradas.

O uso de tecnologias como a de reconhecimento facial pode favorecer e auxiliar na rápida autenticação e identificação de usuários, contudo, caso haja algum equívoco ou falha sistêmica no processo, pode-se incorrer em constrangimento, discriminação ou na negativa de acesso a uma pessoa devidamente legitimada. Por isso, é indispensável que haja previsão de um processo de revisão realizado por humanos.

O processamento de volume elevado de dados e a formação de perfis do usuário com base em suas experiências, pesquisas e comportamentos – realizados por meio de algoritmos de inteligência artificial, *machine learning*¹⁰ ou *big data*¹¹ – são capazes de viabilizar o direcionamento de conteúdo e contribuir para a celeridade de acesso a produtos e serviços. Em que pese as vantagens, esses mecanismos podem, também, restringir o usuário, direcionando-o a um determinado viés sem lhe permitir avaliar outras possibilidades.

Cabe mencionar, ainda, a questão dos dispositivos que coletam a localização em tempo real a fim de viabilizar o uso de serviços como mapas e previsões meteorológicas, ou identificar de forma precisa o local onde um objeto se encontra. Para além dos benefícios, a falta de controles pode culminar no rastreamento contínuo, na formação do histórico de localização e na vigilância indiscriminada.

10 Aprendizado de máquina (tradução livre).

11 Conjunto de dados (tradução livre).

Sem a pretensão de esgotar os exemplos, o avanço na geração de imagens por meio de softwares e ferramentas dotadas de inteligência artificial – que possuem a capacidade de criar imagens extremamente realistas – podem, em pouco tempo, tornar difícil o processo de distinção da realidade e ficção. Vídeos, sons e animações podem ser produzidos e manipulados de forma bastante convincente, com grande potencial de resultar em propagação de notícias e informações falsas, influenciar em resultados e macular decisões.

Um dos pontos cruciais é entender e conceituar certas tecnologias. É certo que qualquer regulamentação sobre o tema deve contar com uma equipe multidisciplinar, composta, minimamente, por representantes com conhecimentos jurídicos e técnicos. O saber técnico é indispensável para o correto entendimento e para a delimitação dos riscos e possibilidades que as novas tecnologias podem gerar.

Também é salutar que seja oportunizado ao usuário o correto entendimento dos mecanismos utilizados para o tratamento de dados. A ausência de conscientização e educação sobre os riscos à privacidade pode levar a comportamentos descuidados por parte do usuário, que se expõe a ameaças por mero desconhecimento.

Estudos recentes demonstram que, no tocante à privacidade, as empresas são desafiadas a conciliar as expectativas dos clientes, acionistas e autoridades regulatórias com a instabilidade geopolítica e o rápido avanço das tecnologias. Por isso, faz-se necessária a realização de uma completa gestão de riscos, uma vez que estes podem surgir com a implementação ou mudanças das tecnologias utilizadas. Entre os principais riscos, destacam-se:

- 1) Ausência de aderência ao princípio da minimização da coleta, resultando na coleta excessiva de dados;
- 2) Falta de controle de acesso adequado;
- 3) Vazamento de dados por ataques cibernéticos, falhas de segurança ou ação intencional de usuário;
- 4) Uso ostensivo de mecanismos de monitoramento, resultando em vigilância massiva;

5) Preconceito, discriminação ou decisões automatizadas injustas ou não aderentes à realidade do solicitante;

6) Criação de perfil do usuário de forma intrusiva, baseada em análise comportamental.

Mapear os riscos dos processos e identificar formas de mitigação, traçando planos de contingência e recuperação, caso não seja possível eliminá-los, são requisitos mínimos para qualquer controlador comprometido com a responsabilidade corporativa.

É um equívoco pensar que a Lei Geral de Proteção de Dados constitui uma barreira para o desenvolvimento de novas tecnologias. Na verdade, a lei possui como fundamentos, justamente, o desenvolvimento econômico, tecnológico e a inovação.

A criação e a aplicação de melhorias às tecnologias já existentes fazem parte do cotidiano da sociedade. Encontrar o equilíbrio entre a inovação tecnológica e a responsabilidade no tratamento dos dados pessoais é fundamental para que os benefícios possam ser colhidos.

Ao garantir o respeito à privacidade desde a fase inicial de desenvolvimento de um novo produto ou serviço, o controlador não apenas conquista a confiança do usuário, mas também obtém diferencial competitivo no mercado. Essa abordagem contribui, ainda, para o fomento da cultura de segurança cibernética, resultando em produtos e modelos de negócios mais sustentáveis.

4. (A FALTA DE) LEGISLAÇÃO APLICÁVEL

Após a promulgação da LGPD, muitos estudiosos do tema têm questionado a necessidade de tutelar outras frentes que se relacionem à proteção de dados.

A regulamentação é um instrumento essencial para assegurar que as novas tecnologias sejam seguras, adequadas e éticas. Importante, ainda, é conseguir nivelar o mercado, visando ao equilíbrio entre os interesses corporativos e individuais dos usuários. Mas os desafios são grandes.

Enquanto o processo legislativo é demorado e demanda a execução minuciosa de processos pré-estabelecidos, a tecnologia está em constante atualização, o que torna improvável a criação de uma legislação que consiga acompanhar a evolução tecnológica de forma concomitante.

Ademais, qualquer legislação sobre o tema precisa considerar os regulamentos sobre proteção de dados já existentes, as medidas mínimas de segurança da informação e a neutralidade, para assegurar o tratamento igualitário a todos os usuários e a não discriminação.

Outro ponto importante é o desafio de identificar qual legislação será aplicada ao caso, em especial, avaliando a existência de marcos regulatórios distintos – em que os titulares podem estar conectados, porém, em ambientes físicos diferentes, regulados por leis diferentes.

As divergências culturais e jurídicas entre os países também podem constituir empecilhos para a regulamentação de certas tecnologias. Além disso, a limitação do conhecimento especializado por parte dos legisladores, frequentemente concentrados apenas no viés jurídico para a criação dos marcos legais, pode resultar na desconsideração das implicações técnicas que a nova tecnologia pode suscitar.

Sobre o tema, Baptista e Keller¹², no artigo denominado “*Por que, quando e como regular as novas tecnologias?*”, esclarecem que:

Além das justificativas tradicionais para intervenção estatal, a regulação de novas tecnologias deve atuar especialmente para promover e preservar a inovação, assegurando a livre concorrência, condição para que a inovação ocorra. Nesse sentido, a regulação inicial de novas tecnologias deve se deter aos domínios da garantia da segurança do usuário e do respeito às liberdades fundamentais. Quanto ao momento de regular, verifica-se que, se a intervenção ocorrer logo que a nova tecnologia surge, pode se revelar prematura; se, por outro lado, aguardar a consolidação da inovação, pode ser tardia, especialmente diante da resistência à regulação do mercado já estabelecido (...)

12 BAPTISTA, P.; KELLER, C. I. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, [S. l.], v. 273, p. 123–163, 2016. DOI: 10.12660/rda.v273.2016.66659. Disponível em: <https://periodicos.fgv.br/rda/article/view/66659>. Acesso em: 6 dez. 2023.

Por fim, há que se considerar os riscos de fragmentação e a falta de harmonização entre os dispositivos legais. Caso o legislador opte por pormenorizar cada nova tecnologia em um regulamento específico, as empresas podem ter dificuldade de atender a todos os padrões e requisitos estabelecidos, tornando improdutivo o cenário da inovação.

5. CONSIDERAÇÕES FINAIS

A adoção dos cuidados necessários para integrar a Lei Geral de Proteção de Dados ao desenvolvimento tecnológico é um mecanismo que contribui de forma inestimável para que as empresas possam manter seus negócios sustentáveis e perenes no mercado em que atuam, uma vez que é causa direta do fortalecimento da confiança do usuário no produto ou serviço contratado.

O grande desafio das empresas é conciliar a inovação tecnológica com a responsabilidade na gestão dos dados pessoais, considerando o atual cenário de baixa maturidade legislativa em que o tema se encontra.

Contudo, a implementação dos conceitos de *privacy by design* e *privacy by default*, cuja atuação proativa assegura que mecanismos aptos a zelar pela privacidade e pela proteção dos dados dos usuários sejam adotados desde a concepção do produto ou serviço, é uma estratégia que favorece e contribui de forma substancial para que o controlador possa demonstrar o seu compromisso com a ética.

Assim, enfrentar esses desafios demanda uma abordagem cuidadosa e preventiva, pautada na adoção de medidas de segurança sólidas e no comprometimento ético com a implementação das tecnologias emergentes.

RERÊNCIAS

BAPTISTA, P.; KELLER, C. I. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. Re-

vista de Direito Administrativo, [S. l.], v. 273, p. 123–163, 2016. DOI: 10.12660/rda.v273.2016.66659. Disponível em: <https://periodicos.fgv.br/rda/article/view/66659>. Acesso em: 6 dez. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Acesso em 04 dez. 2023.

CAVOUKIAN, Ann. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Portal da Privacidade. Disponível em: <https://portaldaprivacidade.com.br/wp-content/uploads/2017/11/Seven-Principles-of-Privacy-by-Design.pdf>. Acesso em: 07 dez. 2023.

IAPP, KPMG. Privacy Risk Study 2023, Executive Summary. Disponível em: <https://iapp.org/resources/article/privacy-risk-study-summary/>. Acesso em: 06 dez. 2023.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à lei geral de proteção de dados pessoais: lei 13.709/2018**. 1. ed. Indaiatuba, SP: Foco, 2022. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 05 dez. 2023.

MARTINS, Ricardo Maffei Martins e GUARIENTO, Daniel Bittencourt. Privacy by design, by default e by redesign. **Migalhas**, 21 maio 2021. Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/345919/privacy-by-design-by-default-e-by-redesign>. Acesso em: 07 dez. 2023.

TAMER, Maurício. **LGPD: comentada artigo por artigo**. 1. ed. São Paulo: Rideel, 2021. E-book. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 07 dez. 2023.

SEGURANÇA DA INFORMAÇÃO E SEU PAPEL ALIADO À LGPD: UMA PERSPECTIVA JURÍDICA

Paula de Paiva Santos¹

Luana Bueno Palma²

INTRODUÇÃO

A sociedade contemporânea está imersa em uma revolução digital que dissolve as fronteiras entre telecomunicações, mídia e informática, caracterizando-a como a sociedade da informação. Essa era histórica testemunha o surgimento de redes complexas dedicadas à produção e utilização da informação, não apenas para sua distribuição no mercado, mas também para a geração de conhecimento e riqueza. Nesse contexto, a falta de uma cultura de proteção de dados pessoais impacta as práticas corporativas, incluindo gestão inadequada de bases de clientes e falhas de segurança.

A conformidade com a Lei Geral de Proteção aos Dados (LGPD) torna-se crucial, exigindo investimento em práticas de segurança da informação e treinamento contínuo para evitar violações decorrentes de condutas inadequadas. A mudança cultural – ainda mais desafiadora que a implementação de tecnologias – é essencial para garantir a segurança da informação e cumprir as normas legais; e é importante não apenas no ambiente corporativo, mas na sociedade como um todo. Empresas que interpretam adequadamente dados digitais des-

1 Mestre em Direito pela Universidade de Brasília (UnB). Pós-graduada em Direito do Consumidor – LFG. Pós-graduada em Direito Civil e Processo Civil – ATAME. Advogada do Banco Bradesco S.A. Docente na Faculdade CCI. Integrante do Grupo de Pesquisa GERN – UnB.

2 Advogada. Pós-graduada em Segurança Cibernética pelo Centro de Ensino Unificado de Brasília (UnICEUB). Pós-graduada em Direito Tributário na Universidade Candido Mendes. Analista de defesa Cibernética no Centro Cooperativo Sicoob.

tacam-se, agregando valor de mercado, tornando a implementação da segurança da informação não apenas importante, mas necessária nos negócios.

A segurança da informação é fundamental para a proteção de dados, juntamente com uma gestão baseada em princípios como confidencialidade e integridade; respaldando-se legalmente para a inclusão da LGPD como fundamento jurídico essencial na implantação da proteção de dados e visando à garantia da continuidade do negócio. No cenário atual, com o aumento dos crimes cibernéticos, destaca-se, mais uma vez, a importância da segurança digital, considerando-se a interligação física e digital das informações e a compreensão dos riscos. A LGPD salienta a comunicação dos riscos no tratamento de dados pessoais, sendo vital na redução de falhas e atos preventivos.

Na era de transformações sociais contínuas, ao posicionar a informação como elemento estruturante, como moeda de desenvolvimento econômico, cultural, social e político, faz-se necessária a substituição de paradigmas anteriores. Essa valorização da informação, embora amplie o acesso ao conhecimento, demanda mais segurança, especialmente em se tratando de dados pessoais. A inserção da LGPD no Brasil é, portanto, um marco regulatório, na medida em que se busca adotar mais medidas de segurança frente às novas tecnologias. A legislação emerge como elemento basilar na preservação da privacidade e proteção dos dados, consolidando-se como instrumento vital para garantir a integridade e confidencialidade das informações, promovendo uma sociedade mais consciente e protegida.

1. A INTEGRAÇÃO ESTRATÉGICA ENTRE SEGURANÇA DA INFORMAÇÃO E LGPD - ABORDAGEM JURÍDICA

A sociedade contemporânea experimenta uma autêntica revolução digital, caracterizada pela dissolução das fronteiras entre telecomunicações, meios de comunicação de massa e informática. Essa era histórica recebe a denominação de sociedade da informação, e trouxe

consigo o surgimento de intrincadas redes profissionais e tecnológicas dedicadas à produção e utilização da informação. Tais redes abrangem não apenas a distribuição da informação pelo mercado, mas também as modalidades de sua aplicação para a geração de conhecimento e riqueza.³ Tal produção social de riqueza está ligada à utilização de recursos inovadores, proporcionados pelos avanços tecnológicos, intrinsecamente associados à produção simultânea de riscos correspondentes.⁴

Nesse cenário, no Brasil, a falta de uma cultura de proteção de dados pessoais impacta as práticas corporativas, causando gestão inadequada de bases de clientes, uso indevido de dados e falhas de segurança, por exemplo. Por essa razão, as organizações precisam investir na revisão de suas práticas de segurança da informação e em treinamento contínuo para os colaboradores, pois a maioria das violações ocorre devido a condutas inadequadas. Além disso, a mudança cultural⁵ representa um desafio significativo, pois acaba sendo mais desafiadora do que própria a implementação de tecnologias e cumprimento das medidas de segurança da informação, em conformidade com a Lei nº 13.709 de 14 de agosto de 2018 – a Lei Geral de Proteção aos Dados⁶.

