Organizadora:
Leide Jane Macedo Da Silva

Coordenadores:
Ana Paula Dos Santos, Anderson Eduardo Pereira, Angélica Maria Dos Santos Costa, Breno Letayf Campos
Fernanda Alves Miranda Moreira, Fernanda Maria Dos Reis, Juliana Capobiango De V. De Barros
Mariana Krollmann Fogli, Melissa Barrioni E Oliveira, Stella Muniz Campos Elias

Perspectivas sobre a Proteção de Dados

com ênfase nos desafios da advocacia

OAB MINAS GERAIS | Comissão de Proteção de Dados

EXPERT EDITORA DIGITAL

O presente livro visa compartilhar conhecimento entre advogados e oferecer suporte diante dos desafios relacionados à proteção de dados. Os textos não apenas distribuem informações, mas também procuram capacitar os advogados para enfrentar questões importantes na sociedade.

A Lei Geral de Proteção de Dados Pessoais nº 13.709/18 (LGPD) tem se tornado central para a comunidade jurídica, exigindo a assistência de especialistas devido à sua complexidade e interação com outras leis e regulamentos.

O livro reúne artigos de especialistas e advogados experientes que abordam a aplicação da LGPD em diversas áreas do Direito, incentivando os leitores a refletir e fazer perguntas.

Além de ser uma obra de referência, oferece uma análise detalhada e uma fonte de inspiração para a compreensão e implementação da LGPD, abordando desde conceitos fundamentais até questões práticas de responsabilidade civil, direito digital e aplicação da lei no setor público e privado.

O texto encerra destacando que o ambiente digital reflete as culturas sociais e convida os leitores a uma leitura envolvente e esclarecedora.

Boa leitura!

Patrocinadores

Apoiadores

ISBN 978-65-6006-075-3

Perspectivas sobre a Proteção de Dados

com ênfase nos desafios da advocacia

Direção Executiva: Luciana de Castro Bastos
Direção Editorial: Daniel Carvalho
Diagramação e Capa: Editora Expert
Revisão: Do Autor
A regra ortográfica usada foi prerrogativa do autor

Dados Internacionais de Catalogação na Publicação (CIP)
SILVA, Leide Jane Macedo Da (Org.)
Titulo: Perspectivas sobre a Proteção de Dados com ênfase nos desafios da advocacia - Belo Horizonte - Editora Expert - 2024
Organizadora: Leide Jane Macedo Da Silva
Coordenadores: Ana Paula Dos Santos, Anderson Eduardo Pereira, Angélica Maria Dos Santos Costa, Breno Letayf Campos
Fernanda Alves Miranda Moreira, Fernanda Maria Dos Reis, Juliana Capobiango De V. De Barros Mariana Krollmann Fogli, Melissa Barrioni E Oliveira, Stella Muniz Campos Elias
ISBN: 978-65-6006-075-3
Modo de acesso: https://experteditora.com.br
1.Direito Digital
2.Lei Geral de Proteção de dados pessoais
3.Responsabilidade Civil
I. I. Titulo.
CDD: 340.0285

Pedidos dessa obra:

experteditora.com.br
contato@editoraexpert.com.br

EXPERT
EDITORA DIGITAL

Patrocínio:
Ordem Dos Advogados Do Brasil
Seção Minas Gerais - OAB/MG

Presidente:
Sérgio Rodrigues Leonardo

Vice-Presidente:
Angela Parreira De Oliveira Botelho

Secretário Geral:
Sanders Alves Augusto

Secretário Geral Adjunto:
Cassia Marize Hatem Guimarães

Tesoureiro:
Fabrício Souza Cruz Almeida

Tesoureiro Adjunto:
Marco Antonio Oliveira Freitas

Diretor Institucional:
Romulo Brasil De Avelar Campos
Wagner Antonio Policeni Parrot

Diretor De Apoio As Subseções:
Alvaro Guilherme Ribeiro Matos

Diretor De Prerrogativas:
Ercio Quaresma Firpe

Diretor De Interiorização:
Bernardo Carvalho Brant Maia
Marcio Facchini Garcia
Rodrigo Carvalho Fernandes Martins Ribeiro

Diretor De Inclusão:
William Dos Santos

Comissão De Proteção De Dados OABMG
Presidente Da Comissão Proteção De Dados:
Melissa Barrioni E Oliveira

Vice-Presidente Da Comissão
De Proteção De Dados:
Stella Muniz Campos Elias

Diretora Do Núcleo De Estudo, Pesquisa E
Extensão Da Comissão De Proteção De Dados:
Leide Jane Macedo Da Silva

Livro: Perspectivas Sobre A Proteção De
Dados Com Ênfase Nos Desafios Da Advocacia

Organizadora:
Leide Jane Macedo Da Silva

Coordenadores:
Ana Paula Dos Santos
Anderson Eduardo Pereira
Angélica Maria Dos Santos Costa
Breno Letayf Campos
Fernanda Alves Miranda Moreira
Fernanda Maria Dos Reis
Juliana Capobiango De Vasconcellos De Barros
Mariana Krollmann Fogli
Melissa Barrioni E Oliveira
Stella Muniz Campos Elias

Apoio De Coordenação:
Nathália Sant'Ana Policarpo
Yulha Dos Santos Nunes

Revisão Ortográfica:
Edson Braz Carvalho Cruz
Jornalista Graduado Na UFMG. Especialista
Em Revisão De Textos Pelo Instituto De
Educação Continuada (Iec) Puc Minas.

APRESENTAÇÃO

O presente livro visa compartilhar conhecimento entre advogados e oferecer suporte diante dos desafios relacionados à proteção de dados.

Os textos não apenas distribuem informações, mas também procuram capacitar os advogados para enfrentar questões importantes na sociedade.

A Lei Geral de Proteção de Dados Pessoais nº 13.709/18 (LGPD) tem se tornado central para a comunidade jurídica, exigindo a assistência de especialistas devido à sua complexidade e interação com outras leis e regulamentos.

O livro reúne artigos de especialistas e advogados experientes que abordam a aplicação da LGPD em diversas áreas do Direito, incentivando os leitores a refletir e fazer perguntas.

Além de ser uma obra de referência, oferece uma análise detalhada e uma fonte de inspiração para a compreensão e implementação da LGPD, abordando desde conceitos fundamentais até questões práticas de responsabilidade civil, direito digital e aplicação da lei no setor público e privado.

O texto encerra destacando que o ambiente digital reflete as culturas sociais e convida os leitores a uma leitura envolvente e esclarecedora.

Boa leitura!

PREFÁCIO

O objetivo do livro "Perspectivas sobre a Proteção de Dados com ênfase nos desafios da advocacia", elaborado pelos membros da Comissão de Proteção de Dados da OAB/MG e coordenado pelo Núcleo de Pesquisa e Extensão da Comissão, é reunir e disseminar conhecimento entre os advogados. Mas os textos são mais do que apenas distribuidores de materiais; eles buscam amparar a advocacia nos desafios enfrentados ao tema, buscando inspirar os leitores a pensar criticamente sobre os assuntos que repercutem com grande importância na sociedade.

Como será explicado nos artigos do livro, a Lei Geral de Proteção de Dados Pessoais nº 13.709/18, ou LGPD, tem ganhado destaque e significado para a comunidade jurídica em sua totalidade. Embora a maioria das pessoas e empresas trabalhem para cumprir os regulamentos, frequentemente se deparam com outras leis, resoluções, padrões internacionais e até mesmo com a Constituição Federal brasileira, necessitando da assistência de especialistas jurídicos.

À medida que exploramos o complexo ambiente jurídico da Lei Geral de Proteção de Dados - LGPD do Brasil, prepare-se para uma viagem jurídica emocionante. Este livro é mais do que simplesmente uma coleção de artigos; é uma contribuição significativa para o domínio da proteção de dados que despertará o seu interesse e captará a sua atenção.

Iniciamos nossa pesquisa ao tema de Proteção de dados pessoais com a dedicação dos membros da Comissão de Proteção de Dados da OAB/MG, por meio do Núcleo de Estudo, Extensão e Pesquisa, que se dedicam a avançar no entendimento e refutar equívocos e dilemas comuns sobre o tema. Encorajamos você a investigar, considerar e fazer perguntas com este livro.

Os artigos desta coleção foram contribuídos por experientes advogados e demais profissionais de áreas comuns ao tema, que assumiram a tarefa de esclarecer peculiaridades e a relevância da

aplicabilidade da LGPD em diversas áreas do Direito. Ao navegar pelas páginas, você se aprofundará cada vez mais em questões jurídicas que transcendem as práticas consuetudinárias.

Queremos que você se junte a nós neste desafio, tire dúvidas, discuta e interaja com a Comissão de Proteção de Dados interagindo com o tema LGPD. Este livro é questionador, mas, para continuar avançando neste assunto em constante mudança, sua compreensão e envolvimento são cruciais.

Tendo tudo isso em mente, tenho certeza de que o leitor encontrará nos textos mais do que uma obra de referência, mais do que uma análise extensa e competente, mais do que uma sistematização atualizada e minuciosa – um convite à contemplação, e a mais importante fonte de inspiração para a incansável e resoluta luta pela consagração da Lei Geral de Proteção de Dados tem sido inegavelmente sua eminente relevância no âmbito jurídico.

Por fim, tudo, desde as definições fundamentais do tema, responsabilidade civil e direito digital até o processamento de informações no setor público e privado, a função do responsável pela proteção de dados, a aplicação da LGPD e as dificuldades para colocá-la em prática, pode ser encontrado aqui.

Devemos ter em mente que o ambiente digital é, em última análise, uma representação das culturas sociais.

Espero, portanto, que todos tenham uma ótima leitura.

Melissa Barrioni e Oliveira

ORGANIZADORA:

Leide Jane Macedo da Silva

Advogada. Mestranda em Direito Privado PUC/MG. Especialista em Direito e Tecnologia pela Faculdade Arnaldo Janssen. Consultora em Privacidade, Proteção de Dados e Governança Corporativa. Data Protection Officer. Professora de Especialização em Direito PUC/MG. Diretora do Núcleo de Estudo, Pesquisa e Extensão da Comissão de Proteção de Dados OAB/MG. E-mail: leidemacedoadv@gmail.com

COORDENADORES

Ana Paula Dos Santos

Advogada. Doutoranda em Direito da Privacidade pela University of the Pacific School of Law, California (USA). Mestre em Negócios Transnacionais pela University of the Pacific School of Law, California (USA). Atualmente, escrevendo artigos em espanhol para D' primera mano magazine com foco em privacidade, crimes cibernéticos e como vítimas de crime podem acessar benefícios no Estado da Califórnia. Membro da Comissão de Proteção de Dados da OAB/MG.

Anderson Eduardo Pereira

Advogado. Bacharel em Direito pela Pontifícia Universidade Católica de Minas Gerais. Consultor em Direito Digital. Mestre e Especialista em Relações de Consumo, LGPD, *GDPR, CCPA* e *Compliance* em Proteção de Dados Pessoais/Corporativos (CPC-PD). Membro da Comissão de Proteção de Dados da Ordem dos Advogados do Brasil de Minas Gerais. Associado *EADPP* (*European Association of Data Protection Professionals*). Associado *AFCDP* (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*). *DPO* (*GDPR Data Protection Officer - University of Derby/Eng*).

Angélica Maria dos Santos Costa

Advogada, DPO na Fundação Gorceix. Pós-Graduada, MBA em Gestão Financeira, Controladoria e Auditoria pela FGV, MBA em Gestão Econômica de Recursos Minerais pelo B.I Internacional, Graduada em Direito pela UFOP, Graduada em Administração pela Faculdade de Administração de Itabirito – FUNJOB. Membro da Comissão de Privacidade e Proteção de Dados da OAB/MG.

Breno Letayf Campos

Advogado e bacharel em Direito pela Faculdades Integradas Vianna Junior. Pós-graduado em LGPD e GDPR pela Fundação Escola Superior do Ministério Público. Atuante no ramo de Direito Empresarial, Direito Digital e Privacidade e Proteção de Dados Pessoais. Secretário da Comissão de Direito Digital, Proteção de Dados e Propriedade Intelectual da OAB/MG da 4ª Subseção de Juiz de Fora e Membro da Comissão de Proteção de Dados da OAB/MG.

Fernanda Alves Miranda Moreira

Advogada. Bacharel em Direito pela Pontifícia Universidade Católica de Minas Gerais. Pós-graduada em Direito Digital, Gestão da Inovação e Propriedade Intelectual pela PUC-Minas. Pós-graduada em Lei Geral de Proteção de Dados e Direito Processual Civil. Membro da APDADOS - Associação Nacional dos Profissionais de Privacidade de Dados e da Comissão de Proteção de Dados da Ordem dos Advogados do Brasil de Minas Gerais.

Fernanda Maria dos Reis

Mestre em Direito e Inovação pela Universidade Federal de Juiz de Fora - UFJF. Professora Universitária. Pós-Graduada em Direito e Processo do Trabalho pela Universidade Estácio de Sá. Pós-Graduada em Direito Empresarial e Econômico pela Universidade Federal de Juiz de Fora - UFJF. Graduada em Direito pelas Faculdades Integradas

Vianna Júnior. Membro da Comissão de Proteção de Dados da OAB/MG.

Juliana Capobiango de Vasconcellos de Barros

Advogada. Graduada em Direito pela Pontifícia Universidade Católica de Minas Gerais, PUC-MINAS - Unidade São Gabriel, Pós-Graduada em Direito e Processo Civil pela PUC/MG e em Direito Digital, Lei Geral de Proteção de Dados e Compliance Trabalhista pela EMD – Escola Mineira de Direito. Membro da Comissão de Proteção de Dados da OAB/MG. Atuante no ramo de Direito do Trabalho, Direito Digital, Compliance, Privacidade e Proteção de Dados Pessoais.

Mariana Krollmann Fogli

Mestre em Direito pela Universidade Federal de Minas Gerais. Pós-Graduada em Direito de Empresa pela Pontifícia Universidade Católica de Minas Gerais. Advogada da Carvalho & Furtado Advogados, e-mail para contato marianakrollmann@hotmail.com.

Melissa Barrioni e Oliveira

Presidente da Comissão de Proteção de Dados da OAB/MG - triênio 2022/2024. Membro Consultora do Conselho Federal da OAB Nacional. Mestranda em Educação Tecnológica pelo CEFET/UFMG. Professora de LGPD da PUC-MG. Professora e Coordenadora da Pós-graduação em Proteção de Dados e Privacidade da ESA/MG e CEDIN. Palestrante. Especializada em LGPD e Proteção de Dados e Privacidade Licenciada em Letras em curso no Instituto Anima de Educação. Pós-graduada em Docência Jurídica e Direito Digital.

Stella Muniz Campos Elias

Advogada Empresarial. Mestra pelo Programa de Pós-Graduação stricto sensu em Direito da Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-Graduada em Direito do Trabalho e

Processo do Trabalho pela Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-graduada em Docência com Ênfase Jurídica. Advogada. Consultora e Especialista em Proteção de Dados. Consultora e Especialista em Proteção Trabalhista. Vice-presidente da Comissão de Proteção de Dados da OAB/MG. Membro do Programa e Comissão do Direito na Escola. Membro do Grupo de Pesquisa e Extensão Capitalismo e Proteção Social na Perspectiva dos Direitos Humanos e Fundamentais do Trabalho e da Seguridade Social.

APOIO DE COORDENAÇÃO

Nathália Sant'Ana Policarpo

Consultora em Proteção de Dados (LGPD). Advogada e Consultora com atuação em Direito Civil. Mestre em Direito pela Universidade Fumec. Especialista em Mediação e Solução de Conflitos pela Faculdade Arnaldo. Especialista em Direito Digital pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Direito de Empresa pelo Cad - Centro de Atualização em Direito. Membro da Comissão de Proteção de Dados da OAB/MG.

Yulha dos Santos Nunes

Consultora em Proteção de Dados (LGPD). Advogada e Consultora com atuação em Direito Civil. Especialista em Direito Civil e Processual Civil pelo Centro Universitário Newton Paiva. Graduada em Direito pelo Centro Universitário Newton Paiva. Curso de Extensão "Lei Geral de Proteção de Dados - Teoria e Prática" pela FGV - Fundação Getúlio Vargas. Curso de Extensão "Adequação a LGPD - Passo a passo", pela Ûdemy. Membro da Comissão de Proteção de Dados da OAB/MG. Membro da Comissão de Direito Condominial da OAB/MG – Subseção do Barro Preto.

REVISÃO ORTOGRÁFICA

Edson Braz Carvalho Cruz

Jornalista graduado na UFMG. Especialista em Revisão de Textos pelo Instituto de Educação Continuada (IEC) PUC Minas.

AUTORES

Anderson Eduardo Pereira

Ana Paula Dos Santos

Angélica Maria dos Santos Costa

Claudio Nunes dos Santos Maulais

Cristiane Duarte Ramalho

Fernanda Alves Miranda Moreira

Fernando Bartolomeu Mendonça Costa

Fernanda Araújo Couto e Melo Nogueira

Henrique Almeida Bazan

Mariana Krollmann Fogli

Plínio Hávila Oliveira Ribeiro

Poliane Almeida Silva Dias

Rafael Marques Silva

Samuel Costa de Jesus Ferreira

Samylle De Oliveira Ribeiro

Stella Muniz Campos Elias

Thamiris Mendes Galdino da Costa

SUMÁRIO

PROTEÇÃO DE DADOS PESSOAIS NA ERA TECNOLÓGICA: DESAFIOS E RESPONSABILIDADE CIVIL

PERSONAL DATA PROTECTION IN THE TECHNOLOGICAL ERA: CHALLENGES AND CIVIL LIABILITY

Angélica Maria dos Santos Costa
Fernando Bartolomeu Mendonça Costa

Angélica Maria dos Santos Costa[1]
Fernando Bartolomeu Mendonça Costa[2]

"Legislar sobre tecnologia é sempre uma atividade desafiadora e ingrata porque como toda legislação legisla sobre o passado, no caso da tecnologia é tudo mais rápido."
(Danilo Doneda)

RESUMO

Neste artigo, exploramos a intrincada paisagem da proteção de dados na era digital, realçando a preeminência das leis de proteção de dados, tais como a LGPD no Brasil e o GDPR na União Europeia. Analisamos o entrelaçamento entre a proteção de dados, a dignidade humana e a preservação da liberdade individual, com ênfase na importância da segurança cibernética na prevenção de violações de dados. Ademais, destacamos o crucial papel da responsabilidade civil das organizações e a necessidade do consentimento informado como base ética na administração de informações pessoais.

Palavras-chave: Segurança cibernética. Proteção de dados. Consentimento. LGPD - Lei Geral de Proteção de Dados. Marco Civil da Internet.

ABSTRACT

This article delves into the intricacies of data protection in the digital age, emphasizing the significance of data protection laws such as LGPD in Brazil and GDPR in the European Union. We explore the intersection of data protection, human dignity, and the preservation of individual freedom, with a spotlight on the importance of cybersecurity

1 Advogada, DPO na Fundação Gorceix. Pós Graduada, MBA em Gestão Financeira, Controladoria e Auditoria pela FGV, MBA em Gestão Econômica de Recursos Minerais pelo B.I Internacional, Graduada em Direito pela UFOP, Graduada em Administração pela Faculdade de Administração de Itabirito –FUNJOB.

2 Advogado, Pós graduando em Direito Ambiental, Minerário e Urbanístico pela PUC-MG, MBA em Licenciamento Ambiental pela UNA-BH. Graduado em Direito e História pela UNI-BH.

in preventing data breaches. Furthermore, we underscore the relevance of organizational civil liability and the necessity of informed consent as an ethical foundation for managing personal information.

Keywords: Cybersecurity. Data protection. Consent. LGPD (Lei Geral de Proteção de Dados - Brazilian data protection law). Marco Civil da Internet (Brazilian Internet Bill of Rights).

1. INTRODUÇÃO

Este artigo tem como objetivo examinar a proteção de dados pessoais na era tecnológica, considerando sua relação com a dignidade humana, a preservação da liberdade individual e a responsabilidade civil das organizações, em um contexto marcado por desafios complexos e ameaças à segurança cibernética. O propósito é fornecer uma visão detalhada sobre as questões relacionadas à proteção de dados pessoais na era digital, destacando sua relevância para a sociedade e a importância da responsabilidade civil na manutenção da segurança e privacidade dos dados.

Para alcançar esses objetivos, este artigo segue uma estrutura organizada. Inicialmente, apresenta uma introdução que enfatiza a importância do tema. Em seguida, explora a evolução do direito à privacidade e da responsabilidade civil. Posteriormente, a análise se aprofunda na esfera da segurança cibernética, explorando a interação entre a soberania digital, a responsabilidade civil e os investimentos em proteção de dados.

O artigo também aborda a importância das políticas de retenção de dados e do compartilhamento seguro de informações pessoais. Além disso, investiga a necessidade do consentimento informado como um alicerce ético na gestão de informações pessoais.

Na perspectiva das legislações de proteção de dados, o trabalho examina as leis de Proteção de Dados tanto do Brasil quanto da União Europeia, destacando as diretrizes rigorosas e as penalidades significativas associadas a elas. A Avaliação de Impacto sobre a Proteção

de Dados (AIPD) também é considerada como uma ferramenta valiosa nesse contexto.

O artigo discute a importância da conscientização e educação para criar um ambiente digital seguro. Finaliza com reflexões sobre a interconexão entre dignidade humana, segurança cibernética e responsabilidade civil na busca por uma efetiva proteção de dados. Em resumo, o objetivo principal deste artigo é proporcionar uma visão abrangente das questões críticas relacionadas à proteção de dados pessoais na era tecnológica.

2. VIOLAÇÕES DE DADOS: IMPACTOS NA PRIVACIDADE E NA SEGURANÇA CIBERNÉTICA

No cenário de 2023, testemunhamos uma ascensão alarmante nos custos associados às violações de dados, que agora atingem uma média global de US$ 4,45 milhões. Isso representa um aumento significativo de 15% em um curto período de três anos, conforme destacado no meticuloso relatório elaborado pela IBM[3] sobre ameaças e violações de dados. Além disso, o Breach Level Index (BLI) da renomada empresa de segurança digital Thales[4] identificou o erro humano como a principal causa por trás dessas violações de dados, lançando luz sobre a crescente importância da soberania digital e os complexos desafios enfrentados na proteção dos ambientes cibernéticos.

O crescimento exponencial na coleta, armazenamento e processamento de informações pessoais traz consigo questões cruciais relativas à salvaguarda dos direitos individuais, à dignidade humana e à ética subjacente ao tratamento de dados. É nesse contexto que este artigo se insere, destacando o papel crucial da proteção de dados na promoção da dignidade humana e enfatizando a responsabilidade civil das organizações. Paralelamente, concentramos nossas atenções

3 Relatório de custo de violação de dados de 2023. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em outubro de 2023

4 Relatório sobre ameaças de dados de 2023. Disponível em: https://cpl.thalesgroup.com/latam-data-threat-report#download-popup. Acesso em outubro de 2023

na necessidade do consentimento informado como alicerce ético fundamental na administração de informações pessoais.

Imagine a divulgação pública de dados pessoais pertencentes a mais de 100 milhões de contas de celular, incluindo informações, como números de telefone, detalhes de chamadas, Registro Geral (RG) e endereços. Essa não é uma conjectura hipotética, mas, sim, uma triste realidade, recentemente descoberta, que tem gerado apreensões generalizadas. Em 2020, enfrentamos um incidente semelhante no qual os Cadastros de Pessoas Físicas (CPF) de 223 milhões de pessoas, quer estejam vivas, quer tenham falecido, vazaram, suscitando justificados receios quanto ao seu uso em golpes e atividades criminosas.

O caso amplamente divulgado pela BBC News[5], referente ao megavazamento de dados, representa apenas um dos muitos exemplos que evidenciam os desafios inerentes à era digital. Tais incidentes estão longe de serem raros; na verdade, eles se apresentam como uma ameaça constante e persistente. As adversidades enfrentadas, tanto por indivíduos como por organizações na proteção de dados pessoais, resultam em violações que não afetam somente a privacidade e a segurança cibernética, mas também têm implicações legais substanciais. Compreender por que essas violações ocorrem e por que são tão difíceis de evitar reveste-se de importância crítica em nossa sociedade cada vez mais digitalizada.

À medida que os avanços tecnológicos seguem inabaláveis, emergem desafios significativos para a proteção de dados pessoais. À proporção que a tecnologia avança, o armazenamento e o processamento de informações pessoais não se configuram mais como uma escolha, mas, sim, como uma necessidade premente. No entanto, essa necessidade intrínseca traz consigo também riscos cibernéticos crescentes e ameaças latentes à privacidade.

A responsabilidade civil emerge como um pilar de destaque no âmbito da segurança e da privacidade dos dados pessoais, estabelecendo-se como um tema de extrema relevância. As

5 Como Mega vazamentos de Dados Acontecem? Disponível em https://www.bbc.com/portuguese/brasil-56031998. Acesso em outubro de 2023

legislações, como a Lei Geral de Proteção de Dados (LGPD)[6] no Brasil, o Regulamento Geral de Proteção de Dados ou General Data Protection Regulation (GDPR)[7] na União Europeia e as abordagens setoriais adotadas nos Estados Unidos, delineiam diretrizes cruciais para as organizações no tocante ao tratamento de dados pessoais. Nesse contexto, um requisito fundamental, que frequentemente é negligenciado, refere-se ao consentimento dos titulares de dados, que deve ser livre, informado e inequívoco, configurando-se como um requisito obrigatório para fins específicos de processamento.

A negligência no cumprimento dessas obrigações legais, por parte das organizações, acarreta o potencial de resultar em sua responsabilidade civil. Empresas que não adotam as medidas necessárias para proteger os dados pessoais que coletam e processam podem se encontrar no centro de ações judiciais por parte dos titulares de dados prejudicados, acarretando sérios danos financeiros e uma mancha irreparável em suas reputações. Assim, com vistas a reduzir os riscos de responsabilidade civil associados à proteção de dados, torna-se imperativo que as organizações adotem abordagens proativas, tais como investimentos em segurança cibernética, treinamento adequado, estrita conformidade com as regulamentações vigentes e pronta notificação às autoridades e aos titulares de dados em caso de violação.

3. RESPONSABILIDADE CIVIL: EVOLUÇÃO DO DIREITO À PRIVACIDADE DE DADOS

Com o passar do tempo, a concepção do direito à privacidade e da responsabilidade civil evoluiu, incorporando a proteção de dados pessoais como um componente integral. Inicialmente vinculado ao conceito de direito à privacidade, essa evolução é notável.

6 Lei 13.709/18

7 Regulamento Geral de Proteção de Dados da União Europeia

A trajetória que levou ao reconhecimento da proteção de dados pessoais como parte indissociável da privacidade e da responsabilidade civil teve seu marco em 1890. Nesse ano, o renomado artigo de Samuel D. Warren e Louis D. Brandeis, intitulado *The Right to Privacy*[8] (O Direito à Privacidade), publicado na *Harvard Law Review*, lançou os fundamentos legais para a consideração da privacidade como um direito fundamental. No entanto, a verdadeira transformação desse cenário ocorreu com o advento da era digital e da Internet, que trouxe consigo a explosão na coleta de dados pessoais.

Conforme observado por Sarlet[9], essa evolução se estendeu para abranger não apenas o direito à privacidade, mas também o direito à proteção de dados pessoais, especialmente no contexto da "intimidade informática."

Na era digital, a proteção de dados tornou-se imperativa devido à crescente dependência da tecnologia. Nossos dados pessoais estão constantemente vulneráveis, seja a organizações legítimas ou a indivíduos mal-intencionados. A coleta global de dados fornece informações detalhadas que são utilizadas para análises, publicidade direcionada e manipulação comportamental. No entanto, isso também traz consigo riscos cibernéticos substanciais, com as violações de dados expondo as pessoas a ameaças como fraudes e roubo de identidade, comprometendo um direito fundamental: a privacidade, que resguarda a liberdade e a dignidade da pessoa humana.

O direito à proteção de dados pessoais emerge como um direito fundamental e uma disciplina autônoma, como sustentado por Doneda[10]. Sua base legal não decorre de uma disposição direta, mas da necessidade premente de proteger a personalidade, a igualdade, a liberdade, a dignidade, a intimidade e a vida privada, sobretudo à luz dos riscos inerentes ao tratamento automatizado de dados. Esse direito

8 The Rihght to PRivacy, disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em outubro de 2023

9 SARLET, Ingo Wolfgang. 2013, p. 418

10 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em outubro de 2023

surgiu na era da informação e, à medida que os avanços tecnológicos conferiram poder aos detentores de informações, tornou-se uma disciplina que complementa o direito à privacidade, abrangendo aspectos para além do seu escopo tradicional. Esse reconhecimento como um direito fundamental precedeu a promulgação da LGPD brasileira, conforme ressaltado por Doneda e enfatizado na Declaração de Santa Cruz de La Sierra[11], assinada pelo governo brasileiro em novembro de 2003. Essa declaração realça a importância das iniciativas regulatórias para proteger a privacidade dos cidadãos.

O GDPR europeu reconhece a "proteção de pessoas singulares"[12] como um direito fundamental. Embora a LGPD brasileira não faça uma declaração explícita nesse sentido, a Emenda Constitucional nº 115/2022, incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais fixando a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. A interpretação do artigo 2º, ainda sugere uma equivalência, uma vez que seus princípios[13] incluem o respeito à privacidade, a autodeterminação

11 Declaração de Santa Cruz de la Sierra, novembro de 2003. Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em outubro de 2023

12 Item 1 dos "Considerandos" do Regulamento (UE) 2016/679 –Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR)

13 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

informativa, a liberdade de expressão, a inviolabilidade da intimidade, o desenvolvimento econômico e tecnológico, a livre iniciativa, a livre concorrência, a defesa do consumidor e os direitos humanos. O fundamento essencial subjacente a esses princípios é a dignidade da pessoa humana, um princípio fundamental com impacto direto nos direitos dos cidadãos no contexto jurídico brasileiro.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), inspirada no GDPR, foi promulgada em 2018 e entrou em vigor em 2020. O cerne da proteção de dados, conforme estabelecido no artigo 2º, VII, da LGPD, é a dignidade da pessoa humana. Esse princípio também é um dos fundamentos essenciais da República Federativa do Brasil, como previsto no artigo 1º, Inciso III, da Constituição Federal. A força normativa da dignidade da pessoa humana desempenha um papel crucial no campo jurídico, influenciando diretamente a compreensão e aplicação dos direitos fundamentais dos cidadãos.

A proteção de dados pessoais está intrinsecamente relacionada ao conceito de dignidade, como argumentado por Soares[14]. Ela reconstrói a aplicação dos direitos fundamentais no sistema jurídico brasileiro, promovendo o direito justo. A dignidade da pessoa humana serve como base para interpretar e integrar o ordenamento jurídico, proporcionando estrutura e coesão.

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

14 SOARES, Ricardo Maurício Freire. O Discurso Constitucional da Dignidade da Pessoa Humana: uma proposta de concretização do direito justo no pós-positivismo brasileiro.
Salvador: UFBA, 2008. Disponível em: http://www.bibliotecadigital.ufba.br/tde_busca/arquivo.php?codArquivo=1918. Acesso em: 29 set. 2023.

Takana[15] destaca que a dignidade é inerente à pessoa desde o nascimento e a relaciona ao direito à proteção de dados, evitando que a pessoa seja tratada como mero objeto. A Constituição declara a dignidade como o princípio orientador na aplicação e proteção de todos os direitos fundamentais, promovendo o bem-estar de todos e garantindo a verdadeira igualdade.

A responsabilidade civil desempenha um papel crucial na proteção dos direitos de privacidade de dados. As organizações que coletam e processam informações pessoais têm a obrigação legal e ética de fazê-lo de maneira responsável e segura. Quando ocorrem violações de dados, as vítimas têm o direito de buscar reparação e compensação por danos sofridos. Mais importante que definir a dignidade da pessoa humana e a proteção de dados é compreender seu propósito subjacente na lei: resguardar os dados pessoais como um fim em si mesmo, não como um meio. A proteção de dados pessoais sensíveis proíbe a redução dessas informações a meros objetivos comerciais, estendendo-se como uma extensão do próprio indivíduo. O direito à proteção de dados pessoais tem raízes no princípio constitucional da intimidade, embora esteja relacionado, mas distinto, da privacidade, abordando aspectos únicos da vida individual e protegendo direitos individuais.

A intimidade desempenha um papel crucial no contexto psíquico, relacionando-se com a identidade pessoal e a singularidade de cada indivíduo. A intimidade e a privacidade, embora frequentemente confundidas, são distintas e complementares no contexto dos direitos individuais e da proteção de dados pessoais. Ambos desempenham um papel fundamental na preservação da dignidade da pessoa humana e na garantia de que cada indivíduo possa viver de acordo com sua própria identidade e valores.

Bittar[16], em suas análises, define o direito à intimidade como tendo um núcleo próprio, distinguindo-o de outros direitos. Esse direito geral à intimidade abrange particularidades, como a imagem,

15 TAKANA, Sônia Yuriko Kanashiro.2015. p.14.

16 BITTAR, Carlos Alberto. 2023

o segredo e a privacidade. Ele protege aspectos íntimos da vida de uma pessoa, compreendendo sua residência, família e correspondência, destacando a importância de preservar essas áreas específicas da vida de um indivíduo, como sua consciência, espaço doméstico, família e correspondência.

Essa perspectiva reflete a compreensão geral de que o direito à intimidade abrange várias dimensões da vida pessoal, reconhecendo a complexidade da esfera privada e a necessidade de proteger diferentes aspectos para preservar a dignidade humana e a autonomia individual. A visão de Bittar está em conformidade com interpretações convencionais desse direito.

Mais amplo do que o simples consentimento, o princípio da autodeterminação informativa aborda o direito das pessoas de controlar suas informações pessoais, incluindo a decisão sobre a coleta, uso e compartilhamento dessas informações. O consentimento, por sua vez, é uma prática específica para implementar esse princípio, permitindo que as pessoas tomem decisões informadas sobre seus dados. Ambos são cruciais para proteger a privacidade e os dados pessoais, especialmente no contexto das regulamentações de proteção de dados.

Em 1983, o Tribunal Constitucional Alemão[17] enfatizou a importância desse princípio ao destacar o risco de os cidadãos se tornarem meros objetos de informação em censos populacionais, caso não fossem tomadas medidas adequadas para proteger seus direitos. Na Alemanha, apesar da existência de um sistema de proteção de dados estabelecido desde a década de 1970, a aprovação de uma polêmica lei de recenseamento permitiu o processamento extensivo de informações pessoais. Esse cenário desencadeou críticas e várias contestações constitucionais, que destacaram a necessidade de abordar a responsabilidade civil em casos de violação de privacidade e proteção de dados. O Tribunal Constitucional Alemão tomou uma medida importante ao declarar essa lei inconstitucional, enfatizando

17 MARTINS. Leonardo.2016,p 56.

a necessidade de proteger a autodeterminação informativa e a privacidade dos cidadãos. Essa decisão serviu como um precedente relevante para a proteção de dados pessoais em censos populacionais, ressaltando a importância de implementar medidas apropriadas para garantir essa proteção e, consequentemente, a responsabilidade civil em casos semelhantes.

A autodeterminação informativa confere aos cidadãos controle e transparência sobre seus dados pessoais, evitando discriminação e perfis digitais invasivos. A responsabilidade civil cria um incentivo para que as organizações adotem medidas proativas a fim de prevenir violações de dados. A LGPD deve concentrar seus esforços na proteção do livre desenvolvimento da personalidade, na dignidade da pessoa humana e no princípio da autodeterminação informativa, assegurando o controle sobre informações pessoais e protegendo a privacidade e a liberdade em um ambiente tecnológico em constante evolução.

Nesse contexto, torna-se evidente que o direito à proteção de dados pessoais e sua interligação com a dignidade humana, a intimidade e a responsabilidade civil são componentes cruciais na paisagem complexa da era digital. A análise desses elementos fundamentais é essencial para entender as implicações éticas e legais da proteção de dados pessoais, bem como para avaliar a influência da segurança cibernética na prevenção de violações de dados e a importância do consentimento informado como base ética na administração de informações pessoais. É para aprofundar essas questões e seus desafios que este artigo se dedica.

4. PROTEÇÃO DE DADOS E RESPONSABILIDADE CIVIL NO ÂMBITO DA SEGURANÇA CIBERNÉTICA

A segurança cibernética, na era tecnológica, emerge como um pilar fundamental da preservação da dignidade humana e da proteção dos direitos individuais no cenário digital. Em um mundo onde a coleta e o processamento de informações pessoais ocorrem em larga escala, garantir a integridade, a confidencialidade e a disponibilidade

dos dados é uma responsabilidade inalienável. Este segmento do artigo explora a intrincada relação entre a proteção de dados e a segurança cibernética, destacando o papel da responsabilidade civil nesse contexto.

4.1. SOBERANIA DIGITAL E SEGURANÇA CIBERNÉTICA

A soberania digital emerge como um conceito crítico, assegurando a capacidade de controle de dados e infraestrutura de TI por nações e organizações. Tal controle não apenas se traduz na segurança dos dados, mas também salvaguarda princípios fundamentais da privacidade e da segurança nacional. Em uma época marcada por ameaças cibernéticas sofisticadas, a necessidade de treinamento em boas práticas de segurança cibernética torna-se premente.

Os desafios na proteção digital incluem a crescente sofisticação dos ataques cibernéticos, a complexa administração de identidades e acessos, bem como a conformidade com regulamentações em constante evolução.

4.1.1. RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS

No âmbito legal, a responsabilidade civil desempenha um papel fundamental. Ela implica que as organizações são legalmente obrigadas a preservar e proteger os dados pessoais que coletam e processam. Diante de uma violação de dados resultante de negligência ou falhas na segurança, essas organizações podem ser alvo de processos civis e encarar sérias repercussões legais.

4.1.2. INVESTIMENTO EM SEGURANÇA CIBERNÉTICA

Investir em segurança cibernética é imperativo, mesmo em tempos de crises financeiras. Essa medida é crucial para garantir a

confidencialidade, a integridade e a disponibilidade dos dados em um ambiente digital complexo e repleto de ameaças. Organizações renomadas, como a Verizon, Privacy Rights Clearinghouse, CISA, Europol e Kaspersky Lab, fornecem relatórios e estudos de casos reais, oferecendo valiosos insights sobre violações de dados e ampliando a compreensão das tendências em segurança cibernética. Tais fontes confiáveis desempenham um papel vital na orientação de ações proativas em prol da proteção de dados.

4.1.3. MEDIDAS CRUCIAIS PARA A SEGURANÇA DE DADOS: AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS (AIPD)

Medidas essenciais para garantir a segurança de sistemas e dados envolvem o uso de firewalls avançados para monitorar e controlar o tráfego de rede, a implementação de criptografia para proteger informações sensíveis, a restrição de acesso exclusivamente a pessoal autorizado por meio de autenticação multifator e senhas robustas, o monitoramento em tempo real para detectar atividades suspeitas, a manutenção de sistemas atualizados para evitar vulnerabilidades conhecidas, o treinamento em segurança cibernética, a realização de testes regulares para identificar vulnerabilidades, a implementação de sistemas de backup e recuperação de dados robustos, bem como o gerenciamento de identidades e permissões de acesso. Essas práticas estabelecem as bases essenciais para garantir a segurança dos dados pessoais.

No Brasil, um instrumento como a Avaliação de Impacto sobre a Proteção de Dados (AIPD)[18], tal como definida no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, não é explicitamente

18 Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. Disponível em: https://www.uc.pt/site/assets/files/475840/20181130_regulamento_798_2018_torna_publico_o_regulamento_1_2018_cnpd.pdf. Acesso: Outubro de 2023

mencionada na Lei Geral de Proteção de Dados (LGPD), a legislação nacional de proteção de dados pessoais.

A LGPD estabelece princípios e diretrizes gerais para o tratamento de dados pessoais, mas não fornece um quadro detalhado para a realização de AIPDs, que é um processo que ajuda as organizações a identificar, avaliar e mitigar os riscos associados ao tratamento de dados pessoais, garantindo a conformidade com as regulamentações de privacidade, como o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia.

A AIPD é especialmente relevante em situações em que o tratamento de dados envolve tecnologias inovadoras, categorias especiais de dados, decisões automatizadas, tratamento em grande escala, controle sistemático de dados pessoais, dados sensíveis, dados relacionados a titulares vulneráveis e quando o tratamento pode impedir os titulares de exercer seus direitos ou utilizar serviços contratuais. A AIPD ajuda a garantir que a organização compreenda os riscos associados ao tratamento de dados e tome medidas adequadas para proteger os direitos e liberdades das pessoas singulares.

Para incorporar um instrumento do tipo da AIPD no Brasil, o País pode considerar algumas abordagens, como:

a. Legislação de Proteção de Dados: O Brasil já possui uma lei de proteção de dados chamada Lei Geral de Proteção de Dados (LGPD). A LGPD estabelece diretrizes para o tratamento de dados pessoais e é em grande parte semelhante ao GDPR da União Europeia. O Brasil pode fortalecer a implementação da AIPD ao especificar, na legislação, as situações em que a avaliação de impacto sobre a proteção de dados é obrigatória, conforme definido no GDPR. Além disso, o órgão regulador de proteção de dados do Brasil, a Autoridade Nacional de Proteção de Dados (ANPD), pode fornecer orientações detalhadas sobre a realização da AIPD.

b. Conscientização e Educação: É fundamental conscientizar as organizações brasileiras sobre a importância da AIPD e fornecer orientação sobre como conduzi-la. A ANPD pode desenvolver diretrizes e oferecer treinamento para profissionais de proteção de dados e organizações.
c. Colaboração Internacional: O Brasil pode buscar colaboração e troca de informações com autoridades de proteção de dados de outros países, especialmente a União Europeia, que tem uma vasta experiência na implementação da AIPD.
d. Promoção de Melhores Práticas: A ANPD pode incentivar as organizações a adotar as melhores práticas em relação à AIPD, fornecendo reconhecimento e incentivos para aquelas que demonstram conformidade eficaz.

A incorporação da AIPD na legislação de proteção de dados e a promoção de boas práticas de conformidade ajudarão o Brasil a enfrentar desafios complexos relacionados à proteção de dados pessoais na era digital, garantindo a proteção dos direitos individuais e a conformidade com as regulamentações de privacidade.

A Avaliação de Impacto sobre a Proteção de Dados (AIPD) é um processo fundamental na proteção de dados pessoais, particularmente em cenários em que o tratamento de dados apresenta riscos significativos para os direitos e liberdades das pessoas singulares. A AIPD envolve a avaliação criteriosa de como os dados pessoais são coletados, processados e utilizados, identificando potenciais riscos e adotando medidas para mitigá-los.

A incorporação da AIPD no Brasil pode ser realizada por meio da legislação, estabelecendo requisitos claros para a realização de AIPDs em situações específicas, como aquelas envolvendo tecnologias inovadoras, categorias especiais de dados ou tratamentos em grande escala. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) pode desempenhar um papel fundamental na orientação e promoção de boas práticas relacionadas à AIPD. O Brasil pode se beneficiar ao

aprender com a experiência da União Europeia no que diz respeito ao GDPR e adaptar essas práticas para garantir a conformidade e a proteção dos direitos individuais em sua própria jurisdição.

4.1.4. POLÍTICAS DE RETENÇÃO DE DADOS E COMPARTILHAMENTO

Adicionalmente, é de extrema importância estabelecer políticas claras de retenção de dados, as quais asseguram que informações pessoais não sejam mantidas indefinidamente, mas, sim, sejam descartadas de acordo com as regulamentações aplicáveis.

No caso de compartilhamento de dados com terceiros, é imperativo monitorar e garantir que esses terceiros adotem medidas de segurança apropriadas. A presença de um plano de resposta a incidentes é crucial para agir rapidamente no caso de uma violação de dados, minimizando os danos e cumprindo as obrigações legais de notificação.

4.1.5. FONTES E REFERÊNCIAS

Todas essas medidas de segurança cibernética se baseiam em práticas recomendadas, amplamente aceitas na área de segurança de dados e tecnologia da informação. Elas não são retiradas de uma fonte específica, mas representam conhecimentos e orientações gerais comumente aceitos na comunidade de segurança cibernética e tecnologia. A "Estratégia Nacional de Segurança Cibernética"[19], disponível no site do Governo Federal, é uma referência relevante que respalda essas práticas.

Na era digital, a segurança cibernética e a conformidade regulatória são questões cruciais para as organizações. Diante do

19 Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.gov.br/gsi/pt-br/dsic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf. Acesso em outubro de 2023

surgimento constante de novas ameaças cibernéticas e da imposição de regulamentações cada vez mais rigorosas, a adaptação e agilidade das organizações se tornam imperativas. A soberania digital surge como um componente essencial nesse contexto, desempenhando um papel crítico na proteção dos ativos digitais e na capacidade de enfrentar desafios complexos, como ataques sofisticados. Portanto, garantir a segurança cibernética e cumprir as regulamentações exige uma abordagem diligente e proativa por parte das organizações.

5. CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS: UM DESAFIO OU UM PILAR DA PRIVACIDADE NA ERA DIGITAL?

O consentimento é um dos princípios fundamentais no contexto da proteção de dados pessoais, desempenhando um papel de destaque na garantia da privacidade e na salvaguarda dos direitos individuais em uma era cada vez mais digitalizada. No Brasil, a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet[20] estabelecem diretrizes essenciais para a coleta e tratamento de informações pessoais, com ênfase no consentimento.

O consentimento, conceitualmente, é a pedra angular sobre a qual repousa a gestão ética e legal de informações pessoais em um mundo cada vez mais conectado. Essencialmente, representa a expressão voluntária de um indivíduo concordando com a coleta, processamento e uso de seus dados pessoais. Essa noção básica de escolha individual deve ser a base de muitas leis de proteção de dados em todo o mundo.

É importante ressaltar que os dados pessoais podem variar de públicos a sigilosos. Alguns dados, como registros de propriedade imobiliária, são públicos e de acesso geral, enquanto informações médicas, orientação sexual, crenças religiosas e dados financeiros

20 Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em outubro de 2023

são consideradas sensíveis e recebem maior proteção sob as leis de proteção de dados.

No entanto, embora o consentimento seja vital, sua implementação prática enfrenta desafios significativos. Um desses desafios é o consentimento informado. Com frequência, os titulares de dados são apresentados a longos e complexos termos de serviço ou políticas de privacidade, que raramente são lidos integralmente. Isso levanta questões sobre a eficácia do consentimento quando os indivíduos não compreendem plenamente as implicações de suas escolhas.

O consentimento é, portanto, uma peça fundamental nas leis de proteção de dados, exigindo que organizações obtenham o consentimento informado, específico e voluntário dos titulares de dados antes de coletar, processar ou compartilhar seus dados pessoais. No entanto, o consentimento não é a única base legal para o processamento de dados, já que a lei pode permitir o processamento sem consentimento em situações específicas, como cumprimento de obrigações legais ou proteção de interesses vitais e funções de interesse público.

Do ponto de vista tecnológico, a gestão do consentimento também é complexa. Sistemas e processos precisam ser implementados para rastrear e gerenciar as preferências de consentimento dos titulares de dados de maneira eficaz.

Grossi[21] destaca a relevância do conceito de interesse legítimo do controlador de dados pessoais, principalmente à luz da Lei Geral de Proteção de Dados (LGPD) no Brasil. Ele explora como esse conceito pode ser aplicado quando não há consentimento direto do titular dos dados, enfatizando a necessidade de que o interesse legítimo não entre em conflito com os direitos individuais do titular.

Ele defende que o interesse legítimo do controlador deve estar alinhado com a boa-fé objetiva, seus deveres e os princípios da LGPD. Qualquer medida que prejudique as expectativas do titular pode ser

21 GROSSI, Bernardo Menicucci. 2020

considerada um abuso de direito, mesmo na ausência de dolo ou culpa, resultando em um ato ilícito.

A validade do consentimento exige que seja livre, informado, inequívoco e com uma finalidade específica. O titular deve decidir conscientemente, sem pressões externas, se deseja compartilhar seus dados e para qual finalidade. As informações fornecidas devem ser claras e compreensíveis, assegurando que o titular compreenda completamente as implicações de seu consentimento.

No entanto, a aplicação prática dos princípios de proteção de dados enfrenta desafios devido à crescente vulnerabilidade dos usuários online e aos avanços tecnológicos. Além da importância do consentimento na proteção de dados pessoais, é essencial reconhecer a complexidade das relações assimétricas, onde uma das partes possui maior poder ou influência. Nestes cenários, a obtenção do consentimento pode ser desafiadora e suscitar questões éticas quanto à verdadeira liberdade de escolha dos titulares de dados. Além disso, a legislação em muitas jurisdições permite o processamento de dados pessoais sem consentimento em determinadas circunstâncias, com base em outras bases legais, como o cumprimento de obrigações legais ou a proteção de interesses vitais e funções de interesse público. Essa preferência dada a outras bases legais ressalta a necessidade de uma análise mais aprofundada sobre como o consentimento se encaixa em um panorama mais amplo de regulamentações de proteção de dados e como ele pode ser adaptado de maneira eficaz em diferentes contextos.

A tecnologia oferece conveniência, facilidades e praticidade, mas também possibilita a coleta massiva de dados pessoais sem consentimento, impactando a privacidade e a liberdade individual.

Nesse contexto, as empresas devem adotar práticas transparentes e éticas de coleta de dados, respeitando o consentimento. A conscientização dos indivíduos sobre seus direitos é crucial para preservar a privacidade e a dignidade na era digital. A proteção de dados é vital para a privacidade, segurança e liberdade em um mundo

tecnológico, como evidenciado pelas regulamentações, como LGPD e GDPR.

A GDPR, em vigor desde 25 de maio de 2018, substituiu a Diretiva de Proteção de Dados da União Europeia de 1995, modernizando e fortalecendo as regras de proteção de dados para se adequar à era digital e aumentar a proteção e a privacidade dos dados, com regras mais rígidas e penalidades severas.

A GDPR introduziu na Europa penalidades substanciais, com multas que podem chegar a €20 milhões de Euros ou 4% da receita anual da organização. Exemplos, os casos emblemáticos, como as multas aplicadas à Google[22], Amazon[23] e Meta[24] na Europa, demonstram a seriedade com que essas regulamentações são cumpridas.

No Brasil, a ANPD aplicou sua primeira multa a uma microempresa de comunicação e multimídia, por várias infrações, incluindo a ausência de registro de operações e a não designação de um Encarregado de Proteção de Dados Pessoais. A Autoridade Nacional de Proteção de Dados (ANPD) também divulgou uma "Lista Negra"[25] de processos de fiscalização, cumprindo seu compromisso de transparência.

Todas essas regulamentações buscam equilibrar a inovação tecnológica com a proteção de direitos individuais, reconhecendo a necessidade de preservar a privacidade e a dignidade na era digital. A responsabilidade civil na proteção de dados torna-se crucial, exigindo medidas rigorosas de conformidade por parte das organizações para evitar consequências legais e danos à reputação. O consentimento

22 Notítcia de multa em desfavor de Google e Amazon. Disponível em: https://www.cartacapital.com.br/mundo/franca-multa-google-e-amazon-por-rastreamento-publicitario-abusivo/. Acesso em setembro de 2023

23 Idem

24 Notícia de Multa em desfavor da empresa META. Disponível em: https://exame.com/mundo/meta-recebe-multa-recorde-de-e-12-bilhao-por-violar-regras-sobre-dados-na-europa/. Acesso em setembro 2023

25 Lista de Processos administrativos ANPD. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-de-fiscalizacao-em-andamento. Acesso em setembro de 2023

informado é o alicerce fundamental da proteção de dados, tornando seu entendimento e aplicação essenciais na era tecnológica.

O desafio de tornar o consentimento mais acessível e eficaz persiste. Organizações e legisladores precisam continuar a aprimorar as práticas de obtenção de consentimento, tornando-as mais transparentes e compreensíveis. Os titulares de dados devem ser capacitados para tomar decisões informadas sobre o uso de suas informações pessoais.

Além disso, a conscientização sobre a importância do consentimento e da proteção de dados deve ser difundida, não apenas entre as organizações, mas também entre os cidadãos. Isso ajudará a criar um ambiente digital mais seguro e ético, onde a privacidade e a dignidade são respeitadas, mesmo na era da tecnologia avançada.

5.1 REFLEXÃO E PERSPECTIVA

O consentimento na proteção de dados pessoais desempenha um papel crítico na manutenção da privacidade, segurança e liberdade individual na era digital. As regulamentações, como a LGPD e a GDPR, estabelecem as bases para a obtenção de consentimento informado, voluntário e específico dos titulares de dados. No entanto, desafios práticos e tecnológicos persistem, especialmente em um cenário de constante avanço tecnológico.

A gestão transparente do consentimento, aliada à educação e conscientização dos cidadãos, é fundamental para superar esses desafios. As organizações devem adotar práticas éticas e responsáveis de coleta e processamento de dados, enquanto os legisladores devem continuar a aprimorar as diretrizes e regulamentos para garantir a proteção dos direitos individuais.

A proteção de dados é vital para a preservação da dignidade humana e da liberdade na era digital. Portanto, o consentimento informado não é apenas um desafio, mas um pilar essencial da

privacidade e da ética em um mundo cada vez mais conectado e dependente da tecnologia.

6. CONSIDERAÇÕES FINAIS

Este artigo proporcionou uma abordagem abrangente dos desafios que cercam a Proteção de Dados na era digital, sublinhando a constante ameaça das violações de dados e a necessidade premente de abordar esse tópico de maneira eficaz e proativa. As legislações como a LGPD no Brasil e o GDPR na União Europeia desempenham um papel central nessa jornada, com o consentimento informado dos titulares de dados emergindo como princípio fundamental.

A proteção de dados está inextricavelmente ligada à dignidade da pessoa humana, à preservação da liberdade e autonomia individuais, e à salvaguarda dos direitos individuais. Além disso, nossa exploração minuciosa revelou a intrincada relação entre a proteção de dados e a privacidade, destacando suas distinções e sinergias em relação aos direitos individuais.

A segurança cibernética, que abordamos, desempenha um papel crucial na prevenção de violações de dados. Ferramentas como criptografia e monitoramento em tempo real são componentes essenciais na defesa contra ameaças cibernéticas que podem comprometer a segurança dos dados.

Além dos desafios já mencionados, é fundamental ressaltar a importância de ferramentas como a europeia - Avaliação de Impacto sobre a Proteção de Dados (AIPD) - em contextos nos quais o tratamento de dados envolve soluções inovadoras e tecnologicamente avançadas, ou quando há um alto risco para os direitos e liberdades das pessoas singulares. A AIPD pode ser uma ferramenta valiosa para avaliar e mitigar os riscos associados ao tratamento de dados em situações complexas, como aquelas em que o consentimento informado é difícil de obter devido a longos termos de serviço ou políticas de privacidade. Portanto, a incorporação das ideias da AIPD nas práticas de proteção de dados no Brasil é relevante para também garantir que os direitos

individuais sejam adequadamente preservados, especialmente em cenários que envolvem categorias especiais de dados ou novas tecnologias.

Em resumo, a responsabilidade civil na proteção de dados emerge como um conceito fundamental que impõe obrigações éticas e legais rigorosas às organizações encarregadas de gerir informações pessoais. Seu objetivo primordial é assegurar a integridade dos direitos e da privacidade dos indivíduos, exigindo um tratamento adequado dos dados e promovendo a estrita conformidade com regulamentações, tais como o GDPR e a LGPD. Nessa perspectiva, incentiva abordagens proativas na prevenção de violações de dados, não apenas evitando consequências prejudiciais, como multas e danos à reputação, mas também fortalecendo a confiança dos clientes nas organizações.

Concluímos, portanto, que a dignidade da pessoa humana, juntamente com a segurança cibernética e a responsabilidade civil, são elementos interconectados e cruciais na busca da proteção eficaz de dados pessoais na era tecnológica.

REFERÊNCIAS

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais**: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com**,** Rio de Janeiro, v. 9, n. 3, p. 1-23, 22 dez. 2020. Disponível também em: <https://civilistica.emnuvens.com.br/redc/article/view/662>. Acesso em: ** set. 2023.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8 ed. São Paulo: Saraiva, 2015.

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

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: ** out. 2023.

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

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Estabelece Norma de Proteção e Defesa do Consumidor. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: ** out. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco da Internet. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: ** out. 2023.

CAPANEMA, Walter Aranha. **A responsabilidade civil da Lei Geral de Proteção de Dados**. Cadernos Jurídicos da Escola Paulista da Magistratura, São Paulo, 2021. Págs. 163-170. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/142288/responsabilidade_civil_lei_capanema.pdf>. Acesso em: ** set. 2023.

Comitê Gestor da Internet no Brasil. (2019). **Pesquisa sobre o uso das tecnologias da informação e comunicação nos equipamentos culturais brasileiros –TIC Cultura 2018**. São Paulo: CGI.br, 2019. Disponível em: <https://www.cetic.br/pt/tics/domicilios/2019/domicilios/A4/>. Acesso em ** out. 2023. . Disponível em: <https://www.cetic.br/pt/tics/domicilios/2019/domicilios/A4/>. Acesso em: ** out. 2023.

DECLARAÇÃO DE SANTA CRUZ DE LA SIERRA 2003. XIII Cimeira Ibero-Americana. **A inclusão social, motor do desenvolvimento da Comunidade Ibero-Americana**. disponível em: <https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>. Acesso em ** out. 2023.

DIVINO, Sthéfano Bruno Santos; DE LIMA, Taisa Maria Macena. **Responsabilidade Civil Na Lei Geral De Proteção De Dados BRASILEIRA**. Revista Em Tempo, v. 20, n. 1, 2020. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3229>. Acesso em: ** set. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. São Paulo: Thomson Reuters Brasil, 2019.

EUROPA. **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/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: **out. 2023.

GARCIA, Laura Rocha. AGUILERA FERNANDES, Edson. GONÇALVES, Rafael Augusto Moreno. PEREIRA BARRETO, Marcos Ribeiro. **Lei Geral de Proteção de Dados (LGPD) guia de implantação.** São Paulo: Blucher, 2020.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 15ª ed. São Paulo, Saraiva, 2014.

GROSSI, Bernardo Menicucci (Org.) **Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. Porto Alegre: Editora Fi, 2020. Disponível em: <https://www.editorafi.org/21dados>. Acesso em: ** set. 2023.

MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na sociedade da informação: profiling e risco de discriminação**. 2018. Dissertação (Mestrado em Direito) - Escola de Direito, PUC-RS, Porto Alegre, 2018.

MARQUES, Paula Cristina Mariano, FRANCISCO, José Carlos. **Marco civil da internet e responsabilidade civil na violação a direitos da personalidade**. 2015. Disponível em: <http://dspace.mackenzie.br/handle/10899/23874>. Acesso em ** out. 2023.

MARTINS. Leonardo. **Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais**. Volume 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung –KAS. 2016. p. 56.

REGULAMENTO n.º 1/2018 **Lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados**. Disponível em:<https://www.uc.pt/site/assets/files/475840/20181130_regulamento_798_2018_torna_publico_o_regulamento_1_2018_cnpd.pdf>. Acesso em ** out. 2023.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 2ª ed. São Paulo: Revista dos Tribunais, 2013, p. 418.

SOARES, Ricardo Maurício Freire. **O princípio constitucional da dignidade da pessoa humana.** São Paulo: Saraiva, 2009.

_____. **O Discurso Constitucional da Dignidade da Pessoa Humana**: uma proposta de concretização do direito justo no pós-positivismo brasileiro.UFBA, 2008. 277 f. Tese (Doutorado em Direito Público) - Faculdade de Direito. Universidade Federal da Bahia, Bahia, 2008, p. 179. Disponível em: <https://repositorio.ufba.br/handle/ri/10500>. Acesso em: ** out. 2023.

TANAKA, Sônia Yuriko Kanashiro. **Direito Constitucional**. São Paulo: Atlas, 2015, p. 104. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/7508283/mod_folder/content/0/7.O.1.%20PIERDON%C3%81.%20Z%C3%A9lia%20Luiza.%20Da%20Ordem%20Social%20parte%20I%20%E2%80%93%20Seguridade%20social.%202015.%20p.%20579-602.pdf?forcedownload=1>. Acesso em ** out. 2023.

ZANINI, Leonardo Estevam de Assis. **O surgimento e o desenvolvimento do right of privacy nos Estados Unidos**. Revista de Doutrina da 4ª Região, Porto Alegre, n.64, fev. 2015. Disponível em: <https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html>. Acesso em ** out. 2023.

TENSÕES GLOBAIS NA INTERFACE ENTRE PROTEÇÃO DE DADOS E INTERNET DAS COISAS

GLOBAL TENSIONS AT THE INTERFACE BETWEEN DATA PROTECTION AND THE INTERNET OF THINGS

Mariana Krollmann Fogli

Mariana Krollmann Fogli[26]

RESUMO

O trabalho analisa os desafios na promoção, em nível internacional, dos princípios da privacidade e da proteção de dados, ligados à dignidade da pessoa humana, quando se observa o progresso de tecnologias envolvidas na Internet das Coisas - IoT. Considerando a disputa geopolítica pelo domínio do fluxo de dados, com a rápida ascensão chinesa e a atuação americana no segmento, estuda-se os padrões de privacidade e de segurança dos Estados, tendo como pano de fundo vulnerabilidades, violações à privacidade e, ainda, a dependência regulatória e tecnológica de países menos desenvolvidos.

Palavras-Chave: Internet das Coisas. Proteção de Dados. Geopolítica

ABSTRACT

The work analyzes the challenges in promoting, at an international level, the principles of privacy and data protection, linked to human dignity, when observing the progress of technologies involved in the Internet of Things - IoT. Considering the geopolitical dispute over the domain of the data flow, as the rapid Chinese rise and the American performance in the follow-up, and security standards by the States are studied, with the background vulnerabilities, violations of privacy, and also the regulatory and technological dependence of less developed countries.

Keywords: Internet of Things. Data Protection. Geopolitics.

26 Mestre em Direito pela Universidade Federal de Minas Gerais. Pós-Graduada em Direito de Empresa pela Pontifica Universidade Católica de Minas Gerais. Advogada da Carvalho & Furtado Advogados, e-mail para contato marianakrollmann@hotmail.com.

Questões sobre a regulação Internacional. 5. Conclusão; Referências Bibliográficas.

1. INTRODUÇÃO

Os dados pessoais tornaram-se um ativo na era digital de fácil captação a partir do desenvolvimento das tecnologias envolvidas na Internet das Coisas e em face das interações pelos titulares de dados.

Acredita-se que a cada dia sejam gerados em torno de 2,5 trilhões de bytes de dados e que 90% dos dados da história do mundo tenham sido criados nos últimos anos[27]. O aumento do volume e dos formatos de dados impulsionou, sem dúvida, o desenvolvimento de ferramentas e tecnologias para gerar uma inteligência a partir de toda a informação que é disponibilizada e armazenada.

A capacidade analítica e em tempo real de processar dados estruturados e não estruturados converteu-se em uma competência-chave[28].

O emprego de aplicações de análise de dados para explorá-los, aumentando a riqueza da informação e do conhecimento que são capazes de proporcionar, popularizou-se no *termo Big Data* que, nascendo na indústria digital, passou a ser aplicada, para além do aspecto comercial e de marketing, em temas como segurança, a gestão de desastres, serviços de saúde ou em projetos de interesse públicos.

Efetivamente, os dados têm importância central para os Estados, tanto no campo da segurança e defesa nacional quanto nas estratégias comerciais e de concorrência econômica. Em adição a isso, a Internet das Coisas (*Internet of Things – IoT*) ganha papel de destaque na busca pela hiperconectividade e facilidade no acesso à informação, direcionando o cotidiano humano.

27 Disponível em: < https://itforum.com.br/noticias/tome-nota-2-5-quintilhoes-de-bytes-sao-criados-todos-os-dias/> Último acesso em 24 de outubro de 2023.

28 IBM. Big data beyond the hype: a guide to conversations for today's data center. McGraw-Hill Professional, 2014.

Nesse contexto, no presente trabalho tem-se a análise da possibilidade de harmonização dos interesses pessoais e econômicos gerados pela interface entre *IoT* e tratamento de dados pessoais, em um contexto de disputa e de monopólios de informações e de tecnologia.

O presente trabalho tem como tema nuclear as tensões geopolíticas envolvidas no domínio do fluxo de dados em relação aos principais detentores de dados na "*Era do Big Data*".

Ressalta-se que no artigo não se busca esgotar o tema, devido à sua complexidade e limitação de escopo, mas, sim, pretende contribuir para o debate recente da interface entre Internet das Coisas e tratamento de dados em massa.

Em uma sociedade movida a dados e com a presença cotidiana de tecnologias, ainda são poucos os trabalhos sobre o tema aplicados às relações internacionais e seus aspectos jurídicos, sendo fundamental sua compreensão para o avanço do campo, o que justifica a elaboração deste trabalho.

2. DADOS E INTERNET DAS COISAS

A partir do uso da internet como meio nas transações econômicas, novas práticas mercadológicas estão sendo incorporadas na era digital, a ponto de permitir se falar em novo estágio ou fase do capitalismo. Observa-se um novo modelo de negócio, baseado na vigilância de pessoas, para definir padrões de comportamento e induzi-las a orientações de consumo.

A internet das Coisas (*Internet of Thinghs – IoT*) pode ser considerada como uma das tendências atuais que impulsionam a Quarta Revolução Industrial[29], tendo como fundamento a confluência das tecnologias dos mundos digitais, físicos e biológicos[30]. Isso pois seria por meio da Internet das Coisas que se permite a agregação entre

29 SCHAWAB, K. A. Quarta Revolução Industrial. São Paulo: Edipro, 2017, p. 11.

30 FILHO, Adalberto Simão; SCHWARTZ. Big em tempos de internet das coisas. In: Direito, Tecnologia e Inovação. V.1. Coordenação de Leonardo Parentoni. Belo Horizonte: D´Plácido, 2019.

dispositivos conectados à Internet, propiciando controle remoto, automações e compartilhamento de informações.

A Internet das Coisas requer uma abrangente coleta e vinculação de dados do usuário para fornecer experiências cada vez mais personalizadas[31]. De fato, integração, facilidade e praticidade são princípios básicos da *IoT* e, assim, fundamental se faz um entendimento completo dos interesses daqueles que utilizarão os dispositivos, que ocorrerá por meio da análise de dados.

Isso é a identificação do usuário é essencial para a eficaz funcionalidade dos aparelhos envolvidos. Desse modo, a coleta e o tratamento de dados podem ser considerados um dos pilares da IoT.

Por muito tempo, em face da ausência de limites e diretrizes para suas operações, não só os dispositivos de *IoT*, mas toda a tecnologia em si, concentrou-se simplesmente em coletar informações de usuários e criar soluções a partir de tais dados, algo que, atualmente, passa a ser questionado em razão dos princípios da proteção de dados e privacidade, já positivados em legislações de alguns países.

Desse modo surge uma série de desafios a serem enfrentados, principalmente em relação ao compartilhamento e à transferência de dados pessoais em dispositivos de *IoT*, o que pode implicar inferências potencialmente invasivas[32].

Como se nota, os dados pessoais passam, então, a ser considerados elementos nucleares para o desenvolvimento político, social e econômico, principalmente diante da presença cada vez mais acelerada da tecnologia no cotidiano.

A facilidade de acessar dados pessoais, principalmente por meio de dispositivos *IoT*, é um campo fértil para a produção de uma quantia elevada de informações, até então inimaginável, no qual os dados passaram a ser processados e estruturados com todo tipo de finalidade,

31 WACHTER, Sandra. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. Computer Law & Security Review, 2016.

32 WACHTER, Sandra. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. Computer Law & Security Review, 2016.

com a apresentação de propostas individualizadas, experiências personalizadas, de acordo com os interesses demonstrados e, ainda, em tempo real.

Em síntese, quanto maior for o volume, a velocidade de processamento e a variedade de dados, maior é a capacidade de geração de valor (capital). Essa lógica abriu precedentes para um novo tipo de "indústria" que opera por meio do acúmulo e monetização de dados digitais.