Diante disso, a relevância da segurança da informação estende-se não apenas ao ambiente corporativo, mas também à sociedade em geral, em cumprimento aos ditames legais da LGPD. As empresas, que possuem uma quantidade significativa de informações, destacam-se na interpretação adequada desses dados digitais como valor agregado de mercado às companhias.⁷ Assim, diante dessas noções, conclui-se que

3 BARRETO JUNIOR, Irineu Francisco. **Atualidade do conceito de sociedade da informação para a pesquisa jurídica**. In: O direito na sociedade da informação. Coord. Liliana Minardi Paesani. São Paulo: Atlas, 2007, p. 61.

4 HASSEMER, W. **Perspectivas de uma moderna política criminal**. Revista Brasileira de Ciências Criminais, São Paulo, v. 2, n. 5, p. 55-69.

5 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: 13 dez. 2023.

6 BRASIL. Lei n. 13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em: 10 dez. 2023.

7 SILVA, T.; TOMAÉL, M. I. **A gestão da informação nas organizações**. Revista Informação & Informação, 12 (2), 375–397. p. 375.

tornou-se não somente importante, como necessária a implementação da segurança da informação nos negócios.

2.1. Implementação da segurança da informação para cumprimento da LGPD – Uma perspectiva jurídica

A segurança da informação configura-se como o conjunto normativo e de práticas que engloba diretrizes, normas, procedimentos, políticas e demais estratégias adotadas com o propósito de salvaguardar o recurso à informação. A ISO/IEC 17799:2005, por sua vez, conceitua a segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Segundo Campos⁸, a gestão da segurança da informação se baseia na aplicação de três princípios:

- a) Confidencialidade: significa garantir o segredo das informações, liberando acesso somente às pessoas autorizadas;
- b) Integridade: significa garantir que a informação não foi alterada indevidamente, ou seja, é confiável;
- c) Disponibilidade: significa garantir a disponibilidade da informação, sempre que necessário

Essa abordagem tem por objetivo assegurar a continuidade das operações comerciais da organização e o cumprimento de sua missão institucional, sempre em conformidade com os preceitos legais e regulatórios aplicáveis à proteção da informação. Nesse contexto, a cláusula geral da boa-fé objetiva impõe deveres anexos às relações jurídicas, como os deveres de informação e de cooperação. Assim, o detentor dos dados ocupa simultaneamente a posição de titular de direitos e de obrigações, inclusive em relação a terceiros que, embora não integrem diretamente a relação obrigacional, possam ser impactados por ela.

8 CAMPOS, André L. N. **Sistema de Segurança da Informação**: controlando os riscos. Florianópolis: Visual Books, 2006.

Ainda, ercebe-se o viés de natureza também legal. No ordenamento jurídico brasileiro, a Lei Geral de Proteção de Dados (LGPD) estabelece princípios fundamentais a serem observados, dentre os quais se destacam os princípios da transparência e da segurança (art. 6º). A norma dispõe, ainda, que o tratamento de dados pessoais deve ocorrer com a garantia de segurança ao titular (art. 6º, inciso VII), sendo considerado irregular caso tal proteção não seja devidamente assegurada, ensejando responsabilização pelos danos decorrentes, nos termos dos arts. 44 e 50 da referida lei.

De forma convergente, o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR) determina que as informações fornecidas aos titulares devem ser concisas, transparentes, inteligíveis, de fácil acesso e redigidas em linguagem clara e simples, devendo permanecer permanentemente disponíveis sempre que solicitadas. Nesse cenário de alta acessibilidade e fluidez na troca de informações, surgem riscos significativos, uma vez que agentes mal-intencionados podem se aproveitar dessas facilidades para causar danos a pessoas físicas e jurídicas.

2.2. Identificação de riscos na execução da segurança da informação

Os crimes cibernéticos e as ameaças⁹ vêm crescendo, praticamente, na mesma proporção que as novas tecnologias, apresentadas nos últimos anos. Acompanhando esse crescimento, está o setor que possibilita o fortalecimento dessa segurança no mundo digital.¹⁰ É de suma importância abordar a segurança de computadores

9 Ameaça é um evento indesejável que pode danificar um ativo, causando impacto nos resultados do negócio. PELTIER, Thomas R. **Information security risk analysis**. 3.ed. Auerbach Publication, v. 1, 2010. p. 331.

10 DOS SANTOS, Eduardo Esteves; SOARES, Tamires; KUROSAKI, Mariana M.; GIRALDO, Marcus V. L. **Riscos, ameaças e vulnerabilidades**: O impacto da segurança da informação nas organizações. Disponível em: 20182S_SANTOSEduardoEstevesdos_OD0529.pdf (cps.sp.gov.br) Acesso em: 12 dez. 2023. p.3-4.

estritamente dentro do contexto digital, onde os acessos aos sistemas ocorrem exclusivamente por meio de redes ou interfaces digitais claramente definidas, sem interação direta ou o uso de ferramentas físicas. No entanto, é imperativo reconhecer que, em última análise, a informação digital encontra-se fisicamente armazenada em determinado local, seja em elétrons, em meios magnéticos ou dispositivos ópticos. O acesso a essa informação demanda a utilização de interfaces que conectam os domínios físico e digital. Consequentemente, a salvaguarda da informação digital deve incorporar métodos destinados a assegurar a integridade física dessa interface.¹¹

Segundo Oliveira¹², o risco consiste na possibilidade de uma ameaça explorar as vulnerabilidades de um ativo, resultando em perdas ou danos. De acordo com o Sistema de Gestão da Segurança da Informação (ISMS - Information Security Management System)¹³, publicado em 2005, a ISO/EIC 27001, que visa reduzir a probabilidade de algum tipo de incidente relacionada com a segurança da informação, conta com três pilares essenciais: a **integridade**, que diz respeito à autenticidade, totalidade e validade da informação; a **disponibilidade**, que se refere à prontidão da informação quando necessária no presente

11 GOODRICH, Michael T; TAMASSIA, Roberto. **Introdução à segurança de computadores**. Porto Alegre. Bookman, 2013. p. 54.

12 OLIVEIRA, W. J. **Segurança da informação: técnicas e soluções**. Florianópolis: Visual Books.

13 A saber ainda existem outros padrões correlacionados:

ISO 27000 - Vocabulário de Gestão da Segurança da Informação (sem data de publicação);

ISO 27001 - Sistema de Gestão da Segurança da Informação - única norma da série 27000 com requisitos de certificação e passível de certificação acreditada.

ISO 27002 - Tecnologia da informação - Técnicas de segurança - Guia de Boas práticas para controles de segurança da informação - Sem certificação acreditada

ISO 27003 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Orientação

ISO 27004 - Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Monitorização, medição, análise e avaliação.

ISO 27005 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos na segurança da informação

ISO 27006 - Tecnologia da informação - Técnicas de segurança - Requisitos para os organismos que fornecem auditoria e certificação de sistemas de gestão de segurança da informação.

e no futuro para os processos de negócios; e a **confidencialidade**, que está associada à proteção de informações sensíveis para prevenir divulgações não autorizadas.¹⁴

Peltier¹⁵ menciona a elaboração de listas de verificação, a análise do histórico de eventos e, por último, a realização de uma sessão de brainstorming com os agentes-chave dos processos organizacionais para identificar as ameaças relacionadas aos ativos em cada etapa dos processos principais da organização. A identificação prévia e analítica da vulnerabilidade do risco, da análise do risco, da identificação do risco, do tratamento do risco e da aceitação do risco possibilitam um impacto menor das ameaças potenciais.¹⁶ Vale mencionar que a própria LGPD dispõe, no art. 44, que dentro do tratamento de dados pessoais, deve-se esperar “os riscos que razoavelmente dele se esperam”, ao passo que, assim que houver ciência da ocorrência do incidente de segurança, o controlador deverá comunicar à autoridade nacional e ao

14 Associação Brasileira de Normas Técnicas. (2013). **Nbriso/iec 27001: gestão de segurança da informação**. Rio de Janeiro: ABNT.

15 PELTIER, Thomas R. **Information security risk analysis**. 3.ed. Auerbach Publication, 2010. v. 1. p. 331.

16 “**Vulnerabilidade** é uma falha ou fraqueza de um bem, ativo ou processo, que, caso seja explorada por uma ameaça, irá causar algum impacto na organização, podendo ser considerada como a suscetibilidade do sistema ou ativo em relação à determinada ameaça.

Análise de Risco: subdividida em Identificação de Riscos, Estimativa de Riscos e Avaliação de Riscos.

Identificação de Risco: após a identificação dos ativos que compõe os processos organizacionais, é feita identificação de ameaças e vulnerabilidades relacionadas a estes ativos. Com as ameaças e vulnerabilidades identificadas, o próximo passo é a probabilidade de ocorrência de cada ameaça x vulnerabilidade, na qual podem ser utilizados dados de incidentes anteriores. Feito isto, a próxima etapa é a análise de impacto, na qual é identificada e classificada, quais as consequências da exploração de determinada vulnerabilidade para a organização.

Tratamento do Risco: Com a definição destes dois últimos itens, é possível elaborar a matriz de Risco, que serve para identificar a criticidade de um risco, levando em consideração o impacto e a probabilidade de ocorrência do risco, conforme Figura 2, que é crucial para a criação e definição dos itens de controle, que visam evitar, tratar ou mitigar os riscos identificados, na forma de políticas de segurança.

Aceitação do Risco: Para os itens que não serão tratados por meio de Políticas de Segurança, é necessário fazer o registro de aceitação do risco, bem como a responsabilidade e justificativa da decisão.”

DOS SANTOS, Eduardo Esteves; SOARES, Tamires; KUROSAKI, Mariana M.; GIRALDO, Marcus V. L. **Riscos, ameaças e vulnerabilidades: O impacto da segurança da informação nas organizações**. Disponível em: 20182S_SANTOSEduardoEstevesdos_OD0529.pdf (cps.sp.gov.br) Acesso em: 12 dez. de 2023. p.5-6.

titular de dados “os riscos relacionados ao incidente”, nos termos do art. 48, inciso IV.

Sendo assim, uma boa política de segurança da informação, conforme disposição do art. 50, § 2º, inciso I, letra ‘d’, da LGPD¹⁷, que objetiva mitigar os riscos, é dividida em três camadas procedimentais: a estratégica – que define as diretrizes e planos; a tática – que define a padronização de normas; e a operacional – que define os procedimentos dos processos.¹⁸ Em um estudo¹⁹ realizado, concluiu-se que:

“Os resultados aqui identificados comprovam que uma maior consciência individual sobre a importância da segurança da informação, essa que surge a partir de uma cultura forte de segurança da informação, pode resultar na diminuição das falhas de segurança”.

17 Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

(...)

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo

(...)

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

BRASIL. Lei n. 13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em: 10 dez. 2023

18 DONDA, Daniel. **Guia Prático de Implementação da LGPD**: tudo o que a sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020. p. 15.

19 SILVEIRA, Jonas R. LUNARDI, Guilherme, L. CERQUEIRA, Lucas S. **Relação entre cultura e Segurança da Informação: como evitar falhas decorrentes do ‘jeitinho brasileiro’?** Disponível em: scielo.br/j/read/a/mXzJBPHSXLkxTFPBVGmHkqs/?lang=pt&format=pdf Acesso em: 10 dez. 2023

2. CASOS JURÍDICOS DE ORGANIZAÇÕES QUE UTILIZAM ESTRATÉGIAS DE SEGURANÇA DA INFORMAÇÃO PARA CONFORMIDADE COM A LGPD

Como discutido no capítulo anterior, ao longo do tempo, a sociedade experimentou transformações sociais e digitais que impactaram diretamente a vida em comunidade. Desse contexto emerge a sociedade da informação, caracterizada pela valorização da informação, reconhecida como um elemento principal de inovação tecnológica, transformação social, cultural, econômica e política.²⁰

3.1. Melhores práticas adotadas de acordo com a gestão de tecnologia da informação na visão da LGPD

A sociedade atual está encravada por uma forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que outrora estruturavam as sociedades agrícola, industrial e rural. Por isso, a informação tem um papel central e adjetivante da sociedade: sociedade da informação, sendo a informação o novo elemento estruturante que reorganiza a sociedade.²¹

A sociedade da informação é caracterizada pela relevância da informação, tendo em vista o alto valor dos dados para o mercado. Percebe-se que essa valorização permitiu acesso ao conhecimento mais amplo e diversificado, melhoria da comunicação entre as pessoas e inovação econômica, social, política e cultural. A valorização da informação trouxe a necessidade, também, de aplicar mais segurança e proteção dos dados, em especial, aqueles relacionados às pessoas. A esse respeito, Oliveira et al. ressaltam que:

20 De acordo com Webster a sociedade da informação é representada por uma sociedade na qual a informação é utilizada intensamente como elemento da vida econômica, social, cultural e política, dependendo de um suporte tecnológico para se propagar, demonstrando que esse processo se tornou um fenômeno social, instaurado dentro da sociedade. BURCH, Sally. Ambrosi, A.; Peugeot, V.; Pimenta, D. **Sociedade da informação/ sociedade do conhecimento**. Desafios das palavras. Ed. VECAM, 2005. p.01.