A problemática se lança na vigilância constante que o titular dos dados se submete, sem permissão prévia e, até então, sem limites, refletidos na geração de dados estruturados ou não. Como possível efeito, discute-se eventual invasão da privacidade e da intimidade na tomada das decisões, que deveriam ser próprias do titular.

De fato, o uso de dados pessoais está intimamente ligado ao conceito de vigilância e, no contexto da IoT, traduz-se na verificação constante de usuários e suas interações com os dispositivos. A vigilância cumulada com os aspectos políticos, econômicos e comerciais envolvidos na análise de dados inaugura o chamado capitalismo de vigilância.

O capitalismo de vigilância, expressão cunhada por Shoshana Zuboff[33] para designar esse estágio da economia capitalista, é a consequência de uma nova lógica de acumulação de dados (*Big Data)*, e se traduz em uma *"nova forma de capitalismo da informação que procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado"*.

Os dados passam a ser vistos como os "ativos de vigilância", e os investimentos que esses ativos atraem são denominados de "capital de vigilância", conforme ensina Zuboff. O capitalismo da informação, que a autora reconhece como "capitalismo de vigilância", torna-se

33 ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F. et al. (orgs.). Tecnologias da vigilância: perspectivas da margem. Trad. H. M. Cardozo et al. São Paulo: Boitempo, 2018. p. 32

um modelo de negócios em que as rotineiras estimativas de valor dependem do monitoramento de informações pessoais[34].

Um dos efeitos colaterais desse capitalismo é o preço da privacidade. Por haver certa obscuridade dos mecanismos utilizados, principalmente diante da complexidade tecnológica, não é possível ter certeza da observância de garantias mínimas de dignidade da pessoa humana no que tange ao tratamento de dados pessoais, o que, de forma alguma, representa uma prática transparente e horizontal.

Em geral, o titular de dados, ao utilizar dispositivos conectados, não tem meios de conhecer todas as informações geradas por suas interações com a plataforma, nem de obter a certeza de que seus dados estão em segurança, tendo em vista a complexidade técnica envolvida na referida tecnologia.

Toda essa complexidade limita a compreensão dos usuários acerca dos riscos associados ao tratamento de dados pelos dispositivos.

Para fins de proteção de dados e responsabilização, é possível dizer que a estratégia regulatória, que consiste na promoção da transparência e da segurança da informação, está sujeita, no contexto da IoT, a diversas limitações, considerando compartilhamento de dados, a racionalidade limitada dos próprios usuários e os altos custos de transação associados à formulação de um consentimento informado, livre, inequívoco e específico.

O problema se agrava ainda mais quando se tem os dados pessoais categorizados como sensíveis, conforme faz a Lei Geral de Proteção de Dados do Brasil (Lei 13.709/2018 - LGPD)[35], em razão do elevado potencial lesivo no que tange, em especial, ao princípio da discriminação e da liberdade de autodeterminação informativa.

Diante desse contexto, é perfeitamente racional que as pessoas deixem de fazer boas avaliações dos riscos de privacidade e não gerenciem sua privacidade de forma eficaz, visando à rápida

34 ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F. et al. (orgs.). Tecnologias da vigilância: perspectivas da margem. Trad. H. M. Cardozo et al. São Paulo: Boitempo, 2018. p. 32

35 Art. 5º, inciso II e art. 11 da LGPD

comunicação e ao uso de bens e serviços com as mais diversas funcionalidades. Gerenciar a privacidade de uma pessoa é um projeto complexo e que não pode ser dimensionado em termos simples e práticos, sendo virtualmente impossível fazê-lo de forma abrangente.

Há uma realidade dinâmica em que haverá riscos nem sempre previsíveis e deveres acessórios que, no geral, não estarão previstos de forma expressa e compreensível para os usuários de dispositivos *IoT*.

Assim, a ausência de clareza acaba por desmantelar a ideia de autogerenciamento informativo, que pode ser proposital e, consequentemente, lesivo aos interesses coletivos de pessoas que não dispõem de instrumentos básicos para que possam exercer plenamente o controle e a proteção da vida privada e da dignidade da pessoa humana[36].

A cultura de vigilância normaliza as condutas abusivas dessa nova política econômica, dificultando a conscientização das pessoas quanto aos abusos praticados, principalmente quanto à extração e análise dos seus dados sem consentimento e sem observar a devida transparência, o que acarreta severas violações aos direitos fundamentais[37].

A falta de controle, somada ao desenvolvimento da tecnologia, com facilidades de captação de dados, está levando o capitalismo de vigilância a invadir, cada vez mais, a privacidade das pessoas que, por sua vez, entregam mais de seus dados comportamentais incondicionalmente.

Esse modelo de negócio se tornou um problema global e requer uma solução global. Aliás, o referido debate ultrapassa questões privadas e comerciais, envolvendo política, segurança, cybersegurança e disputas geopolíticas.

36 FOGLI, Mariana. Autogerenciamento da privacidade no acesso às redes digitais: comportamento dos usuários e a proteção legal dos dados pessoais e da privacidade. Tese de Mestrado. Universidade Federal de Minas Gerais, 2023.

37 FOGLI, Mariana. Autogerenciamento da privacidade no acesso às redes digitais: comportamento dos usuários e a proteção legal dos dados pessoais e da privacidade. Tese de Mestrado. Universidade Federal de Minas Gerais, 2023.

3. TENSÕES GLOBAIS E O MONOPÓLIO DA TECNOLOGIA E DA INFORMAÇÃO

A pressão global por inovação é acompanhada de incertezas jurídicas e práticas relacionadas ao tratamento de dados pessoais, que podem implicar o aumento das vulnerabilidades, violações à privacidade e, ainda, na dependência regulatória, econômica e/ou tecnológica de países menos desenvolvidos e/ou emergentes.

No Ocidente, são as grandes instituições privadas norte-americanas, sobretudo as *big techs*, as detentoras do desenvolvimento e pesquisa em *IoT* e B*ig Data*. Elas detêm os maiores datacenters mundiais e controlam a infraestrutura do fluxo de dados internacionais.

Ao objetivar o desenvolvimento pleno da tecnologia, tem-se como pano de fundo regulamentações abertas e não abrangentes no país americano, principalmente em relação à privacidade e proteção de dados. Com isso, as empresas norte-americanas adquiriram grande poder mundial, sendo capazes de exercer forte *lobby* na política do país e influenciar decisões a favor de seus interesses. Tal situação implica desafios para a promoção da proteção de dados pessoais em nível global, principalmente a partir de uma análise comparativa com a União Europeia.

Por sua vez, no Oriente, verifica-se a ascensão tecnológica chinesa e o progresso em aparelhos e sistemas voltados para o *IoT*, incluindo o monopólio na fabricação de chips. Atualmente, o país aumentou suas despesas públicas com Pesquisa e Desenvolvimento (P&D), principalmente em tecnologias de ponta. Isso fez com que a China se tornasse referência em tecnologias como inteligência artificial e na rede 5G, setores antes dominados pelos EUA.

Hoje, a China pode ser considerada a maior exportadora de alta tecnologia. Os chineses consolidaram as bases de suas próprias *big techs* detentoras de dados, como o Alibaba Group, Baidu, Tencent e Huawei. Grande parte desses dados são utilizados para alimentar o "sistema de crédito social" do país, que avalia o comportamento dos cidadãos.

Assim sendo, tem-se no aspecto da privacidade, a observância de possível tratamento inadequado de dados, a partir de extrema vigilância e condutas discriminatórias. Em outro viés, mas da mesma forma como observado na prática estadunidense, tal situação também implica desafios para a promoção da proteção de dados pessoais em nível global, considerando o monopólio de mercado.

Os impactos práticos da observância ou não de limites e diretrizes acerca da proteção de dados em nível global são relevantes.

No caso, o posicionamento político e a existência de regulação capaz de afetar o desenvolvimento de tecnologias e a utilização de dispositivos que trabalham com dados pessoais dão margem para um contexto de disputas internacionais.

Para fins de melhor compreensão de como a *IoT* e a ferramenta de *Big Data* podem influenciar tensões globais em meio a um novo modelo de negócio, é imperioso que se levante a disputa internacional em relação ao uso de equipamentos Huawei para uso em redes da 5ª geração de dados sem fio.

Apesar de o 5G, como padrão de tecnologia de quinta geração para redes móveis e de banda larga, não ser um aplicativo loT, sua maior velocidade de conexão elevará a potencialidade e a simultaneidade da conexão entre indivíduos e dispositivos, sendo essencial para o desenvolvimento do loT. As redes 5G proporcionam uma infraestrutura expansiva, dando suporte para os variados setores, como governamental, militar, comercial, financeiro e de transporte.

Nesse sentido, por operarem em um nível mais amplo e veloz do que os dispositivos loT individuais, por óbvio, como tratado no tópico anterior, podem constituir uma nova e maior ameaça no que tange à proteção de dados e privacidade, por facilitar, ainda mais, a coleta, o monitoramento e o compartilhamento de informações.

Nesse contexto, o governo americano, em meio a acusações de espionagem, segundo um relatório de 2005 elaborado pela Rand Corporation e patrocinado pela Força Aérea dos EUA, rejeitou e tentou persuadir outros países a rejeitar o equipamento 5G da empresa chinesa Huawei, alegando que isso exporia esses outros estados a ataques

cibernéticos na forma de espionagem ou ameaças à infraestrutura crítica[38].

Aliás, a Huawei, até então, dominava as vendas de equipamentos para as redes 4G e 5G mais recentes que sustentam muitas tecnologias de IoT, fornecendo conexões de dados móveis para carros autônomos, fábricas automatizadas e muito mais.

O gerenciamento de riscos e de ameaças em equipamentos de telecomunicações e a incapacidade contínua de garantir a efetiva segurança tem como pano de fundo a política chinesa de exigir que empresas nacionais privadas, como a Huawei, apoiem a coleta de inteligência. Inclusive, o Artigo 7 da Lei de Inteligência Nacional da China de 2017 exige que empresas e cidadãos chineses apoiem e cooperem com o trabalho de inteligência do país. Assim, o fato de uma empresa ser privada não garante que ela não participará de atos do governo chinês, ante a segurança cibernética[39].

Avaliando uma abordagem mais rigorosa que se concentra nas percepções da confiabilidade dos fornecedores e dos governos de seus países de origem, em vez de tentar avaliar itens específicos, o governo dos EUA proibiu, por meio do Ato de Autorização de Defesa Nacional (NDAA), as compras do governo federal de equipamentos de rede da Huawei e passou a impedir as empresas americanas de usar equipamentos de telecomunicações fabricados na china, como pela Huawei e pela ZTE.

A Seção 889 da Lei de Autorização de Defesa Nacional de 2019 proíbe o uso de fundos federais para adquirir equipamentos ou serviços de telecomunicações cobertos, cujo termo inclui, entre outros, certos equipamentos de telecomunicações produzidos pela Huawei Technologies Company ou ZTE Corporation ou suas afiliadas.

Mesmo com a posse do presidente democrata Joe Biden, as restrições delimitadas pelo presidente Donald Trump continuaram

38 Disponível em: < https://g1.globo.com/tecnologia/noticia/2021/11/05/5g-entenda-a-briga-entre-estados-unidos-e-china.ghtml > Acessado em 24 de outubro de 2023.

39 DeNardis, Laura, and Mark Raymond. "The Internet of Things as a Global Policy Frontier." U.C. Davis Law Review, vol. 51, no. 2, December 2017, p. 475-498

nos EUA. Os EUA permaneceram afirmando que a China poderia usar equipamentos de rede de empresas de telecomunicação instalados no exterior para espionagem ou interferir no funcionamento da infraestrutura de outros países.

Em 2021, inclusive, Joe Biden, sancionou uma legislação para impedir empresas consideradas ameaças à segurança dos EUA, como as chinesas Huawei ZTE Corp, de receberem novas licenças das autoridades reguladoras norte-americanas para seus equipamentos. Essa Lei de Equipamentos Seguros, que representa o mais recente esforço do governo dos EUA para reprimir as empresas chinesas de telecomunicações e tecnologia.

A ação dos EUA é influenciada por um objetivo geoeconômico de negar a supremacia tecnológica à China em uma competição de segurança focada em tecnologia, potencializada pelo uso do 5G[40]. Para tanto, a China e a Huawei negam as acusações e dizem que o interesse dos EUA é minar o crescimento tecnológico chinês, que vem avançando e fazendo frente aos americanos.

A tensão geopolítica, contudo, expande-se para o resto do mundo.

Diante da impossibilidade de se confiar nas redes 5G da Huawei, uma vez que apresentam riscos para fábricas inteligentes e todos de outros usos de loT no cotidiano humano, os EUA declararam que não estariam dispostos a compartilhar informações de segurança confidenciais com estados que aceitam equipamentos de rede Huawei, alegando que essas informações de segurança confidenciais se tornariam inseguras pela transmissão por meio de uma rede baseada na Huawei.

A ideia é a de que os Estados Unidos afiem a sua ponta inovadora, buscando se unir como uma potência econômica das democracias de todo o mundo, a fim de contrapor a influência crescente da China em assuntos globais

40 DeNardis, Laura, and Mark Raymond. "The Internet of Things as a Global Policy Frontier." U.C. Davis Law Review, vol. 51, no. 2, December 2017, p. 475-498

Nesse cenário, o Reino Unido, a princípio, decidiu permitir que a Huawei operasse no país, dizendo que os riscos são controlados. Contudo, em julho de 2020, após o impacto das novas sanções impostas pelos EUA, o governo britânico voltou atrás e decidiu pela proibição do uso de equipamentos da chinesa Huawei para redes 5G, sendo suspensas a compra de novos equipamentos da marca e a remoção de dispositivos já existentes até 2027,

Assim, a companhia Huawei passou a ser barrada na Austrália, Canadá, Nova Zelândia, Reino Unido –países que fazem parte do grupo "Five Eyes" (Cinco Olhos), com o qual os EUA mantêm relações de cooperação estreitas em inteligência.

No caso do Brasil, a China é um dos maiores parceiros comerciais, participando de forma expressiva nas exportações de minério, carne e soja. Mas, ainda assim, ausente nos dias atuais uma relação efetivamente harmônica, como se pretendia no surgimento dos BRICS, o grupo formado por países emergentes como Brasil, Rússia, China, Índia e África do Sul.

Na época das definições para o leilão do 5G, realizado em novembro de 2021, os Estados Unidos chegaram a pressionar o Brasil a barrar a entrada de empresas da China na infraestrutura da nova geração de internet no país.

Contudo, o leilão do 5G, realizado em novembro de 2021, foi feito apenas com operadoras de telefonia, não contando com a participação de empresas fabricantes de cabos e antenas, como a Huawei. Mesmo assim, o edital do leilão não impôs qualquer regra que impedisse as operadoras de usar tecnologia da Huawei.

Em seguida, a Softex (Associação para Promoção da Excelência do Software Brasileiro) apresentou na MWC 2022, feira de tecnologia móvel do mundo, realizada em Barcelona, duas propostas para o desenvolvimento de 5G e inteligência artificial no Brasil — com o apoio do governo brasileiro e da gigante chinesa Huawei[41].

41 Disponível em: < https://www.uol.com.br/tilt/noticias/redacao/2022/03/01/apos-polemica-com-5g-brasil-faz-as-pazes-com-huawei-e-anuncia-parceria.htm > Acessado em 24/10/2023

No início do ano de 2023, o então presidente Luis Inácio Lula da Silva visitou um centro de inovação em tecnologia da Huawei, em Xangai. A visita incluiu um encontro com executivos da companhia e contato com iniciativas da empresa[42]. Apesar de o Brasil sempre apostar em uma postura imparcial no embate entre China e Estados Unidos, o encontro ocorrido neste ano gerou a certeza de que a empresa chinesa pretende aprofundar as relações com o Brasil.

Se o Brasil continuar a não seguir o alinhamento com o comando dos Estados Unidos, evidentemente, poderá sofrer alguma espécie de retaliação, no sentido da ameaça de não compartilhamento de informações dos serviços de inteligência e/ou de sofrer sanções econômicas, tais como eventual redução na compra de algum produto da pauta de exportações brasileira.

Além disso, outros riscos geopolíticos envolvem a execução do acordo de cooperação internacional no setor de lançamento de satélites na Base de Alcântara, localizada no Maranhão, conforme estabelece o Decreto Legislativo n. 64/2019 do Senado Federal. Toda a tecnologia aeroespacial norte-americana é objeto de proteção especial.

Também, outro risco geopolítico é os Estados Unidos suspenderem as ações de cooperação no setor de defesa, uma vez que o Brasil foi declarado como membro não oficial da OTAN. Assim, o Brasil poderá perder a condição de acesso preferencial na aquisição de armamento dos Estados Unidos.

A valer, independente do posicionamento político assumido, é fundamental que o Brasil construa uma política de proteção das comunicações de brasileiros e empresas brasileiras contra tratamento indevido de dados pessoais, elevada vigilância, interceptação das comunicações realizadas pelos Estados Unidos e/ou China ou qualquer outro governo estrangeiro.

É de responsabilidade do governo brasileiro conduzir uma política de segurança das redes de comunicações contra incidentes e interferências indevidas. A proteção de dados e de comunicações

42 Disponível em: < https://veja.abril.com.br/economia/os-planos-da-huawei-para-o-brasil-apos-visita-de-lula-a-china> Acessado em 24/10/2023

nacionais é uma medida decorrente da soberania e da segurança nacional.

Destaca-se, nesse sentido, o referencial teórico de Samuel Warren e Louis Brandeis[43], em que direito à privacidade é inaugurado na contemporaneidade no texto "*The Right to Privacy*".

Na referida obra, a privacidade encontra-se diretamente ligada ao isolamento do indivíduo e em sua tranquilidade[44], o que na realidade atual, diante do desenvolvimento da tecnologia e dos meios de comunicação, apresenta-se de forma muito mais complexa. Contudo, o presente trabalho se vale dos desdobramentos demonstrados na obra centenária.

Ora, naquela época, já se demonstrava a privacidade como direito fundamental relacionado aos interesses e comportamentos do indivíduo para com a proteção de seus dados quando utilizados por terceiros, que merece ser observado mesmo diante da hiperconectividade oferecida pela IoT e pela tecnologia 5G.

A valer, acompanhando o desenvolvimento tecnológico, também como base teórica, Stefano Rodotà[45], em seu texto publicado em 1995, "*Tecnologie e diritti*", inaugura um uma tentativa de equilíbrio entre direito, política e tecnologia, visto que se busca alcançar estabilidade entre o digital e as liberdades individuais, o que deve ser observado pelas noções mundiais.

Isto é, a discussão em torno da privacidade está intimamente ligada aos princípios democráticos e liberdades civis. O conceito de privacidade deve ser notado a partir de seu impacto para com a pessoa, e não em seu *aspecto privado*.

Com a introdução da tecnologia de informação em várias áreas da vida econômica e social, e a importância e poder crescentes do processamento automatizado de dados, há de se ter um consenso internacional relativo à política internacional sobre a proteção da

43 WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890)

44 *"the right to be alone"* in WARREN, Samuel D.; BRANDEIS, Louis D. idem, p.196

45 RODOTÁ, Stefano. Tecnologie e diritti. Bologna: 1l Mulino, 1995

privacidade e dos fluxos transfronteiriços de dados pessoais, como buscou a União Europeia, a partir da atual lei de proteção de dados em vigor, qual seja a *General Data Protection Regulation* (GDPR).

Já é conhecido o fenômeno de globalização regulatória das leis europeias, que faz com que as empresas e países se alinhem às normas da União Europeia, principalmente, para ter franqueado seu acesso ao pujante mercado europeu.

No contexto atual, de disseminação e hegemonia crescente das tecnologias digitais, a proteção de dados, seguida da autodeterminação informacional é pré-condição absoluta para o debate democrático.

Os Governos e as grandes empresas privadas, em especial estadunidense, detêm quantidades incomensuráveis de dados pessoais (*Big Data*), e ferramentas de análise potencialmente invasivas tornam necessária a criação de recursos para o enfrentamento das profundas assimetrias de poder e de informação que se configuram, bem como para combater práticas discriminatórias que visem a beneficiar grupos hegemônicos.

Dessa forma, regimes de proteção de dados desempenham papel fundamental em países democráticos, que respeitam os direitos humanos, oferecendo mecanismos de proteção à privacidade.

Ora, não se pretende criar entraves econômicos ao editar normas para a utilização de dados pessoais, compreendendo a enorme importância dos dados pessoais para o funcionamento atual da economia. A valer, regimes de proteção de dados devem sinalizar um compromisso com valores democráticos, com a dignidade da pessoa humana e com o direito ao livre desenvolvimento da personalidade.

Para além disso, ainda que a LGPD acentue o princípio da transparência e da segurança da informação - sugerindo que dispositivos, plataformas e aplicativos disponham abertamente sobre os possíveis riscos dos sistemas, a existência de ferramentas robustas de obscuridade que permitem aos usuários restringir análises e sobre planos de contingência para mitigar os riscos de privacidade se os sistemas forem comprometidos - é difícil que se alcance todas as

implicações possíveis acerca do tratamento de dados no âmbito da *IoT*[46].

Contudo, diante da recente vigência da legislação no país, ainda há mecanismos a serem estudados, tanto em seu aspecto jurídico quanto técnico. Tem-se como exemplo as metodologias de *Privacy by Design* e *Privacy by Default,* criadas pela canadense Ann Cavoukian[47], comissária de informação e privacidade de Ontário (Canadá).

O conceito de *Privacy by Design* prevê que qualquer projeto de uma empresa que envolva o processamento de dados pessoais deve ser realizado mantendo a proteção e a privacidade dos dados a cada passo, desde a sua concepção. Isso inclui o desenvolvimento de produtos, desenvolvimento de software, sistemas de TI e mais. Na prática, deve-se garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida daquele produto ou sistema, a partir da promoção da segurança e da transparência.

Já o *Privacy by Default* significa que, assim que um produto ou serviço for lançado, as configurações mais seguras de privacidade deverão ser aplicadas por padrão, sem interposição manual. Além disso, todos os dados pessoais fornecidos pelo usuário para permitir o uso ideal de um produto devem ser coletados e mantidos apenas quando necessário para fornecer o produto ou serviço.

Tais conceitos são mencionados de forma expressa no artigo 46, §2, da LGPD, assim como no artigo 25 do GDPR (*General Data Protection Regulation*). No caso, tal previsão representa uma mudança no modo de garantir a privacidade e a proteção de direitos e liberdades dos indivíduos, já que é pensado e incorporado às práticas de negócio antecipadamente.

Tem-se mecanismos capazes de permitir que a proteção de dados seja parte integrante do desenvolvimento tecnológico e também da maneira como um produto ou serviço é criado. Aliás, para

46 FOGLI, Mariana. Autogerenciamento da privacidade no acesso às redes digitais: comportamento dos usuários e a proteção legal dos dados pessoais e da privacidade. Tese de Mestrado. Universidade Federal de Minas Gerais, 2023.

47 CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009

o uso adequado de tais mecanismos muitas vezes não será suficiente atualizar os processos herdados com um verniz de privacidade, mas pode ser necessário construir novos processos e sistemas ou redesenhar significativamente os existentes.

Considerando a implantação da nova tecnologia 5G e a adaptação dos dispositivos, tem-se o momento adequado para que o *Privacy by Design* e *by Default* passem a estar presentes nas tecnologias de *IoT*, sendo utilizadas em empresas públicas e privadas, multinacionais ou startups, todas que processam de alguma forma os dados pessoais de seus clientes, colaboradores e fornecedores.

Inclusive, imperioso trazer destaque para o tema em face das startups, que em razão de sua natureza contar com uma base tecnológica forte, há consideráveis operações envolvendo dados nas redes. Por ser um modelo de negócio escalável e sustentável, padrões de privacidade passam a fazer parte da inovação de tais negócios, que se amplia em face da possibilidade de atuação em diferentes áreas e mercados.

4. QUESTÕES SOBRE A REGULAÇÃO INTERNACIONAL.

Há uma tendência global de acreditar que a União Europeia tenha sido pioneira em questões regulatórias, como se viu recentemente no embate do bloco continental com o *Google Analytcs*, que tem como pano de fundo a anulação do acordo *Privacy Shield*[48] assinado em 2016 entre a União Europeia e os Estados Unidos para transferência de dados pessoais de usuários do bloco europeu para os norte-americanos.

Inclusive, e tornando ainda mais evidente o "efeito Bruxelas", o uso de *IoT* pode implicar a transferência internacional de dados. No caso de informações coletadas em países europeus para outras entidades ou países, tem-se a obrigatoriedade de se obedecer às regras de transferência internacional previstas no GDPR.

48 Disponível em: <https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf > Acessado em 24/10/2023

Dentre essas, a que oferece maior segurança, previsibilidade e conveniência às empresas é a "*adequacy decision*"[49]. Isso é, a possibilidade de transferência de dados somente é possível quando um país possui níveis adequados de proteção de dados pessoais comparáveis à proteção garantida pelo GDPR.

É importante mencionar que uma decisão de adequação não é apenas uma empreitada jurídica, mas também envolve questões econômicas e políticas.

Após a aprovação da decisão de adequação, o país solicitante pode passar a transferir dados para o bloco da UE sem a necessidade de se utilizar de outros mecanismos de transferência, como cláusulas contratuais padrão, BCRs, selos, certificações. Dessa forma, a decisão de adequação cumpre um papel de promover o amplo fluxo transnacional de dados, sem os entraves burocráticos existentes ou outros mecanismos de transferência mais restritivo.

Evidentemente que este é um grande benefício às relações internacionais destes países, fortalecidas pela diminuição da burocracia e da incerteza no trato comercial. Logo, obter *adequacy decision* pode ser fundamental para impulsionar o comércio entre o qualquer país e a União Europeia.

Países como o Brasil tendem a se consolidar como desenvolvedores, mas também como adquirentes de tais tecnologias. Tal cenário propicia um ambiente frutífero para a disseminação de parcerias comerciais na área tecnológica, assim como exige novas regulações sobre as relações entre países e suas companhias no que tange ao tratamento de dados pessoais.

A legislação pátria, que inaugurou o debate de forma expressa a partir do Marco Civil de Internet, segue a tendência mundial com a publicação da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709 em 2018, que regula as atividades de tratamento de dados pessoais.

49 UE. GDPR. Chapter 5 - Transfers of personal data to third countries or international organisations. https://gdpr-info.eu/chapter-5/

A princípio, no tocante ao funcionamento da Autoridade Nacional de Proteção de Dados - ANPD, a LGPD parecia não estar plenamente em conformidade com os parâmetros descritos no GDPR, que exige a existência e o funcionamento de uma Autoridade de controle independente, como um dos elementos para o reconhecimento da adequação do grau de proteção de dados pessoais oferecido pelo país estrangeiro.

Isso porque, após o veto presidencial aos dispositivos da LGPD que dispunham sobre a criação da ANPD, o que se justificou na alegação de inconstitucionalidade por vício de iniciativa, a estrutura administrativa da ANPD passou a ser prevista como órgão integrante da Presidência da República por meio da Medida Provisória nº 869/18, convertida na Lei nº 13.853/201912.

O fato de a ANPD estar vinculada à administração direta atrai críticas no sentido de que esse órgão, responsável pelo controle e fiscalização do cumprimento da lei de proteção de dados no Brasil, pode não possuir a independência que seria esperada.

Contudo, com a promulgação da Lei 14.460/2022, a ANPD foi transformada em uma autarquia. O objetivo da mudança foi justamente evitar a descontinuidade administrativa da ANPD e trazer mais confiabilidade ao sistema regulatório de proteção de dados. No novo formato, a ANPD passa a ser compatível com outros regimes regulatórios e experiências internacionais, por exemplo, a GDPR. Trata-se de um grande avanço na busca pela *adequacy decision*.

5. CONCLUSÃO

Os dados pessoais podem ser considerados elementos nucleares para o desenvolvimento político, social e econômico. Assim, essa nova era, sedimentada na comunicação digital, constrói-se a partir da evolução tecnológica recente que, conforme ensina Bruno Bioni,

"criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imagináveis"[50].

E, nesse caso, a facilidade de tratar dados pessoais, ainda mais sensíveis, principalmente em relação ao uso em larga escala das plataformas virtuais, aplicativos, dispositivos e redes sociais, é preocupante, ao considerar o direito à liberdade, igualdade e, ainda, à intimidade.

Trata-se de um assunto de extrema relevância. Por meio do presente trabalho foi possível concluir a necessidade de firmar um debate, envolvendo Estados e Organizações Internacionais, acerca do tratamento de dados pessoais no contexto da *Internet das Coisas*, de forma a compatibilizar o desenvolvimento tecnológico e evitar vulnerabilidades e violações à privacidade, em face dos direitos dos titulares, considerando as garantias fundamentais e os princípios da dignidade da pessoa humana, da privacidade e da liberdade.

Mesmo diante de certa ascensão do princípio da privacidade no cotidiano e ainda que seja possível observar avanços legislativos acerca da proteção de dados, não há uma harmonização dos interesses pessoais e econômicos gerados pela interface entre Internet das Coisas e Big Data, que possa levar, em nível global, à completa proteção da privacidade ou, ainda, à efetividade da autodeterminação informativa.

Tem-se a confirmação da existência de um conflito entre o desenvolvimento da tecnologia e a necessidade de gerar a efetiva segurança de dados, cuja solução, na opinião desta Autora, far-se-á a partir do diálogo entre tecnologia, política e direito, a fim de possibilitar a condição para o titular de dados de interagir na sua proteção ou na busca pela tutela preventiva.

Nesse sentido, por meio deste trabalho se alcança a conclusão da necessidade de que sejam estudados limites técnicos precisos, a serem considerados em regulações internacionais, para que os princípios da proteção de dados e privacidade estejam inseridos na tecnologia por padrão e desde a sua concepção, com objetivo de evitar o uso indevido

50 BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. Fls. 4.

de dados pessoais, que podem não só trazer à tona danos de cunho moral e de personalidade aos titulares de dados, como ainda levantar disputas geopolíticas, o que pode colocar em xeque o exercício de Estados Democráticos de Direito.

REFERÊNCIAS

AGOSTINELLI, Joice. ***A Importância Da Lei Geral De Proteção De Dados Pessoais No Ambiente Online***. ETIC 2018 –Encontro de Iniciação Científica, ISSN 21-8498.

BIONI, Bruno. ***Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundan*tes.** São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

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

BUCAR, Daniel; VIOLA, Mario. ***Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamento*s**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.

CAVOUKIAN, Ann. ***Privacy by Desig*n: The 7 Foundational Principles**. August, 2009

CHAVES, Natália Cristina; COLOMBI, Henry (Orgs.) ***Direito e Tecnologia:*** *novos modelos e tendências [recurso eletrônico]* / Natália Cristina Chaves; Henry Colombi (Orgs.) -- Porto Alegre, RS: Editora Fi, 2021

DE LIMA, Cíntia Rosa Pereira; MACIEL; Renata Mota. ***Direito e Internet IV: S****istema de Proteção de Dados Pessoais (De acordo com a Lei n.º 13.709, de 14 de agosto de 2018 e a Lei n.º 13.853 de 08 de julho de 2019, que converteu a lei Medida Provisória n.º 869, de 27 de dezembro de 2018)***.** São Paulo: Editora Quartier Latin, 2019.

DE LUCCA, Newton. ***A disciplina Normativa que Faltava***. In: DE LUCCA, Newton; FILHO, Adalberto Simão; DE LIMA, Cíntia Rosa Pereira; MACIEL; Renata Mota Direito e **Internet IV**: Sistema de Proteção

de Dados Pessoais (De acordo com a Lei n.º 13.709, de 14 de agosto de 2018 e a Lei n.º 13.853 de 08 de julho de 2019, que converteu a lei Medida Provisória n.º 869, de 27 de dezembro de 2018) São Paulo: Editora Quartier Latin, 2019.

DENARDIS, Laura, and Mark Raymond. ***"The Internet of Things as a Global Policy Frontier."*** U.C. Davis Law Review, vol. 51, no. 2, December 2017, p. 475-498. HeinOnline.

DONEDA, Danilo. ***Da privacidade à proteção de dados pessoais***. Rio de Janeiro: Renovar, 2ª edição de 2019.

FOGLI, Mariana. **Autogerenciamento da privacidade no acesso às redes digitais:** comportamento dos usuários e a proteção legal dos dados pessoais e da privacidade. Tese de Mestrado. Universidade Federal de Minas Gerais, 2023.

FOITZIK, Piotr. ***Publicly available data under the GDPR: Main considerations*.** Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/>. Acesso em: junho 2022.

FRAZÃO, Ana. **Nova LGPD:** as demais hipóteses de tratamento de dados pessoais**.** Jota. 19.09.2018. Disponível em [https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018]. Acesso em: junho 2022.

FURBINO, Meire; SAMPAIO, José Adércio Leite; MENDIETA, David. ***Capitalismo De Vigilância E A Ameaça Aos Direitos Fundamentais Da Privacidade E Da Liberdade De Expressão***. Revista Jurídica Unicuritiba. Curitiba.V.01, n.63, p.89-113, Janeiro-Março. 2021.

HSING, Chen Wen. **Coleta de dados pessoais e paradoxo da privacidade:** um estudo entre usuário de aplicativos móveis. São Paulo, 2016.

IAB Europe. ***A Guide to the Post Third-Party Cookie Era.***, 2020.

JURCYS, Paul;DONEWALD, Chris; GLOBOCNIK, Jure; LAMPINEN, *Markus.* ***My Data, My Terms: A Proposal For Personal Data Use Licenses***. Harvard Journal of Law & Technology Volume 33, Digest Spring 2020.

KONDER, Carlos Nelson. ***O tratamento de dados sensíveis à luz da Lei 13.709/2018***. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Editora Revista dos Tribunais, 2019

LEONARDI, Marcel. ***Fundamentos de Direito Digital***. Revista dos Tribunais, 3ª triagem, 2019.

LÓPEZ, Santiago Ramírez. ***Informing Consent****: Giving Control Back to the Data Subject from a Behavioral Economics Perspective*, (2018) JIPITEC 35.

MENDES, Laura Schertel; DONEDA, Danilo. ***"Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil"***. Revista de Direito do Consumidor, v. 120, p. 555, 2018.

MULHOLLAND, C. S. (2018). ***Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados*** *(Lei 13.709/18)*. Revista De Direitos E Garantias Fundamentais, 19(3), 159-180. https://doi.org/10.18759/rdgf.v19i3.1603.

OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OLIVEIRA, Nairobi Spiecker; GOMES, Moises Alexandre; LOPES, Ronaldo; Nobre, Jéferson C. ***Segurança da Informação para Internet das Coisas (IoT)****: uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)*. Curso Superior de Tecnologia em Segurança da Informação Universidade do Vale do Rio dos Sinos (UNISINOS): São Leopoldo/RS, 2018.

PARENTONI, Leonardo.**Proteção de Dados Pessoais no Brasil**. In: DE LUCCA, Newton; FILHO, Adalberto Simão; DE LIMA, Cíntia Rosa Pereira; MACIEL; Renata Mota **Direito e Internet IV**: Sistema de Proteção de Dados Pessoais (De acordo com a Lei n.º 13.709, de 14 de agosto de 2018 e a Lei n.º 13.853 de 08 de julho de 2019, que converteu a lei Medida Provisória n.º 869, de 27 de dezembro de 2018) São Paulo: Editora Quartier Latin, 2019.

PASQUALE, Frank. ***The black box society : the secret algorithms that control money and information.*** Harvard University Press: Cambridge, Massachusetts London, En gland 2015

PFEIFFER, Roberto. **A Saga da ANPD**. In: DE LUCCA, Newton; FILHO, Adalberto Simão; RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. ***A Proteção de Dados Pessoais na Internet no Brasil****: Análise de decisões proferidas pelo Supremo tribunal Federa*l. In: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936 Acesso em 30 de junho de 2022.

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

RODOTÁ, Stefano. ***Tecnologie e diritti***. Bologna: 1l Mulino, 1995

ROVER, Aires José (org). ***Dados E Informações Na Internet****: É Legítimo O Uso De Robôs Para Formação De Base De Dados De Clientes?* Direito e Informática. SP: Manole, 2003, p. 27-40.

SANTOS, Lino. ***Cyberspace Regulation****: Cesurists And Traditionalists Janus.Net*, e-journal of International Relations, vol. 6, núm. 1, mayo-octubre, 2015, pp. 86-99

SOLOVE, Daniel J..**The Myth of the Privacy Paradox**. 2020.

TAMÒ-LARRIEUX, A. (2018). ***Privacy Protection in an Internet of Things Environment. In: Designing for Privacy and its Legal Framework.*** **Law, Governance and Technology Series**, vol 40. Springer, Cham. https://doi.org/10.1007/978-3-319-98624-1_4

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. ***Tratamento de dados pessoais na LGPD: estudo sobre as bases legais.*** **Civilistica**.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>. Acesso em: junho 2022..

TRACHTMAN, Joel P. ***"Cybersecurity versus Trade in Internet of Things Products."*** *Manchester Journal of International Economic Law*, vol. 16, no. 3, December 2019, p. 301-340. HeinOnline.

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

WARREN, Samuel D.; BRANDEIS, Louis D. T**he Right to Privacy.** Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

WESTIN ,Alan F. ***Privacy And Free*****dom**, 25 Wash. & Lee L. Rev. 166 (1968).

SCHAWAB, K. A. ***Quarta Revolução Industria****l*. São Paulo: Edipro, 2017, p. 11.

FILHO, Adalberto Simão; SCHWARTZ. ***Big em tempos de internet das coisas. In: Direito, Tecnologia e Inovação***. V.1. Coordenação de Leonardo Parentoni. Belo Horizonte: D´Plácido, 2019.

ZUBOFF, Shoshana. B**ig other: capitalismo de vigilância e perspectivas para uma civilização de informação**. In: BRUNO, F. et al. (orgs.). Tecnologias da vigilância: perspectivas da margem. Trad. H. M. Cardozo et al. São Paulo: Boitempo, 2018. p. 17-68

WACHTER, Sandra. N**ormative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. Computer Law & Security Review**, 2016.

O PRINCÍPIO DA TRANSPARÊNCIA NO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

The Principle of Transparency in the Context of the General Data Protection Law

Fernanda Araújo Couto e Melo Nogueira

Fernanda Araújo Couto e Melo Nogueira[51]

RESUMO

Vivemos a era do capitalismo de vigilância, em que as informações são alçadas a protagonistas nos processos de tomada de decisão, desde as grandes questões públicas até as questões mais íntimas na esfera privada. Nesse contexto, aumenta-se constantemente a consciência da importância da proteção dos dados para garantia da liberdade das pessoas e, ao mesmo tempo, é cada vez mais difícil respeitar essa premissa, na medida em que exigências de segurança, interesses de mercado e a Administração Pública reclamam o tratamento de mais dados, levando à diminuição ou mesmo ao desaparecimento de garantias essenciais. Por meio do presente artigo, analisa-se o alcance do Princípio da Transparência no âmbito da LGPD por intermédio do exame dos seus elementos essenciais, quais sejam: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. A obrigação de transparência permeia toda a legislação e deve ser observada, independentemente da base legal que fundamenta juridicamente o tratamento, em todas as etapas do ciclo de vida dos dados, sendo que a observância do Princípio da Transparência constitui requisito legal mínimo a embasar o tratamento de dados em conformidade com a LGPD, dando concretude ao direito fundamental à proteção dos dados pessoais.

Palavras-chave: Privacidade. Princípio da Transparência. Proteção de Dados. LGPD. Princípios.

51 Sócia do João Bosco Leopoldino Advocacia e Consultoria. Graduada em Direito pela Universidade FUMEC, em 2008. Mestre em Ciências Jurídico-Empresariais pela Faculdade de Direito da Universidade de Lisboa, em 2013. MBA –Gestão Estratégica de Negócios pela Universidade FUMEC, 2016/2017. Certificada em Proteção de Dados (LGPD), pela Exin –PDPE, 2021. Membro da Comissão de Proteção de Dados da OAB/MG.

ABSTRACT

We live in the era of surveillance capitalism, in which information is elevated to protagonists in decision-making processes, from major public issues to the most intimate matters in the private sphere. In this context, there is a growing awareness of the importance of data protection for ensuring people's freedom, at the same time, it is increasingly difficult to respect this premise, as security requirements, market interests and the Administration Public demand the processing of more data, leading to the reduction or even disappearance of essential safeguards. Through this article, the scope of the Principle of Transparency within the scope of the LGPD is analyzed by examining its essential elements, which include providing data subjects with clear, accurate, and easily accessible information about data processing and the respective data processors. The obligation of transparency permeates all legislation and must be observed regardless of the legal basis that legally grounds the processing, at all stages of the data life cycle. Compliance with the Transparency Principle represents the minimum legal requirement for data processing in accordance with the LGPD, giving substance to the fundamental right to personal data protection.

Keywords: Privacy. Principle of Transparency. Data Protection. LGPD. Principles.

INTRODUÇÃO

Vivemos a era da informação. A sociedade tem sua dinâmica atualmente organizada em torno das informações, as quais foram alçadas a protagonistas nos processos de tomada de decisão, desde as grandes questões públicas de ordem política e econômica até as questões mais íntimas na esfera privada.

Por meio da captação e do tratamento massivo de recursos informacionais, a sociedade do novo milênio é impulsionada por uma evolução tecnológica que prima por desenvolver mecanismos cada

vez mais sofisticados para o processamento de dados, transpondo limites físicos e geográficos e, segundo Bioni[52], criando uma nova compreensão da relação tempo-espaço.

E, conforme Coelho[53], um dos problemas mais complexos da humanidade, passou a ser exatamente o uso e a proteção desses dados pessoais, especialmente pelo fato de que o combustível para toda essa revolução tecnológica são as pessoas, seus hábitos e sua produção diária de conteúdo no trabalho e na sua vida cotidiana.

Por isso mesmo, e conforme Schertel[54], com os inúmeros avanços da tecnologia da informação, fala-se, também, em uma verdadeira "morte da privacidade", decorrente da dificuldade (impossibilidade) de se preservarem fatos e elementos da esfera íntima e privada dos titulares.

Verifica-se, portanto, uma contradição endógena na sociedade da informação na medida em que se aumenta constantemente a consciência da importância da proteção dos dados para garantia da liberdade das pessoas e, ao mesmo tempo, segundo Rodotá[55], é cada vez mais difícil respeitar essa premissa, na medida em que exigências de segurança, interesses de mercado e a própria gestão da Administração Pública reclamam o tratamento de mais dados, levando à diminuição ou mesmo ao desaparecimento de garantias essenciais.

Nesse contexto, o mercado, em vez de contribuir para a superação da assimetria de informações e consequente vulnerabilidade do cidadão, acaba por intensificá-la, fazendo emergir a necessidade de uma atuação proativa do Estado para a proteção dos dados pessoais.

De acordo com Rodotá[56], a ausência de clareza quanto ao tratamento dos dados pessoais pelos agentes de tratamento transforma as pessoas em seres cada vez mais transparentes, e, por isso mesmo,

52 BIONI, 2019, p. 20.
53 COELHO, 2020.
54 SCHERTEL, 2008, p.8
55 RODOTÁ, 2008, p. 13.
56 Idem, 2008, p. 15.

mais frágeis, acarretando um rearranjo de poderes econômicos, políticos e sociais.

Assim, em busca da preservação (ou proteção) da dignidade humana, os ordenamentos jurídicos de diversos países passaram a tutelar expressamente os dados pessoais de seus cidadãos, merecendo, inclusive, tutela constitucional.

Concordando com Rodotá[57], percebe-se como é essencial a busca contínua pelo efetivo desenvolvimento e amadurecimento da tutela jurídica dos dados pessoais, garantindo-se a proteção efetiva aos direitos da personalidade mediante normatização própria e autônoma, e, fundamentalmente, garantindo-se a própria capacidade de autodeterminação do ser humano.

O início dos debates doutrinários a respeito do direito à privacidade tem como marco referencial a publicação do emblemático artigo nomeado *The right to privacy*[58], na Harvard Law Review, ainda em 1890, pelos juristas Samuel Warren e Louis Brandeis. No texto, os autores discorreram sobre a necessidade de ampliar a concepção do direito à privacidade, para abranger o "direito de ser deixado em paz" (*the right to be left alone*), dada a crescente divulgação, à época, de notícias sensacionalistas e de fofocas decorrentes dos avanços tecnológicos que facilitavam a captação e divulgação desse tipo de conteúdo, especialmente a invenção das máquinas fotográficas portáteis. É importante ressaltar que o ineditismo do artigo consistiu, não apenas em identificar um direito à privacidade, mas em fundamentar esse direito na proteção da personalidade, evidenciando a relevância desse direito em face dos avanços da tecnologia e de tornar possível o reconhecimento futuro desse direito como um direito protegido constitucionalmente.

Deve-se ressaltar que Warren e Brandeis, ao identificarem o direito à privacidade, buscaram igualmente definir os seus limites,

57 "(...). No entanto, a forte proteção dos dados pessoais continua a ser uma "utopia necessária" (S. Simitis) se se deseja garantir a natureza democrática de nossos sistemas políticos". (Rodotá, 2008, p. 15)

58 Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 01/02/2021.

propondo o seguinte: i) o direito à privacidade não impede a divulgação do que é publicado ou do que é de interesse geral; ii) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito; iii) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; iv) o consentimento do afetado exclui a violação do direito; v) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; vi) a ausência de dolo também não exclui a violação desse direito.

Segundo Rodotá[59], do artigo *The right to privacy* publicado por Brandeis e Warren emergiu também a visão de que a privacidade constitui uma ferramenta de proteção a minorias e a opiniões dissonantes, sendo essencial para a garantia da livre manifestação e do direito do livre desenvolvimento da personalidade.

Já, em 1948, após a II Guerra Mundial, a proteção à privacidade ganha reconhecimento no âmbito internacional com a publicação da Declaração Universal dos Direitos Humanos (DUDH), como uma norma comum a ser alcançada por todos os povos e nações –estabelecendo, em seu artigo 12, que "ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".[60]

Logo adiante, na década de 1970, surgem várias leis e decisões judiciais –expedidas em diversos países que, em diferentes graus, compartilham o entendimento de que a privacidade constitui uma projeção da personalidade, merecendo, portanto, tutela jurídica (MACIEL, 2019, p. 8).

A consolidação da concepção de privacidade relacionada à proteção dos dados pessoais veio na década de 1980, quando cooperaram importantes instrumentos internacionais e transnacionais

59 RODOTÁ, 2008, p. 16.

60 Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acessado em: 01/02/2021.

versando sobre o assunto. Por exemplo, as Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, publicada em 1980; e, ainda, a Convenção 108 do Conselho da Europa, de 1981, que trata da "proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal".

Cumpre também referenciar o, segundo Vieira[61], importante e paradigmático reconhecimento do direito à privacidade informacional pelo Tribunal Constitucional Alemão, em dezembro de 1983, ao declarar nulos os dispositivos da Lei do Censo alemã relacionados à comparação e transmissão dos dados pessoais coletados referentes à profissão, moradia, domicílio e renda para repartições públicas, reconhecendo o direito à autodeterminação informativa do cidadão, ou seja, garantindo a cada indivíduo o direito de controlar e proteger os seus próprios dados pessoais, considerando os dispositivos tecnológicos e os meios de processamento existentes à época.

Com a evolução contínua da compreensão sobre a necessidade de tutelar juridicamente o direito à privacidade e a proteção dos dados pessoais, em 23 de novembro de 1995, o Parlamento Europeu e o Conselho da União Europeia publicaram a Diretiva 95/46/CE, relativa à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[62]. No entanto, tal Diretiva não conseguiu evitar a fragmentação da sua aplicação no âmbito da União Europeia. Assim, a fim de assegurar um maior nível de segurança jurídica para a circulação de dados pessoais na União Europeia, optou-se por criar o Regulamento Geral de Proteção de Dados (GDPR)[63], que, revogando a Diretiva 95/46/CE (Regulamento

61 VIEIRA, 2007, p. 27.

62 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acessado em: 05/02/2021.

63 "Considerando (9): Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos

Geral sobre a Proteção de Dados), estabeleceu regras de proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, o qual passou a ser aplicável a partir de 25 de maio de 2018.

Paralelamente, no Brasil, consoante Blum[64], desde à Constituição de 1988 percebe-se um esforço contínuo do legislador para garantir a proteção dos direitos da personalidade, reforçando o entendimento de que os direitos da personalidade são uma cláusula geral aberta alinhada com o princípio da dignidade da pessoa humana de maneira que não se trata de direitos estanques e "engessados" mas, por sua natureza, têm interpretação versátil e flexível, podendo ser adaptável conforme a realidade que se apresenta.

O princípio da dignidade da pessoa humana constitui um dos fundamentos do Estado Democrático de Direito (valor supremo da Democracia) e, enquanto tal, estrutura o ordenamento jurídico brasileiro. A CR/88 apresenta em seu artigo primeiro a dignidade da pessoa humana como um dos fundamentos do Estado Democrático de Direito[65] e serve como referencial para a interpretação do restante do texto constitucional, operando, também, como fator de integração para dar coerência ao resto do ordenamento. Verifica-se uma valoração absoluta (dignidade) em relação ao homem, valor este a ser respeitado por todos da sociedade.

Ademais de prever como um de seus fundamentos a dignidade da pessoa humana, a Constituição da República, embora de forma genérica, já anteviu a garantia ao cidadão do direito à privacidade por

---

Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE". Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acessado em: 20/02/2021.

64 BLUM, 2008, p. 35.

65 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.

meio dos incisos X e XII do seu art. 5º[66], em sua dimensão negativa, resguardando o titular de intromissões de terceiros em sua esfera de intimidade e vida privada.

A partir da década de 1990, surgiram outros diplomas legais em âmbito nacional que alçaram a proteção da privacidade e dos dados pessoais a um novo patamar. Citam-se, como os principais:

i. O Código de Defesa do Consumidor (Lei 8.078/1990), que disciplina a criação de bancos de dados de consumidores e que prevê o direito de o consumidor ter livre acesso aos dados arquivados sobre a sua pessoa;
ii. A Lei do Habeas Data (Lei 9.507/1997), que é, em sua essência, a ferramenta jurídica para assegurar o conhecimento e a retificação de dados.
iii. O Código Civil (Lei 10.406/2002), que detalhou os direitos inerentes à personalidade, dentre os quais se encontram a privacidade e a intimidade; e que previu expressamente a adoção de medidas necessárias, pelo juiz, mediante pedido do interessado, para cessar eventual violação à sua vida privada;
iv. A Resolução do Conselho Federal de Medicina n.º 1.821/2007, que dispõe sobre o prontuário eletrônico e a proteção de dados médicos e a Resolução do Conselho Federal de Medicina nº 2.336/2023, sobre publicidade e propaganda médicas;
v. A Lei do Cadastro Positivo (Lei n.º 12.414/2011), que disciplina a formação e a consulta a bancos

66 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.

de dados com informações de adimplemento de pessoas, naturais e jurídicas –visando à formação de histórico de crédito –, bem como reconhece os direitos dos titulares dos dados, atrelando o tratamento à finalidade pretendida;

vi. A Lei de Acesso à Informação (Lei n.º 12.527/2011), que disciplina o tratamento dos dados pessoais no âmbito de sua aplicação; e

vii. O Marco Civil da Internet (Lei n.º 12.965/2014 e o Decreto n.º 8.771/2016), que abordam consideravelmente o tratamento de dados pessoais em trânsito pelo ambiente da internet.;

Finalmente, em 14 de agosto de 2018, foi publicada a Lei Federal n.º 13.709/2018 (LGPD), que trata especificamente a proteção de dados pessoais e é claramente inspirada no GDPR, embora apresente pontos de divergência. A LGPD busca harmonizar e atualizar conceitos de modo a mitigar riscos e a estabelecer regras claras sobre a proteção dos dados pessoais[67].

Como visto, ao mesmo tempo em que o mundo se deslumbra com os novos rumos do conhecimento, a invasão da tecnologia da informação no cotidiano molda o comportamento das pessoas, transformando os padrões culturais, as formas de relacionamento e gerando uma forma de "ultrainteratividade" que inexoravelmente expõe a intimidade e vida privada de todos.

Com vistas a garantir ao titular dos dados o direito de exercer o controle sobre informações a seu respeito, a LGPD impõe uma série de obrigações negativas e positivas aos agentes de tratamento, sendo imperiosa a observação do Princípio da Transparência. É nesse cenário que se situa a análise abarcada por este artigo.

Interessa-nos analisar, no presente artigo, o alcance do Princípio da Transparência no âmbito da LGPD por meio do exame dos seus elementos essenciais, quais sejam: garantia, aos titulares, de

67 MALDONADO; BLUM, coord. 2019, p. 23.

informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

Sem pretensão de esgotar o tema, o que se oferece é uma possível interpretação do alcance do referido Princípio no contexto da LGPD tendo como referência o contexto normativo brasileiro.

Cumpre esclarecer que o presente artigo traz considerações gerais acerca do Princípio da Transparência no âmbito da LGPD, independentemente das especificidades de cada setor, e da regulamentação própria a que cada agente de tratamento se submete. Nesse sentido, o presente artigo apresenta considerações genéricas e mais abrangentes, não pretendendo abordar as características específicas eventualmente existentes e aplicáveis a um determinado setor.

1. BREVE CONTEXTO NORMATIVO

Como já falamos, a LGPD, Lei Federal n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade do homem (pessoa física). Referida lei versa sobre as possibilidades e requisitos para a legitimidade do tratamento de dados pessoais pelos agentes de tratamento, sejam tais agentes pessoas físicas ou jurídicas, de direito público ou privado.

Nos termos da LGPD, dado pessoal é aquele que se encontra atrelado à projeção, à extensão ou à dimensão de uma determinada pessoa, tanto na sua esfera individual como em sua esfera relacional. Nos termos do artigo 5º da LGPD, dado pessoal é qualquer "informação relacionada à pessoa natural, identificada ou identificável", sendo considerado dado pessoal sensível –e passível de tratamento diferenciado –o "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".

As hipóteses de tratamento de dados pessoais estão taxativamente elencadas no artigo 7º, o qual descreve as 10 (dez) bases legais autorizadoras para o tratamento de dados pessoais, *verbis*:

> I - mediante o fornecimento de consentimento pelo titular[68];
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

68 Para mais detalhes sobre o tratamento de dados baseado no consentimento, recomendamos a leitura do nosso artigo "*O consentimento na lei geral de proteção de dados: autonomia privada e o consentimento livre, informado, específico e expresso*", disponível em: https://www.editorafi.org/21dados. Acessado em: 20/02/2021.

> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018)

Mas, as hipóteses de tratamento indicadas acima não conferem aos agentes de tratamento poderes amplos e absolutos. Diferentemente, existem limites para quaisquer operações envolvendo tratamento de dados que são determinados pela boa-fé e demais princípios previstos no Art. 6º da mesma norma.

É mandatório que, antes de dar início ao tratamento de dados pessoais, o agente se certifique da adequabilidade, necessidade e qualidade daqueles dados para se atingir especificamente a finalidade pretendida, sendo essencial ainda que seja oportunizada ao titular a ciência sobre o referido tratamento, de forma clara e explícita.

2. O PRINCÍPIO DA TRANSPARÊNCIA NA LGPD

A transparência é um dos elementos há muito perseguidos pelo direito brasileiro[69]. O que se pretende, em sentido amplo, é a geração de um sentimento de confiança nos cidadãos relativamente ao objeto da norma impositiva de transparência.

Na Lei Geral de Proteção de Dados, o Princípio da Transparência está previsto no artigo sexto, conforme abaixo descrito:

69 A CR/88 garante, em seu art. 5º, inciso XIV, o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional"; e no inciso XXXIII, o direito de todos os cidadãos a "receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". Ademais, a CR/88 traz expressamente a obrigação de observância do Princípio da Transparência nos seus artigos 40; 212; e 216-A. Em vários artigos consta a obrigação de conceder acesso e/ou prestar esclarecimentos, notadamente, nos art. 37, 163-A, 202, 216, dentre outros.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> (...)
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (BRASIL,2018)

Com a adoção da transparência, pretende-se conferir uma relação de lealdade entre aqueles que têm acesso e que realizam o tratamento de dados (agentes) e os titulares dos dados. Nas palavras de VAINZOF (2019, p. 150):

> O titular dos dados carece da ampla informação sobre o tratamento dos seus dados para que consiga enxergar cristalinamente, a legalidade, a legitimidade e a segurança do tratamento de acordo com o seu propósito, adequação e necessidade. Assim, terá condições para refletir sobre o tratamento e tomar decisões de acordo com os seus direitos.

Conforme sustentado pelo GT29 (Grupo de Trabalho do Artigo 29) em seu estudo sobre a transparência no contexto do GDPR, a transparência está intrinsecamente ligada à lealdade e ao Princípio da Responsabilização, o qual impõe aos agentes de tratamento a transparência das operações para que possam comprovar o cumprimento das suas obrigações[70].

70 O art. 24º, n.º 1 do GDPR estabelece a obrigação dos agentes de tratamento de aplicarem medidas técnicas e organizativas para assegurar e poder comprovar a conformidade do tratamento, *verbis*: "Artigo 24.: **Responsabilidade do responsável pelo tratamento:** 1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com

Na LGPD, podemos fazer similar conexão com o Princípio da Responsabilização e prestação de contas, o qual institui a obrigação de demonstração, pelo agente, da adoção de medidas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas, conforme previsto no art. 6º, X[71].

Ao longo de toda LGPD verificam-se comandos quanto à forma de prestação de informações e acesso a serem adotados pelos controladores, bem como instruções e garantias quanto ao exercício dos direitos pelos titulares. Cita-se, como principais artigos relacionados ao Princípio da Transparência os seguintes: Art. 9º; Art. 9º § 1º; Art. 10. § 2º; Art. 14 § 6º; Art. 19; Art. 20 § 1º; Art. 23; Art. 33; Art. 40; Art. 41. § 1º; Art. 50; e Art. 55-J.

Do explicitado acima, pode-se dizer que Princípio da Transparência abrange três esferas centrais na LGPD, quais sejam: i) a prestação de informações claras, precisas e facilmente acessíveis aos titulares dos dados, relativamente à realização de tratamento de dados; ii) a prestação de informações sobre os próprios agentes de tratamento; e iii) a conduta dos agentes relativamente à facilitação do exercício dos direitos dos titulares elencados no artigo 9º[72] e nos artigos 17 e 18[73].

---

o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades".

71 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

72 Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

73 Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos

Depreende-se, daí, que a adequação dos agentes de tratamento de dados pessoais no que tange à transparência impõe uma verdadeira transformação cultural que deve alcançar os níveis estratégico, tático e operacional das instituições.

Tal transformação envolve, necessariamente, a promoção de ações de conscientização para incorporação dos princípios fundamentais do tratamento de dados por todos os membros da instituição, bem como a adoção de boas práticas relacionadas à privacidade e à proteção dos dados pessoais desde a concepção dos produtos e serviços até o término de sua execução e consequente término do tratamento dos dados (*Privacy by Design*).

Associado aos Princípios da Finalidade, Adequação e Necessidade, a concretização do Princípio da Transparência mediante a prestação de informações claras, precisas e facilmente acessíveis ao titular, garante a legalidade do tratamento permitindo ao agente a comprovação do cumprimento das disposições legais ao mesmo tempo que empodera o titular e garante a ele a necessária consciência sobre o tratamento dos seus dados pessoais. Nesse sentido, podemos dizer que a concretização do Princípio da Transparência capacita os titulares a exercerem maior controle sobre os seus dados pessoais ao impor a adoção de condutas positivas dos agentes de tratamento quando prestam ou dão acesso a informações.

Para além do cumprimento do dever de informar, o Princípio da Transparência requer dos agentes que a informação prestada aos

---

termos desta Lei.
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, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; 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.

titulares seja altamente qualificada e permita efetivamente o acesso e a compreensão adequados do conteúdo que se pretende divulgar.

A prestação de informações **claras**, **precisas** e **facilmente acessíveis** impõe ao controlador a obrigação de estabelecer com o titular dos dados uma comunicação efetiva e eficiente, com acesso e compreensão facilitados e adequados didaticamente a quem se dirige. Nesse aspecto, exemplificativamente, a lei prevê expressamente no parágrafo 6º do artigo 14 –que aborda o tratamento dos dados pessoais de crianças e adolescentes –a obrigação do controlador de fornecer as informações sobre o tratamento dos dados de maneira simples, clara e acessível, "consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança" (BRASIL, 2018).

A clareza relaciona-se diretamente com a eleição da forma de comunicação que permita que o conteúdo seja o mais convincente e compreensivo possível por uma pessoa média do público visado. A União Europeia, em 2010, publicou uma cartilha muito didática sobre como "redigir com clareza", na qual apresenta várias dicas que auxiliam no alcance de uma redação apropriada[74].

Quanto à precisão da informação, relaciona-se com a escolha rigorosa de palavras e expressões que possam traduzir o conteúdo a ser apresentado aos titulares, evitando-se a adoção de textos prolixos, inexatos e que deem margem a várias interpretações possíveis. O que se pretende é que, com a informação precisa, o titular não tenha dúvidas quanto ao que será executado pelos agentes de tratamento, bem como quanto a quem são os agentes de tratamento e como poderá vir a exercer seus direitos.

Relativamente à acessibilidade, a informação deve estar disponível de forma ostensiva e facilitada, e o seu formato de apresentação deve ser adequado. Vale dizer: a informação deve ser

74 Disponível em: https://op.europa.eu/en/publication-detail/-/publication/725b7eb0-d92e-11e5-8fea-01aa75ed71a1/language-pt.

disponibilizada de modo a permitir a compreensão do conteúdo. É preciso que a mensagem seja inteligível para o seu destinatário e, também, é preciso que seja destacada e encontrada sem dificuldades. Portanto, as informações relacionadas ao tratamento de dados devem diferenciar-se claramente de outras informações não relacionadas especificamente com o tratamento.

Acrescente-se, quanto à qualificação da informação a ser prestada, a boa prática de se adotar, um tanto ou quanto possível, formato conciso e direto para não expor ou, na medida do possível, minimizar a exposição do titular a uma fadiga informativa, desviando ou mesmo impedindo a compreensão dos tratamentos realizados.

Em caso de incerteza quanto ao nível de inteligibilidade e transparência das informações e de eficácia das interfaces propostas, os agentes podem realizar testes e consultas preliminares com o público-alvo, testes destes parâmetros e ainda realizar consulta formal junto às autoridades competentes, notadamente perante a Autoridade Nacional de Proteção de Dados –ANPD e, em regra, aos órgãos de defesa do consumidor.

Um importante aspecto a ser levado em conta quanto à observância do Princípio da Transparência pelos agentes de tratamento relaciona-se à adoção de boas práticas no que tange à segurança da informação. Conforme artigo 48 da LGPD, o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Para concretização de uma postura responsável de transparência, além da prestação das informações sobre o tratamento de dados e sobre os agentes de tratamento, recomenda-se que seja concedido ao titular dos dados o poder determinar antecipadamente qual o âmbito do tratamento e quais as possíveis consequências decorrentes desse tratamento, bem como informar os possíveis danos que lhe serão acarretados em eventual situação de incidente. A adoção dessas medidas oportuniza ao titular uma visão geral dos tipos de tratamento que podem ter maior impacto nos seus direitos e

liberdades fundamentais em relação à sua privacidade e à proteção de seus dados.

3. CONSIDERAÇÕES FINAIS

Por tudo exposto, resta evidente que a obrigação de transparência permeia toda a legislação e deve ser observada independentemente da base legal que fundamenta juridicamente o tratamento, em todas as etapas do ciclo de vida dos dados: desde o início do tratamento de dados, informando os titulares acerca de como se dá o tratamento e quais os direitos que lhe são garantidos, perpassando por todo o período de processamento dos dados para o exercício de direitos pelos titulares e para outras situações, por exemplo, em caso de alteração na forma ou na finalidade do tratamento, até o encerramento do ciclo ou ainda em situações envolvendo incidentes de segurança que acarretem ou possam acarretar violação de direitos dos titulares.

Em verdade, a observância do Princípio da Transparência constitui requisito legal mínimo a embasar o tratamento de dados em conformidade com a LGPD, dando concretude ao direito fundamental à proteção dos dados pessoais.

Portanto, a busca pela concretização de uma utopia protetiva dos dados pessoais deve continuar para, mediante adoção de mecanismos responsáveis e transparentes de tratamento de dados, dar-se a materialização da garantia dos direitos dos cidadãos do novo milênio.

REFERÊNCIAS

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

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em 14 de novembro de 2023.

BRASIL. Lei Geral de Proteção de Dados Pessoais. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 14 de novembro de 2023.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção de dados do consumidor**. São Paulo: Almedina, 2018.

COELHO, Alexandre Zavaglia. Disponível em: https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/transparencia-do-algoritmo-decisoes-automatizadas-e-direito-a-explicacao. Acesso em 14 de novembro de 2023.

COMISSÃO EUROPEIA. Redigir com clareza. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/725b7eb0-d92e-11e5-8fea-01aa75ed71a1/language-pt. Acesso em 13 de novembro de 2023.

FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em < www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018>. Acesso em 14 de novembro de 2023.

GOBBI, de Thais; MINASSE, Elton; RIBEIRO, Yuri Camelo. Interface entre a nova lei do cadastro positivo e a lei geral de proteção de dados. Disponível em <https://www.machadomeyer.com.br/pt/

inteligencia-juridica/publicacoes-ij/tecnologia/interface-entre-a-nova-lei-do-cadastro-positivo-e-a-lei-geral-de-protecao-de-dados>. . Acesso em 13 de novembro de 2023.

Grupo de trabalho do artigo 29. Orientações relativas à transparência na aceção do Regulamento 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. . Acesso em 10 de novembro de 2023.

LEME, Carolina da Silva. Proteção e Tratamento de Dados sob o Prisma da Legislação Vigente. Disponível em: <http://www.veirano.com.br/upload/content_attachments/920/591112_FID_01_Protecao_tratamento_dados_original.pdf>. Acesso em 10 de novembro de 2023.

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

NOGUEIRA, Fernanda A.C. M.N., e da FONSECA, Maurício L. O consentimento na lei geral de proteção de dados: autonomia privada e o consentimento livre, informado, específico e expresso. In**: Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. Org. Bernardo Menicucci Grossi. Porto Alegre: Editora Fi, 2020.

PECK, Patrícia. LGPD e saúde: os fins justificam os meios? Disponível em < https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude>. Acesso em 02 de novembro de 2023.

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

SCORSIM. Ericson Meister. Lei brasileira de proteção de dados pessoais: análise de seu impacto para os titulares de dados

pessoais, empresas responsáveis pelo tratamento de dados pessoais e setor público. Disponível em: < https://www.migalhas.com.br/dePeso/16,MI286453,21048-Lei+brasileira+de+protecao+de+dados+pessoais+analise+de+seu+impacto. . Acesso em 10 de novembro de 2023.

SOARES. Pedro Silveira Campos. A Questão do Consentimento da Lei Geral de Proteção de Dados. Disponível em < https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados#_ftn1>. Acesso em 11 de novembro de 2023.

VAINZOF, Rony. Disposições preliminares. In: **LGPD: Lei Geral de Proteção de Dados comentada**. Org. Viviane Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters Brasil, 2019.

VIEIRA, Tatiana Malta. O Direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação de Mestrado. Universidade de Brasília, 2007. Disponível em: https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf. . Acesso em 04 de novembro de 2023.

REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA LGPD: ANÁLISE DAS LEIS EXISTENTES E O PROJETO DE LEI 2.338/23

REGULATION OF ARTIFICIAL INTELLIGENCE IN THE LGPD: ANALYSIS OF EXISTING LAWS AND BILL 2,338/23

Ana Paula Dos Santos

Ana Paula Dos Santos[75]

> *Artificial intelligence is the elucidation of the human learning process, the qualification of the human thinking process, the explication of human behavior, and the understanding of what makes intelligence possible.*
> (kai -Fu Lee)

RESUMO

Este artigo tem como foco principal a análise da regulamentação da inteligência artificial no Brasil. Tendo em vista que os benefícios trazidos pela inteligência artificial são incontáveis, assim como os riscos que esta expõe ao fazer uso indiscriminado de dados pessoais. O objetivo foi pesquisar o contexto histórico da inteligência artificial e as leis existentes no ordenamento jurídico brasileiro relacionadas à tecnologia, em especial a Lei Geral de Proteção de Dados, bem como analisar o Projeto de Lei 2.338/23. Nesse contexto, chegou-se à conclusão de que as leis existentes não atendem às demandas dos sistemas de inteligência artificial. No entanto, entende-se que o Brasil está no caminho correto de regulamentação, por meio do Projeto de Lei 2.338/23.

Palavras-chave: Lei Geral de Proteção de Dados. Inteligência Artificial. Dados Pessoais. Tecnologia. Projeto de Lei.

ABSTRACT

This article's main focus is the analysis of the regulation of artificial intelligence in Brazil. The benefits of artificial intelligence are countless, as are the risks it poses when making indiscriminate use of

75 * Advogada. Doutoranda em Direito da Privacidade pela University of the Pacific School of Law, California (USA). Mestre em Negócios Transnacionais pela University of the Pacific School of Law, California (USA). Atualmente, escrevendo artigos em espanhol para D' primera mano magazine com foco em privacidade, crimes cibernéticos e como vítimas de crime podem acessar benefícios no estado da Califórnia. Membro da Comissão de Proteção de Dados da OAB/MG e da Comissão Especial de Privacidade de Dados e Inteligência Artificial OAB/SP.

personal data. The objective was to research the historical context of artificial intelligence and the existing laws related to technology laws in the Brazilian legal system, especially the General Data Protection Law, and analyze Bill 2,338/23. In this context, it was concluded that existing laws do not meet the demands of artificial intelligence systems. However, it is understood that Brazil is on the correct path of regulatory pursuit through Bill 2,338/23.

Keywords: General Data Protection Law. Artificial Intelligence. Personal Data Technology. Bill 2,338/23.

1. INTRODUÇÃO

A inteligência artificial (IA) incorporada a diferentes tipos de tecnologia transformou o mundo. A facilidade de comprar, acessar, ler e executar quase todas as funções por meio do telefone celular sem sair de casa alterou de forma drástica a maneira que todos interagem com o mundo. [76] Alguns exemplos desta transformação podem ser encontrados no cotidiano, como: a Alexa da Amazon,[77] a possibilidade de encontrar soluções através de assistentes virtuais, como a Bia do Bradesco,[78] Smart TVs programadas para sugerir o que assistir baseando-se nas seleções anteriores. IA também está presente nos escritórios de advocacia usando tecnologia para diminuir o tempo em diversas funções que antes levavam horas e hoje são resolvidas em segundos,[79] tribunais de justiça utilizando SAVIA,[80] ou o Programa de

76 SOLOVE, Daniel, 2004 p.1

77 O que é Alexa? Disponível em: https://www.amazon.com.br/b?ie=UTF8&nod19949683011. Acesso em: 10 out.2023.

78 Assistente virtual Bia. Disponível em: https://banco.bradesco/canaisdigitais/conheca-bia.shtm. Acesso em: 10 out. 2023.

79 Glauce Cavalcanti, Escritórios de advocacia usam inteligência artificial para ganhar agilidade e prever decisões, O Globo, disponível em: https://oglobo.globo.com/economia/negocios/noticia/2022/11/escritorios-de-advocacia-usam-inteligencia-artificial-para-ganhar-agilidade-e-prever-decisoes.ghtml Acesso em: 10 out. 2023.

80 O Sistema Assistente Virtual de Inteligência Artificial (SAVIA) auxilia magistrados, servidores e colaboradores do TJMG na redação de textos. Disponível em: https://

Justiça Eficiente (PROJEF 5.0).[81] Empregando o uso de dados pessoais para treinamento de programas, a IA consegue atingir resultados inimagináveis. No entanto, tais comodidades ameaçam a privacidade e expõem dados sensíveis a riscos que podem levar a vários colapsos sociais, tais como: perfilamento, preconceitos raciais, exclusão de grupos sociais, julgamento incorreto e manipulação de grupos sociais.[82] Já se entendeu que existem vantagens e desvantagens no uso de IA.

Assim, a análise da regulamentação de IA devido ao seu impacto na questão da privacidade, causado pelo constante uso de dados pessoais, torna-se imperativo.[83] O presente artigo tem como objetivo responder às seguintes indagações: como a regulamentação da IA tem evoluído historicamente no contexto brasileiro? Qual é a importância da regulamentação da IA em relação à proteção de dados pessoais e à privacidade dos cidadãos no Brasil? De que maneira o Projeto de Lei 2.338/23 aborda as complexidades e desafios da regulamentação da IA no cenário brasileiro? Quais são as principais lacunas e desafios na regulamentação da IA que ainda precisam ser abordados no Brasil?

---

www.tjmg.jus.br/portal-tjmg/noticias/tjmg-apresenta-savia-nova-ferramenta-de-inteligencia-artificial.htm

81 O Programa Justiça Eficiente (PROJEF 5.0) utiliza programas de tecnologia visando o aumento de eficiência jurisdicional. Disponível em: https://www.tjmg.jus.br/portal-tjmg/informes/programa-justica-eficiente-projef-5-0.htm Acesso em: 10 out. 2023.

82 SOLOVE, Daniel, 2004, p.2; outros exemplos dos riscos decorrentes do uso de inteligência artificial. https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence

83 Conflitos de privacidade existem por mais tempo do que podemos imaginar. Os primeiros casos sobre a invasão de privacidade têm raízes profundas nas tradições anglo-americanas. Ver Gee v. Pritchard, 2 Swans. 402, 36 Eng. Rep. 670 (1818), relacionado a publicações de cartas privadas. Prince Albert v. Strange, 2 De G. & Sm. 652, 41 Eng. Rep. 1171, 1 Mac. & G. 25, 64 Eng. Rep. 293 (1849), o tribunal concedeu uma liminar ao príncipe Albert para que suas gravuras de um catálogo não fossem publicadas por um estranho. No entanto, diz-se que o direito à privacidade tem sua origem no direito consuetudinário. Em seu famoso livro, A *Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract* publicado em 1878, o Juiz Thomas Cooley, em uma classificação de direito da responsabilidade civil, identificou a imunidade pessoal como um direito de imunidade completa: "to let alone" de ser deixado em paz. Em 1980, Samuel Warren e Louis Bradeis confiaram na classificação do juiz Cooley e cristalizaram o direito à privacidade como "the right to bel et alone."

Neste estudo, analisam-se as leis do ordenamento jurídico que atualmente regulamentam a inteligência artificial e como o Projeto de Lei 2.338/23, ainda em fase preliminar, atende ou não aos anseios de estudiosos, empresas e sociedade, como forma de prevenir conflitos entre privacidade e avanços tecnológicos.[84] Assim, mostra-se necessário o presente estudo para verificar se o projeto de lei é adequado para regulamentação de IA, tendo em vista que uma legislação eficaz necessita de disposições que contemplem o equilíbrio entre tecnologia e privacidade. Desse modo, para este estudo, foi utilizada a pesquisa bibliográfica qualitativa, agregando informações de diferentes estudos arquivísticos e especialistas que pesquisam o tema e apresentam abordagens distintas em periódicos acadêmicos, livros, livros eletrônicos, revistas e recursos on-line, bem como sites, organizações e catálogos de bibliotecas.

Primeiramente, este artigo aborda um breve histórico da evolução da inteligência artificial. Logo após, discorre sobre o marco legal e uma visão geral de leis relacionadas à tecnologia. Em seguida, faz a análise de artigos específicos da LGPD aplicáveis à proteção de dados relacionados à IA. Por fim, sintetiza o Projeto de Lei 2.338/23, referente à regulamentação de IA.

2. INTELIGÊNCIA ARTIFICIAL: BREVE EVOLUÇÃO

Os primeiros trabalhos com redes neurais começaram em 1956, quando Jonh McCarthy, da Universidade de Dartmouth, nos EUA, organizou um projeto de pesquisa de dez semanas chamado "Um Estudo de Inteligência Artificial."[85] O objetivo do programa de verão era reunir um grupo de cientistas para desenvolver máquinas que pudessem aprender o que os humanos fazem. Partindo do pressuposto de que o processo de aprendizagem pode ser descrito com precisão, o projeto

84 BRASIL. Senado Federal. Projeto de Lei 2338/23. Brasília. 2023. Disponível em: documento (senado.leg.br). p.04.

85 Para mais informações sobre o projeto. https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth Acesso em: 10 oct. 2023.

de pesquisa de dez semanas foi um ponto crucial na IA.[86] Seguindo os desenvolvimentos a partir daí, jovens acadêmicos começaram a explorar novas ideias. Por exemplo, o programa "Logic Theorist"[87] foi a criação de Hebert Simon trabalhando com Allen Newell e Cliff Shaw.[88] O programa foi projetado para ler mais do que números. Além disso, é considerado o primeiro programa de IA desenvolvido.

Posteriormente, outros programas e avanços foram ganhando destaque. No final da década de 1950, John McCarthy fez mais do que promover a fundação do Laboratório de Inteligência Artificial do Massachusetts Institute of Technology (MIT).[89] McCarthy também desenvolveu outros programas relacionados à linguagem de programação. Em 1961, McCarthy elaborou a ideia do compartilhamento de tempo que criou a Internet e a computação em nuvem. [90]

Assim, os primeiros objetivos dos desenvolvedores de IA começaram a florescer mediante máquinas fortes com programas direcionados às capacidades humanas. Um incentivo importante para esses programas e descobertas avançadas, foi o apoio e o interesse do Governo americano em promover a indústria para desenvolver novas tecnologias para conquistas específicas, como o programa espacial Apollo e outros projetos relacionados à Guerra Fria.[91] Entre os anos de 1970 e 1980, a IA foi quase suspensa devido a crises econômicas e outras questões que afetaram os fundos para o desenvolvimento da tecnologia, chamada inverno da IA.[92] A IA teve alguns avanços e

86 TAULLI, Tom, 2019, ch.1

87 Logic Theorist foi um programa inventado para copiar a habilidade humana de resolver conflitos. Disponível em: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ Acesso em: 10 oct. 2023.

88 Para mais informações sobre esses inventores.
Disponível em: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ Acesso em: 10 out. 2023.

89 Bibliografia completa de Jonh McCarthy considerado o pai da inteligência artificial. Disponível em: http://jmc.stanford.edu/ Acesso em: 12 out. 2023.

90 TAULLI, Tom, 2019, ch.1

91 Idem.

92 Ibidem.

descobertas posteriores, e hoje é uma inovação líder que transformou como os humanos veem o mundo. Geoffrey Hinton descreve o conceito moderno de IA comparando de forma genérica a ideia do cérebro humano. Tudo vai depender dos estímulos e exposição de aprendizagem. Uma máquina pode aprender com exemplos em vez de ser programada, significa que a IA também é um processo obtido por meio de *deep-learning*, aprendizagem profunda.[93]

Dessa forma, no *machine learning,* aprendizado de máquina, muitas imagens que às vezes apresentam rostos humanos são fornecidas à IA.[94] Nesse processo de treinamento, o computador cria seu algoritmo, conhecido como aprendizado de máquina não supervisionado, quando a máquina não possui alguém orientando o processo.[95] Esse processo também pode acontecer com supervisão humana, conhecida como aprendizado de máquina supervisionado ou semissupervisionado.[96] O aprendizado de máquina profundo é o processo pelo qual a máquina usa várias camadas de redes neurais artificiais para aprender com os dados de treinamento.[97] Talvez isto possa ser comparado à forma como os humanos aprendem, que é através de exemplos, estudo, leitura e audição; e, depois de tudo isso, o processo de aprendizagem está finalizado.[98] Assim, entende-se que o processo de aprendizado de máquina busca ser semelhante ao processo de aprendizagem humana.

Cientistas que estudam o comportamento do cérebro humano encontraram uma maneira não de programar, mas, sim, de treinar máquinas da mesma forma que a mente humana funciona.[99] Na

93 ARRUDA, 2017 apud HINTON.

94 MARR, Bernard; WARD, Matt 2019, ch.1

95 Idem.

96 Informações sobre aprendizado de máquina supervisado não supervisionado. Disponível em: https://www.ibm.com/blog/supervised-vs-unsupervised-learning/ Acesso em: 12 out. 2023.

97 MARR, Bernard; WARD, Matt 2019, ch.1

98 Id., a respeito da história de IA de forma mais detalhada ver e.g., (DOS SANTOS, Ana Paula, 2020.p. 28)

99 Ibidem.

verdade, a IA converte tarefas complexas em tarefas práticas que são mais fáceis de gerir.[100] No entanto, a completa definição de IA é um desafio por se tratar de uma tecnologia de vasta aplicação e em constante expansão.

Atualmente, IA generativa é capaz de produzir novos conteúdos, que vão desde texto até vídeos.[101] Alguns exemplos de sistemas que utilizam a IA generativa são o ChatGPT, DALL-E[102] e o Bard.[103] Talvez até a edição completa deste artigo essas últimas ferramentas citadas sejam consideradas obsoletas, tendo em vista a velocidade dos avanços de sistemas de IA. Dessa forma, faz-se necessário um estudo da evolução do marco legal brasileiro referente a leis que regulam tecnologia ou conferem proteção aos dados pessoais.

3. MARCO LEGAL NO ORDENAMENTO JURÍDICO BRASILEIRO

O estudo do marco legal é relevante para entender como as leis foram elaboradas e adaptadas para solucionar o existente atrito entre privacidade e IA.

No ordenamento brasileiro, a proteção de dados está disposta de forma indireta no Código de Defesa do Consumidor, Lei n.º 8.078 de 11 de setembro de 1990. Artigo 43 da lei. "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." Dispõe sobre a exigência de cadastro de indivíduos, bem como a forma

100 STEPHENSON, David, 2018, ch.1

101 Informações mais completes sobre IA generativa. Disponível em: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai#/ Acesso em: 12 out. 2023.

102 A descrição completa destes dois sistemas de IA generativa. Disponível em: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai#/ Acesso em: 12 out. 2023.

103 Informações sobre o Bard AI da Google. Disponível em:https://blog.google/technology/ai/bard-google-ai-search-updates/ Acesso em: 12 out. 2023.

de comunicação com o interessado sobre a abertura de cadastro. Contudo, tal lei foi voltada para regulamentação de banco de dados, a problemática de consentimento ao recolher tais dados não foi tomada como prioridade.[104] Posteriormente, a Lei de Acesso à Informação (LAI), Lei n.º 12.527/11, voltada para o princípio da publicidade dos atos administrativos, permitiu aos cidadãos o direito ao acesso às informações sobre a execução de políticas públicas. Depois, a Lei do Marco Civil da Internet (MCI), de n.º 12.965 de 2014, que regula os direitos e deveres na utilização da internet, visando garantir a proteção dos dados pessoais e a privacidade dos usuários. Ressalta em seu artigo 7:

> Art. 7 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;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a

104 ANDRADE; Diego; MOURA, Plínio, 2019, p.115.

> aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; (BRASIL, 2014)

É preciso salientar, a partir da análise do artigo 7 da MCI, a importância da proteção de dados pessoais já consolidada na Constituição Federal no artigo 5º, inciso X da CF/88 "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." (BRASIL, 1988).

A MCI destaca, no artigo 7, o sigilo estrito de armazenamento de dados e a possibilidade de indenização em caso de violação. Ressalta, no inciso VII, o não compartilhamento de dados pessoais com terceiros sem o consentimento e descreve como será realizada a exclusão de dados, bem como a troca de prestador de serviços. No artigo 25, inciso III, dispõe sobre as aplicações de internet para as entidades do poder público a compatibilidade quanto aos meios humanos ou automatizados. No entanto, não faz previsão para empresas privadas ou menção de tratamento de dados pessoais por meio de automatização.

Entretanto, a emenda constitucional nº115 de 2022 trouxe a completa ampliação da proteção dos direitos fundamentais, disposta no artigo 5º da constituição, incluindo a proteção de dados pessoais

nos meios digitais, "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais." (BRASIL, 2022) Tal emenda apenas consolida o disposto na Lei n.º 13.709 de 14 de agosto de 2018, mais conhecida como a Lei Geral de Proteção de Dados (LGPD), que concerne sobre a proteção de dados pessoais realizada por empresas nos setores público e privado, abrangendo desde empresas individuais, pequenas, médias e grandes até multinacionais.

A LGPD é considerada uma lei mais robusta e moderna. Esta regula de forma indireta a IA em alguns de seus artigos, pois não faz menção à IA. Contudo, estabelece a restrição do uso de dados pessoais em decisões automatizadas. Todavia, entende-se que as leis existentes no ordenamento jurídico brasileiro não abordam a complexidade dos sistemas de IA. Dessa forma, a análise de alguns dispositivos da LGPD aplicáveis a IA é necessária.

4. INTELIGÊNCIA ARTIFICIAL E A LEI GERAL DE PROTEÇÃO DE DADOS

Conforme descrito na segunda parte deste artigo, IA tem como principal combustível informações pessoais. Por meio do constante treinamento de máquinas, partindo-se de comportamentos humanos, fotos, vídeos, escrita e outras formas de treinamento, programas utilizando-se de IA estão cada vez mais semelhantes à mente humana.[105] Entretanto, é importante destacar alguns dos riscos que AI apresenta para a sociedade, tais como a disfunção no mercado de trabalho, problemas relacionados à privacidade, a falta de transparência nos sistemas, discriminação, ética, segurança, a dependência em sistemas de IA, a manipulação de informação, a corrida armamentista de IA, e muitas outras consequências imprevisíveis.[106] Não obstante, a

105 Theodora (Theo) Lau, When AI Becomes a Part of Our Daily Lives, Harvard Business Review (May, 23.2019), https://hbr.org/2019/05/when-ai-becomes-a-part-of-our-daily-lives

106 Outros exemplos dos riscos oferecidos por IA Em:https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificialintelligence/?sh=7abc94b02706;

necessidade de maior controle de sistemas de IA é imperativa. Assim, a análise de alguns artigos da LGPD na regulamentação do uso de IA é crucial.

A LGPD no artigo 20 confere proteção à utilização de dados pessoais em automatização:

> Art. 20 O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (BRASIL, 2018)

Tal dispositivo empodera o titular dos dados ao direito de revisão em decisões tomadas unicamente por máquinas. Incluindo-se todas as questões que porventura causem dano aos interesses do indivíduo, abrangendo desde o âmbito pessoal até aspectos da personalidade. Tratando-se de segredos industriais ou comercial, a lei inova, trazendo a possibilidade de o indivíduo realizar o pedido de revisão por meio

ver <https://thehill.com/policy/technology/4007018-openai-ceo-senators-weigh-ai-risks-and-regulations/ > Acesso em 16 de maio de 2023.

da autoridade nacional para realização de auditoria e apuração de discriminação por meio de algoritmos.[107]

Dessa maneira, o direito à revisão retira o caráter único de decisões realizadas por máquinas e retoma o aspecto de correção de dados contemplado no artigo 18, III.[108] Não obstante, o tratamento automatizado de dados sujeita-se às disposições gerais descritas nos

107 É importante frisar que decisões feitas por algoritmos necessitam atenção devido aos vários riscos que indivíduos estão expostos como preconceito, redução de escolhas e outras situações únicas nos setores públicos e privados. HOFFMAN, David; MASUCCI, Riccardo, Intel's AI Privacy Policy White Paper, 22 Out. 2018, https://www.intel.com/content/dam/www/public/us/en/ai/documents/Intels-AI-Privacy-Policy-White-Paper-2018.pdf

108 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: III - correção de dados incompletos, inexatos ou desatualizados. [...] (BRASIL, 2018)

artigos 7[109] e 11[110] respectivamente, dispondo quando o tratamento de

109 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o comprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

110 Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os

dados poderá ser realizado de forma geral e de forma específica em relação aos dados sensíveis. Consequentemente, o direito à revisão, disposto no artigo 12, parágrafo segundo da lei a despeito de dados utilizados para a "formação de perfil comportamental,"[111] segue a regra do artigo 20, tendo em vista que indivíduos têm a oportunidade de pedir revisão do perfil comportamental. No entanto, é válido frisar que, embora as características mensuráveis possam ser úteis para determinados fins de identificação e análise, elas fornecem uma perspectiva limitada sobre a complexidade da identidade humana.[112] Assim, a redução da identidade de um indivíduo a características mensuráveis deve ser abordada com cautela.[113]

IA é também regulada na LGPD no artigo 46, que dispõe sobre a necessidade de desenvolvedores da IA considerar a privacidade

direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica. § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (BRASIL, 2018)

111 Art. 12 [...] § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. (BRASIL, 2018); LASMAR. A.; Marco e MARANHÃO, Juliano, 2023. P.8.

112 GADY, Oscar H.2000.p.1.100

113 SOLOVE, Daniel J., 2004.p.117

durante todo o processo de elaboração da nova tecnologia, conhecido como *privacy by design*.[114]

> 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.

No *caput* do artigo, nota-se a imposição aos agentes de tratamento de dados que devem, por medidas de segurança, adotar técnicas administrativas de proteção de dados pessoais. O primeiro parágrafo atribui à autoridade nacional a autonomia de definir quais seriam estes padrões de segurança, tendo em vista a categoria de dados pessoais e a atividade desenvolvida.

Não obstante, o parágrafo terceiro reitera que tais medidas de segurança devem ser levadas em consideração em todas as fases da produção. Sendo adotadas, desde a fase inicial do produto até a fase de execução. Assim, ainda que as proteções dispostas nos artigos analisados da LGPD sejam plausíveis, estes não abarcam toda a sofisticação e complexidade utilizadas em IA, que muitas vezes

114 O conceito de "privacy by design" foi desenvolvido por Ann Cavoukian, Ph.D. através de 7 princípios fundamentais.

requerem um alto nível técnico para entender como um algoritmo fornece os resultados.

Consequentemente, ainda que a possibilidade de revisão das decisões automatizadas, com medidas de segurança adotadas do início ao fim do processo de produção sejam reguladas, as nuances e outros riscos que IA expõe aos indivíduos não foram elencadas na LGPD. Portanto, é essencial analisar o projeto de lei ainda em fase preliminar com o intuito de verificar se este funcionará como um mecanismo de extensão das proteções dispostas na LGPD.

5. PROJETO DE LEI 2.338/23

O Projeto de Lei (PL) 2.338/23, proposto pela Comissão de Juristas responsável por subsidiar a elaboração sobre inteligência artificial (CJSUBIA) apresentado pelo Presidente do Senado Federal Senador Rodrigo Pacheco, estabelece em seus 45 artigos, normas pertinentes a regulamentação dos sistemas de IA.[115] O PL 2338/2023 visa uma abordagem legal mais técnica de IA para "proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e de desenvolvimento científico e tecnológico."[116] O PL busca estabelecer equilíbrio entre a regulamentação de riscos e a proteção de direitos na implementação e uso de sistemas de inteligência artificial. Enfatiza a necessidade de mecanismos de governança, prestação de contas e envolvimento social para garantir que os sistemas de IA sejam desenvolvidos e utilizados de maneira responsável e ética. A proposta define sistemas de inteligência artificial como:

115 O marco regulatório dos sistemas de inteligência artificial conta com outras proposições legislativas no Senado e nas Câmera dos Deputados sendo estes Projeto de Lei (PL) nº 5.051, de 2019, de autoria do Senador Styvenson Valentim, que estabelece os princípios para o uso da Inteligência Artificial no Brasil; o PL nº 21, de 2020, do Deputado Federal Eduardo Bismarck, que estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências.

116 BRASIL. Senado Federal. Projeto de Lei 2338/23. Brasília. 2023. Disponível em: documento (senado.leg.br). Art.1°

> sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real.[117]

Na definição de sistemas de inteligência artificial, encontra-se a delimitação do objeto a ser regulado. O PL busca promover a transparência e permitir que os usuários tomem decisões informadas ao utilizar serviços que envolvem inteligência artificial.

A transparência é fundamental para estabelecer a confiança dos usuários e garantir que eles compreendam o funcionamento e as implicações do software baseado em IA que está sendo utilizado. Além disso, a acessibilidade das informações é importante para garantir que todas as partes envolvidas possam compreender e tomar decisões informadas.[118]

Nesse sentido, indivíduos afetados por sistemas de IA poderão solicitar esclarecimentos sobre a decisão, previsão ou recomendação realizadas por sistemas de IA, bem como os fatores que influenciaram a previsão ou decisão específica. Abrangendo desde a racionalidade lógica, nível de contribuição do sistema, critérios adotados, mecanismos de contestar tais decisões até a possibilidade de solicitação de intervenção humana.[119] Levando em consideração

117 BRASIL. Senado Federal. Projeto de Lei 2338/23. Brasília. 2023. Disponível em: documento (senado.leg.br).
Art. 4°

118 BRASIL. Senado Federal. Projeto de Lei 2338/23. Brasília. 2023. Disponível em: documento (senado.leg.br).
Art.3°

119 BRASIL. Senado Federal. Projeto de Lei 2338/23. Brasília. 2023. Disponível em: documento (senado.leg.br).
Art.11.

que esclarecimentos deverão ser prestados de maneira gratuita, utilizando-se de linguagem que permita o entendimento do resultado ou previsão.

Os artigos que se seguem do PL dispõem sobre o direito de solicitar a correção, anonimização, bloqueio dos dados, eliminação de dados incorretos ou desatualizados, retomando parte da descrição do artigo 18 da LGPD.[120] Outro ponto importante é a exigência de interferência humana em decisões que se utilizam de sistemas de IA, em que os riscos sejam de escala irreversível.

O Artigo 13 do PL estabelece a responsabilidade dos fornecedores de sistemas de IA, documentarem o grau de riscos, criando a possibilidade de categorização por autoridade competente. Já no artigo 17, o PL aborda a classificação de atividades de alto risco e o uso da biometria no âmbito da segurança pública quando houver previsão em lei federal específica em atividades que envolvam persecução penal.

Destacam-se no PL os parâmetros de governança com a exigência de processos internos para a mitigação de riscos no desenvolvimento de sistemas de IA. Tais critérios seriam: medidas de segurança, consultas públicas nos casos de utilização de sistemas de IA que envolvam alto risco por órgãos públicos da União, Estados, Distrito Federal e Municípios. Dessa forma, determina-se a avaliação contínua do funcionamento do sistema, incluindo testes para apurar potenciais discriminatórios, níveis de acurácia, precisão e cobertura.[121]

A promoção e o incentivo ao uso de tecnologia são retomados no artigo 38 ao dispor que a autoridade competente poderá autorizar o funcionamento de ambiente de testes experimentais, o chamado

120 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: [...] III - correção de dados incompletos, inexatos ou desatualizados; (BRASIL, 2018)

121 BRASIL. Senado Federal. Projeto de Lei 2338/23. Brasília. 2023. Disponível em: documento (senado.leg.br). p.04.

sandbox regulatório.[122] O PL trata também de disposições gerais e penalidades para o não cumprimento das disposições descritas.

Em uma perspectiva geral, o PL abrange muitas das tecnicalidades de IA com linguagem clara. Em análise preliminar, a Autoridade Nacional de Proteção de Dados (ANPD) ressalta vários pontos da PL em um documento de 31 páginas.[123] Tal documento destaca muitos pontos de interação do PL 2338/23 com a LGPD, por exemplo, o direito da revisão elencados no artigo 20 LGPD, sendo que, no artigo 9 do PL, os requisitos são mais restritos e não fazem a menção ao artigo 20 da LGPD. A ANPD, recomendou um maior destaque às questões relativas ao sandbox regulatório e realizou uma análise comparativa, dando ênfase às medidas de governança propostas pelo PL que fazem a direta correlação com disposições da LGPD, como o princípio da transparência, e o conceito de *privacy by design.*

No entanto, a ANPD alertou para a competência exclusiva na aplicação de sanções no que se refere à proteção de dados e por isso ressalvou que, em diversos países, as Autoridades de Proteção de Dados estão fazendo uso de suas atribuições para regular sistemas de IA. No final da análise, a ANPD recomendou que se resumem em harmonização entre o PL e a LGPD, promoção à proteção de dados em *sandboxes* de IA e fortalecimento do papel da ANPD como autoridade central para assuntos relacionados à IA e proteção de dados no Brasil.

Nota-se que a abordagem e nível de tecnicidade do PL 2338/23 preenche as lacunas encontradas na LGPD que não foi uma lei criada para regular IA. No entanto, como já explicado, para a IA, o principal

122 Sandboxes regulatórios são colaborações que reúnem reguladores e organizações com novas tecnologias e processos para testar as inovações em relação ao quadro regulamentar. DATASPHERE INITIATIVE. Sandboxes for data: creating spaces for agile solutions across borders. Disponível em: https://www.thedatasphere.org/datasphere-publish/sandboxes-fordata/. Acesso em: 10 out. 2023
https://www.gov.br/startuppoint/pt-br/iniciativas/sandbox-regulatorio /. Acesso em: 10 out.2023; Regulatory Sandboxes in Artificial Intelligence, OECD Digital Economy Papers, OECD,
https://www.oecd.org/publications/regulatory-sandboxes-in-artificial-intelligence-8f80a0e6-en.htm Acesso em: 10 out. 2023.

123 ANPD,2023.

combustível são dados pessoais, daí a importância de leis que se complementem e possam ser aplicadas em conjunto.

Recentemente a ANPD publicou a segunda análise do PL 2338/23, que consiste em uma nota técnica elaborada pela Coordenação Geral de Tecnologias e Pesquisa (CGTP).[124]

Em resumo, o documento aborda a conexão existente entre o PL e a LGPD no que concerne à tutela de direitos dos cidadãos e da governança de tecnologias emergentes e assinala os correspondentes artigos na LGPD e no PL. A nota técnica também ressalta as competências da ANPD, que já vem sendo reconhecida pelas boas práticas regulatórias e que, com a experiência já adquirida, poderia ser reconhecida como autoridade reguladora de IA no Brasil. Em seguida cita alguns exemplos de atuação centralizada de autoridade de proteção na União Europeia, na França, na Holanda, na Espanha e no Canadá.

No entanto, a nota técnica propõe um modelo institucional de regulamentação de sistemas de IA com quatro instâncias complementares, sendo estas: poder executivo, órgãos reguladores setoriais, poder consultivo e a ANPD como órgão central.

Sobre a proposta, a diretora da ANPD Mirian Wimmer ponderou a respeito da necessidade de centralização regulatória para evitar interpretações conflituosas por diferentes órgãos. Contudo, a busca da normatização de IA requer todas essas discussões e estudos profundos acerca da temática. Ainda que a segunda análise apresente uma perspectiva diferente sobre forma de controle, esta auxilia a ter uma visão de como funcionaria a forma de controle descentralizada.[125]

124 ANDP; CGTP, 2023.

125 Ver comentários da segunda análise realizada pelo CGTP. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-segunda-analise-do-projeto-de-lei-sobre-inteligencia-artificial Acesso em: 24 out. 2023.

6. CONSIDERAÇÕES FINAIS

Após uma análise sucinta da história da inteligência artificial para entender um pouco sobre sistemas de IA, verifica-se que a regulamentação de IA é imprescindível, uma vez que tais sistemas já estão incorporados a quase todas as ferramentas tecnológicas atualmente utilizadas. Seja esta utilização na esfera privada, pública, comercial ou jurídica. Já não é possível negar que IA é parte da era digital e carrega consigo riscos e benefícios para a sociedade. Por isso, a busca pelo equilíbrio e o uso ético de IA é pauta de discussão legislativa.

Dessa forma, o estudo do marco legal do ordenamento jurídico brasileiro demonstrou que a única lei existente que regula de maneira indireta a IA é a LGPD. No entanto, vislumbrou-se que esta aplica-se aos sistemas de IA de maneira indireta em alguns artigos. A LGPD não atende a todos os pressupostos de regulamentação da IA, uma vez que essa não dispõe de regras tratando das especificidades técnicas da IA. Portanto, não existe uma lei normatizando o uso de IA no Brasil.

Embora em fase de análise preliminar, o PL 2338/23 atende à muitas das tecnicidades exigidas pela IA. Não é um PL que tem como foco a descrição de sistemas de IA, no entanto, tem regras claras, de fácil interpretação e entendimento. Como foi elaborada por uma comissão de juristas, vê-se que pesquisas extensivas foram realizadas visando apresentar um PL que atendesse às demandas atuais e que, de forma preventiva, regulamentasse a IA. Ainda que não tenha sido aprovado, o PL 2338/23 mostra-se um avanço na normatização de sistemas de IA no Brasil.

REFERÊNCIAS

ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v.5, n.1, p.110-133, jan/jun. de 2019.

ANPD, Análise Preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial. 07 jul. de 2023.

ANYOHA, Rockewell. The History of Artificial Intelligence. **Harvard University The Graduate School of Arts and Sciences**, 28, ago.2017. Disponível em: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/. Acesso em: 10 out. 2023.

ARRUDA, Andrew. Defining Artificial Intelligence with AI pioneers Bengio, Hinton, Ovbiagele & P M Tradeau. Ross, 6, nov. 2017. Disponível em: https://blog.rossintelligence.com/post/ai-pioneers--bengio-hinton-ovbiagele-pm-trudeau. Acesso em: 10 out. 2023.

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

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 5 out. 2023.

BRASIL, **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco da Internet disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 5 out. 2023.

BRASIL. Senado Federal. **Projeto de Lei 2338/23.** Brasília. 2023. Disponível em: documento (senado.leg.br).

CAVOUKIAN, Ann Ph.D., Privacy by Design The 7 Foundational Principles, Information & Privacy Commissioner, Revised Jan. 2011.

CGPT; ANPD, Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023, Nota Técnica nº 16/2023/CGTP/ANPD. Acesso em: 24 out. 2023.

COOLEY M. Thomas. A Treatise On The Law Of Torts: Or The Wrongs Which Arise Independently Of Contract. Callaghan. 1932.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2019.