21 BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3 ed. Rio de Janeiro: Forense, 2021. p. 04-05.

“A preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela “Quarta Revolução Industrial”, cujo tom é dado pelo fenômeno da informatização da sociedade”, iniciado na década de 1970. Seus reflexos impactam diretamente tanto a atividade econômico-empresarial, quanto a atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações.”²²

A informação é elemento essencial para todos os processos da organização. A definição de segurança da informação está diretamente ligada à proteção de dados de propriedade das organizações e/ou sob sua guarda, podendo ser de pessoa física e jurídica, que requerem esforços para garantir a mitigação de riscos e a continuidade das operações.²³ O ato de aplicar a segurança da informação a qualquer tipo de dado implica utilizar processos de governança empresarial, que envolvam recursos humanos, de infraestrutura e lógicos (computacionais).²⁴ Neste sentido, a LGPD, que representa um marco regulatório sobre o tratamento de dados pessoais no Brasil, tem como um dos seus pilares a proteção desses dados, envolvendo conceitos que remetem a atividades relacionadas à segurança da informação, à governança de dados e à gestão de riscos.

A lei dispõe, no capítulo VII, que as organizações (públicas ou privadas), no papel de agentes de tratamento de dados, devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. São obrigadas, ainda, a garantir a segurança da informação dos dados pessoais, mesmo após o término do tratamento, e os sistemas utilizados para o tratamento de dados pessoais

22 NAKAMURA, Emilio; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. **Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais**. In: Anais do V Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança. SBC, 2019. p. 11-16.

23 CAMPOS, André L. N. **Sistema de Segurança da Informação: controlando os riscos**. Florianópolis: Visual Books, 2006.

24 CAMPOS, A. **Sistema de Segurança da informação**. 2 ed. Ed. Florianópolis: Visual Books, 2007.

devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na lei.

Um importante ponto é o gerenciamento de riscos relacionados à segurança da informação, um processo que consiste em identificar, quantificar e gerenciar tais ameaças dentro da organização – esse procedimento visa a obter um equilíbrio eficiente entre a concretização de oportunidades de ganhos e a minimização de vulnerabilidades e perdas. Portanto, independentemente do tamanho da organização ou do seu setor de atuação, assegurar a proteção e a segurança das informações representa um grande desafio. Nesse sentido, é importante a implementação, a manutenção e o aprimoramento contínuo de um sistema de gestão de segurança da informação²⁵. É imperativo proteger os dados pessoais sob responsabilidade da organização, considerando seus ativos, ameaças, vulnerabilidade e salvaguardas existentes.

A norma ISO/IEC 29151:2020 fornece orientação às organizações sobre como implementar controles de segurança eficazes para proteger dados pessoais.²⁶ Os controles devem ser baseados em requisitos legais, normas de segurança e avaliações de riscos. Eles devem ser adequados aos diferentes níveis da organização e devem garantir a integridade, a confidencialidade e a disponibilidade dos dados. O objetivo é protegê-los contra riscos potenciais, como acesso não autorizado, destruição ou perda durante todo o tratamento dos dados.

Importante mencionar que as medidas adotadas pelas organizações devem fomentar um ambiente seguro, reduzindo os riscos e garantindo a segurança e a proteção do fluxo informacional da organização. Alguns controles de tratamento de dados e relacionados à segurança da informação incluem:

25 ISO 27001 - Sistema de Gestão da Segurança da Informação - única norma da série 27000 com requisitos de certificação e passível de certificação acreditada.

26 ISO 29151 - Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de dados pessoais.

- a) Autenticação e autorização: o acesso aos dados pessoais deve ser concedido apenas a usuários autenticados e apenas aos dados necessários para execução das atividades;
- b) Criptografia: os dados pessoais armazenados ou transmitidos devem ser criptografados, visando à proteção contra acesso não autorizado;
- c) Backup e recuperação: realização de backups periódicos dos dados pessoais para proteger contra perda ou destruição. Importante também ter um plano de recuperação para restaurar os dados pessoais em caso de incidente de segurança;
- d) Monitoramento e detecção de ameaças: os sistemas e redes devem ser continuamente monitorados, a fim detectar possíveis ameaças à segurança dos dados pessoais;
- e) Resposta a incidentes: criação de um plano de resposta para abordar incidentes de segurança que envolvam dados pessoais;
- f) Políticas de retenção e descarte de dados: criação de políticas com definições claras sobre o período de retenção e descarte dos dados quando não forem mais necessários;
- g) Treinamento e conscientização: os colaboradores devem ter treinamentos regulares sobre práticas adequadas e seguras no tratamento dos dados;
- h) Mapeamento de dados: mapeamento para identificar as informações que são coletadas, processadas e armazenadas;
- i) Avaliação de impacto à proteção de dados (DPIA): sempre que ocorrer o tratamento de dados pessoais de alto risco, essa ação contribui para minimizar riscos à privacidade.²⁷

A gestão da segurança da informação é um processo abrangente, que envolve o estabelecimento de políticas, a aplicação de controles, a implementação de governança e a seleção de tecnologias. O objetivo

27 Segurança da informação para agentes de tratamento de pequeno porte. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps_defeso_eleitoral.pdf. Acesso em: 10 nov. 2023.

da gestão é salvaguardar a confidencialidade, a integridade e a disponibilidade dos dados e informações. Em última análise, é possível afirmar que a gestão da informação desempenha um papel fundamental na conformidade com a LGPD, isso porque uma gestão eficiente da informação é essencial para garantir o cumprimento dos requisitos normativos estabelecidos por essa legislação.

3.2. Considerações sobre a regulamentação da proteção de dados e segurança jurídica no tratamento de dados

As organizações podem e devem decidir pelo grau de segurança jurídica de suas atividades – destacando que as empresas possuem um bem muito valioso, a informação, um ativo intangível e que não pode ser negligenciado.²⁸ Considerando o valor da informação, a LGPD destaca, em seu artigo 46,²⁹ que organizações que realizam o tratamento de dados pessoais têm o dever de adotar medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais.

28 SLEIMAN, C. M. **Quanto Vale a Informação da sua Empresa? Ela está Devidamente Protegida?** Revista Eletrônica Direito & TI, v. 1, n. 1, 2015. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/view/20>. Acesso em: 11 dez. 2023. p.4.

29 Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

BRASIL. Lei n. 13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)** https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 11 dez. 2023.

Pinheiro³⁰ comenta que, cada vez mais, o trabalho de desenvolvimento de segurança da informação exige um preparo adequado do ponto de vista de blindagem legal, de modo a evitar riscos no uso das próprias medidas de proteção da empresa. É preciso aplicar mais segurança jurídica ao processo, tendo em vista que, com aumento do uso da mobilidade, o cenário atual é complexo – seja pelo acesso remoto de equipes, seja pelo crescimento das estações de trabalho do tipo notebook e smartphones, associados a um perfil de “colaborador 2.0”, que conhece mais de tecnologia, que testa os limites e os controles estabelecidos pela empresa.

A manutenção da segurança jurídica nos processos que envolvem tratamento de dados é, também, um dos principais objetivos da Lei Geral de Proteção de Dados. A lei traz um conjunto de regras e princípios a serem seguidos pelos agentes de tratamento de dados pessoais. A manutenção da segurança jurídica é importante para que as empresas e os indivíduos possam confiar no sistema de proteção de dados vigente no Brasil. O estabelecimento de regras claras e objetivas possibilita a compreensão dos direitos e obrigações, ajuda a prevenir conflitos e a garantir que as decisões sejam baseadas em parâmetros específicos.

Martins e Faleiros Jr.³¹ destacam a intenção positiva do legislador brasileiro quanto ao estabelecimento de um marco regulatório que complementa o conjunto normativo e reforça o contexto de proteção a direitos fundamentais que, por outro lado, não pode nisto se esgotar. Se a privacidade é, nesta nova sociedade da informação, reinterpretada em razão de seu principal corolário, o direito fundamental à proteção de dados pessoais, deve-se primar pelo atingimento do escopo essencial da autodeterminação e das funções do consentimento para a exata compre-

30 PINHEIRO, Patrícia Peck. **Segurança Jurídica e Segurança da Informação**. Disponível em: <https://www.migalhas.com.br/depeso/80698/seguranca-juridica-e-seguranca-da-informacao>. Acesso em: 10 dez. 2023

31 Martins, Guilherme M.; Faleiros Júnior, José Luiz de Moura. **Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais**. Editora: Revista do Ministério Público do Estado do Rio de Janeiro nº 78. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/2026467/Guilherme_Magalh%C3%A3es_Martins_%26_Jos%C3%A9_Luiz_de_Moura_Faleiros_J%C3%BAnior.pdf. Acesso em: 12 dez. 2023.

ensão da extensão da proteção conferida aos dados pessoais, que passa pela segurança da informação e pela governança.

É necessário considerar, também, a atuação da Agência Nacional de Proteção de Dados Pessoais (ANPD). Este órgão regulador reforça a segurança jurídica da LGPD, sendo responsável por fiscalizar o cumprimento da lei, investigar e punir infrações, além de emitir orientações e recomendações sobre a aplicação da LGPD.

Dessa forma, torna-se evidente que a LGPD representa um marco crucial na preservação da privacidade, da segurança e da proteção dos dados pessoais. A legislação desempenha papel fundamental ao estabelecer diretrizes para o tratamento de informações pessoais, contribuindo significativamente para a segurança jurídica. Essa regulação se revela essencial para fomentar o desenvolvimento econômico, político e social do país, ao criar um ambiente em que o tratamento de dados ocorre de maneira ética, transparente e responsável. A LGPD, portanto, consolida-se como um instrumento vital para garantir a integridade e a confidencialidade das informações pessoais, promovendo uma sociedade mais consciente e protegida.

CONSIDERAÇÕES FINAIS

A sociedade contemporânea passa por um processo de revolução digital que modela a sociedade da informação, com supervalorização da informação, que passa a ocupar o papel de elemento estruturante da sociedade.³² O reconhecimento do valor da informação trouxe consigo a imperativa necessidade de reforçar a segurança e a proteção dos dados. Nesse contexto, a LGPD surge como resposta a essa transformação, exigindo a proteção dos dados e tendo em vista que a informação, agora, é mais acessível, diversificada e valiosa, carecendo de segurança e proteção, especialmente quando o tratamento e a manipulação envolvem dados pessoais.

No entanto, a cultura de proteção de dados ainda é enfraquecida no Brasil. Por isso, é necessário fomentá-la nos ambientes corpora-

32 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

tivos. É preciso investir em um processo de acultramento que alcance toda coletividade e, principalmente, as organizações públicas e privadas de alta gestão – que, uma vez sensibilizadas sobre a importância do tema, possam fomentar programas de conscientização e treinamento dos seus colaboradores, diante do seu papel sobre a gestão de dados.

Essa integração entre o mundo físico e digital aumenta os riscos de crimes cibernéticos, portanto, é importante que as organizações adotem medidas efetivas para garantir a segurança dos dados, principalmente de terceiros. Assim, investir em um processo de gestão da segurança da informação com a implementação de controles e tecnologias, a fim de garantir a confidencialidade, a integridade e a disponibilidade dos dados torna-se essencial – não só para a conformidade com a LGPD, mas também a fim de manter a saúde financeira dos negócios.

A LGPD destaca a importância da segurança jurídica, elemento fundamental para organizações que tratam dados pessoais. A atuação da ANPD reforça essa segurança quando fiscaliza a atuação das organizações que tratam dados e exige delas o fiel cumprimento da lei. Tudo isso contribui para a criação de um ambiente regulatório transparente e confiável. Em última análise, a LGPD representa um marco crucial na proteção dos direitos fundamentais de liberdade, de privacidade e da livre formação da personalidade de cada indivíduo e consolida-se como um instrumento vital para garantir uma sociedade mais consciente e protegida diante dos desafios dessa nova sociedade – a da informação.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. (2013). **Nbriso/iec 27001**: gestão de segurança da informação. Rio de Janeiro: ABNT.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. (2020). **Nbriso/iec 29151**: tecnologia da informação – técnica de segurança – código de práticas para proteção de dados pessoais. Rio de Janeiro: ABNT.

BARRETO JUNIOR, Irineu F. Atualidade do conceito de sociedade da
352

informação para a pesquisa jurídica. Coord. Liliana Minardi Paesani. In: **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

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

BRASIL. Lei n. 12.965 de 23 de abril de 2013. **Marco Civil da Internet**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm Acesso em: 10 dez. 2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em: 10 dez. 2023.

BURCH, Sally. Ambrosi, A.; Peugeot, V.; Pimenta, D. Desafios das palavras. **Sociedade da informação/sociedade do conhecimento**. Ed. VECAM, 2005.

CAMPOS, André L. N. **Sistema de Segurança da Informação: controlando os riscos**. Florianópolis: Visual Books, 2006.

CORREA, Leonardo. **É importante não perder o foco da segurança jurídica no âmbito da LGPD**. 2019. Disponível em: <https://www.conjur.com.br/2019-mar-03/leonardo-correa-seguranca-juridica-ambito-lgpd/>. Acesso em 11 dez. 2023.

DONDA, Daniel. **Guia Prático de Implementação da LGPD: tudo o que a sua empresa precisa saber para estar em conformidade**. São Paulo: Labrador, 2020.

DOS SANTOS, Eduardo Esteves; SOARES, Tamires; KUROSAKI, Mariana M.; GIRALDO, Marcus V. L. **Riscos, ameaças e vulnerabilidades: O impacto da segurança da informação nas organizações**. Disponível em: 20182S_SANTOSEduardoEstevesdos_OD0529.pdf (cps.sp.gov.br) Acesso em: 12 dez. de 2023.

FONTES, E. **Segurança da informação: o usuário faz a diferença**. São Paulo. Saraiva, 2006.

FRANCOSKI, Denise; TASSO, Fernando. A Lgpd e os Novos Paradigmas da Tecnologia da Informação no Poder Judiciário In: FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Da-**

dos Pessoais: Lgpd: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. São Paulo: Editora Revista dos Tribunais. 2021. Disponível em: <https://www.jusbrasil.com.br/doutrina/a-lei-geral-de-protecao-de-dados-pessoais-lgpd-aspectos-praticos-e-teoricos-relevantes-no-setor-publico-e-privado/1279975732>. Acesso em: 12 dez. de 2023.