DOS SANTOS, Ana Paula. The Impact of Artificial Intelligence on Data Protection: A Legal Analysis, University of the Pacific, McGeorge School of Law Dissertations. 4, 2020.Disponível em: https://scholarlycommons.pacific.edu/mcgeorge-dissertations/4/ Acesso em: 10 out. 2023.

GANDY. J, Oscar. Exploring Identity and Identification in Cyberspace, 14 Notre Dame Journal of Law, Ethics & Public Policy, 2000.

LASMAR ALMADA, M. A.; SOUZA DE ALBUQUERQUE MARANHÃO, J. Contribuições e Limites da Lei Geral de Proteção de Dados para a Regulação da Inteligência Artificial no Brasil. **Revista Direito Público**, *[S. l.]*, v. 20, n. 106, 2023. DOI: 10.11117/rdp.v20i106.6957. Disponível em:<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6957>.Acesso em: 23 out. 2023.

LEE, Kai-Fu. AI Super Powers China, Silicon Valley and The New World Order. Houghton Mifflin Harcourt Bos. N.Y.C.2018.

MARR, Bernard, and WARD, Matt. Artificial Intelligence In Practice: How 50 Successful Companies Used AI and Machine Learning To Solve Problems. 2019.

What is Generative AI? Mckinsey & Company, 2023. Disponível em:< https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai#/> Acesso em: 15 out. 2023.

PICHAI, Sundar. An Important Next step on our AI Journey. **Blog Google.** 06 feb. 2023. Disponível em:< https://blog.google/technology/ai/bard-google-ai-search-updates/> Acesso em: 10 out. 2023.

SOLOVE, Daniel J. The Digital Person Technology and Privacy in Information Age, N.Y.U Press. 2004.

STEPHENSON, David. Big Data Demystified: How To Use Big Data and Data Science to Make Better Business Decisions and Gain Competitive Advantage, FT Publishing International, 2018.

TAULLI, Tom. Artificial Intelligence Basics: A Non- Technical Introduction. Apress.2019.

A LGPD E AS IMPLICAÇÕES LEGAIS DA AUDIÊNCIA PÚBLICA NO STF: PROVEDORES DE INTERNET E A ANÁLISE DA REMOÇÃO DE CONTEÚDO POR USUÁRIOS VIA NOTIFICAÇÃO EXTRAJUDICIAL

THE LGPD AND THE LEGAL IMPLICATIONS OF THE PUBLIC HEARING IN THE SUPREME FEDERAL COURT: INTERNET SERVICE PROVIDERS AND THE ANALYSIS OF CONTENT REMOVAL BY USERS THROUGH EXTRAJUDICIAL NOTIFICATION

Anderson Eduardo Pereira
Fernanda Alves Miranda Moreira

Anderson Eduardo Pereira[126]
Fernanda Alves Miranda Moreira[127]

RESUMO

O artigo aborda a audiência pública realizada pelo STF sobre o Marco Civil da Internet, destacando a importância da Lei Geral de Proteção de Dados (LGPD) a partir da possibilidade de remoção de conteúdos via notificação extrajudicial. As implicações constitucionais, além da liberdade de expressão e a proteção de dados pessoais. Análise de responsabilidade dos provedores de internet em relação ao conteúdo gerado por terceiros e a discussão da necessidade de equilibrar a liberdade de expressão com a privacidade e a segurança dos dados. Além disso, enfatiza o papel central do Poder Judiciário como agente exclusivo de controle na avaliação da ilicitude do conteúdo on-line e a importância de criar regulamentações que respeitem esses direitos em um mundo digitalmente conectado.

PALAVRAS-CHAVE: STF (Supremo Tribunal Federal). LGPD (Lei Geral de Proteção de Dados Pessoais). Marco Civil da Internet. Remoção de conteúdos a partir de notificação extrajudicial.

126 Advogado. Bacharel em Direito pela Pontifícia Universidade Católica de Minas Gerais. Consultor em Direito Digital. Mestre e Especialista em Relações de Consumo, LGPD, *GDPR, CCPA* e *Compliance* em Proteção de Dados Pessoais/Corporativos (CPC-PD). Membro da Comissão de Proteção de Dados da Ordem dos Advogados do Brasil de Minas Gerais. Associado *EADPP* (*European Association of Data Protection Professionals*). Associado *AFCDP* (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*). *DPO* (*GDPR Data Protection Officer - University of Derby/Eng*).

127 Advogada. Bacharel em Direito pela Pontifícia Universidade Católica de Minas Gerais. Pós-graduada em Direito Digital, Gestão da Inovação e Propriedade Intelectual pela PUC-Minas. Pós-graduada em Lei Geral de Proteção de Dados e Direito Processual Civil. Membro da ANPPD - Associação Nacional dos Profissionais de Privacidade de Dados e da Comissão de Proteção de Dados da Ordem dos Advogados do Brasil de Minas Gerais.

a constitucionalidade do art. 19 do Marco Civil da Internet; 4. Considerações finais; 5. Referências bibliográficas.

ABSTRACT

The article addresses the public hearing held by the STF on the Internet Civil Framework, highlighting the importance of the General Data Protection Law (LGPD) based on the possibility of removing content via extrajudicial notification. The constitutional implications, in addition to freedom of expression and the protection of personal data. Analysis of the responsibility of internet providers in relation to content generated by third parties and the discussion of the need to balance freedom of expression with privacy and data security. Furthermore, we emphasize the central role of the Judiciary as the exclusive agent of control, in assessing the illegality of online content and the importance of creating regulations that respect these rights in a digitally connected world.

KEYWORDS: STF (Supreme Federal Court). LGPD (General Data Protection Law). Civil Rights Framework for the Internet. Removal of content based on extrajudicial notification.

1. INTRODUÇÃO

Com grande notoriedade, repercussão midiática e amplos debates nos anais jurídicos especializados, em 28/02/2023, o STF, por meio dos ministros Dias Toffoli e Luiz Fux, promoveu audiência pública sobre regras do Marco Civil da Internet.

Os balizadores do tema, em si, focaram o Marco Civil da Internet sem, contudo, enfatizar os pressupostos da Lei nº 13.709/18 (LGPD), que, em 2022, por meio da EC nº 115/2022, determinou a proteção de dados pessoais como garantia constitucional fundamental.

A discussão na Corte Suprema buscou readequar e aclarar de forma objetiva "*a responsabilidade de provedores de aplicativos ou de ferramentas de internet por conteúdo gerado pelos usuários e a possibilidade de remoção de conteúdos que possam ofender direitos de personalidade,*

incitar o ódio ou difundir notícias fraudulentas a partir de notificação extrajudicial".

Partindo da premissa de que o objetivo do STF é suprimir a inércia do Congresso Nacional Brasileiro em legislar (o que, em tese, não fere o sistema de freios e contrapesos da democracia), bem como otimizar/aprimorar a Lei Federal nº 12.965/2014 (ante as decisões dos Recursos Extraordinários 1.037.396 e 1.057.258 - temas 533 e 987 da Repercussão Geral), o foco é alcançar a estabilização e a segurança jurídica.

Sabemos, pelos conceitos da sociologia jurídica, que o Direito não é resultado de uma visão individual. É conceituado como ciência social hermenêutica (em busca de um mundo ideal), enquadrando-se como ciência da natureza com pressupostos valorativos ou mesmo axiológicos. É, portanto, o tutor/regulador de fenômenos ou de fatos que ocorrem no meio social. Assim, somente após o surgimento de um fato social é que surge a regra - o Direito. A sociedade digital, com sua gênese no século XX (entre os anos de 1950 e 1970), tornou-se inexorável no século XXI. Todavia, os normativos legais reguladores dessa nova sociedade digital, ainda possuem um déficit de realidade sem precedentes. A tecnologia avança de tal forma que a obrigação de atualização legislativa é diária. Mas isso não ocorre em toda a sociedade que se encontra no plano do fato social, ou está sem norma reguladora atualizada ou mesmo sem qualquer norma.

Nesse contexto, a busca por um consenso entre os agentes, a proteção de dados pessoais e a liberdade de expressão desempenham papéis essenciais. A responsabilidade dos provedores deve equilibrar a liberdade de expressão com a proteção da privacidade dos cidadãos, respeitando o devido processo legal e os princípios de um Estado Democrático de Direito.

O debate sobre a responsabilidade dos provedores é fundamental em nossa sociedade altamente conectada, pois afeta questões como o acesso à informação, à liberdade de expressão e à privacidade.

2. RESPONSABILIDADE DOS PROVEDORES DE INTERNET E OS DESAFIOS DA LIBERDADE DE EXPRESSÃO: UMA ANÁLISE SOB A INTERPRETAÇÃO DE JÜRGEN HABERMAS E A LGPD

Há que se enfrentar o tema sob os contextos filosóficos e sociológicos, invocando, para tanto, Jürgen Habermas. Temáticas essas que, epistemologicamente, devem nos remeter a uma análise de interesse prático (o que não permeou a discussão no STF), em que "*nem as teorias estão já construídas de modo dedutivo, nem as experiências se encontram organizadas em vista do êxito das operações. Em vez da observação, é a compreensão de sentido que abre o acesso aos factos*" (HABERMAS, 1968, p. 138)[128].

A busca perpetrada nas discussões da Suprema Corte brasileira, em tese, não observou a racionalidade comunicativa, em razão do entendimento do "*possível consenso dos agentes no âmbito de uma autocompreensão transmitida*" (HABERMAS, 1968, p. 139)[129]. Tal digressão proposta no presente artigo, deriva da nítida impressão de que o conteúdo do artigo 1º da LGPD - "*com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade*" - não integrou a pauta da Suprema Corte pátria.

A fim de se justificar a posição sobre as 2 (duas) discussões propostas pelo STF, deve-se frisar que, antes da aferição de responsabilidades dos provedores por conteúdos de usuários, há direitos consolidados a esses mesmos usuários, resguardados em normativos nacionais e internacionais. Portanto, há uma previsão de devido processo legal - o que se destacou no Brasil como efetiva proteção (ainda que no campo teórico), a rigor do já previsto no GDPR. Como narrado de forma preliminar nesse artigo, no Brasil, há norma. Contudo, já integrada a amplas discussões sobre sua efetividade - o que prova que, por mais recente que seja, possui significativo déficit

128 HABERMAS, Jürgen. **Técnica e Ciência como «Ideologia**». Lisboa: Edições 70, 1968.

129 Idem

diante da realidade social e da evolução tecnológica dos meios de comunicação.

Com o advento da Emenda Constitucional nº 115/2022, de 10/02/2022, a proteção de dados pessoais no Brasil foi alçada à condição de direito fundamental, integrando o rol do artigo 5º da CF/88[130].

A Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais), no que concerne à discussão promovida pelo STF, deveria ser a norma balizadora da temática e que é aqui promovida ao debate:

> "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. (...)".
> "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> *I - o respeito à privacidade*; (...).
> *III - a liberdade de expressão, de informação, de comunicação e de opinião*;
> *IV - a inviolabilidade da intimidade, da honra e da imagem*; (...).
> *VII - os direitos humanos*, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

Preponderante ilustrar esse posicionamento que aqui se articula, de forma complementar pelas premissas da Lei nº 12.965/14 (Marco Civil da Internet) - cerne legal invocado pelo STF - nos seguintes dispositivos:

130 LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

> "Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como (...).
> *II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais*".
> "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> *I - garantia da liberdade de expressão, comunicação e manifestação de pensamento*, nos termos da Constituição Federal. (...)
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; (...)
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte".
> "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (...)
> §2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º".

Já o Decreto nº 678/92, promulgou a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica de 22/11/1969), com fundamentos que, em muito, antecederam conceitos que fomentaram a nossa atual Constituição e o Direito Digital com suas proteções:

> "Reafirmando seu propósito de consolidar neste Continente, dentro do quadro das instituições

democráticas, um regime de liberdade pessoal e de justiça social, fundado no respeito dos direitos essenciais do homem;
Reconhecendo que os direitos essenciais do homem não derivam do fato de ser ele nacional de determinado Estado, mas, sim, do fato de ter como fundamento os atributos da pessoa humana, razão por que justificam uma proteção internacional, de natureza convencional, coadjuvante ou complementar da que oferece o direito interno dos Estados americanos;
Considerando que esses princípios foram consagrados na Carta da Organização dos Estados Americanos, na Declaração Americana dos Direitos e Deveres do Homem e na Declaração Universal dos Direitos do Homem e que foram reafirmados e desenvolvidos em outros instrumentos internacionais, tanto de âmbito mundial como regional;
Convieram no seguinte:

ARTIGO 1
Obrigação de Respeitar os Direitos
1. Os Estados-Partes nesta Convenção comprometem-se a respeitar os direitos e liberdades nela reconhecidos e a garantir seu livre e pleno exercício a toda pessoa que esteja sujeita à sua jurisdição, sem discriminação alguma por motivo de raça, cor, sexo, idioma, religião, opiniões políticas ou de qualquer outra natureza, origem nacional ou social, posição econômica, nascimento ou qualquer outra condição social.

ARTIGO 2
Dever de Adotar Disposições de Direito Interno
Se o exercício dos direitos e liberdades mencionados no artigo 1 ainda não estiver garantido por disposições legislativas ou de outra natureza, os Estados-Partes comprometem-se a adotar, de acordo com as suas normas constitucionais e com as disposições desta Convenção, as medidas legislativas ou de outra

natureza que forem necessárias para tornar efetivos tais direitos e liberdades.

ARTIGO 8
Garantias Judiciais
1. Toda pessoa tem direito a ser ouvida, com as devidas garantias e dentro de um prazo razoável, por um juiz ou tribunal competente, independente e imparcial, estabelecido anteriormente por lei, na apuração de qualquer acusação penal formulada contra ela, ou para que se determinem seus direitos ou obrigações de natureza civil, trabalhista, fiscal ou de qualquer outra natureza.
2. Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias mínimas:
b) comunicação prévia e pormenorizada ao acusado da acusação formulada;

ARTIGO 11
Proteção da Honra e da Dignidade
1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.

ARTIGO 13
Liberdade de Pensamento e de Expressão
1. Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e ideias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha.

> O exercício do direito previsto no inciso precedente não pode estar sujeito a censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei a ser necessárias para assegurar:
> a) o respeito aos direitos ou à reputação das demais pessoas; ou
> b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.
> 3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões.
>
> ARTIGO 14
> Direito de Retificação ou Resposta
> 1. Toda pessoa atingida por informações inexatas ou ofensivas emitidas em seu prejuízo por meios de difusão legalmente regulamentados e que se dirijam ao público em geral, tem direito a fazer, pelo mesmo órgão de difusão, sua retificação ou resposta, nas condições que estabeleça a lei.
> 2. Em nenhum caso a retificação ou a resposta eximirão das outras responsabilidades legais em que se houver incorrido.
> 3. Para a efetiva proteção da honra e da reputação, toda publicação ou empresa jornalística, cinematográfica, de rádio ou televisão, deve ter uma pessoa responsável que não seja protegida por imunidades nem goze de foro especial".

Feitas tais digressões e apontados os dispositivos legais que orientam o tema, ainda assim este não se pacifica/estabiliza. Como resultado, temos a imprevisibilidade, comumente descrita como insegurança jurídica.

É mais que sugestivo contribuir para que o maior espectro possível de cidadãos brasileiros tenha capacidade mínima de compreender e saber opinar sobre o tema. Afinal, ninguém pode se escusar das consequências da lei, sob o argumento de desconhecê-la (Artigo 3º da Lei de Introdução às Normas do Direito Brasileiro e Artigo 21 do Código Penal). Trata-se de uma discussão que afeta toda a nossa sociedade hiperconectada e literalmente dependente das informações presentes nos meios digitais (em muitos casos, exclusivamente em tais meios).

Os provedores de internet não têm competência técnica e legal para estabelecer regras de postagem (no que concerne ao conteúdo interpretativo - que é subjetivo - mas permitido ante a liberdade de expressão dos artigos retrocitados), sob pena de, ao fazê-lo, legislarem - condição privativa do Estado. A questão é saber se há ou não excessos nesse direito/liberdade de expressão. E, como sabemos, a legislação já possui meios para tutelar tais excessos, por meio do devido processo legal e da garantia constitucional à proteção de dados pessoais.

Ainda que os provedores possam ser responsabilizados por atos de seus usuários, isso deve convergir com a premissa de que "não há crime sem lei anterior que o defina" (Artigo 1º do Código Penal) e "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" (inciso II do artigo 5º da CF/88).

Portanto, como opinião legal, cabe apenas o rito de propor alteração de lei federal (por quem de direito), para que norma alterada ou nova, preveja (e não conflite com a CF/88 e acordos ou tratados que o Brasil seja signatário) a responsabilização de provedores - de forma objetiva. Mas, acima de tudo, não colida com o preceito constitucional de proteger os dados pessoais inseridos nesse contexto.

Há garantias infraconstitucionais e constitucionais no Brasil (citadas nos artigos e normas/pacto acima) que garantem ao cidadão a livre expressão, combinada com a proteção constitucional de seus dados pessoais. Assim, antes de determinar, ainda que por nova lei, que o provedor seja responsabilizado (por algo que ainda não está normatizado e/ou regulamentado) ou tome medidas via ordem

judicial, deve-se respeitar tais direitos dos cidadãos, já previstos - e até mesmo derivados de acordos internacionais (como o Pacto de São José da Costa Rica). Deve-se observar o devido processo legal contra quem publicou algo em domínios dos provedores (exigindo-se, aí, formas automáticas e legalmente aceitas de preservação de tais provas para seu eventual julgamento), pelas vias legais e com amplo e prévio direito de defesa. Só após, medidas podem ser tomadas.

"*A possibilidade de remoção de conteúdos que possam ofender direitos de personalidade, incitar o ódio ou difundir notícias fraudulentas a partir de notificação extrajudicial*"[131]. Portanto, fora do contexto protetivo de uma ação judicial que é compulsoriamente tutelada pelo Estado, há controvérsia com a proteção dos dados pessoais. O ambiente extrajudicial, ainda que tutelado pela LGPD, não deve ser o caminho para o pleno, o independente e o imparcial julgamento e decisão final contra conteúdos postados nos meios digitais. Parece-nos que a discussão tende a ser inócua em função da simples previsão constitucional (inciso XXXV da CF/88).

3. CONCILIANDO A LIBERDADE DE EXPRESSÃO COM A RESPONSABILIDADE CIVIL DOS PROVEDORES: A CONSTITUCIONALIDADE DO ART. 19 DO MARCO CIVIL DA INTERNET

A audiência pública para debater a questão da responsabilidade civil dos provedores de aplicativos por danos decorrentes de conteúdo gerado por terceiros, decorreu do reconhecimento da repercussão geral em relação à constitucionalidade do artigo 19 da Lei nº 12.965/14.

Dentro desse contexto, é importante destacar que o entendimento predominante atual, tanto no Superior Tribunal de Justiça (STJ) quanto em tribunais estaduais brasileiros, é baseado na responsabilidade civil subjetiva dos provedores de aplicação, quando se trata de

131 https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=503467&ori=1

conteúdo gerado por terceiros, nos termos do Marco Civil da Internet. Portanto, mantém-se a posição de que o tema está sempre sujeito à apreciação do Poder Judiciário - destoando da hipótese permissiva de regulação de conteúdos via notificação extrajudicial. Isso implica que a ocorrência de dano só se configura quando há o descumprimento de uma ordem judicial que obrigue a remoção do conteúdo, com as exceções previstas em lei, como é o caso de conteúdo sexual ou nudez, bem como violações de direitos autorais[132].

Parte significativa da comunidade jurídica brasileira argumenta a favor da declaração de inconstitucionalidade desse dispositivo, alegando que a legislação atual coloca obstáculos injustos para que as vítimas obtenham a devida indenização, favorecendo excessivamente os provedores de internet. Isso ocorre com base na alegação de que a legislação atual é incompatível com os princípios constitucionais que garantem a intimidade, a honra, a reputação e a imagem das pessoas, conforme estabelecido no inciso X do artigo 5º da Constituição Federal.

Todavia, existem argumentos jurídicos válidos que se baseiam nos princípios da liberdade de expressão e na proibição da censura, conforme estabelecido nos incisos IV, IX e XIV do artigo 5º e §2º do artigo 220, todos da Constituição Federal[133]. Esses princípios justificam

132 Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (...)

133 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:
IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional
Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

a aplicação do artigo 19 do Marco Civil da Internet, argumentando que, se os provedores de internet fossem responsáveis por determinar o que é apropriado ou não, isso poderia restringir de forma desproporcional à liberdade de expressão e à livre manifestação do pensamento.

Nesse contexto, é indiscutível que é importante combater discursos de ódio, ataques à democracia e desinformação. Mas é inviável delegar aos provedores de internet a tarefa de avaliar a licitude de cada conteúdo produzido por seus usuários. A declaração de inconstitucionalidade do artigo 19 da legislação em questão teria um grande impacto na sociedade, abrangendo praticamente qualquer conteúdo gerado pelos usuários da rede, incluindo aqueles de natureza subjetiva.

Assim, é de se esperar que o Poder Judiciário desempenhe, com exclusividade, um papel fundamental na análise da ilicitude de conteúdo gerado na internet, evitando a censura prévia e garantindo a liberdade de expressão e de manifestação do pensamento, que são princípios essenciais do Estado Democrático de Direito.

É importante notar que, embora haja desacordos sobre o assunto, a legislação atual não é inconstitucional em si. Ela representa uma escolha legislativa que resultou de amplo debate no âmbito do Poder Legislativo, que tem a prerrogativa de ponderar os interesses da sociedade e de determinar quais devem ser protegidos pelo ordenamento jurídico. Além disso, a própria Constituição Federal prevê o direito de resposta e de indenização por excessos no exercício da liberdade de expressão.

Portanto, é possível compatibilizar os dispositivos legais pertinentes e promover um ambiente regulatório que respeite tanto a liberdade de expressão quanto os interesses dos cidadãos. A proteção dos usuários de boa-fé e a prevenção de ações arbitrárias por parte dos provedores de internet são objetivos igualmente importantes.

4. CONSIDERAÇÕES FINAIS

Por fim, havendo alteração da legislação vigente, não se pode olvidar que essa deverá observar os acordos internacionais que o Brasil já é signatário. Não há legalidade em se requisitar algo dessa natureza, fora de um processo judicial e/ou inquérito, salvo se houver acordos/pactos formais entre Estados com tal previsão.

A eventual inércia do Poder Legislativo poderá causar a supressão de suas próprias prerrogativas e acometer toda a sociedade em acatar decisões proferidas por quem não é (em sua gênese) hábil a legislar, seja por não nos representar via voto, seja pelo conceito de separação dos poderes nos Estados Democráticos de Direito.

A complexa questão da responsabilidade dos provedores de internet em relação ao conteúdo gerado por terceiros se destaca como um tema de crescente importância e nuances legais. A análise, sob a interpretação das ideias de Jürgen Habermas, balizou os aspectos filosóficos e sociológicos dessa discussão, enfatizando a necessidade de buscar consensos entre os agentes envolvidos na esfera digital. A incorporação da Lei Geral de Proteção de Dados Pessoais (LGPD) nesse contexto reforça a proteção dos direitos fundamentais dos cidadãos, como a privacidade e a liberdade de expressão. A recente Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais à condição de direito fundamental, sinaliza a evolução legal nesse âmbito.

Assim, o desafio reside em equilibrar a responsabilidade dos provedores para preservar a liberdade de expressão, para garantir a proteção dos dados pessoais e para resguardar a integridade das informações on-line. O Poder Judiciário desempenha um papel crucial na análise da ilicitude de conteúdos gerados na internet, defendendo a liberdade de expressão e evitando a censura prévia. A busca por um ambiente regulatório que respeite a liberdade de expressão e os direitos dos cidadãos continua sendo uma prioridade, na medida em que o mundo se torna mais conectado digitalmente.

REFERÊNCIAS

BRASIL, Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> Acesso em 24/10/2023.

BRASIL, Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em 24/10/2023.

BRASIL, Lei de Introdução às normas do Direito Brasileiro. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Disponível em: https://www.planalto.gov.br/ ccivil_03/decreto-lei/del4657compilado.htm> Acesso em 24/10/2023.

BRASIL, Lei Geral de Proteção de Dados - Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 24/10/2023.

BRASIL, Marco Civil da Internet. Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 24/10/2023.

BRASIL, Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm> Acesso em 24/10/2023.

BRASIL, Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica) - Decreto nº 978, de 6 de novembro de 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm> Acesso em 24/10/2023.

FONTES, Paulo Vitorino. *A reflexão epistemológica de Habermas e a sua proposta de racionalidade comunicativa.* Griot. Revista de Filosofia, Amargosa – BA, v.20, n.1, p.277-288, fevereiro de 2020.

HABERMAS, Jürgen. *Técnica e Ciência como «Ideologia»*. Lisboa: Edições 70, 1968.

HABERMAS, Jürgen. *Racionalidade e Comunicação*. Lisboa: Edições 70, 1996.

NACIONAL, Congresso. Atribuições do Congresso Nacional. Disponível em: https://www.congressonacional.leg.br/institucional/atribuicoes> Acesso em 24/10/2023.

STF. Audiência pública vai discutir regras do marco civil da internet. Os temas abrangem a responsabilidade de provedores e as formas de retirada de conteúdos ofensivos. Disponível em https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=503467&ori=1> Acesso em 24/10/2023.

STF, RE 1057258. Repercussão Geral Tema: 533. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numeroTema=533> Acesso em 24/10/2023.

STF, RE 1077396. Repercussão Geral Tema: 987. Disponível em: <<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549> Acesso em 24/10/2023.

STF, Convenção Americana sobre Direitos Humanos. Anotada com a jurisprudência do Supremo Tribunal Federal e da Corte Interamericana de Direitos Humanos. 2ª ed. Brasília. 2022. Disponível em: https://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/STF_ConvencaoAmericanaSobreDireitosHumanos_SegundaEdicao.pdf> Acesso em 24/10/2023.

STF. Audiência pública vai discutir regras do marco civil da internet. Os temas abrangem a responsabilidade de provedores e as formas de retirada de conteúdos ofensivos. Disponível em <https://portal.

stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=503467&ori=1> Acesso em 24/10/2023.

STF, RE 1077396. Repercussão Geral Tema: 987. Disponível em: <<https://portal.stf.jus.br /processos /detalhe.asp?incidente=5160549> Acesso em 24/10/2023.

AFINAL, O QUE REPRESENTA A CONSTITUCIONALIZAÇÃO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS?

AFTER ALL, WHAT DOES THE CONSTITUTIONALIZATION OF THE RIGHT TO PROTECTION OF PERSONAL DATA REPRESENT?

Henrique Almeida Bazan

Henrique Almeida Bazan[134]

RESUMO

a Emenda Constitucional n° 115/2022 incorporou no rol de direitos fundamentais do cidadão brasileiro o direito à proteção de dados pessoais. Nesse sentido, o presente artigo busca compreender o que esse processo legislativo representa, tendo em vista teorias de autores constitucionalistas clássicos. O artigo é introduzido a partir de uma reconstrução histórica sobre proteção de dados pessoais e perpassa os trabalhos de Joseph Syeies, Joel Cólon-Rios e Edoardo Celeste. Em sede de conclusão, aponta-se que a constitucionalização de direitos é fruto de um processo de constituição viva, que é sensível a construções sociais e prevê caminhos legítimos para que haja emendas, como a n° 115/2022.

Palavras-chave: Constitucionalismo digital. Proteção de dados. Emenda constitucional.

ABSTRACT

Constitutional Amendment N°. 115/2022 incorporated the right to the protection of personal data into the list of fundamental rights of Brazilian citizens. In this sense, this article seeks to understand what this legislative process represents, taking into account theories from classical constitutionalist authors. The article is introduced based on a historical reconstruction on the protection of personal data and covers the works of Joseph Syeies, Joel Cólon-Rios and Edoardo Celeste. In conclusion, it is pointed out that the constitutionalization of rights is the result of a process of living constitution, which is sensitive to social constructions and provides legitimate paths for amendments, such as N°. 115/2022.

134 Mestrando em Direito e Bacharel na Universidade Federal de Minas Gerais. Advogado com área de atuação em Direito Digital. É pesquisador do IDP Privacy Lab e do grupo Constituições: constitucionalismo e comparativismo. Contato: henriquebazan7@gmail.com

Keywords: Digital constitutionalism. Data protection. Constitutional amendment.

1. INTRODUÇÃO

Em tempos de sociedade em redes (CASTELLS, 2005, p. 98) caracterizada pela rápida disseminação de informação entre usuários hiperconectados, a proteção de dados pessoais é tema de grande impacto social, político e econômico. Esse fenômeno, e sua possibilidade de afetar a vida em sociedade, teve debate extremamente fomentado a partir do caso Cambridge Analytica[135], no qual dados de usuários do Facebook foram indevidamente utilizados para fins de manipulação política eleitoral.

De forma a expandir mecanismos de prevenção ao tratamento abusivo de dados, Estados construíram arcabouços normativos correlatos à proteção de dados pessoais. Inspirada pela norma de proteção de dados europeia (General Data Protection Law), entrou em vigor no Brasil, em 2020, a Lei Geral de Proteção de Dados[136] (LGPD). Um ano depois, entraram em vigor as sanções por descumprimento à LGPD, cabendo à Autoridade Nacional de Proteção de Dados sua fiscalização. Em continuidade, em fevereiro de 2022, buscando maior força normativa à temática de proteção de dados, o Senado Federal promulgou a Emenda Constitucional 115/2022[137], acrescentando o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais do cidadão no art. 5° da Constituição Brasileira.

Deseja-se debater no presente artigo, a partir de uma perspectiva clássica sobre constitucionalismo, o que representa a

135 BRASIL, BBC News. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 06 jul. 2023.

136 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 6 jun. 2023.

137 BRASIL. **Emenda Constitucional, de 10 de fevereiro de 2022**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 6 jun. 2023.

constitucionalização do direito à proteção de dados pessoais no Estado Brasileiro. Serão abordados como autores compreendem o fenômeno da constitucionalização e o que isso significa no cenário normativo brasileiro.

É hipótese do autor que a constitucionalização do direito à proteção de dados pessoais, além de seu impacto normativo direto, fomenta o amadurecimento social da temática de proteção de dados e serve de orientação hermenêutica para tribunais. São indícios da hipótese o caráter democrático e popular que processos de constitucionalização pós-soberanos tendem a retratar (ARATO, 2017, p. 381).

Objetivando compreender o problema abordado, serão explorados os trabalhos de Emmanuel Joseph Sieyés, Colón-Ríos e Edoardo Celeste para compreender e analisar o que representa a constitucionalização do direito à proteção de dados. Espera-se que os conceitos e ideias desenvolvidos por esses autores possam iluminar a discussão proposta.

Espera-se também que, a partir dessa reconstrução dogmática, seja evidenciada a importância conferida ao tema de proteção de dados com sua constitucionalização. Ademais, é desejo do autor que se torne nítido como conceitos e compreensões de processos de constitucionalização podem ser verificados no processo de constitucionalização do direito à proteção de dados pessoais.

O artigo está dividido em três partes. Finalizada a presente introdução, discorre-se sobre o trabalho de constitucionalistas, de forma a embasar e fomentar a compreensão do que significa a constitucionalização do direito à proteção de dados. Na conclusão, serão sintetizados pontos centrais das análises realizadas anteriormente e será respondido o que representa a inserção do direito à proteção de dados na Constituição Brasileira.

2. DAS PERSPECTIVAS TEÓRICAS

Nos próximos tópicos será abordada parte dos trabalhos dos autores Emmanuel Joseph Sieyés, Joel Cólon-Ríos e Edoardo Celeste. Busca-se que as reflexões expostas sirvam como referência teórica, para que seja realizada análise dos impactos da Emenda Constitucional 115/2022, que adicionou na Constituição de 1988 o direito à proteção de dados. Todos os trabalhos analisados podem ser relacionados com a constitucionalização do direito à proteção de dados e foram selecionados de forma a fomentar a discussão proposta.

2.1 O PODER CONSTITUINTE

A teoria do Poder Constituinte surge em um momento de grande disputa na França revolucionária sobre quem é o soberano. Buscando afastar a monarquia do poder e propor um modelo político exequível à sociedade francesa, Emmanuel Joseph Sieyés afirmou que o poder político pertence ao povo, mas que a forma de exercê-lo estava limitada à representação.

O político francês buscou por meio de sua teoria eliminar riscos que julgava inerentes à ideia de soberania popular e de soberania nacional. Sieyés defendeu um sistema político que fosse conduzido pela burguesia e que a liberdade dos cidadãos não fosse afetada. O poder constituinte originário pertenceria ao povo, todavia, sob a justificativa de que seria inviável que todos o exercessem de forma direta e contínua, representantes eleitos agiriam em nome dos detentores originários do poder. O povo exerceria o poder constituinte originário ao eleger representantes e lhes delegar a formulação de uma constituição. Após esse momento inicial extraordinário, os representantes deixariam de fazer uso desse poder constituinte e passariam a atuar nos limites da constituição, deixando o povo supostamente livre para realizar práticas de sua predileção.

A inserção do direito à proteção de dados no texto constitucional brasileiro se dá em momento posterior ao estabelecimento da Constituição, portanto sem que fosse feito uso do poder constituinte originário previsto por Sieyés. Nesse sentido, a aprovação de uma emenda constitucional faz uso do poder constituinte derivado, que é subordinado e condicionado (DE MORAIS, 2016, p. 88). Classifica-se este poder enquanto derivado reformador, caracterizado por alterar o texto constitucional por meio de um órgão representativo, no caso brasileiro o Congresso Nacional.

O poder constituinte derivado é subordinado, pois se encontra limitado a normas expressas e implícitas do texto constitucional. Incabível seria uma emenda constitucional que alterasse preceitos basilares da democracia brasileira ou, de modo específico, que previsse a liberalidade de empresas ou do Estado para realização de um tratamento massivo de dados pessoais, pois estaria em contrariedade a normas já postas na Constituição, como o direito à intimidade e a vida privada. O poder constituinte derivado é condicionado, pois seu exercício deve seguir condições e regras estabelecidas no texto da Constituição Federal.