GOODRICH, Michael T; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Porto Alegre. Bookman, 2013.

GUALDA, Diego de L. **Desafio Cultural da Proteção de Dados.** Disponível em: <https://www.aarb.org.br/desafio-cultural-da-protecao-de-dados> Acesso em: 03 dez. 2023.

HASSEMER, W. **Perspectivas de uma moderna política criminal.** Revista Brasileira de Ciências Criminais, São Paulo, v. 2, n. 5, p. 55-69.

MARTINS, Guilherme M.; FALEIROS JÚNIOR, José L. de M. **Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais.** Editora: Revista do Ministério Público do Estado do Rio de Janeiro nº 78. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/2026467/Guilherme_Magalh%C3%A3es_Martins_%26_Jos%C3%A9_Luiz_de_Moura_Faleiros_J%C3%BAnior.pdf. Acesso em: 12 dez. de 2023.

NASSIF, Mônica E.; RESENDE, Walisson da C. **Gestão da informação e do conhecimento e suas relações com segurança da informação, tecnologias da informação e compartilhamento.** Ciência da Informação, v. 45, n. 3, 2016.

NEVES, Denise Lemes Fernandes. **A segurança da informação de encontro às conformidades da LGPD.** Revista Processando o Saber, v. 13, 2021.

OLIVEIRA, W. J. **Segurança da informação: técnicas e soluções.** Florianópolis, SC: Visual Books, 2001.

PELTIER, Thomas R. **Information security risk analysis.** 3.ed. Auerbach Publication, v. 1, 2010.

PINHEIRO, Patrícia P. **Segurança Jurídica e Segurança da Informação.** Disponível em: <https://www.migalhas.com.br/depeso/80698/seguranca-juridica-e-seguranca-da-informacao>. Acesso em: 10 de dez. 2023

Records management and security. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-management-and-security/>. Acesso em: 12 de dez. de 2023.

Regulamento Geral sobre a proteção de Dados. Artigo 12 UE Regulamento Geral sobre a Proteção de Dados. Privacy/Privazy according to plan. (privacy-regulation.eu) Acesso em: 06 de dez. de 2023.

Segurança da informação para agentes de tratamento de pequeno porte. Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em: 10 de nov. 2023.

SILVA, T.; Tomaél, M. I. **A gestão da informação nas organizações.** Revista Informação & Informação, 12 (2), 375–397.

SILVEIRA, Jonas; LUNARDI, Guilherme R.; CERQUEIRA, Lucas S. L. **Relação entre cultura e Segurança da Informação:** como evitar falhas decorrentes do ‘jeitinho brasileiro’? Disponível em: scielo.br/j/read/a/mXzJBPHSXLkxTFPBVGMhkqs/?lang=pt&format=pdf Acesso em: 11 dez. 2023.

SLEIMAN, C. M. **Quanto Vale a Informação da sua Empresa? Ela está Devidamente Protegida?** Revista Eletrônica Direito & TI, [S. l.], v. 1, n. 1, p. 4, 2015. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/view/20>. Acesso em: 11 dez. 2023.

TEPEDINO, Gustavo; SCHREIBER, Anderson. **Código civil comentado:** direito das obrigações – artigos 233 a 420. São Paulo: Atlas, v. IV, 2008.

SANÇÕES E PENALIDADES NA ERA DA LGPD

Roberto Arylton P. Ramos¹

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD)² é a lei brasileira que busca garantir a privacidade e a segurança dos dados pessoais dos cidadãos. Ela foi inspirada em regulamentações estrangeiras, principalmente na *General Data Protection Regulation* (GDPR) da União Europeia, e reflete a preocupação global com a manipulação e uso dos dados pessoais.

Desde que entrou em vigor, as empresas e entidades que lidam com dados pessoais no Brasil estão submetidas a uma legislação que estabelece direitos para os titulares e impõe obrigações àqueles que lidam com os dados. Além disso, a LGPD prevê sanções e punições para quem descumprir suas disposições.

Esse ensaio explora o surgimento da LGPD e suas principais disposições, faz um passeio pelas legislações estrangeiras que tratam do tema e analisa as sanções em caso de descumprimento dos dispositivos legais. Buscou-se destacar a importância do cumprimento dessa lei para a preservação da privacidade e integridade dos dados pessoais.

1 Mestrando em Direito (IDP); Mestrando em Economia (IDP); Especialista Ordem Jurídica e Ministério Público – FESMPDFT (2023); MBA – Direito Econômico – FGV (2001); Graduação em Computação – Universidade Católica de Brasília (1985); Graduação – Administração de Empresas – UDF (1992); Graduação em Direito – UDF (1996); Advogado Inscrito na OAB-DF (1997); Membro da Comissão de Privacidade e Proteção de Dados da OAB-DF (2023).

2 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

1. SOCIEDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Em 1962, Marshall McLuhan cunhou a expressão “aldeia global”, afirmando que o avanço das tecnologias de informação e comunicação encurtaria as distâncias no mundo e facilitaria as trocas culturais entre os diferentes povos. O filósofo canadense acreditava que, devido à diminuição das distâncias e barreiras geográficas, o planeta se reduziria a uma organização semelhante à das aldeias, onde tudo e todos estariam interconectados.³

Na mesma época, Arthur C. Clarke, escritor britânico, também ficou famoso. Ele foi o autor do conto “*The Sentinel*”, que inspirou o diretor Stanley Kubrick a produzir e dirigir, em 1968, o clássico da ficção científica “2001 – Uma Odisseia no Espaço”. Além disso, Clarke também foi roteirista do filme. Sua genialidade permitiu que ele também fizesse previsões, profetizando o computador pessoal e um mundo interconectado por meio dos computadores.

Em seus livros “A Terceira Onda” e “O Choque do Futuro”, Alvin Toffler, escritor norte-americano, vislumbrou, já nos anos 70, a importância que a informação viria a ter na sociedade. Para ele, o mundo físico e o mundo digital iriam conviver e moldar a sociedade do futuro.⁴

Para Toffler⁵, a sociedade humana viveu três ondas que foram decisivas para sua evolução, quebrando paradigmas. A primeira onda foi a transição do nomadismo para a agricultura. A segunda onda acontece com a Revolução Industrial, quando passamos a utilizar máquinas em substituição à mão de obra humana. A terceira onda aconteceu com a revolução dos meios de comunicação e a invenção do telefone, do rádio, do cinema e da televisão. Outro evento que contribuiu muito para a terceira onda foi a revolução da eletrônica, que possibilitou a invenção dos computadores.

3 PINHEIRO, Patrícia Peck. Direito Digital. 6 ed. São Paulo. Saraiva, 2016.

4 Ibid.

5 TOFFLER, Alvin. A Terceira Onda. Petrópolis: Editora Record, 1980.

Hoje, em retrospectiva, podemos afirmar que a visão dos futuristas estava correta, pois o surgimento e expansão da sociedade da informação somente foi possível em razão do extraordinário avanço da tecnologia dos meios de comunicação e do desenvolvimento dos computadores que, ano após ano, aumentaram exponencialmente a velocidade de processamento e a capacidade de armazenamento de dados.

Esse mundo virtual exige que as pessoas executem cada vez mais tarefas, acessem cada vez mais informações, não importando mais o tempo e o espaço. As tarefas são executadas em paralelo, ao mesmo tempo, por inúmeros indivíduos, em diferentes locais, em qualquer horário. O fluxo de dados é ininterrupto e global, ultrapassando fronteiras e limitações geográficas. A tecnologia veio para ficar. As referências estão mudando, a globalização se implementou com o avanço da tecnologia.

Devemos lembrar que o dado é uma matéria prima que, ao ser processada, transforma-se em informação. A informação é o diferencial estratégico. Os computadores processam dados e seus sistemas geram informações. Hoje, no mundo digital, tudo acaba sendo dado. A foto, o vídeo, o texto, a voz, o som – tudo pode ser digitalizado, tudo pode ser dado; daí sua relevância.

Neste mundo informatizado, os dados são ativos de alto valor, avidamente disputados pelos agentes econômicos. Essa nova dinâmica levou ao desenvolvimento do modelo de negócios da economia digital, que está totalmente vinculado ao grande fluxo de dados.

É inevitável fazer parte desse mundo. Porém, a exposição das pessoas a esse cenário veloz e ultraconectado enseja algumas preocupações: percebe-se que é necessário defender o cidadão dos perigos desse aparato cibernético.

Nos dias de hoje, compartilhar dados é pré-requisito para participar das redes sociais ou para ter acesso a bens e serviços na internet. Para participar da vida virtual, é preciso confiar seus dados pessoais e financeiros às plataformas e sites de comércio eletrônico.

Como enfatizado por Rosenvald,⁶ surgem questões como: “em sociedades plurais e complexas, como lidar com o tratamento de dados? Vivemos numa sociedade governada por algoritmos? Temos direito de manter controle sobre a própria informação?”. Perguntas com as quais devemos nos preocupar para tentar compatibilizar essa nova realidade com os direitos fundamentais. Sob essa perspectiva, os titulares de dados estão vulneráveis.

O trânsito ininterrupto de dados expõe seus titulares ao perigo de perceber suas informações pessoais sendo usadas sem autorização, seja para campanhas de marketing, seja para buscar algum proveito econômico ou, em uma situação mais grave, para a prática de crimes. Portanto, as pessoas podem ter seus dados utilizados de maneira indevida, sem sequer perceberem que isso está ocorrendo.

Como bem pontuado por Rosenvald, “as violações de dados pessoais (...) ocorrem, causam danos e o direito precisa contar com instrumentos eficazes contra esses danos”.⁷

A bem da verdade, a preocupação com a proteção de dados remonta aos anos 70 quando, na Alemanha, surgiu a primeira lei que tratava do tema. É a notícia trazida por Reinaldo⁸:

“Embora o “direito à privacidade” (*right to privacy*) tenha se desenvolvido originalmente na jurisprudência e doutrina norte-americanas, foi a Europa que se notabilizou como a fonte dos principais e mais completos conjuntos de leis sobre proteção de dados pessoais, que emergiram nessas décadas. Em 1970, o Estado alemão de Hesse editou a primeira lei sobre essa matéria. A Suécia conta com o Datalegen, Lei 289 de 11 de maio de 1973. Desde 1977, a Alemanha

6 ROSENVALD, Nelson; BRAGA NETTO, Felipe. *Leis Civis Comentadas*. 2 ed. São Paulo. Juspodivm, 2023.

7 ROSENVALD, Nelson; BRAGA NETTO, Felipe. *Leis Civis Comentadas*. 2 ed. São Paulo. Juspodivm, 2023.

8 REINALDO FILHO, Demócrito. A Diretiva Europeia sobre proteção de dados pessoais. Uma análise de seus aspectos gerais. *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 18, n. 3507, 6 fev. 2013. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 26 dez. 2023.

tem uma lei federal de proteção de uso ilícito de dados pessoais. A Dinamarca regulamenta a questão da proteção de dados pelas Leis 243 e 244, ambas de 08 de julho de 1978, que estenderam a proteção também para as pessoas jurídicas. A França tem a Lei 78-77, de 06 de janeiro de 1978. A Espanha tem a peculiaridade de ter uma regra constitucional determinando a regulamentação da proteção da privacidade contra invasões da atividade informática (art. 18, par. 1º). A Constituição de Portugal de 1977 tem texto ainda mais completo (art. 35), pois contempla a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para a qual foram recolhidos e, ainda, de retificá-los (em caso de erro) e de atualizá-los.”.

2. LEGISLAÇÃO PROTETIVA

Em 2016, a União Europeia (UE), com o intuito de minimizar o risco de mau uso e abusos no tratamento, coleta e manipulação de dados, aprovou uma regulamentação que, por sua qualidade e abrangência, passou a ser um marco para as legislações de proteção de dados do mundo. O regulamento europeu, ao normatizar a privacidade e a proteção de dados pessoais no âmbito digital, deveria ser seguido por todos os membros da UE. Surge, então, o *General Data Protection Regulation* (GDPR) – em português, Regulamento Geral de Proteção de Dados.

Porém, os europeus perceberam que, mesmo com uma nova regulamentação no âmbito de sua jurisdição, a proteção ficaria seriamente debilitada se os dados circulassem sem controle fora de suas fronteiras. Para minimizar esse risco, a União Europeia passou a exigir que as empresas que tivessem relações comerciais com a Europa, ou seja, que ofertassem produtos ou serviços aos países europeus, mesmo que sem presença física naquele território, tivessem uma legislação de proteção de dados. Em resumo, aqueles que desejassem estabelecer relações comerciais com os membros da União Europeia deveriam possuir, em suas respectivas jurisdições, uma regulamentação de proteção de dados.

A exigência funcionou como um verdadeiro catalisador, já que, a partir de então, muitos países viriam a estabelecer suas próprias leis de proteção de dados para preservar suas relações comerciais com o bloco europeu.

De fato, no caso brasileiro, desconsiderar o alerta europeu significaria prejudicar diversos setores, enfraquecendo a competitividade e a inovação da economia devido à impossibilidade de transacionar com os países-membros da União Europeia.

A proteção de dados no âmbito nacional já vinha sendo debatida há algum tempo, porém não havia, ainda, o consenso necessário para a elaboração de uma legislação reguladora nacional. A regulamentação evoluiu de forma dispersa, prejudicando a segurança jurídica.

O artigo 5º, inciso X, da Constituição Federal de 1988 já apontava como direito fundamental a inviolabilidade da vida privada, da honra e das imagens dos indivíduos, com direito a indenização pelo dano material ou moral decorrente de sua violação. Outras leis, como a Lei de Acesso à Informação (LAI), o código do consumidor (CDC), o Marco Civil da Internet (MCI), a Lei de Cadastro Positivo e a Lei de Delitos Informáticos eram aplicadas em casos de violação de dados pessoais.⁹

Com o objetivo de unificar e organizar o cenário de regulamentações dispersas, foi promulgada, em 14 de agosto de 2018, a Lei nº 13.709 – a Lei Geral de Proteção de Dados (LGPD).