Por fim, esse poder é derivado, pois retira sua força do Poder Constituinte originário. O art. 60 da Constituição de 1988 prevê a possibilidade de emenda constitucional e daí a legitimidade e legalidade do ato de adição à Magna Carta de direitos. Aliás, é importante que haja tal previsão e um procedimento formal para alteração constitucional, haja vista que a alterabilidade constitucional deve conservar um valor integrativo (DE MORAIS, 2016, p. 1054) ao texto já escrito, em ordem com os fundamentos da constituição. No caso da Emenda Constitucional 115/2020, é perceptível que sua inserção no texto constitucional encontra-se de acordo com o caráter social da Constituição de 1988, prevendo um direito que fortalece a defesa do consumidor e que está de acordo com outros direitos fundamentais, como o direito à vida privada e a intimidade.

Dessa forma, mesmo que a Emenda Constitucional 115/2022 não tenha sido originada de um processo de assembleia constituinte

ou de ruptura constitucional, esta tem direta relação com o poder constituinte originário. O processo de formulação da constituição, que, de acordo com Sieyés, se daria em um momento de representação extraordinária, irradia influência em processos posteriores, sendo, no caso brasileiro, prevista a possibilidade de emenda constitucional, que terá de contar com votos de três quintos dos parlamentares das duas casas do Congresso Nacional.

2.2 A IDENTIDADE E OS LIMITES DO SUJEITO CONSTITUINTE

Ainda que de grande importância, a teoria de Sieyés não deu ponto final a discussão quanto a como compatibilizar o texto constitucional e a possibilidade de realização de emendas constitucionais. Conforme Joel Colón-Ríos (CÓLON-RÍOS, 2020) retratou, a disputa foi alterada de "quem é soberano" para "quem tem autoridade soberana para alterar leis fundamentais".

Em resgate doutrinário, o autor traz reflexões de pensadores que divergiam quanto à possibilidade de que emendas constitucionais fossem realizadas. Em interpretação a Paul Pradier-Fodéré[138], o autor menciona que deveria haver norma constitucional que permita emendas constitucionais e que representantes eleitos, após a confecção do texto constitucional, deveriam simplesmente agir nos limites do que adotou a constituição.

Já em interpretação do trabalho de José María Quimper[139], Cólon-Ríos discorre que o autor não entende que há possibilidade de alteração do texto constitucional por meio de representantes. Para Quimber, o poder constituinte não poderia ser delegado, sendo o poder constituinte exercitado periodicamente, com períodos entre

138 FODÉRÉ, Paul Pradier. **Principes Genéraux de Droit, de Politique et de Legislation**. Paris, 1869.

139 QUIMPER, José María. **Derecho Político General**. Lima, 1887, vol. 2.

assembleias constitucionais nos quais haja estrito respeito ao texto constitucional.

Diante da divergência doutrinária, Cólon-Ríos entende que emendas constitucionais devem ser previstas, já que a ausência dessa ferramenta tornaria constituições prisões da democracia participativa[140]. Nesse mesmo sentido, a Emenda Constitucional 115/2022 mostra-se solução normativa pontual e necessária, haja vista que o cenário de erosão constitucional vivenciado no Brasil (MEYER, 2021) não se mostra convidativo à convocação de uma assembleia constituinte, não deixando com que seja latente a necessária intervenção normativa em alguns pontos, como na esfera de proteção de dados pessoais.

2.3 CONSTITUCIONALISMO DIGITAL, UMA TENDÊNCIA PROTETIVA

O ecossistema digital tem presença e relevância cada vez mais proeminente nos Estados-nação. O uso de tecnologias digitais apresenta novas funcionalidades cotidianamente, trazendo tanto facilitações à sociedade como desvios e problemas sociais. Nesse aspecto, o modo com que indivíduos exercem e compreendem direitos fundamentais ganha novos contornos em um cenário de digitalização de serviços governamentais. Esse fenômeno pode ser identificado no Brasil[141] mesmo diante da grande desigualdade de infraestrutura tecnológica e literacia digital existente no país[142], questão que não é objeto direto do presente estudo, ainda que usuários despreparados sejam mais vulneráveis nas redes.

140 COLÓN-RÍOS, Joel I. **Weak Constitutionalism: Democratic legitimacy and the question of constituent power**. Routledge, 2012, p. 20.

141 QUEIROZ, Vitória. **Digitalização dos serviços do governo federal alcança 89%**. 2023. Disponível em: https://www.poder360.com.br/economia/digitalizacao-dos-servicos-do-governo-federal-alcanca-89/. Acesso em: 06 jul. 2023.

142 BR, NIC. **TIC DOMICÍLIOS 2019**. 2015. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123115919/resumo_executivo_tic_dom_2019.pdf. Acesso em 06 jul.2023.

Para Edoardo Celeste[143], vivemos em um período que o autor define enquanto "momento constitucional" caracterizado por reações do sistema constitucional a novos desafios correlatos ao mundo digital. Disputas por direitos foram transpostas ao ambiente de redes sociais, sendo pulsante a ressignificação do que se entende enquanto espaços de arenas públicas (OLIVEIRA, REPOLÊS, PRATES, 2020). Não parece equivocado afirmar que no cenário contemporâneo plataformas sutilmente movem a vida pública (GILLESPIE, 2018, p. 13), até mesmo tomando do domínio do Estado poderes antes exclusivos e centralizados.

Como resposta ao momento constitucional observado, o autor define constitucionalismo digital enquanto novos valores e princípios que guiam a restauração do equilíbrio constitucional. Dessa forma, não haveria uma regra específica para regular e remediar os impactos das tecnologias digitais, mas existiriam fundamentos e princípios gerais que reequilibrariam estruturas normativas para o ecossistema digital. A Emenda Constitucional 115/2022 pode ser considerada um exemplo de medida do constitucionalismo digital, tendo em vista seu caráter inovador e que advém da necessidade de novas formas de equilibrar poderes em espaços digitais. Outro ponto tratado por Celeste foi o de que o constitucionalismo digital pode ser observado em legislações infraconstitucionais e, até mesmo, em instrumentos de instituições transfronteiriças, como é o caso da Corporação da Internet para Atribuição de Nomes e Números (ICANN).

Ainda, Celeste identifica três categorias de reações normativas ao desequilíbrio constitucional oriundos de tecnologias digitais: normas que reconhecem a crescente possibilidade de que sejam exercidos direitos fundamentais intermediados por tecnologias digitais; normas que almejam limitar o crescimento de violações à direitos fundamentais; e normas que almejam restaurar o equilíbrio entre poderes existentes. A inserção do direito à proteção de dados na Constituição de 1988 busca resguardar cidadãos brasileiros, ao

143 CELESTE, Edoardo. **Digital constitutionalism: a new systematic theorisation**. International Review of Law, Computers & Technology, v. 33, n. 1, p. 76-99, 2019.

lhes assegurar, de modo principiológico, que se trata de um direito fundamental tê-los protegidos. O aprofundamento do vigilantismo por governos (ZUBOFF, 2018, p. 20) e o tratamento massivo de dados por empresas tornou latente a necessidade de que a sociedade se mobilizasse por novas formas de proteção normativa.

Portanto, o constitucionalismo digital no Brasil pode ser percebido na Emenda Constitucional 115/2022. Outros instrumentos também são parte do arcabouço normativo brasileiro que busca equilibrar os desvios oriundos de tecnologias digitais: o Marco Civil da Internet[144] e a própria Lei Geral de Proteção de Dados. Ainda, é discussão crescente o Projeto de Lei 2.630/2020, hoje referido no projeto enquanto Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, cujo objeto em suas primeiras versões era o combate à desinformação e agora apresenta escopo mais amplo, relacionando-se com outros tópicos correlatos à regulação de plataformas digitais, como transparência algorítmica e direitos autorais. O direito à proteção de dados pessoais é evidência que o legislador brasileiro considerou que a governança de dados pessoais foi desequilibrada com a emergência de tecnologias de processamento de dados em volume, velocidade e variedades (BIONI, 2015, p. 48) antes não observadas, reagindo com a aprovação da Emenda Constitucional 115/2022.

3. CONSIDERAÇÕES FINAIS

O estudo realizado buscou relacionar teorias do constitucionalismo desenvolvidas em diferentes contextos sociais à Emenda Constitucional 115/2022, que adicionou no art. 5° da Constituição de 1988 o direito fundamental à proteção de dados pessoais.

144 BRASIL. Lei 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 7 jun.2023.

Relativo à teoria de Sieyés, foi possível observar que, no momento de realização da assembleia constituinte para formulação da Constituição Brasileira, houve uso do poder constituinte originário para prever a possibilidade de emendas constitucionais. A alteração constitucional realizada é identificada enquanto poder constituinte derivado, tendo sua legitimidade extraída do texto constitucional.

Ao aplicar a concepção de José Colón-Ríos, observou-se que a possibilidade de alteração do texto constitucional sem que houvesse uma ruptura constitucional é medida necessária e acertada. O cenário político brasileiro não se mostra propício à convocação de nova assembleia constituinte e mais eficaz o uso do poder constituinte derivado.

Ainda, o direito à proteção de dados pessoais é medida que converge ao constitucionalismo digital, previsto por Edoardo Celeste. O legislador identificou um desequilíbrio entre poderes, causado pelas tecnologias digitais cujo uso encontra-se em franca expansão, de modo que buscou remediar impactos e restaurar o equilíbrio constitucional.

Entende-se, portanto, que a constitucionalização de um direito é fruto de um processo que perpassa por disputas políticas-sociais, além do processo legislativo. A Constituição é, também, política, não se limitando apenas a esfera normativa (BERCOVICI, 2004, p. 24). Nesse sentido, a inserção do direito à proteção de dados pessoais é fruto de um processo contínuo de diálogo político composto por agentes que exercitam cotidianamente a cidadania. O tema de privacidade e proteção de dados pessoais ganha evidência no Brasil principalmente a partir do caso Cambridge Analytica, todavia há um longo caminho de amadurecimento social até que haja a constitucionalização do direito à proteção de dados.

Em geral, textos constitucionais possuem pretensão de validade futura, mas nem sempre abrangerão tópicos efervescentes em sociedade. Daí o poder constituinte derivado, para legitimar eventuais emendas constitucionais. Também é igualmente importante que haja a possibilidade de inclusão de dispositivos oriundos de construção coletiva, sem a necessidade que ocorram rupturas institucionais.

Verifica-se que direitos fundamentais podem surgir conforme alterações da ordem política-cidadã, como prevê o próprio constitucionalismo digital. Por isso, a constitucionalização do direito à proteção de dados foi tão importante. Atendeu as necessidades de uma sociedade cujo uso de plataformas digitais gerou diversos impactos aos cidadãos, busca inibir abusos à titulares de dados pessoais e cumpriu com os requisitos normativos, para que a higidez do processo democrático que levou à criação da emenda não fosse maculada.

REFERÊNCIAS

ARATO, Andrew. **The Adventures of Constituent Power: Beyond Revolutions?** Cambridge: Cambridge University Press, 2017. 5: Post-Sovereign Constitutionalism: The Domestication of Revolution?

BERCOVICI, Gilberto. **Constituição e política: uma relação difícil**. Lua Nova: revista de cultura e política, p. 5-24, 2004.

BIONI, Bruno Ricardo. "Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil." *São Paulo: GPoPAI/USP* (2015), p. 48.

BRASIL, BBC News. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 06 jul. 2023.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 7 jun. 2023.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 6 jun. 2023.

BRASIL. **Emenda Constitucional, de 10 de fevereiro de 2022**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 6 jun. 2023.

BR, NIC. **TIC DOMICÍLIOS 2019**. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123115919/resumo_executivo_tic_dom_2019.pdf. Acesso em 06 jul. 2023.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e terra, 2005.

CATTONI DE OLIVEIRA, Marcelo A.; SALCEDO REPOLÊS, Maria F.; PRATES, Francisco C. **A tensão entre público e privado no exercício das liberdades comunicativas nas redes sociais: o caso de mensagens públicas de autoridades governamentais por meio de contas "privadas"**. Libertas: Revista de Pesquisa em Direito, Ouro Preto, v. 6, n. 2.

CELESTE, Edoardo. **Digital constitutionalism: a new systematic theorisation**. International Review of Law, Computers & Technology, v. 33, n. 1, p. 76-99, 2019.

CÓLON-RÍOS, Joel. **Constituent Power and the Law.** Oxford: Oxford University Press, 2020. 6: The Identity and Limits of the Constitutional Subject.

COLÓN-RÍOS, Joel I. **Weak Constitutionalism:** Democratic legitimacy and the question of constituent power. Routledge, 2012.

DE MORAES, Alexandre. **Direito constitucional**. 2016.

FODÉRÉ, Paul Pradier. **Principes Genéraux de Droit, de Politique et de Legislation**. Paris, 1869.

GILLESPIE, Tarleton. **Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media**. Yale University Press, 2018, p. 13.

MEYER, Emílio Peluso Neder. **Constitutional Erosion in Brazil**. Bloomsbury Publishing, 2021.

QUEIROZ, Vitória. **Digitalização dos serviços do governo federal alcança 89%**. 2023. Disponível em: https://www.poder360.com.br/economia/digitalizacao-dos-servicos-do-governo-federal-alcanca-89/. Acesso em: 06 jul. 2023.

QUIMPER, José María. **Derecho Político General**. Lima, 1887, vol. 2.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**, p. 20.

RESSARCIMENTO DE DANOS NA LGPD: UMA ANÁLISE QUANTO À RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO

COMPENSATION FOR DAMAGES IN THE LGPD: AN ANALYSIS OF THE CIVIL LIABILITY OF DATA PROCESSING AGENTS

Plínio Hávila Oliveira Ribeiro
Samylle De Oliveira Ribeiro

Plínio Hávila Oliveira Ribeiro[145]
Samylle De Oliveira Ribeiro [146]

RESUMO

Em um mundo cada vez mais digital e interconectado, a proteção dos dados pessoais se tornou uma questão de extrema importância. Diante disso, o Brasil instituiu a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Este marco legislativo estabelece princípios e regras a serem observados pelos agentes de tratamento de dados. E, para maior efetividade, disciplina ainda as possibilidades de responsabilização e ressarcimento de danos em decorrência das operações de dados pessoais. Contudo é silente quanto à natureza jurídica da responsabilidade civil adotada, se é objetiva ou subjetiva. Assim, propõe-se a analisar os argumentos existentes na doutrina atual no que diz respeito ao regime de responsabilidade civil pretendido pelo legislador. Para tanto, utiliza-se da pesquisa bibliográfica e documental, por meio do método hipotético-dedutivo para solucionar a problemática.

Palavras-chave: Proteção de Dados. Responsabilidade Civil na LGPD. Responsabilidade civil dos agentes de tratamento.

ABSTRACT

In an increasingly digital and interconnected world, the protection of personal data has become an issue of extreme importance. Given this, Brazil established the General Data Protection Law (Law No. 13,709/2018). This legislative framework establishes principles and rules to be observed by data processing agents. And, for greater effectiveness, it also regulates the possibilities of liability and compensation for damages resulting from personal data

145 Advogado, graduado em Direito pela Faculdade Verde Norte (FAVENORTE), membro da Comissão de Proteção de Dados da OAB/MG.

146 Advogada, especialista em Direito Digital, graduada em direito pela Faculdade Verde Norte (FAVENORTE), pós-graduada em Direito Digital e Compliance pela Faculdade Descomplica, membro da Comissão de Proteção de Dados da OAB/MG.

operations. Conduto is silent regarding the legal nature of the civil liability adopted, whether it is objective or subjective. Therefore, it is proposed to analyze the existing arguments in current doctrine with regard to the civil liability regime intended by the legislator. To this end, bibliographical and documentary research is used and the hypothetical-deductive method is used to solve the problem.

Keywords: Data Protection. Civil Liability in the LGPD. Civil liability of processing agents.

1. INTRODUÇÃO

A discussão sobre proteção de dados pessoais alcançou relevância com a capacidade cada vez maior de processamento de dados por meio de recursos computacionais. Com a crescente quantidade de informações sendo coletadas, armazenadas e processadas, surge uma tendência global em regulamentar a temática de proteção de dados.

Nesse contexto, institui-se no Brasil a Lei Geral de Proteção de Dados (LGPD) –Lei nº 13.709/18 –com o intuito de proteger a pessoa titular dos dados, garantindo-lhe direitos e controle de suas informações pessoais. A referida lei regulamenta as atividades de tratamento de dados pessoais no território nacional e estabelece uma série de deveres e obrigações para os agentes de tratamento de dados.

Quando a Lei menciona agentes de tratamentos, refere-se ao controlador e ao operador[147]. Ao primeiro competem as decisões referentes ao tratamento de dados pessoais[148], enquanto o segundo realiza o tratamento de dados pessoais em nome do controlador[149] e conforme a finalidade por este delimitada[150]. Ambos podem ser pessoas naturais ou jurídicas de direito público ou privado, nos termos do art. 5º, incisos VI e VII da LGPD.

147 Art. 5º, IX, da LGPD.

148 Art. 5º, VI, da LGPD.

149 Art. 5º, VII, da LGPD.

150 ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, v. 2.0, abr. 2022, p. 6.

Vale lembrar que os servidores públicos e os funcionários, isto é, os indivíduos subordinados, não são considerados controladores ou operadores[151]. Na verdade, o controlador, se pessoa jurídica, será a própria organização. Esta determina as diretrizes para o tratamento de dados, a serem desempenhadas por seus representantes ou prepostos[152].

Entre os deveres dos agentes de tratamento de dados, destaca-se a adoção de medidas de segurança, técnicas e administrativas, aptas para proteger os dados pessoais de incidentes de segurança[153], sob pena de serem responsabilizados. Para tanto, o artigo 42 da Lei estabelece a obrigação de reparar os danos causados a terceiros em razão do exercício de suas atividades de tratamento de dados pessoais.

Contudo, por mais que a LGPD disponha sobre a "responsabilidade e o ressarcimento de danos" no âmbito das atividades de tratamento de dados, não diz claramente qual é a natureza jurídica da obrigação de indenizar. Não consta no texto legal expressões como "independentemente de culpa" para externar um regime objetivo de responsabilidade, mas também não faz menção direta à culpa.

Desse cenário surge o desafio relativo à correta interpretação da lei e, por conseguinte, indaga-se: em matéria de proteção de dados, o legislador optou pelo regime objetivo ou subjetivo de responsabilidade civil?

Para a construção deste estudo, pleiteando os resultados, surgem duas hipóteses. Na primeira hipótese, a obrigação de indenizar atribuída aos agentes de tratamento alicerça-se na teoria objetiva, aquela independentemente de culpa, bastando à prova do dano e do nexo de causalidade. Na segunda hipótese, sob outra perspectiva, é preciso examinar se o dano decorre de uma conduta voluntária ou de uma conduta negligente, imperita ou imprudente do controlador e do

151 ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, v. 2.0, abr. 2022, p. 7.

152 ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, v. 2.0, abr. 2022, p. 7.

153 Art. 46, da LGPD.

operador de dados para responsabilizá-los civilmente, aplicando-se, portanto, o regime subjetivo como regra na LGPD.

O objetivo do presente artigo, portanto, é identificar a natureza jurídica da responsabilidade civil dos agentes de tratamento de dados –controlador e operador –existente na Lei Geral de Proteção de Dados. Com esse fim, realizou-se uma pesquisa exploratória com uma abordagem hipotético-dedutiva. Já como técnica de pesquisa utilizou-se a bibliográfica e documental, baseada em doutrinas e artigos científicos, bem como em legislações e regulamentos nacionais e estrangeiros.

2. RESPONSABILIDADE E RESSARCIMENTO DE DANOS NA LGPD

A LGPD possui uma seção específica cujo título é "Da Responsabilidade e do Ressarcimento de Danos" (art. 42 a 45). Estes dispositivos tratam de regras específicas de responsabilidade civil nas relações em que há tratamento de dados.

O art. 42, em seu *caput*, dispõe 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".

Em outros termos, se uma organização que atua como controladora ou operadora de dados pessoais violar a legislação de proteção de dados e, como resultado, causar danos a alguém, seja financeiramente, moralmente, individualmente ou coletivamente[154], ela é responsável por reparar esses danos.

Com o fim de garantir a efetiva indenização ao titular de dados, o §1º do referido artigo, em seus incisos, assegura a possibilidade de responsabilização solidária do operador com o controlador e entre dois ou mais controladores. Destaca-se que o intuito deste dispositivo

154 O art. 42, §3º, da LGPD, prevê a reparação de danos coletivos.

é traçar uma distinção entre os agentes de tratamento quanto à responsabilidade solidária, e não apontar o regime objetivo ou subjetivo de responsabilidade civil aplicável na LGPD.

Para melhor didática, o inciso I pode ser dividido em duas partes: a) "o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados"; b) "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".

Tal disposição acerca da responsabilidade solidária é positiva, pois, ainda que o dano seja ocasionado pelo operador, o titular de dados poderá demandar o controlador, agente pelo qual ele forneceu e confiou as suas informações. Isso facilita, e muito, já que o titular de dados desconhece a rede de operadores que recebeu o compartilhamento de dados do controlador.

Na prática, se no curso do processo o controlador argumentar que o dano, em razão de violação à legislação de dados, decorreu de ação do operador, apesar disso, ele será responsabilizado solidariamente. Por sua vez, se o controlador provar que o operador tratou os dados de forma estranha à que foi estipulada, este é tratado como se fosse o próprio controlador em termos de responsabilidade.

Nesse caso, se ainda assim o controlador for condenado a reparar o dano, ele poderá se utilizar o seu direito de regresso, previsto no § 4º do mesmo artigo, em face do operador para que este possa indenizá-lo na medida de sua participação no evento danoso.

Percebe-se que o intuito do artigo 42, parágrafo primeiro, é facilitar a reparação de danos ao titular de dados. Tanto é verdade que o inciso II segue a mesma lógica ao prever a responsabilidade solidária entre controladores. A referida norma dispõe que "os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei".

Dessa forma, se vários controladores estiverem tratando os dados conjuntamente e ocasionar algum dano, ambos poderão ser

responsabilizados, e a pessoa afetada pode buscar compensação junto a qualquer um deles, não sendo necessário determinar qual é o único causador do dano. Ocorre que o tratamento de dados pessoais, frequentemente, envolve mais de um agente, e não se poderia, de fato, impor ao titular dos dados o ônus de descobrir, dentro de uma cadeia econômica, quem deu causa ao dano[155].

No entanto, é importante observar que, conforme a parte final dos incisos I e II, do art. 42, existem exceções à responsabilização dos agentes de tratamento. O art. 43 prevê três possibilidades de exclusão de responsabilidade, as quais serão discutidas nos tópicos seguintes.

Outro dispositivo determinante para compreender a temática é o art. 44, pois define em quais ocasiões o tratamento de dados pessoais seria irregular: "quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar". Ou seja, se o agente de tratamento não estiver em conformidade com a legislação ou se quebrar a expectativa do titular por não adotar medidas de segurança adequadas para proteger os dados pessoais, pratica tratamento irregular.

Além disso, os incisos apontam ainda as circunstâncias relevantes para que o tratamento de dados seja considerado irregular, as quais estão associadas ao modo como é realizado, ao resultado e risco razoável do tratamento esperado pelo titular, bem como a utilização de técnicas de segurança eficazes à época do tratamento.

O parágrafo único desse artigo ainda reforça a obrigação de reparar o dano resultante de violação da segurança dos dados ao deixar de adotar as medidas de segurança previstas no art. 46 da Lei.

Importante lembrar que, embora as regras de responsabilidade e ressarcimento de danos sejam aplicáveis a qualquer operação de tratamento, a LGPD é específica quanto ao tratamento de dados nas relações de consumo. Quando a atividade de tratamento de dados pessoais gerar danos a consumidores, a LGPD dispõe em seu

155 BRUNO, Marcos Gomes da Silva. In: Viviane Nóbrega Maldonado e Renato Opice Blum (Coord.), LGPD: *Lei Geral de Proteção de Dados comentada*. São Paulo: Revista dos Tribunais, 2019, p. 323.

art. 45, que se aplique a legislação pertinente, ou seja, o Código de Defesa do Consumidor (CDC). Sendo assim, o CDC, em seus artigos 12 e 14, disciplina claramente a responsabilidade civil nas relações de consumo.

Constata-se de uma leitura diligente desses dispositivos que a legislação consumerista incorpora a responsabilidade objetiva. É possível chegar a essa conclusão diante da expressão "independentemente de culpa", ao se referir à responsabilização nos casos de incidentes de consumo, seja decorrente do fato do produto (CDC, art. 12), seja do fato do serviço (CDC, art. 14).

Em contrapartida, a regra geral de responsabilidade civil aplicável aos agentes de tratamentos de dados pessoais ainda é motivo de debate, uma vez que a Lei não indica expressamente o tipo de responsabilidade cabível nos dispositivos relativos ao ressarcimento de danos na LGPD. Em razão disso, é possível notar na literatura jurídica o surgimento de pelo menos duas correntes.

2.1. SINAIS DE ADOÇÃO DO REGIME OBJETIVO DE RESPONSABILIDADE CIVIL NA LGPD

A primeira delas, conduzida por Danilo Doneda, Laura Shertel Mendes, Caitlin Sampaio Mulholland, Cíntia Rosa Pereira de Lima e Glenda Godin, defende a adoção do regime objetivo com base na teoria do risco e em analogias com o CDC.

Essa parte da doutrina professa que a opção por um regime objetivo se justifica em razão de a legislação ter como um de seus fundamentos principais a diminuição do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares[156]. Por isso, o princípio da necessidade disposto no inciso III do art. 6º prevê o tratamento de dados ao mínimo necessário,

156 MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *In: Revista de Direito do Consumidor*, Brasília, v. 120, n. 2, p. 469-483, nov/dez. 2018, p. 477.

assim como o art. 16 determina a eliminação dos dados depois de o controlador ter alcançado a finalidade desejada.

Para essa corrente, em uma sociedade caracterizada pela hiperconectividade e pela demanda insaciável por exposição, o tratamento de dados pessoais é atividade que suscita risco excessivo[157]. Por essa razão, embora no art. 42 não haja a expressão "independentemente de culpa", trata-se na verdade, de aplicação da cláusula geral de responsabilidade objetiva, prevista na parte final do parágrafo único do art. 927 do Código Civil Brasileiro de 2002 (CC/02)[158].

Alguns autores entendem que para chegar a um modelo de responsabilidade civil necessita-se de uma análise sistemática da LGPD, ou seja, é preciso analisar não só os arts. 42 a 45 como também toda a estrutura da Lei. É como pensam André Luis Novakoski e Samyra Naspolini[159] ao afirmarem:

> A atividade de tratamento de dados pessoais, por envolver um atributo do direito de personalidade do titular, apresenta riscos potenciais, que são explicitamente mencionados pela LGPD, cuja interpretação sistemática evidencia a adoção da teoria da responsabilidade civil objetiva, decorrente da violação das obrigações de resultado previstas na lei, que somente pode ser excepcionada nas hipóteses de ruptura do nexo causal reguladas na própria LGPD.

De igual modo, Caitlin Mulholland assevera a necessidade de análise dos elementos estruturantes da LGPD, em especial ao princípio

157 SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In:* BIONI, Bruno *et. al.* (Coord. Exec.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 330-349.

158 Art. 927. (...). Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

159 NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade Civil na LGPD: Problemas e Soluções. Conpedi Law Review, v. 6, n. 1, p. 158-174, 2020, p. 172.

da segurança, prevenção e responsabilização e prestação de contas, os quais permitem ao intérprete considerar a proteção do titular de dados como o escopo central da legislação[160].

Devido a esse arcabouço protetivo, não se pode ignorar a inevitável comunicabilidade entre a LGPD e outras normas que já se ocupam, em alguma medida ou setorialmente, do tratamento de dados pessoais, incluindo o próprio CDC[161].

Diante de uma era marcada pela coleta massiva de dados, é fácil constatar o titular em uma posição claramente desfavorável[162]. Pensando nisso, a LGPD permite a inversão do ônus da prova (art. 42, §2º), o que demonstra uma "inequívoca inspiração no CDC, ao admitir a inversão do ônus da prova tanto nas hipóteses de hipossuficiência quanto nas situações de verossimilhança das alegações do consumidor[163].

É importante destacar também a tendência de objetivação da responsabilidade no sistema jurídico brasileiro. Ao considerar essa questão André Luis Novakoski e Samyra Naspolini[164] entendem que

> a exigência de prova da culpa para a caracterização do dever de indenizar por violação dos princípios e regras de proteção de dados pessoais instituídas pela LGPD, a despeito de ponderáveis argumentos, ignora a

160 MULHOLLAND, Caitlin Sampaio. *In*: Simpósio de Responsabilidade Civil e Proteção de Dados, 1, 2020, IBERC - Responsabilidade Civil. *YouTube*, 06 ago. 2020.

161 SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In:* BIONI, Bruno *et. al.* (Coord. Exec.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 330-349.

162 TEIXEIRA, Tarcísio; ARMELI, Ruth Maria Guerreiro da Fonseca. *Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD***:** um Cotejamento com o CDC. *In:* DE LIMA, Cíntia Rosa Pereira. Comentários à Lei Geral de Proteção de Dados. Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020, p. 297-326.

163 SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In:* BIONI, Bruno *et. al.* (Coord. Exec.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 330-349.

164 NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade Civil na LGPD: Problemas e Soluções. Conpedi Law Review, v. 6, n. 1, p. 158-174, 2020, p. 172.

> coerência interna do sistema de responsabilidade civil no direito brasileiro e todo a trajetória do instituto ao longo do Século XX e sua transição da teoria da culpa para a do risco da atividade.

A discussão sobre haver sinais de responsabilidade objetiva –ou subjetiva –na LGPD é ainda mais calorosa quando se examina o seu art. 43, que estipula as hipóteses de excludentes de responsabilidade do controlador e operador.

Em linhas gerais, a LGPD estabelece que os agentes não serão responsabilizados se provarem que não realizaram o tratamento de dados a que lhes foram atribuídos (art. 43, I); ou quando os agentes tiverem realizado o tratamento, mas "não houve violação à legislação de proteção de dados" (art. 43, II); ou ainda quando o dano for causado por culpa exclusiva do titular ou de terceiro (art. 43, III).

Para Divino e Lima, ao se utilizar da expressão "só não serão responsabilizados quando provarem" (art. 43, *caput*), entende-se que a responsabilidade pelos ilícitos praticados pelos agentes de tratamento é, em regra, objetiva[165]. Ou seja, a não responsabilização ou o exame da culpa é a exceção, conforme delimitado em lei.

Mais uma vez identifica-se uma similaridade desse dispositivo com as normas do CDC, quando este diploma prevê, no art. 14, §3º, que o fornecedor de serviços não responde quando provar que o defeito inexiste ou a culpa exclusiva do consumidor ou de terceiro[166]. Assim como a legislação consumerista, e pela própria estrutura do

165 DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Maria Macena de. *Responsabilidade na Lei Geral de Proteção de Dados Brasileira*. *Revista Em Tempo*, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858.

166 TEIXEIRA, Tarcísio; ARMELI, Ruth Maria Guerreiro da Fonseca. *Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD:* um Cotejamento com o CDC. *In:* DE LIMA, Cíntia Rosa Pereira. Comentários à Lei Geral de Proteção de Dados. Lei n. 13.709/2018,com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020, p. 297-326.

dispositivo relativo às excludentes de responsabilidade civil na LGPD, entende-se existir uma responsabilidade objetiva[167].

Em reforço, André Luis Novakoski e Samyra Naspolini, ao comentar o art. 43 da LGPD, defendem que as hipóteses descritas nos incisos I a III do aludido artigo não guardam qualquer vínculo com a comprovação de negligência, imprudência ou imperícia do agente de tratamento de dados, mas se relacionam com as hipóteses de ruptura do nexo de causalidade[168].

Outro dispositivo alvo de discussão em ambas as correntes doutrinárias é o art. 44 da LGPD. Embora ele não tenha uma conotação normativa quanto a responsabilidade civil dos agentes, é pertinente por elucidar o que seria um tratamento de dados irregular.

Para a LGPD, "o tratamento será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes" (art. 44). Estas dizem respeito ao modo pelo qual é realizado (art. 44, I) o resultado e os riscos que o titular razoavelmente dele (agente de tratamento) se espera (art. 44, II); ou a disponibilidade das técnicas de tratamento à época em que foi realizado (art. 44, III).

Essa redação é muito semelhante à do art. 14, §1º do CDC, o qual dispõe que o serviço é tido como defeituoso caso não forneça a segurança que o consumidor dele (fornecedor e prestador de serviço) pode esperar[169].

Os autores defensores do regime objetivo na LGPD argumentam que o art. 44 traz um fundamento de responsabilidade por risco ao

167 TEIXEIRA, Tarcísio; ARMELI, Ruth Maria Guerreiro da Fonseca. *Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD:* um Cotejamento com o CDC. *In:* DE LIMA, Cíntia Rosa Pereira. Comentários à Lei Geral de Proteção de Dados. Lei n. 13.709/2018,com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020, p. 297-326.

168 NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade Civil na LGPD: Problemas e Soluções. *Conpedi Law Review*, v. 6, n. 1, p. 158-174, 2020.

169 Art. 14, §1º do CDC. O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido.

fazer alusão à atividade irregularmente realizada no tratamento de dados por não cumprir com a segurança esperada, sendo essa segurança necessária devido ao risco na atividade de tratamento de dados[170] tal como acontece na legislação consumerista. Assim,

> a melhor conclusão seria pela responsabilidade objetiva do agente, não apenas pela tendência de objetivação, mas também porque a verificação da culpa, ainda que de forma objetiva, através da análise do descumprimento de deveres legais, pode impedir a reparação integral da vítima[171].

Diante disso os autores visualizam a exigência da aferição de culpa na eventualidade de um tratamento irregular ou de um incidente de segurança na atividade de tratamento de dados como meio para dificultar, quiçá impedir, a reparação do dano sofrido pelo titular dos dados. Daí a defesa do regime objetivo de responsabilidade civil na LGPD.