A principal finalidade da LGPD é resguardar os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural. Além disso, busca estabelecer um ambiente de segurança jurídica por meio da padronização de regulamentos e práticas, garantindo a proteção dos dados pessoais de qualquer indivíduo em território brasileiro, em conformidade com os padrões internacionais vigentes.

A legislação estabelece a definição de dados pessoais e dados pessoais sensíveis, determinando que todos os dados tratados, tanto no

9 VILELA, Gabriel Badim. LGPD: Um Estudo Sobre as Principais Responsabilidades e Penalidades Previstas na Lei. Monografia (Graduação em Engenharia de Computação) - Pontifícia Universidade Católica de Goiás (PUC-GO), Goiânia, 2021.

meio físico quanto no digital, estão sujeitos à sua regulação. Além disso, determina que a lei se aplica sempre que houver o processamento de informações de indivíduos, independentemente de sua nacionalidade, desde que estejam em território nacional. O consentimento do titular é considerado elemento essencial para o tratamento de seus dados, sendo dispensável apenas nas hipóteses das sete alíneas do inciso II do artigo 11 da LGPD.

O cidadão tem o direito de solicitar a exclusão de seus dados pessoais, podendo, assim, revogar um consentimento previamente concedido. São garantias asseguradas ao cidadão. Não existe liberdade irrestrita para o uso dos dados; o tratamento desses dados deve ser informado ao titular com antecedência, especificando a finalidade e a necessidade dessa manipulação.

3. PANORAMA DAS LEGISLAÇÕES DE OUTROS PAÍSES¹⁰

Nesta seção, será feito um panorama das principais legislações de proteção de dados pessoais existentes no mundo.

O Canadá garante a privacidade dos indivíduos por meio de diversas leis provinciais e territoriais que regulamentam a coleta, o uso, a divulgação e o processamento de dados pessoais no setor privado, sendo as principais delas:

- *A Personal Information Protection and Electronic Documents Act (PIPEDA)*;
- *A Personal Information Protection Act – PIPA Alberta and PIPA BC*; e
- *O Act Respecting the Protection of Personal Information in the Private Sector (“Quebec Privacy Act”)*, que compõe o conjunto dos *“Canadian Privacy Statutes”*.

10 LGPD BRASIL. Conheça as leis de proteção de dados ao redor do mundo. Disponível em: <https://www.lgpdbrasil.com.br/conheca-as-leis-de-protecao-de-dados-ao-redor-do-mundo/> acesso em: 19 de dezembro de 2023.

Nos Estados Unidos, não há uma legislação única e abrangente para a proteção de dados. Em vez disso, a proteção de dados é uma colcha de retalhos, composta de leis setoriais e estatais. Alguns exemplos incluem:

- *Health Insurance Portability and Accountability Act (HIPAA)*;
- *Financial Services Modernization Act (Gramm-Leach-Bliley Act, GLBA)*;
- *Children's Online Privacy Protection Act (COPPA)*;
- *California Consumer Privacy Act (CCPA)*; e
- *Massachusetts Regulation 201 CMR 17.00*.

O México assegura a proteção do tratamento legítimo de dados pessoais armazenados por entidades privadas em todos os setores, sejam esses dados processados no país ou fora dele, em nome de um controlador de dados mexicano. A principal legislação que regula essa proteção é a *Federal Law on the Protection of Personal Data Held by Private Parties*, voltada à privacidade no setor privado.

Observe que essa lei se aplica apenas a indivíduos e entidades privadas; e não ao governo, agências de relatórios de crédito ou pessoas e organizações que coletam dados sem o propósito de divulgação ou uso comercial.

Em geral, as nações latino-americanas carecem de regimes de proteção de dados. A seguir, são apresentados exemplos de países que constituem exceções, acompanhados de seus principais dispositivos legais:

- Argentina: *Personal Data Protection Law 25.326*;
- Brasil: Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018;
- Colômbia: *Law 1266/08, Law 1581/2012, Decree 1377/2013*;
- Costa Rica: *Undisclosed Information Law 7975, General Law on the Protection of Personal Data 8968*;

- Peru: *Data Protection of Personal Data* 29.733; e
- Uruguai: *Data Protection Act* 18.331, *Decree* 414/009.

O Reino Unido adotou o GDPR da União Europeia como o seu principal regime de proteção de dados, apesar dos efeitos do “*Brexit*”. Ou seja, seus cidadãos continuam protegidos pelo GDPR, o que gera impactos de longo prazo para organizações em todo o mundo que tratam dados pessoais de titulares do território britânico.

Além do GDPR, outras legislações do Reino Unido incluem:

- Privacy and Electronic Communications Regulations 2003 (PECR);
- Financial Conduct Authority’s Principles for Business (PRIN 2.1).

A União Europeia é considerada líder na integração da privacidade aos valores fundamentais do seu regime jurídico. Seu principal instrumento é o já mencionado GDPR, que tem impactos de grande alcance tanto para os Estados-membros da UE quanto para organizações e governos de outras nações que lidam com dados pessoais dos seus cidadãos. Os seus artigos tratam principalmente das expectativas de um tratamento justo e transparente, da capacitação dos titulares dos dados, das expectativas de segurança, dos requisitos de transferência transfronteiriça e das sanções por violação.

Em geral, os países do Oriente Médio carecem de proteções unificadas para dados pessoais, com algumas exceções importantes:

- Abu Dhabi Global Market (ADGM): *ADGM Data Protection Regulations* (DPR 2015);
- Barein: *Data Protection Law* (Law No. 30 of 2018);
- Dubai International Financial Centre (DIFC): *Data Protection Law* (DIFC Law No. 1 2007);
- Israel: *Protection of Privacy Law* 5741-1981 (PPL);
- Catar: *Data Protection Law* (Law No. 13 of 2016);
- Turquia: *Law on the Protection of Personal Data* 6698 (LPPD); e

- Emirados Árabes Unidos: *Digital Payment Regulation*.

A República Popular da China (RPC) estabeleceu sua primeira lei nacional que aborda a segurança cibernética e a proteção da privacidade de dados, a Lei de Segurança Cibernética da RPC, que entrou em vigor em 2017. Outras regras que protegem dados pessoais são encontradas em diversas leis e regulamentos, tais como:

- *The Decision on Strengthening Online Information Protection*; e
- *National Standard of Information Security Technology — Guideline for Personal Information Protection within Information System for Public and Commercial Services*.

A Coréia do Sul estabeleceu uma variedade de leis que regem a privacidade de dados, incluindo uma lei abrangente apoiada por vários regulamentos específicos do setor, incluindo:

- Personal Information Protection Act (PIPA);
- *Act on Promotion of Information and Communication Network Utilization and Information Protection (IT Network Act)*;
- *Use and Protection of Credit Information Act (UPCIA)*; e
- *Act on Real Name Financial Transactions and Guarantee of Secrecy (ARNFTGS)*.

O Japão criou uma agência central que atua como uma organização governamental de supervisão para questões de proteção da privacidade. A lei mais significativa que rege os dados pessoais é a *Act on the Protection of Personal Information (APPI)*.

Já no sudeste da Ásia, destacam-se:

- Na Malásia, o *Personal Data Protection Act 2010 (PDPA)*;
- Nas Filipinas, o *Data Privacy Act of 2012* ou *Republic Act No. 10173*; e
- Em Singapura, o *Personal Data Protection Act of 2012*.

A Austrália dispõe de uma variedade de leis de proteção de

dados a nível federal. Os mais significativos são o *Privacy Act 1988* e os *Australian Privacy Principles*, que aplicam-se aos setores governamental e privado, bem como a outras nações que processam dados de cidadãos australianos. Outras leis estaduais e territoriais também se aplicam às agências governamentais e às empresas privadas que interagem com elas.

4. LGPD E PENALIDADES

O desrespeito a uma norma criada pelo Estado tem como consequência a imposição de uma sanção, que será mais ou menos severa, a depender da norma violada e do bem por ela protegido.

Sendo assim, a Lei Geral de Proteção de Dados (LGPD), para atingir o objetivo de proteger os dados pessoais dos cidadãos, estabeleceu uma série de sanções para quem violar seus regramentos. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) é a entidade responsável pela fiscalização e aplicação das sanções previstas na LGPD.

As sanções são gradativas e abrangem desde uma advertência até a proibição total do exercício de atividades relacionadas à proteção de dados.

A ANPD, sujeito ativo para aplicação das sanções, é uma “autarquia de natureza especial, dotada de autonomia técnica e decisória com patrimônio próprio e com sede e foro no Distrito Federal.”, nos termos da Lei nº 14.460 de 25 de outubro de 2022.¹¹ Tal autarquia tem a missão de zelar pelos direitos fundamentais dos titulares de dados, para isso, assegurando o cumprimento das disposições da LGPD e demais normas que protejam a privacidade dos dados pessoais.

Além de apurar os descumprimentos à LGPD e aplicar as sanções, a ANPD tem o compromisso de atuar preventivamente, orientando os envolvidos no tratamento de dados sobre os dispositivos da lei, além das outras competências descritas no artigo 55-J da LGPD.

11 BRASIL. Lei nº 14.460 de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial.

A legislação estabelece que o responsável por gerir dados pessoais também deve adotar normas de governança e medidas preventivas de segurança, assim como seguir boas práticas e cumprir certificações existentes no mercado. Além disso, deve elaborar planos de contingência e realizar auditorias, sendo incumbida de informar aos titulares de dados afetados e à ANPD sobre eventuais violações da integridade e da segurança dos dados sob sua custódia.

A ANPD é composta, nos termos do artigo 55-C da LGPD, por um conselho diretor, um conselho nacional de proteção de dados pessoais e da privacidade, uma corregedoria, uma ouvidoria, uma assessoria jurídica e por unidades administrativas.

O conselho diretor, composto de 5 diretores, é nomeado pelo presidente da República e sabatinado pelo Senado Federal, o que demonstra apoio político e institucional para o desempenho das funções estatutárias.

Para garantir a independência do órgão, os diretores nomeados para a autarquia têm mandato fixo de quatro anos; o primeiro mandato, excepcionalmente, pode ter de dois a seis anos. Os diretores dispõem de autonomia técnica e decisória.

A independência é fundamental para a atuação do órgão, tendo em vista a possibilidade de condução de questões sensíveis relacionadas à segurança pública, inclusive dados resultantes da investigação de infrações penais.

A apuração e aplicação de sanções é apenas uma das facetas da ANPD. Outras relevantes tarefas incluem a cooperação com autoridades de dados de outros países, a elaboração de estudos técnicos, a promoção da conscientização sobre o tema de proteção de dados e a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade.

No que diz respeito à aplicação das penalidades previstas em lei, a ANPD deverá seguir a normatização contida na Resolução CD/ANPD nº 1, de 28 de outubro de 2021, que trata do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.

Somente após a instauração e conclusão do procedimento administrativo as sanções poderão ser aplicadas. O processo administrativo sancionador deve assegurar aos pretensos infratores a oportunidade de defesa, seguindo o devido processo legal, com as garantias do contraditório e da ampla defesa.

O procedimento deve necessariamente considerar, na aplicação das sanções, a gravidade e a natureza da infração, a lesão aos direitos pessoais dos afetados, a boa-fé do infrator, as possíveis vantagens auferidas pelo infrator, sua condição econômica, o grau do dano causado, se há reincidência e se houve a cooperação do infrator para o esclarecimento dos fatos, tudo nos termos do parágrafo 1º do artigo 52 da LGPD.¹²

A favor do infrator, será levada em conta a implementação consistente e comprovada de mecanismos e procedimentos internos que contribuam para a minimização do dano, bem como a adoção institucionalizada de políticas e boas práticas de governança. A ANPD deve observar a proporcionalidade entre a gravidade da infração e a severidade da sanção aplicada.

Os parâmetros para assegurar a aplicação segura das sanções administrativas encontram-se na Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, que regulamenta a dosimetria e aplicação de sanções administrativas no âmbito da LGPD.

A ponderação na aplicação das penalidades e a análise meticulosa do caso concreto são posturas indispensáveis para a atuação da ANPD. As penalidades dos incisos X, XI e XII do artigo 52 somente podem ser aplicadas como segunda *ratio*, ou seja, se o infrator já tiver, anteriormente, sofrido uma das sanções dos incisos de II a VI do *caput* do artigo 52, tudo nos termos do parágrafo 6º do mesmo artigo 52.

Tendo em vista que pode haver incidente de vazamento de dados mesmo que o operador siga rigorosamente as melhores práticas e aplique todos os controles corretamente e que, de fato, não há sistema de segurança que consiga evitar todos os riscos da atividade, é impor-

12 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

tante que os agentes de tratamento exerçam a atuação preventiva de controle do risco da atividade para evitar as vulnerabilidades que são exploradas pelos infratores.

É importante lembrar que, embora haja a independência das instâncias no ordenamento jurídico brasileiro, a própria Constituição estabelece o acesso ao Poder Judiciário como um direito fundamental. Nos termos do inciso XXXV, do artigo 5º da Carta Magna, “a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”.¹³

Dessa forma, a responsabilidade administrativa por meio de sanções não isenta o infrator da possibilidade da responsabilização civil e da indenização de danos pelo Poder Judiciário.

Os sujeitos passíveis de sanções são os agentes de tratamento de dados que, segundo o artigo 5º, inciso IX, da LGPD, incluem o controlador e o operador. O mesmo artigo define, no inciso VI, que o controlador “é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. Já de acordo com o inciso VII, “operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.¹⁴

As sanções administrativas estão descritas no *caput* do artigo 52, a saber:¹⁵

13 BRASIL. Constituição da República Federativa do Brasil, 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

14 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

15 MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] 2ª Ed. São Paulo, Thomson Reuters Brasil, 2020.

I – Advertência, com indicação de prazo para adoção de medidas corretivas;

É a pena mais branda e teve como paradigma o inciso I do artigo 12 da Lei 12.965, de 23 de abril de 2014, o Marco Civil da Internet. A advertência deve ser acompanhada de um prazo para a adoção das medidas que, não sendo efetivadas, podem implicar a imposição de penalidade mais gravosa.

II – Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

- Valor: até 2% do faturamento, com limite de R\$ 50.000.000,00 (cinquenta milhões de reais);
- Base de cálculo: faturamento no último exercício, excluídos tributos;
- Destinatário: pessoa jurídica de direito privado, grupo ou conglomerado no Brasil;
- Recorrência: por infração.

A primeira questão que se coloca diz respeito ao destinatário. O artigo 3º da LGPD dispõe que esta lei “aplica-se a qualquer operação de tratamento realizada por pessoa natural ou pessoa jurídica de direito público ou privado (...)”, portanto, o destinatário da multa, em tese, pode ser uma pessoa natural. Sendo assim, qual seria a base de cálculo para estabelecer a multa? Parte da doutrina¹⁶ tem opinado que, nesse caso, a multa poderia ser aplicada à pessoa física e, usando uma interpretação extensiva, dever-se-ia usar como base de cálculo a receita auferida pela pessoa natural em decorrência da atividade de tratamento

16 Ibid.

de dados pessoais. Outra parte da doutrina¹⁷ entende que, embora as sanções do artigo 52 sejam dirigidas aos agentes de tratamento (que podem ser pessoas jurídicas ou naturais), como a lei não fixou explicitamente parâmetros para que pessoas naturais sejam multadas, não haveria como aplicar a penalidade às pessoas naturais. A jurisprudência vai resolver a questão.

Outro aspecto a ser considerado diz respeito à recorrência necessária à aplicação da multa. A lei indica expressamente a multa por infração. Alguns autores¹⁸ entendem que seria possível que a infração fosse considerada pelo número de titulares afetados, pelo número de incidentes de violação de proteção de dados ocorridos ou pelo número de dispositivos violados. Seriam possibilidades que, sendo adotadas, levariam o infrator a uma situação financeira muito complicada. A interpretação que mais se alinha ao princípio da razoabilidade é aquela que utiliza os parâmetros estabelecidos no parágrafo 1º do artigo 52 da LGPD, ou seja, analisar o caso concreto e ponderar a melhor maneira de fazer com que a sanção cumpra suas funções de prevenção geral (desestimular a reincidência) e prevenção especial (servir de exemplo para desestimular que outros agentes cometam infrações)¹⁹.

O parágrafo 3º do artigo 52 exclui a aplicação de multa do rol de possíveis sanções aplicáveis às entidades e órgãos públicos.

A LGPD não aborda explicitamente a questão da prescrição, o que permite a aplicação do prazo de 5 anos estabelecido pela Lei 9.873/99, que define o prazo prescricional para o exercício da ação punitiva pela Administração Pública Federal.

17 ROSENVALD, Nelson; BRAGA NETTO, Felipe. *Leis Civis Comentadas*. 2 ed. São Paulo. Juspodivm, 2023.

18 MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD: Lei Geral de Proteção de Dados comentada* [livro eletrônico] 2. ed. São Paulo, Thomson Reuters Brasil, 2020.

19 BITENCOURT, Cezar Roberto. *Manual de direito penal - Parte geral*. São Paulo: Ed. RT, 1999.

Os valores arrecadados devem ser destinados ao Fundo de Defesa dos Direitos Difusos, para financiar projetos voltados à reparação de danos causados pela violação de direitos relacionados à proteção de dados pessoais, mas também se estende a dados consumeristas, ambientais e patrimoniais, nos termos do parágrafo 5º do artigo 52.

III – Multa diária, observado o limite total a que se refere o inciso II;

A multa diária tem natureza distinta da multa simples, citada no inciso II. A multa diária funciona como uma medida coercitiva e seu objetivo é forçar o infrator a cumprir uma obrigação. Essa multa tem natureza de *astreintes* e não é uma punição pela violação em si, mas um recurso para motivar o infrator a cumprir alguma obrigação, de fazer ou de não fazer. Na aplicação dessa penalidade, a ANPD deve observar que, em razão de sua natureza, ela não deve ser de tal montante que a caracterize como uma penalidade em si, sob pena de ilegalidade. Portanto, não deve alcançar o limite do inciso II, apesar da expressa possibilidade, por falta de proporcionalidade. Os valores arrecadados devem ser destinados ao Fundo de Defesa dos Direitos Difusos.

IV – Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

Tem por objetivo desincentivar outras condutas correlatas, na medida em que atinge diretamente a reputação do infrator. Neste inciso, é possível invocar a questão da finalidade da pena,²⁰ seja por prevenção geral, que tem por objetivo estabelecer nas pessoas o respeito pelo direito, seja por prevenção especial, que tem por objetivo intimidar o infrator, com o objetivo decuidade evitar a reincidência. Por outro lado,

20 CUNHA, Rogerio Sanches. Manual de Direito Penal – Parte Geral. 9 ed. Salvador, Juspodivm, 2021.

deve a ANPD observar certos limites para evitar a aplicação de uma penalidade infame, o que seria vedado pelo ordenamento jurídico. A publicização deve estar condicionada à confirmação da prática delitiva.

V – Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

Equivale a uma limitação temporária do tratamento de dados pelo infrator. Lembrando que o bloqueio pode ser revertido tão logo a situação seja regularizada.

VI – Eliminação dos dados pessoais a que se refere a infração;

Essa penalidade tem por objetivo apagar definitivamente os dados a que se refere a infração, de modo que fiquem permanentemente inacessíveis, assegurando que não exista a possibilidade de recuperação, nem mesmo por meio do uso de tecnologias de recuperação de dados.

Incisos VII, VIII e IX foram vetados;

X – Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

Essa sanção foge ao padrão esperado para coibir a prática ilícita. A restrição de uso recai sobre a base de dados, sem afetar diretamente a atividade de tratamento ou o agente responsável por esse tratamento. Importante observar que a sanção se refere especificamente aos dados pessoais vinculados à infração e não a todo o acervo. Ao vetar o inciso VI, que possuía prescrição semelhante, o presidente da Re-

pública alertou para possíveis prejuízos caso o banco de dados ficasse inacessível, pois a restrição alcançaria outros atores. Resta aguardar a posição da jurisprudência.

XI – Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período;

Essa penalidade possibilita a suspensão da atividade e deve ser aplicada juntamente com o inciso XII, considerando a possibilidade de graduar a sanção. Inicialmente, pode-se suspender a atividade e, em caso de reincidência, aplicar a proibição parcial; nos casos mais graves, pode-se adotar a proibição total da atividade.

XII – Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Essa penalidade possibilita à autoridade de dados agir, inclusive de forma cautelar, em situações de violações graves à LGPD. Trata-se de uma medida que pode excluir do ambiente de tratamento de dados agentes que não atendem aos requisitos mínimos para a prestação de um serviço cuidadoso e de qualidade – o que é, inclusive, prestigiado pela doutrina.

Além das penalidades administrativas aqui examinadas, a LGPD também aborda a responsabilidade civil dos agentes de tratamento em caso de prejuízos decorrentes do tratamento e manipulação de dados. O artigo 42 determina que “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”.²¹

21 BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

Conforme o artigo 43 da LGPD, os agentes de tratamento somente isentam-se de responsabilidade se provarem que não realizaram tratamento dos dados em questão, se provarem que embora tenham realizado o tratamento não houve violação à legislação ou se provarem que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Já o artigo 44 dispõe das hipóteses em que o tratamento de dados é considerado irregular, podendo ensejar reparação civil a ser discutida diretamente no Poder Judiciário.

CONSIDERAÇÕES FINAIS

A proteção de dados não é apenas responsabilidade das organizações, mas também dos próprios indivíduos. Além disso, titulares dos dados têm o direito de entender como suas informações estão sendo usadas e de conceder ou revogar consentimento para o seu processamento.

As organizações devem entender a importância da conformidade com a LGPD não apenas para evitar penalidades, mas também para promover uma cultura de respeito à privacidade, construir uma relação de confiança com os consumidores e proteger sua reputação.

É importante investir na conscientização dos colaboradores acerca da relevância dos dados pessoais e da necessidade de protegê-los. Na mesma toada, é preciso que haja investimento expressivo em medidas de proteção adequadas, que englobam segurança física e virtual. Ataques vindos de *hackers*, por exemplo, estão cada dia mais sofisticados. Os processos e tecnologias devem ser constantemente auditados e atualizados para evitar acessos indevidos.

A conformidade com a LGPD deve ser objetivo de todas as organizações, uma vez que todas lidam com a coleta, o tratamento e o uso de dados pessoais.

Um fato é indiscutível: a implementação da LGPD e a regular atuação da ANPD são demonstrações do empenho do Brasil em preservar a privacidade e proteger os dados pessoais de forma efetiva.

REFERÊNCIAS

ARAÚJO, Valter Shuenquener de. **O princípio da interdependência das instâncias punitivas e seus reflexos no Direito Administrativo Sancionador**. Revista Jurídica da Presidência Brasília v. 23 n. 131, out. 2021/jan.2022 p. 629-653, disponível em: <http://dx.doi.org/10.20499/2236-3645.RJP2022v23e131-1875>, acesso em: 18 de dezembro de 2023.

BITENCOURT, Cezar Roberto. **Manual de direito penal - Parte geral**. São Paulo: Ed. RT, 1999.

BRASIL. **Constituição da República Federativa do Brasil**, 5 de outubro de 1988. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

BRASIL. Lei nº 9.873 de 23 de novembro de 1999. Estabelece prazo de prescrição para o exercício de ação punitiva pela Administração Pública Federal, direta e indireta, e dá outras providências.

BRASIL. Lei nº 14.460 de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial.

CUNHA, Rogerio Sanches. **Manual de Direito Penal – Parte Geral**. 9 ed. Salvador, Juspodivm, 2021.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

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

EUR-LEX. **GDPR - General Data Protection Regulation**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=cele-x:32016R0679>, acesso em: 25 de dezembro de 2023.

LGPD BRASIL. **Conheça as leis de proteção de dados ao redor do mundo**. Disponível em: <https://www.lgpdbrasil.com.br/conheca-as-leis-de-protecao-de-dados-ao-redor-do-mundo/> acesso em: 19 de dezembro de 2023.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada** [livro eletrônico] 2. ed. São Paulo, Thomson Reuters Brasil, 2020.

MARTIN, Beatriz. **Aplicação das Penalidades da Lei Geral de Proteção de Dados**. Conhecimento Interativo, São José dos Pinhais/PR (ISSN 1809-3442), V. 14, N. 2, p. 88-107, jul/dez. 2020.

MENKE, Fabiano. **Spiros Simitis e a primeira lei de proteção de dados do mundo**. Migalhas, 19 de novembro de 2021. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo>, acesso em: 21 dezembro de 2023.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6 ed. São Paulo. Saraiva, 2016.

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

REINALDO FILHO, Demócrito. **A Diretiva Europeia sobre proteção de dados pessoais. Uma análise de seus aspectos gerais**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3507, 6 fev. 2013. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 26 dez. 2023.

TOFFLER, Alvin. **A Terceira Onda**. Petrópolis: Editora Record, 1980.

VAUGHN, Gustavo Favero, BERGSTRÖM, Gustavo Tank, FABER, Bárbara Breda. **Primeiras Impressões Sobre a Lei de Proteção de Dados**. Ribeirão Preto, Migalhas, 2021.

VILELA, Gabriel Badim. **LGPD: Um Estudo Sobre as Principais Responsabilidades e Penalidades Previstas na Lei**. Monografia (Graduação em Engenharia de Computação) - Pontifícia Universidade Católica de Goiás (PUC-GO), Goiânia, 2021.

A LGPD E SEUS EFEITOS NO MARKETING DIGITAL: ANÁLISE DAS PRINCIPAIS PRÁTICAS DE MERCADO E SUAS IMPLICAÇÕES NA PRIVACIDADE DE DADOS

Tatiana Venâncio de Rezende¹

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representou um marco na regulamentação do tratamento de dados pessoais no Brasil. Ela impactou diversos setores, incluindo o marketing digital, que precisa se adaptar às novas diretrizes de respeito à privacidade dos titulares de dados.

A era digital trouxe consigo uma transformação na maneira como vivemos, interagimos e como o capitalismo se vem desenvolvendo ao longo das décadas. Surge, assim, uma economia movida a dados, que se utiliza de tecnologia, como a Internet das Coisas (“Internet of Things, ou IoT”), para interconectar dispositivos e permitir a coleta e troca de dados em tempo real.

Os dados pessoais, anteriormente considerados meras formalidades para selar relações entre pessoas e organizações, viram elementos essenciais capazes de personalizar relações e proporcionar vantagens competitivas às empresas que os detém.

Empresas passam a ter acesso a uma quantidade sem precedentes de informações sobre o comportamento do consumidor, o que as possibilita antecipar desejos e moldar estratégias de vendas. A busca

¹ Advogada e Compliance Officer, especialista em Direito Empresarial pela FGV/RJ, membra da Comissão de Privacidade e Proteção de Dados da OAB/DF e da Comissão Especial de Compliance da OAB/SP.

por liderança de mercado e o constante investimento em tecnologias digitais disruptivas, como a *Advanced Analytics* (análise avançada de dados), passa a ser a prioridade dos principais CEOs do mundo².

Esse ciclo, embora eficiente para sucesso dos negócios, levanta preocupações sobre a prática do monitoramento constante e a manipulação sutil dos indivíduos. À medida em que a coleta de dados se intensifica, as barreiras entre o pessoal e o público tornam-se cada vez mais tênues. O controle sobre informações escapa das mãos dos indivíduos, dando lugar a preocupações sobre autonomia e liberdade na era digital.

O desafio reside em encontrar um equilíbrio entre os benefícios inegáveis dessas tecnologias e o respeito pelos direitos individuais.

1. BASES LEGAIS PARA TRATAMENTO DE DADOS PESSOAIS NO MARKETING DIGITAL

Qualquer tipo de tratamento de dados pessoais precisa estar enquadrado em uma das bases legais previstas na LGPD. Conforme será exposto a seguir, as bases legais mais adequadas ao marketing digital são o consentimento e o legítimo interesse, sendo que este último possui caráter residual.

1.1. Consentimento

A base legal do consentimento costuma ser a preferencial em se tratando de marketing digital, pois é mais facilmente comprovada e a que representa menor risco para as empresas. Contudo, o consentimento precisa ser fornecido de forma **livre**, ou seja, ausente de qualquer tipo de coação, **informada** e, portanto, só existe se ficar evidenciado

² Em pesquisa realizada pela McKinsey sobre excelência dos CEOs, visando avaliar como as prioridades dos principais CEOs estão evoluindo e quais as ações que estão empreendendo para dar conta delas, 62% responderam que investimento em tecnologias digitais disruptivas, como a *Advanced Analytics* (análise avançada de dados) estava no topo da lista. Ver <https://www.mckinsey.com/featured-insights/destaques/os-planos-de-acao-dos-melhores-ceos-para-2023/pt> nos de ação dos melhores CEOs para 2023 | McKinsey.

que todas as informações sobre o tratamento dos dados foram disponibilizadas ao titular, e **inequívoco**, ou seja, deve ter sido concedido por meio de uma ação positiva do titular.

A prática que, não raras vezes, vemos ocorrer no meio digital, de atrelar o fornecimento de produtos ou serviços ao posterior envio de e-mail marketing, não está em *compliance* com a LGPD, pois este não se trata de um consentimento livre e, tampouco, específico para determinada finalidade.

Diferentemente do que pode se estar pensando, a LGPD não tem o intuito de eliminar as práticas de marketing digital. Ao contrário disso, a sua observância pode vir a beneficiar as empresas e estreitar ainda mais sua relação com clientes (*customers*) e potenciais clientes (*suspects*, na terminologia do marketing). Isso porque, ao se estabelecer uma relação de transparência com os consumidores e titulares de dados, enviando conteúdos desejados, ao invés de bombardeá-los com abordagens intrusivas e aleatórias, certamente a percepção de valor agregado será maior e ambas as partes poderão desfrutar dos benefícios dessa relação.

1.1.1. Base legada

A LGPD estabelece, no artigo 63, que a ANPD criará normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da lei, consideradas a complexidade das operações de tratamento e a natureza dos dados. De acordo com essa disposição as bases de dados legadas não precisam ser apagadas de forma imediata. As empresas podem mapear quais dos seus tratamentos de dados necessitam do consentimento, e verificar, gradativamente, como, e se, esse consentimento foi obtido.

Essa análise pode, inclusive, ser utilizada para que as empresas identifiquem melhorias em seus processos, e revejam a pertinência de manutenção ou não do armazenamento de dados. Como se sabe, a coleta e guarda excessiva de dados representa risco para as empresas, além de custos com servidores ou espaço em nuvem.

1.2. Legítimo interesse

A LGPD não estabelece uma hierarquia entre as diferentes bases legais que possibilitam o tratamento de dados pessoais, no entanto, em se tratando de marketing digital, o consentimento é a base mais indicada, por ser mais facilmente comprovada e por acarretar menos riscos para os agentes de tratamento. Isso não quer dizer que as empresas não podem se valer da base legal do legítimo interesse. Se respeitadas as liberdades civis dos indivíduos e mitigados os riscos de potencial lesão a seus direitos fundamentais, essa pode ser uma alternativa diante da dificuldade de obtenção do consentimento em determinadas situações.

Na LGPD, o legítimo interesse está associado à legítima expectativa do titular de dados. O controlador precisa ponderar se seus interesses legítimos são compatíveis com as expectativas razoáveis dos titulares. É fundamental, ainda, que ao utilizar o legítimo interesse como base legal, o controlador realize uma avaliação sobre os riscos e potenciais impactos no direito à privacidade dos indivíduos. Além disso, é necessário fornecer informações claras aos titulares sobre o motivo pelo qual seus dados estão sendo processados com base no legítimo interesse.

No contexto das atividades de marketing, a avaliação do legítimo interesse pode ser exemplificada pela prática conhecida como “adesão flexível” ou “*soft opt-in*” em campanhas virtuais. Ele é geralmente aplicado em cenários nos quais exista um relacionamento prévio entre o remetente (empresa ou organização) e o destinatário (cliente ou usuário). Esse relacionamento pode surgir a partir de uma transação anterior, como uma compra ou registro de serviço, e o envio subsequente de comunicações de marketing estar relacionado a produtos ou serviços semelhantes.

A ideia central é a de que, se um cliente forneceu seu endereço de e-mail durante uma interação anterior e não se opôs ao recebimento de comunicações de marketing, há uma permissão implícita para esse tipo de abordagem. Contudo, é crucial oferecer uma opção fácil para que os destinatários cancelem a assinatura a qualquer momento, tam-

bém conhecida como “*opt-out*”. O “*soft opt-in*” não deve ser uma maneira de forçar os usuários a receberem comunicações indesejadas.

No que tange ao tratamento de dados sensíveis, como os de orientação religiosa, política, sexual, entre outros, a utilização da base legal do legítimo interesse não é uma opção viável. A LGPD estabelece que, neste caso, o controlador precisa obter o consentimento específico e destacado do titular dos dados ou se basear em outras hipóteses legais, como o cumprimento de obrigação legal ou regulatória, por exemplo.

2. GESTÃO DOS DIREITOS DOS TITULARES

A LGPD introduziu uma série de direitos aos titulares de dados, tanto procedimentais como instrumentais, que podem ter o condão de prevenir ameaças a violação de privacidade. Ferramentas como os painéis de controle de privacidade desempenham um papel fundamental na promoção da autodeterminação informativa, um princípio crucial da previsto na LGPD.

Ao fornecer uma interface intuitiva e acessível, os painéis possibilitam que os titulares de dados compreendam como suas informações pessoais são coletadas e utilizadas, em observância ao princípio da transparência, e restabelecem o poder dos indivíduos, permitindo-lhes controlar o fluxo de dados a eles relacionados.

Dentre os direitos conferidos aos titulares, estão a possibilidade de manifestação de discordância da pessoa em relação ao tratamento de suas informações pessoais, que pode ser sanada com a revogação do consentimento concedido anteriormente, a anonimização ou bloqueio de informações coletadas de forma desnecessária, o pedido de eliminação dos dados e a oposição a um tratamento realizado de forma irregular.

Além disso, o titular também pode solicitar a confirmação de que seus dados estão sendo efetivamente tratados, o seu acesso integral, a informação sobre compartilhamentos com terceiros, a portabilidade para outras entidades e a atualização ou correção dos mesmos. Portanto,

a intenção da LGPD é garantir que as práticas de marketing sejam realizadas de maneira responsável, prezando pela manutenção de ambiente digital seguro e confiável.

Ultrapassada a análise das duas principais bases legais para o tratamento de dados pessoais no marketing digital, passaremos a tratar das práticas mais comuns no marketing digital e que podem ter impactos na privacidade de dados.

3. COLETA DE *LEADS*

Dentro do contexto do marketing e de estratégias comerciais, os termos *prospects*, *leads* e *customers* referem-se a diferentes estágios do ciclo de vida do cliente, representando a progressão de um contato inicial até a conversão em um cliente pagante.

Suspects são indivíduos ou empresas que podem ter um perfil que os torna potenciais interessados nos produtos ou serviços de uma empresa, mas ainda não demonstraram um interesse ativo. Geralmente, os *suspects* são identificados com base em critérios demográficos, comportamentais ou contextuais, mas ainda não foram qualificados como *leads*.

Os *prospects* são pessoas ou empresas que demonstraram algum nível de interesse ou engajamento com a marca, produto ou serviço. Eles estão um passo à frente dos *suspects*, pois já iniciaram uma interação com a empresa. O interesse pode ser manifestado por meio de interações como visitas ao site, downloads de conteúdo, inscrições em newsletters ou participação em eventos.

Leads são contatos que foram mais qualificados e estão mais próximos de se tornarem clientes. Eles expressaram um interesse mais significativo nas ofertas da empresa e forneceram informações que permitem a comunicação direta. São normalmente classificados com base em critérios como a probabilidade de conversão, o valor potencial do cliente e a adequação aos produtos ou serviços oferecidos.

Por fim, os *customers* são os clientes reais, ou seja, aqueles que realizaram uma transação e adquiriram produtos ou serviços da empresa. Eles já passaram pelo funil de vendas, converteram-se e,

idealmente, estão satisfeitos com a experiência, tornando-se parte da base de clientes.

Esses conceitos e a distinção entre os diferentes tipos de categorias de partes envolvidas é importante, pois evidencia qual a relação existente entre uma empresa e o titular de dados pessoais e permite o melhor enquadramento em uma das bases legais para tratamento de dados previstas na LGPD.

Em interações mais próximas, como com *leads* e clientes, o uso da base legal do legítimo interesse se torna mais viável, aumentando as chances de uma estratégia de marketing bem-sucedida. Já nas interações mais distantes e genéricas, que ocorrem com *suspects* e *prospects*, muito provavelmente a única base legal de tratamento de dados pessoais cabível será a do consentimento.

3.1. Comercialização de listas de e-mail marketing

A venda de listas de e-mail marketing e bancos de dados, muitas vezes segmentados com base em diferentes critérios como interesses, demografia ou comportamentos, tornou-se um mercado lucrativo, impulsionado pela crescente demanda por estratégias eficazes para que as empresas alcancem seu público-alvo de maneira assertiva. No entanto, com o advento LGPD, é crucial que os envolvidos compreendam os requisitos legais para evitar a violação da privacidade dos titulares dos dados.

Para que a prática não seja considerada ilegal, é essencial obter o consentimento dos titulares dos dados antes de comercializar suas informações. Além disso, os princípios da LGPD relacionados à necessidade, finalidade e adequação desempenham um papel crucial na conformidade. A coleta de dados deve ser limitada ao estritamente necessário, com uma finalidade clara e legítima, evitando excessos e desvios de uso.

Na esteira da possibilidade de autorregulação prevista no art. 50 da LGPD, a ABEMD – Associação Brasileira De Marketing De Dados editou o “Código de Autorregulamentação para prática de E-mail Marketing - CAPEM”.

Além da necessidade obtenção de permissão dos titulares de dados, seja por *Opt-in* ou *Soft Opt-in*, o CAPEM também prevê que deve haver a identificação clara do remetente, o uso exclusivo de domínio próprio no endereço de e-mail e que o assunto do e-mail tenha relação com seu conteúdo. Além disso, a veiculação de conteúdo HTML ou TXT é permitida, desde que não oculte o código original da mensagem.

A importância da transparência é enfatizada, com a exigência de divulgação da política de privacidade e uso de dados no website do remetente. O descadastramento (*Opt-out*) é obrigatório, com a disponibilização de recursos para que os destinatários possam remover seus endereços das bases em um prazo definido. Para além das diretrizes da ABEMD, é recomendável, ainda, que seja firmado um contrato entre vendedor e comprador de listas, detalhando a origem lícita da lista, quando e onde foi adquirida. A clareza e a licitude na origem dos dados proporcionam não apenas segurança jurídica, mas também sustentam a confiança entre as partes envolvidas.

A discussão sobre a utilização do legítimo interesse como base legal para a venda de listas de e-mail marketing é um ponto relevante no contexto da proteção de dados. A LGPD prevê diferentes bases legais para o tratamento de dados pessoais, sendo o consentimento uma das principais. No entanto, o legítimo interesse é uma alternativa que pode ser considerada, desde que respeite os direitos e liberdades fundamentais dos titulares dos dados.

Em conclusão, a venda de listas de e-mail marketing, embora promissora, exige uma abordagem ética e legal. A conformidade rigorosa com a LGPD, o respeito aos direitos dos titulares dos dados e a transparência nas práticas comerciais são fundamentais para navegar por esse cenário desafiador, garantindo não apenas a conformidade legal, mas também a construção de relacionamentos sólidos e confiáveis no mercado.

3.2. *Profiling*, análise automatizada e análise preditiva de dados

O *profiling*, ou perfilagem, refere-se à prática de coletar e analisar uma variedade de informações sobre indivíduos, usando algoritmos de análise de dados, *machine learning* (aprendizado de máquina) e outras técnicas estatísticas, para criar perfis detalhados que descrevem suas características, comportamentos, preferências e propensões. Os perfis resultantes são frequentemente utilizados para fins comerciais, como publicidade direcionada, personalização de conteúdo, recomendações de produtos, e até mesmo tomadas de decisão em setores como serviços financeiros.

A realização do *profiling* envolve o uso de uma variedade de tecnologias para coletar, processar e analisar dados. Cookies e pixels são usados para rastrear a atividade online dos usuários, permitindo a coleta de dados de navegação em sites. Aplicativos móveis também são responsáveis por coleta de dados por meio de sensores e funcionalidades dos dispositivos. Algoritmos de aprendizado de máquina são cruciais para identificar padrões nos dados e criar modelos preditivos.

A análise preditiva na publicidade direcionada é uma prática na qual algoritmos são utilizados para prever o comportamento dos consumidores com base em seu comportamento *online*. Esses modelos permitem que os anunciantes se antecipem aos desejos de seus clientes e personalizem mensagens publicitárias para públicos específicos, aumentando a relevância e a probabilidade de conversão.

Apesar de gerar uma experiência mais direcionada para os usuários, surgem preocupações sobre a falta de transparência e controle sobre como esses dados são usados, o que pode comprometer privacidade dos consumidores e gerar uma possível manipulação informacional.

Além disso, práticas de *profiling* mal concebidas podem resultar em discriminação, impactando negativamente a equidade no acesso a serviços essenciais³.

³ Suponha que uma plataforma utilize algoritmos de *profiling* para direcionar anúncios de aluguel ou compra de casas. Se, historicamente, dados utilizados por esses algoritmos refletirem padrões discriminatórios, como associar erroneamente certos bairros a grupos étnicos específicos, o algoritmo pode, inadvertidamente, perpetuar esses estereótipos. Como resultado, anúncios de propriedades podem ser direcionados de maneira discriminatória, impactando o acesso à informação sobre habitação para determinados grupos. Por exemplo, se o algoritmo associa indevidamente um bairro a um grupo étnico minoritário com base em dados históricos enviesados, pode direcionar menos anúncios de propriedades para esse grupo, limitando suas opções de escolha

Tim Wu⁴, em seu livro intitulado “*The attention merchants: the epic scramble to get inside our heads*”, analisa como a atenção humana se tornou uma mercadoria disputada e destaca que o verdadeiro modelo de negócio de alguns agentes de tratamento, como os *Data Brokers*, consiste em utilizar dados para influenciar consciências e, a partir do conhecimento das informações mais íntimas das pessoas, manipulá-las para diversos fins.

No contexto da publicidade direcionada e análise preditiva, o *profiling* é uma ferramenta valiosa para personalizar ofertas e mensagens, mas é importante equilibrar os benefícios comerciais com a necessidade de proteger a privacidade e os direitos dos consumidores. A regulamentação e as práticas éticas desempenham um papel fundamental na garantia de um uso responsável da perfilagem de dados.

Isso confere ao titular de dados os direitos de explicação e revisão, previstos expressamente na LGPD. O direito de explicação implica que os titulares de dados têm o direito de ser informados sobre o processo de tomada de decisão automatizada, compreendendo os critérios, a lógica envolvida e as implicações associadas. Já o direito de revisão assegura aos titulares a oportunidade de contestar decisões automatizadas que os afetem adversamente. Isso pode incluir a solicitação de intervenção humana e a revisão dos critérios utilizados.

Ambos os direitos são fundamentais para garantir que o uso de algoritmos e inteligência artificial seja ético, justo e alinhado com os princípios de proteção de dados.

3.3. Data brokers

Data brokers, ou corretores de dados, são empresas que coletam, compilam e analisam uma variedade de informações sobre consumidores⁵ e os vendem para outras organizações, como empresas de

4 WU, Tim. *The attention merchants: the epic scramble to get inside our heads*. New York: Knopf, 2016.

5 Informações que podem incluir histórico de compras, registros de transações financeiras, interesses pessoais, atividades online e offline, entre outros.

marketing, agências de publicidade, seguradoras entre outras. Um problema significativo associado aos *data brokers* é a falta de transparência. Muitas vezes, os consumidores não têm conhecimento sobre quais dados estão sendo coletados e como suas informações estão sendo usadas.

Em artigo publicado em 2019, Ana Frazão analisa um relatório de 2014 da *Federal Trade Commission* norte-americana, e conclui que:

*“o modelo de negócios dos data brokers apresenta incompatibilidades gritantes com o GDPR europeu e a LGPD brasileira, a começar pelo fato de não obedecer ao princípio da finalidade específica do tratamento de dados nem à necessidade do consentimento livre, informado e específico do titular de dados”*⁶.

Alguns exemplos mencionados no artigo sobre como essa indústria funciona incluem: coleta de dados sem consentimento dos consumidores e em volume muito maior do que os que são utilizados; o desenvolvimento de modelos complexos para prever o comportamento dos consumidores e para extrair inferências potencialmente sensíveis a respeito deles; fornecimento de escolha aos titulares de dados amplamente invisíveis e incompletas com grande ausência de transparência, entre outros.

Esse mercado se sustenta sob o argumento de que o amplo acesso a informações pessoais serviria de moeda de troca pela inovação e progresso tecnológico do ambiente digital. Contudo, o papel dos *data brokers* na economia de dados moderna levanta questões mais amplas sobre o poder que detêm na influência de decisões e na formação de perfis detalhados sobre os indivíduos, o que pode ter implicações sociais significativas, conforme exploraremos no próximo tópico.

6 FRAZÃO, Ana. A indústria dos dados pessoais e os data brokers. Reflexões sobre os riscos da atuação de tais agentes no mercado de dados pessoais. Jota. Disponível em: [https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-industria--dos-dados-pessoais-e-os-data-brokers-20032019](https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-industria-dos-dados-pessoais-e-os-data-brokers-20032019).

3.4. Manipulação informacional ou desinformação

A influência das *Big Techs* na sociedade proporciona acesso a ferramentas poderosas, mas também levanta preocupações sérias sobre o uso indevido de dados. A manipulação e venda de dados para operadores de desinformação são questões críticas. Esses dados podem ser explorados para influenciar eventos políticos, como eleições, podendo minar a integridade do processo democrático.

Os algoritmos alimentados por dados coletados pelas *Big Techs* têm o potencial de perpetuar sistemas de opressão. Se esses algoritmos são treinados com dados enviesados, refletindo desigualdades históricas, podem inadvertidamente ampliar e perpetuar essas disparidades. Por exemplo, algoritmos de recrutamento que favorecem candidatos com base em padrões históricos podem reproduzir preconceitos existentes.

As bolhas de filtro são o resultado do algoritmo de recomendação personalizada que apresenta aos usuários conteúdos com base em suas preferências anteriores. Embora isso possa aumentar a satisfação do usuário ao oferecer conteúdo relevante, também pode gerar uma bolha informativa, expondo-o apenas a perspectivas que reforçam suas crenças. Como consequência, a diversidade de informações pode ser reduzida, favorecendo a polarização de opiniões.

A análise preditiva também é explorada no contexto da desinformação, onde algoritmos podem ser usados para segmentar audiências específicas com informações enganosas ou distorcidas. Isso é particularmente preocupante em ambientes online, onde a desinformação pode se espalhar rapidamente, influenciando opiniões e decisões. O fenômeno das “bolhas de desinformação” ocorre quando os usuários são expostos principalmente a conteúdos que confirmam suas crenças, amplificando assim a disseminação de informações falsas.

Embora esses modelos ofereçam benefícios substanciais em termos de eficiência e personalização, também levantam questões éticas. A coleta e o uso extensivo de dados para fazer inferências podem resultar em decisões automatizadas que afetam a vida dos indivíduos, desde oportunidades de emprego até ofertas de crédito. Isso destaca a importância da transparência, justiça e equidade no desenvolvimento e aplicação desses modelos.

3.5. *Dark patterns*

Dark patterns, ou padrões sombrios ou escuros em português, diz respeito a técnicas de design utilizadas em plataformas digitais que buscam manipular o comportamento dos usuários online de maneira muitas vezes enganosa e prejudicial. Esses padrões são projetados para induzir os usuários a tomar decisões que podem não ser do seu melhor interesse, por meio de opções de consentimento confusas e que, muitas vezes, acabam resultando em ações que beneficiam a empresa ou plataforma que os emprega.

Certos *dark patterns* podem ser projetados para criar *nudges*⁷ enganosos que incentivam os usuários a realizarem compras adicionais ou a assinarem serviços. Essas táticas podem explorar a vulnerabilidade do usuário ou induzi-los a ações que não seriam tomadas de outra forma⁸.

O fornecimento de informações claras e abrangentes sobre o tratamento dos dados pessoais dos consumidores (o que inclui detalhes sobre a finalidade do processamento, categorias de dados envolvidas, identificação do controlador e possíveis compartilhamentos), bem como a sua liberdade de escolha são requisitos essenciais para que o consentimento possa ser considerado válido, nos termos da LGPD.

Pelo que se extrai das informações aqui expostas, a utilização de *dark patterns* representam exatamente o oposto disso. Essas estratégias

7 *Nudges* são estímulos ou sugestões que influenciam o comportamento das pessoas de maneira previsível, muitas vezes de maneira sutil. Na publicidade direcionada, esses nudges podem ser empregados para incentivar o consumo adicional. Por exemplo, ao mostrar ofertas personalizadas ou criar um senso de urgência, os consumidores podem ser incentivados a realizar compras impulsivas. Embora isso possa ser benéfico para os negócios, também levanta questões sobre a autonomia do consumidor e a manipulação comportamental.

8 São considerados *dark patterns*: obstrução, que envolve a criação de barreiras para dificultar a realização de ações desejadas pelo usuário, como tornar confuso o processo de cancelamento de assinaturas; desvio de atenção do usuário para elementos específicos, enquanto esconde informações cruciais. Pop-ups intrusivos e cores vibrantes são exemplos comuns; confusão, com utilização linguagem e layout confusos ou design enganoso para induzir o usuário a agir de forma indesejadas, como, por exemplo, compra não planejada de produtos adicionais; impedimento de escolha: desfavorecimento de escolha informada do usuário ao restringir as opções disponíveis, de forma a direcionar a tomada de decisões que favorecem a empresa e falsa urgência, ao pressionar o usuário a tomar decisões precipitadas, levando, muitas vezes, a manifestação de consentimentos não informados.

gias enganosas vão totalmente na contramão do conceito de privacidade por padrão, que preceitua a não exigência de qualquer ação por parte do titular para que este tenha a sua privacidade garantida.

A LGPD estipula que a privacidade deve ser parte integrante do *design* desde a concepção de produtos e serviços, reforçando a ideia de que a proteção de dados não deve ser uma reflexão tardia, mas sim um elemento fundamental desde a fase inicial de qualquer projeto.

3.6. Neuromarketing

O neuromarketing é uma disciplina que combina princípios de neurociência, psicologia e marketing para entender como o cérebro responde aos estímulos de marketing, como anúncios, embalagens de produtos e mensagens de marca, e como essas respostas podem influenciar o comportamento do consumidor. A ideia central por trás do neuromarketing é utilizar técnicas de neurociência, como ressonância magnética funcional, eletroencefalografia e *eye tracking*, para analisar as reações cerebrais e padrões de atividade neural.

Uma ênfase importante no neuromarketing é a de identificar padrões cerebrais associados a diferentes emoções e analisar como essas emoções podem influenciar as decisões de compra dos consumidores. O neuromarketing ajuda a adaptar mensagens e estratégias para maximizar o impacto em grupos específicos. Ao entender melhor as preferências e respostas individuais, as empresas podem personalizar suas abordagens de marketing para diferentes segmentos de consumidores.

No entanto, a evolução das neurotecnologias tem levantado preocupações no que concerne à potencial violação de privacidade dos dados cerebrais e a necessidade de regulamentação desse tratamento.

No contexto do neuromarketing, há uma preocupação legítima de que essas tecnologias atuem no subconsciente das pessoas, antecipando desejos que elas próprias ainda não reconheceram. E essa realidade não está distante. Um exemplo disso é uma interface cérebro-computador (BCI), ainda em fase de testes, desenvolvida por cientistas

na Califórnia, nos Estados Unidos. Criada para ajudar pacientes com danos neurológicos a recuperar a fala, essa tecnologia já conseguiu decodificar palavras a uma velocidade de até 62 por minuto.

Tudo isso fez surgir um movimento de proteção dos chamados *neurorights* (direitos neurais ou neurodireitos), que já estão sendo tutelados no Chile, primeiro país a contemplar o assunto em sua Constituição, em 2021. No Brasil, está em trâmite A PEC dos Neurodireitos (PEC 29/2023), que propõe a alteração da Constituição para incluir, entre os direitos e garantias fundamentais dos brasileiros, “a proteção à integridade mental e à transparência algorítmica.

Além disso, A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em dezembro de 2019, traçou nove princípios globais sobre as recomendações a respeito das inovações em neurotecnologia, dentre eles a proteção de dados cerebrais pessoais e outras informações⁹.

Em resumo, o neuromarketing é uma abordagem inovadora que utiliza insights da neurociência para compreender e influenciar o comportamento do consumidor. No entanto, seu uso levanta considerações éticas e requer uma abordagem responsável para garantir o respeito pelos direitos e privacidade dos consumidores.

4. CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados (LGPD) trouxe transformações significativas para o marketing digital no Brasil, impondo novas exigências e desafiando profissionais e empresas a repensarem suas es-

9 1. Promover a inovação responsável; 2. Priorizar a avaliação de segurança; 3. Promover a inclusão; 4. Promover a colaboração científica; 5. Permitir a deliberação social; 6. Habilitar a capacidade de supervisão e órgãos consultivos; 7. Proteger dados cerebrais pessoais e outras informações; 8. Promover culturas de administração e confiança nos setores público e privado; 9. Antecipar e monitorar o uso não intencional e/ou uso indevido potencial. Disponível em OECD. Recommendation on Responsible Innovation in Neurotechnology. <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>.

estratégias de coleta, uso e tratamento de dados. As mudanças necessárias não são apenas de natureza técnica ou legal, mas também ética, exigindo uma nova postura em relação à privacidade e ao consentimento dos usuários.

As empresas que se adaptam rapidamente e incorporam os princípios da LGPD em suas operações ganharão uma vantagem competitiva, melhorando a confiança e a fidelidade do cliente. O marketing digital, portanto, deve evoluir para ser mais transparente, responsável e centrado no usuário, alinhando-se não apenas com as normativas legais, mas também com as expectativas crescentes dos consumidores por maior controle sobre seus dados pessoais.

Por fim, este artigo sublinha a importância de uma abordagem proativa e inovadora no marketing digital diante da LGPD, enfatizando que a adaptação a essas mudanças é uma oportunidade para as empresas reforçarem seu compromisso com a ética e a transparência, proporcionando, assim, um valor agregado significativo à sua marca e serviços.

REFERÊNCIAS

MCKINSEY. **Pesquisa sobre excelência dos CEOs**, <https://www.mckinsey.com/featured-insights/destaques/os-planos-de-acao-dos-melhores-ceos-para-2023/pt> nos de ação dos melhores CEOs para 2023 | McKinsey.

FRAZÃO, Ana. **A indústria dos dados pessoais e os data brokers. Reflexões sobre os riscos da atuação de tais agentes no mercado de dados pessoais**. Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-industria--dos-dados-pessoais-e-os-data-brokers-20032019>.

OECD. **Recommendation on Responsible Innovation in Neurotechnology**. <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>.