2.3. SINAIS DE ADOÇÃO DO REGIME SUBJETIVO DE RESPONSABILIDADE CIVIL NA LGPD

Em sentido oposto, defendida por Bruno Bioni, Daniel Dias, Gustavo Tepedino, Aline Terra, Gisela Sampaio da Cruz Guedes e Marcos Gomes da Silva Bruno, sustentam a responsabilidade civil subjetiva como regra na LGPD. Um de seus argumentos centrais se funda na disposição da lei em determinar aos agentes de tratamento de dados o cumprimento de uma série de deveres, o que revelaria a análise de culpa nos casos de violação.

170 MULHOLLAND, Caitlin Sampaio. *In*: Simpósio de Responsabilidade Civil e Proteção de Dados, 1, 2020, IBERC - *Responsabilidade Civil. YouTube*, 06 ago. 2020. Disponível em: https://www.youtube.com/watch?v=igbbxkbqeKI&t=1085s. Acesso em: 05 set. 2023.

171 GONDIM, Glenda Gonçalves. *A responsabilidade civil no uso indevido dos dados pessoais*. *Revista IBERC*, v. 4, n. 1, p. 19-34, 9 mar. 2021.

Como já exposto, a LGPD requer uma postura ativa do controlador e do operador em observar um conjunto de princípios e regras ao tratar dados pessoais. Exemplo disso é a dedicação de um capítulo específico relativo à "segurança e boas práticas", que ainda se divide em duas seções. A primeira exige dos agentes a adoção de padrões mínimos de segurança técnicas e administrativas (art. 46); já a segunda prescreve a criação de normas de boas práticas e governança em privacidade e proteção de dados (art. 50).

Para Bruno Bioni e Daniel Dias, esta técnica legislativa –um capítulo autônomo sobre segurança e boas práticas –é um sinal para deflagrar a responsabilidade civil subjetiva na LGPD, uma vez que há um arranjo normativo que opta por um juízo de valor em torno da conduta do agente de tratamento de dados[172]. Verifica-se, no caso concreto, quais medidas foram adotadas anteriormente pelo agente que visavam prevenir o evento danoso assim como as ações realizadas para mitigar os prejuízos.

Em outros termos o legislador estabeleceu um verdadeiro *standard* de conduta –um padrão de conduta socialmente esperado –a ser seguido pelos agentes para evitar incidentes de segurança, sob a pena de virem a ser responsabilizados[173].

Apesar de o art. 42 da LGPD não fazer menção direta ao risco da atividade ou à culpa[174], a obrigação de reparar o dano surge em decorrência da "violação à legislação de proteção de dados pessoais", ou seja, quando houver descumprimento do *standard* içado pela lei. Afinal, não seria coerente criar deveres a serem seguidos pelos agentes

172 BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*, v. 9, n. 3, p. 1-23, 22 dez. 2020.

173 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil*. 2. ed. vol. 4. Rio de Janeiro: Forense, 2021.

174 A LGPD se limita a dizer o seguinte: "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" (art. 42).

se o que se pretende é responsabilizá-los, ainda que tenham cumprido perfeitamente com as normas da legislação[175].

Diferentemente das interpretações feitas pelos autores do subtópico anterior, ao examinar os demais artigos relativos à responsabilidade e ressarcimento de danos na LGPD (arts. 43 e 44), esta doutrina destaca elementos nesses dispositivos que os distanciam da lógica aplicada no CDC e os aproximam do regime de responsabilidade fundado na culpa.

Segundo os autores Tepedino, Terra e Guedes, diferentemente dos incisos I e III do art. 43, que nitidamente se referem à relação de causalidade, o inciso II remete à ideia de culpa como fundamento da responsabilidade civil e sua redação é bem diferente da empregada pelo legislador no art. 12, § 3º, inciso II, do CDC"[176]. Já que, diferentemente da legislação consumerista, a LGPD preferiu dispensar a obrigação de indenizar caso comprovem que "embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II).

Ao comentar o *caput* do art. 43, os juristas entendem que o texto na negativa ("só não serão responsabilizados quando") evidencia na verdade a preocupação com a conduta dos controladores e operadores de dados, elegendo uma redação similar à do art. 493, "2", do Código Civil português e do art. 2.050 do Código Civil italiano, que adotaram sistemas de presunção de culpa[177].

175 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil*. 2. ed. vol. 4. Rio de Janeiro: Forense, 2021.

176 O Código Civil Português dispõe em seu art. 493º, 2, o seguinte: "Quem causar danos a outrem no exercício de uma *activida* de, perigosa por sua própria natureza ou pela natureza dos meios utilizados, é obrigado a repará-los, exceto se mostrar que empregou todas as providências exigidas pelas circunstâncias com o fim de os prevenir"; enquanto o art. 2.050 do Código Civil italiano estipula que "qualquer um que cause dano a outros no desenvolvimento de uma atividade perigosa, por sua natureza ou pela natureza dos meios utilizados, é obrigado ao ressarcimento se não provar ter adotado todas as medidas idôneas a evitar o dano".

177 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil*. 2. ed. vol. 4. Rio de Janeiro: Forense, 2021.

De uma leitura atenta dos dispositivos estrangeiros, constata-se que o causador do dano é obrigado a repará-lo, salvo "se mostrar que empregou todas as providências exigidas pelas circunstâncias com o fim de preveni-los" (art. 493, 2, do Código Português) ou se "provar ter adotado todas as medidas idôneas a evitar o dano" (art. 2.050 do Código italiano). Para os defensores do regime subjetivo na LGPD, nesses sistemas jurídicos

> presume-se a culpa do agente, mas esta pode ser afastada se ele conseguir demonstrar que observou o *standard* de conduta esperado, empregando medidas idôneas para evitar o dano. A presunção é, portanto, relativa. O art. 43 da LGPD seguiu exatamente esse caminho, preferindo estabelecer um sistema de presunção de culpa, do que adotar o modelo objetivo de responsabilidade e, nesse aspecto, afasta-se completamente do Código de Defesa do Consumidor[178].

Seguindo a mesma lógica, nas hipóteses de danos resultantes da violação da segurança dos dados, o agente de tratamento ainda assim não será responsabilizado quando "adotar as medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação" (art. 46).

Em síntese, assim como as expressões "em violação à legislação" do art. 42 e "embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação" do inciso II do art. 43, o parágrafo único do art. 44, ao citar expressamente "ao deixar de adotar as medidas de segurança", também faz menção à culpa, afastando a ideia de responsabilidade objetiva na LGPD.

178 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil*. 2. ed. vol. 4. Rio de Janeiro: Forense, 2021, p. 292.

Além disso, ao examinar as versões antecedentes ao Projeto de Lei que deu origem à LGPD até a sua publicação, nota-se que, embora o art. 6º do seu texto inicial tenha considerado o tratamento de dados pessoais como "atividade de risco"[179] e o art. 31 do Anteprojeto de Lei de 2015 enuncie o dever dos agentes de reparar os danos "independentemente de culpa"[180], ambas as expressões foram retiradas no curso do processo legislativo.

Para essa doutrina o histórico de tramitação da LGPD[181] deixa clara a decisão do legislador em não adotar um regime de responsabilidade civil objetiva[182], pois não permaneceram os indícios de objetividade para fins de responsabilização como a expressão "independentemente de culpa" ou alguma outra sentença equivalente, como assim o faz o CDC e o CC/02.

Importante observar ainda que a lei determina a realização do Relatório de Impacto à Proteção de Dados Pessoais (Art. 5º, XVII) nos casos de tratamento de dados capaz de gerar riscos a direitos e liberdades dos titulares, isto é, a LGPD não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado[183], e por mais que se reconheça a teoria do risco no sistema jurídico pátrio, é evidente que não se pode admitir como risco toda e qualquer atividade, sob a pena de banalização do instituto[184].

---

179 BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.060* de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012.

180 Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.

181 *DATA PRYVACY BRASIL*. *Memória da LGPD*. Observatório da Privacidade e Proteção de Dados Pessoais. Disponível em: http://35.227.175.13/memorias/. Acesso em: 05 set. 2023.

182 BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*, v. 9, n. 3, p. 1-23, 22 dez. 2020.

183 BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*, v. 9, n. 3, p. 1-23, 22 dez. 2020.

184 BRUNO, Marcos Gomes da Silva. *Dos Agentes de Tratamento de Dados Pessoais:* Do controlador e do operador. *In*: Viviane Nóbrega Maldonado e Renato Ópice Blum

Por fim, sustenta-se que se fosse o regime objetivo de responsabilidade a regra na LGPD, a remissão para o CDC no art. 45, seria inócua[185]. Os autores julgam incoerente o legislador atribuir a responsabilidade civil objetiva para as relações de consumo se esse já fosse o regime aplicável a toda a legislação. Esse fato, segundo eles, leva a interpretar novamente a adoção do regime subjetivo de responsabilidade como regra na LGPD.

CONCLUSÃO

Apesar da redação imprecisa da LGPD, pode-se concluir que o legislador adotou como regra a responsabilidade civil subjetiva, e admite-se a aplicação da responsabilidade civil objetiva excepcionalmente nas relações de consumo.

De fato, exige-se a análise da conduta do controlador e operador a partir do momento que determina as ações ideais a serem adotadas por eles. Ao referir-se expressamente a citações como "em violação a legislação" (art. 42), "não houve violação à legislação" (art. 43) e "danos decorrentes da violação da segurança" (art. 44), verdadeiramente demonstra sua intenção na aplicação de um regime subjetivo.

Dessa forma, responsabilizar os agentes de tratamento de dados, por um incidente de segurança mesmo que tenha feito tudo que estava ao seu alcance para evitar, bem como para mitigar o prejuízo vai de encontro a um dos desideratos da lei, além de desmotivá-los a estarem em conformidade com a lei.

Para, além disso, considerar qualquer atividade de tratamento como atividade de risco, sem indicação legal expressa –como faz o CC/02 e o CDC –em uma sociedade que se depara com o novo a cada dia, é ser imprudente. Embora a parte final do parágrafo único do

(Coord.), LGPD: *Lei Geral de Proteção de Dados comentada*. São Paulo: Revista dos Tribunais, 2019, p. 309-331.

185 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil.* 2. ed. vol. 4. Rio de Janeiro: Forense, 2021.

art. 927 do CC/02 admita a teoria do risco, não se pode aplicá-la sem fundamentos sólidos.

É evidente que um dos objetivos da LGPD é proteger os direitos à privacidade, personalidade, e liberdade do titular de dados, fornecendo a ele instrumentos para ter controle dos seus dados. Contudo, não se pode olvidar que a legislação também tem como fundamento o desenvolvimento econômico, a livre iniciativa e a inovação.

Em última análise, extrai-se da lei que o objetivo do legislador não é proteger unicamente o titular de dados com o fim de garantir-lhe o controle de suas informações e responsabilizar o controlador e o operador de dados a todo custo.

Portanto, a escolha da responsabilidade civil subjetiva na LGPD representa um compromisso entre a proteção dos direitos de privacidade e a promoção da inovação e desenvolvimento econômico.

REFERÊNCIAS

ANPD. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, v. 2.0, abr. 2022, p. 6. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 26 out. 2023.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*, v. 9, n. 3, p. 1-23, 22 dez. 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 20 out. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.060* de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filenme=PL+4060/2012. Acesso em: 24 out. 2023.

BRASIL. *Lei 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 07 out. 2023.

BRASIL. *Lei 8.078*, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasilia, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 17 out. 2023.

BRASIL. *Lei nº 10.406*, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 13 out. 2023.

BRUNO, Marcos Gomes da Silva. *Dos Agentes de Tratamento de Dados Pessoais:* Do controlador e do operador. *In*: Viviane Nóbrega

Maldonado e Renato Ópice Blum (Coord.), LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019, p. 309-331.

DATA PRYVACY BRASIL. *Memória da LGPD*. Observatório da Privacidade e Proteção de Dados Pessoais. Disponível em: http://35.227.175.13/memorias/. Acesso em: 05 out. 2023.

DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Maria Macena de. Responsabilidade na Lei Geral de Proteção de Dados Brasileira. *Revista Em Tempo*, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3229. Acesso em: 04 out. 2023.

ITÁLIA. R.D. 16 de março de 1942, n. 262. *O Código Civil Italiano*. Publicado na edição extraordinária do Diário da República, n.º 79 de 4 de abril de 1942. Disponível em: http://www.jus.unitn.it/cardozo/Obiter_Dictum/codciv/Lib4.htm. Acesso em: 25 out. 2023.

GONDIM, Glenda Gonçalves. A responsabilidade civil no uso indevido dos dados pessoais. *Revista IBERC*, v. 4, n. 1, p. 19-34, 9 mar. 2021. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/140. Acesso em: 07 out. 2023.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *In: Revista de Direito do Consumidor*, Brasília, v. 120, n. 2, p. 469-483, nov/dez. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116. Acesso em: 20 out. 2023.

MULHOLLAND, Caitlin Sampaio. *In*: Simpósio de Responsabilidade Civil e Proteção de Dados, 1, 2020, IBERC - Responsabilidade Civil. *YouTube*, 06 ago. 2020. Disponível em: https://www.youtube.com/watch?v=igbbxkbqeKI&t=1085s. Acesso em: 05 out. 2023.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade Civil na LGPD: Problemas e Soluções. *Conpedi Law Review*, v. 6, n. 1, p. 158-174, 2020. Disponível em: https://indexlaw.org/index.php/conpedireview/article/view/7024. Acesso em: 08 out. 2023.

PORTUGAL. *Decreto-Lei n.º 47344*, de 25 de Novembro de 1966. Aprova o Código Civil e regula a sua aplicação. Ministério da Justiça, 1966. Disponível em: https://dre.pt/web/guest/legislacaoconsolidada//lc/147103599/202107051318/73906010/diploma/índice. Acesso em: 05 out. 2023.

SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In:* BIONI, Bruno *et. al.* (Coord. Exec.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 330-349. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 03 out. 2023.

TEIXEIRA, Tarcisio; ARMELI, Ruth Maria Guerreiro da Fonseca. Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD: um Cotejamento com o CDC. *In:* DE LIMA, Cíntia Rosa Pereira.*Comentários à Lei Geral de Proteção de Dados. Lei n. 13.709/2018, com alteração da lei n. 13.853/2019*. São Paulo: Almedina, 2020, p. 297-326. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 16 out. 2023.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil*. 2. ed. vol. 4. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530989941/. Acesso em: 01 out. 2023.

A PROTEÇÃO MULTINÍVEL DOS DADOS PESSOAIS DOS TRABALHADORES À LUZ DA LEI Nº 13.709 DE 14 DE AGOSTO DE 2018

THE MULTI-LEVEL PROTECTION OF WORKERS' PERSONAL DATA IN LIGHT OF LAW No. 13,709 OF AUGUST 14, 2018.

Stella Muniz Campos Elias

Stella Muniz Campos Elias[186]

RESUMO

A Lei Geral de Proteção de Dados - LGPD- foi trazida ao ordenamento jurídico brasileiro para proteger todas as pessoas físicas detentoras de dados pessoais, cuja denominação trazida pela lei para estes indivíduos foi nomeá-los como titulares de dados. Estes titulares detêm o controle do gerenciamento de todo e qualquer tratamento destes dados, os quais devem ser realizados de forma transparente e adequada para todos os impactados nas operações internas ou externas da empresa. Consequentemente, é necessário que seja garantida a proteção desses dados em âmbito infraconstitucional, constitucional e, ainda, supranacional como um direito fundamental da pessoa humana, resultando em uma garantia global, denominada proteção multinível dos dados pessoais. Com isso, qualquer indivíduo, quando passa para a qualidade de trabalhador, leva consigo estas proteções, as quais devem ser resguardadas pelas empresas, especialmente para assegurar desde a contratação o direito destes trabalhadores a autorizar, ou não, nas hipóteses em que seja exigido, o tratamento dos próprios dados pessoais.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados; Titular de Dados; Proteção Multinível dos Dados Pessoais; Trabalhadores.

ABSTRACT

The General Data Protection Law - LGPD- was brought into the Brazilian legal system to protect all natural persons holding personal data, whose name brought by the law for these individuals

186 Advogada Empresarial. Mestra pelo Programa de Pós-Graduação *stricto sensu* em Direito da Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-Graduada em Direito do Trabalho e Processo do Trabalho pela Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-graduada em Docência com Ênfase Jurídica. Advogada. Consultora e Especialista em Proteção de Dados. Consultora e Especialista em Proteção Trabalhista. Vice-presidente da Comissão de Proteção de Dados da OAB/MG. Membro do Programa e Comissão do Direito na Escola. Membro do Grupo de Pesquisa e Extensão Capitalismo e Proteção Social na Perspectiva dos Direitos Humanos e Fundamentais do Trabalho e da Seguridade Social.

was to name them as data holders. These holders have control over the management of any and all processing of this data, which must be carried out in a transparent and appropriate manner for everyone impacted by the company's internal or external operations. Consequently, it is necessary to guarantee the protection of these data at infraconstitutional, constitutional and even supranational levels as a fundamental right of the human person, resulting in a global guarantee, called multilevel protection of personal data. As a result, any individual, when they become a worker, takes with them these protections, which must be safeguarded by companies, especially to ensure, from the moment they are hired, the right of these workers to authorize, or not, in the cases in which it is required, the processing of your own personal data.

KEYWORDS: General Data Protection Law; Data Holder; Multilevel Protection of Personal Data; Workers.

INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como a Lei Geral de Proteção de Dados –LGPD-, trouxe uma proteção específica aos dados pessoais dos indivíduos ao serem tratados ou armazenados dentro das corporações, sejam elas públicas ou privadas, alcançando desde as empresas individuais, pequenas, médias e grandes empresas até as multinacionais.

Ao proteger os dados pessoais da pessoa física, esta lei nos remete, inicialmente, aos aspectos da personalidade civil da pessoa natural, cuja previsão está na Parte Geral do Código Civil e a qual estabelece a proteção dos bens inerentes à pessoa humana, tais como o nome e a vida privada.

Nesse sentido, também há no nosso ordenamento jurídico a Lei nº 12.965 de 2014, conhecida como Lei do Marco Civil da Internet, que regula direitos e deveres dos internautas na navegação, com o intuito de proteger os dados pessoais e a privacidade dos usuários.

Além disso, a Constituição da República de 1988 também prevê expressamente a proteção dos direitos fundamentais à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assim como o "direito à proteção dos dados pessoais, inclusive nos meios digitais", no art. 5º, LXXIX.

Nesse compasso, é necessário ir além e trazer para esta análise a proteção dos dados pessoais como expressão dos Direitos Humanos, uma vez que a própria Declaração Universal de Direitos Humanos já versava, em 1948, sobre a tutela à vida privada.

Com isso, verifica-se que a proteção de dados pessoais tem proteção não só infraconstitucional, mas também tem proteção constitucional e, indo além, tem ampla tutela internacional.

Essa proteção multinível dos dados pessoais faz com que o indivíduo tenha um verdadeiro direito humano à proteção da privacidade, intimidade, vida privada e aos dados pessoais e, consequentemente, estes direitos são inerentes à pessoa humana detentora da titularidade destes dados pessoais, não conseguindo se desvencilhar de tais direitos.

Justamente por esta razão, quando o indivíduo passa a integrar uma relação de emprego, também leva consigo esta proteção multinível dos próprios dados pessoais para dentro das corporações.

Dessa forma, o presente artigo demonstrará que a legislação existente não pode separar a proteção ao direito humano à intimidade, vida privada, privacidade e, especialmente, aos dados pessoais dentro de uma relação entre trabalho e capital, sendo o estudo dividido em três capítulos e a conclusão. O primeiro tratará sobre a previsão legal dos direitos de personalidade no direito infraconstitucional e a proteção de dados no direito brasileiro. Já o segundo abordará sobre a proteção constitucional e as peculiaridades da privacidade no ordenamento jurídico pátrio e, por fim, o último capítulo versará sobre a proteção dos dados pessoais como direitos humanos e os reflexos na pessoa humana que trabalha.

1. A PREVISÃO LEGAL INFRACONSTITUCIONAL DOS DIREITOS DE PERSONALIDADE E A PROTEÇÃO DE DADOS NO DIREITO BRASILEIRO

Inicialmente, não podemos pensar na proteção dos dados pessoais sem antes discorrer sobre os direitos de personalidade, os quais são definidos, de acordo com Maria Helena Diniz (2012, p. 134) como sendo "os direitos subjetivos da pessoa de defender o que lhe é próprio, ou seja, a identidade, a liberdade, a sociabilidade, a reputação, a honra, a autoria etc.".

Esta abordagem se faz necessária, uma vez que a própria Lei Geral de Proteção de Dados –LGPD –indica, entre outros, o direito à privacidade como um de seus fundamentos legais, direito este que integra o direito de personalidade.

Portanto, imperioso apontar as normas legais que tratam sobre o direito à privacidade tanto no Código Civil de 2002 quanto na Lei do Marco Civil da Internet de 2014, antes mesmo de adentrar na proteção específica dos dados pessoais.

Vale ressaltar que o direito à privacidade possui origem burguesa e, de maneira geral, permaneceu restrito à burguesia até o final da primeira metade do século XX. Este cenário começou a apresentar mudanças mais significativas no decorrer da década de 1960, tendo impulsionado, sobretudo, o aumento da circulação de informações, vez que houve ascensão do aprimoramento tecnológico na coleta de informações, o que resultou em uma "capacidade técnica cada vez maior de recolher, processar e utilizar a informação". (DONEDA, 2006, p. 12).

Neste sentido, o art. 21 do Código Civil dispõe que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Dessa forma, verifica-se que a privacidade, por ser um dos direitos de personalidade trazidos pelo próprio Código Civil, não pode ser violada, salvo os casos excepcionais expressamente previstos na

lei, devendo o judiciário, inclusive, intervir quando motivado para garantir que esta norma seja devidamente cumprida.

Neste compasso, o art. 3º, inciso II, da Lei do Marco Civil da Internet, traz como princípio, dentre outros, a proteção da privacidade, além de estabelecer, no inciso III do mesmo artigo, a proteção expressa dos dados pessoais.

Além destes artigos, a Lei do Marco Civil da Internet também fixou explicitamente, no art. 7º, tanto os direitos e garantias do usuário quanto a proteção ao direito à privacidade, assim como garantiu expressamente, no art. 8º, que o direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Por fim, a Lei Geral de Proteção de Dados veio para dar ainda mais proteção ao tratamento dos dados pessoais dos indivíduos, visando garantir que o titular dos dados seja cientificado de todo e qualquer tratamento de seu dado pelas empresas, fixando, inclusive, diversas sanções administrativas diferentes para penalizar aquele que descumprir as regras estabelecidas e lesar os titulares dos dados.

Com isso, verifica-se que a proteção aos dados pessoais dos indivíduos, apesar de atualmente ter normas específicas, sempre esteve ligada ao direito à vida privada, direito este inserido no rol exemplificativo dos direitos de personalidade.

2. A PROTEÇÃO CONSTITUCIONAL DA PRIVACIDADE E SUAS PECULIARIDADES NO ORDENAMENTO JURÍDICO PÁTRIO

A Constituição da República de 1988 estabeleceu no rol dos direitos fundamentais do art. 5º, mais especificadamente no inciso X, que os direitos à intimidade, à vida privada, à honra e à imagem das pessoas são invioláveis.

Em 2022, foi promulgada a EC 115, a qual incluiu o inciso LXXIX ao mesmo artigo anteriormente citado, que expressamente passou

a garantir que a proteção aos dados pessoais fosse elevada para tratamento no plano dos direitos e garantias fundamentais.

Nesse sentido, a EC 115/2022 também incluiu o inciso XXVI do art. 21 para estabelecer que compete à União "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei", bem como fixou a competência privativa deste ente federativo, no inciso XXX do art. 22, para legislar sobre a "proteção e tratamento de dados pessoais".

Dito isso, vale pontuar que privacidade ou vida privada, de acordo com Bernardo Gonçalves Fernandes (2015, p. 421-422), é um "direito que um indivíduo tem de se destacar (se separar) de um grupo, isolando-se da observação deste ou como, ainda, o direito ao controle das informações veiculadas sobre si mesmo."

Além disso, Fernandes (2015, p. 422) também pontua que

> "a restrição ao direito à privacidade", somente pode ocorrer a partir do consentimento daquela própria pessoa, uma vez que "os direitos fundamentais, mesmo não sendo passíveis de renúncia plena, comportam formas de autolimitação. Se a restrição é feita espontaneamente, com o seu titular falando sobre sua intimidade como em uma entrevista, o caso é de mais fácil problematização."

Dessa forma, nota-se que já havia uma garantia constitucional aos direitos inerentes à pessoa humana, em especial quanto ao direito à privacidade, e que, com a importância do tema à sociedade civil, elevou a proteção aos dados pessoais das pessoas físicas ao *status* constitucional, sendo diretamente ligada à vida privada, uma vez que ambos pertencem ao indivíduo e são tutelados pelo direito de personalidade.

3. A PROTEÇÃO DOS DADOS PESSOAIS COMO EXPRESSÃO DOS DIREITOS HUMANOS E OS REFLEXOS NA PESSOA HUMANA QUE TRABALHA

No Brasil, a proteção inequívoca à vida privada das pessoas se fundamenta juridicamente tanto no Código Civil quanto na Lei do Marco Civil da Internet, além de também ser expressamente tutelada na Constituição da República.

Mas devemos ir além das fronteiras do ordenamento jurídico pátrio.

O direito à vida privada é um direito inerente à pessoa humana, cuja proteção também se projeta no plano internacional, como se pode verificar no artigo 12 na Declaração Universal dos Direitos Humanos, que dispõe "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

Com isso, verifica-se que a vida privada –diretamente ligada à proteção aos dados pessoais –constitui um verdadeiro direito humano e tem proteção não só nas leis infraconstitucionais, mas também constitucionais e, ainda, internacionais.

Da mesma forma acontece com a proteção aos dados pessoais da pessoa humana, uma vez que é diretamente ligada à vida privada e, portanto, também está guarnecida da tutela nas três esferas: infraconstitucional, constitucional e no direito internacional dos direitos humanos.

Assim, pode-se dizer que há uma proteção multinível do direito à privacidade e, consequentemente, dos dados pessoais da pessoa humana, tornando-os verdadeiros direitos humanos.

Justamente por essa estreita relação entre direito à vida privada e direito à proteção dos dados pessoais que o indivíduo, quando passa a integrar uma relação de emprego, também leva consigo o direto à proteção multinível dos próprios dados pessoais, devendo o empregador, por consequência, coletar o consentimento dos seus

empregados de forma prévia, informada, livre e inequívoca sempre que necessitar tratar os respectivos dados, nas hipóteses em que o consentimento for exigido como fundamento legal nas transações internas de dados dos funcionários da empresa.

Se a proteção ao direito à vida privada está diretamente ligada à proteção dos dados pessoais, e sendo a pessoa humana a única que detém o poder de permitir ou não o manuseio dos seus dados, não há como desvincular estas prerrogativas da pessoa humana que trabalha, uma vez que são direitos inerente ao direito de personalidade dos indivíduos.

Nesse compasso, Fernandes (2015, p. 421) afirma que "a divulgação de erro e/ou dificuldades acaba por inibir ou aniquilar os esforços de autossuperação, razão pela qual a esfera da privacidade", logo dos dados pessoais, "visa a fornecer um ambiente de tranquilidade emocional fundamental para uma autoavaliação de metas e objetivos pessoais".

É exatamente por esta razão que a Lei Geral de Proteção de Dados estabeleceu, em seu art. 7º, o consentimento como uma das formas que permite o manuseio dos dados pessoais alheios.

Portanto, a pessoa humana que trabalha tem garantido o direito a autorizar, ou não, nas hipóteses em que seja exigido, o tratamento dos próprios dados pessoais, por força das normas infraconstitucionais, constitucionais e supranacionais, devendo a empresa assegurar esta prerrogativa desde a contratação do funcionário.

Nesse sentido, Adalcy Rachid Coutinho (2020, p. 298) afirma que

> As relações entre empregador e empregado, não obstante gravitem no espaço interprivado e por força de um contrato celebrado, não isentam as partes da observância das normas convencionais internacionais, constitucionais relativas aos direitos fundamentais e, ainda, no que tange aos dados, da Lei de Proteção de Dados –Lei n. 13.709/2018.

Dessa forma, a proteção multinível da privacidade e, sobretudo, dos dados pessoais, está garantida nas leis infraconstitucionais, na própria Constituição da República e ainda tem a tutela no direito internacional dos direitos humanos, devendo o empresário garantir a aplicabilidade dessas normas nas relações de emprego, uma vez que a pessoa que trabalha é a titular destes direitos.

CONCLUSÃO

Os direitos da personalidade, tais como privacidade, intimidade, honra e imagem são tutelados tanto no plano infraconstitucional, pela Parte Geral do Código Civil de 2002 e pelos arts. 7º e 8º da Lei do Marco Civil da Internet de 2014, como nos direitos fundamentais do art. 5º, especificamente nos incisos X, da Constituição da República, estando direta e intimamente ligados à proteção aos dados pessoais dos indivíduos, mesmo quando estamos tratando dos dados digitais destas pessoas, conforme consignado no art. 5º, LXXIX, pois se trata do direito humano de se ter prerrogativa em gerir os direitos inerentes à vida, à liberdade, à igualdade, à segurança e à propriedade destas pessoas físicas.

Por privacidade, entende-se que é o direito de o indivíduo realizar o controle do que veicular ou não sobre as próprias informações, direito este que está diretamente ligado à proteção de dados pessoais, uma vez que esta é exatamente a finalidade da Lei nº 13.709 de 14 de agosto de 2018, mais conhecida como a Lei Geral de Proteção de Dados –LGPD-.

A LGPD trouxe uma proteção específica aos dados pessoais dos indivíduos para que tomem conhecimento de todas as operações que envolvam o tratamento ou armazenamento dos dados dentro das corporações, sejam elas públicas ou privadas, alcançando desde as empresas individuais, pequenas, médias e grandes empresas até as multinacionais.

Nesse sentido, a Lei nº 12.965 de 2014, conhecida como Lei do Marco Civil da Internet, veio abranger a aplicabilidade tanto do direito

à privacidade como da proteção aos dados pessoais ao tratar sobre os direitos e deveres dos internautas na navegação, com o intuito de proteger os dados pessoais e a privacidade dos usuários.

Neste compasso, a Constituição da República de 1988 também previu expressamente a proteção dos direitos fundamentais à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e, ainda, dos dados pessoais.

Além disso, a proteção da privacidade e, consequentemente dos dados pessoais, é expressão dos direitos humanos desde 1948, com a Declaração Universal de Direitos Humanos, que tutela a vida privada no plano internacional por meio do artigo 12.

Com isso, tanto o direito à vida privada como a proteção dos dados pessoais gozam de tutela infraconstitucional, constitucional e supranacional, resultando, assim, em uma proteção multinível destes direitos.

É justamente por esta razão que, quando o indivíduo passa a integrar uma relação de emprego, também leva consigo esta proteção multinível dos próprios dados pessoais para dentro das corporações, devendo o empresário garantir a aplicabilidade destas normas nas relações de emprego, em especial, quando a hipótese de tratamento destes dados é a do consentimento do titular de dados, neste caso, o próprio trabalhador.

Dessa forma, a pessoa humana que trabalha deve sempre ter garantido o direito a autorizar, ou não, nas hipóteses em que seja exigido, o tratamento dos próprios dados pessoais, por força das normas infraconstitucionais, constitucionais e supranacionais, devendo a empresa assegurar esta prerrogativa desde a contratação do funcionário.

REFERÊNCIAS

BRASIL. [Constituição de (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 14.dez. 2020.

BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10088.htm#art5>. Acesso em: 14.dez.2020.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 14.dez.2020.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14.dez.2020.

COUTINHO, Aldacy Rachid. Proteção de dados do trabalhador e a questão do necessário consentimento: uma abordagem a partir da Lei n. 13.709/2018. In: **Futuro do trabalho: os efeitos da revolução digital na sociedade**. CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz, FONSECA, Vanessa Patriota da (Org.). Brasília: ESMPU, 2020.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. Teoria do direito civil. 29ª ed. São Paulo: Saraiva, 2012.

DONEDA, Danilo. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade.** Disponível

em: <https://www.academia.edu/23345532/Considera%C3%A7%C3%B5es_iniciais_sobre_os_bancos_de_dados_informatizados_eo_direito_%C3%A0_privacidade>. Acesso em: 13.dez.2020.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 7ª ed. Salvador: Juspodvm, 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** 1948. Rio de Janeiro: UNICRIO, 2009. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em 15.dez.2020.

CRIMES CIBERNÉTICOS
UMA ANÁLISE ACERCA DA APLICABILIDADE DO PROGRAMA DE COMPLIANCE INTEGRADO À LEI GERAL DE PROTEÇÃO DE DADOS COMO MEDIDA DE PREVENÇÃO E MITIGAÇÃO DE RISCOS RELACIONADOS A CRIMES CIBERNÉTICOS

CYBER CRIMES
AN ANALYSIS OF THE APPLICABILITY OF THE COMPLIANCE PROGRAM INTEGRATED TO THE GENERAL DATA PROTECTION LAW AS A PREVENTION AND MITIGATION MEASURE OF RISKS RELATED TO CYBER CRIMES

Thamiris Mendes Galdino da Costa
Samuel Costa de Jesus Ferreira

Thamiris Mendes Galdino da Costa[187]
Samuel Costa de Jesus Ferreira[188]

RESUMO

Este estudo versa sobre a aplicabilidade dos programas de compliance integrados à Lei Geral de Proteção de Dados (Lei nº 13.709/2018, alterada pela Lei nº 13.853/2019), a fim de prevenir e mitigar riscos relacionados aos crimes cibernéticos. Assim, será apresentada uma breve introdução sobre a evolução tecnológica e a proteção de dados. Em seguida, será abordado o conceito de crime cibernético e ciberespaço, trazendo à luz do conhecimento jurídico e das empresas quais são os crimes mais comuns cometidos contra o patrimônio das organizações, envolvendo todos seus ativos, inclusive os dados pessoais da cadeia produtiva direta e indireta de uma organização. Posto isso, será discutido como a LGPD pode contribuir para proteger dados pessoais por meio de ações preventivas, tais como: mapeamento de dados, comitê de diligências para ação e reação contra possíveis incidentes de segurança, treinamentos, entre outros. Em complemento, os programas de *compliance* serão demonstrados para manutenção e conformidade das ações envolvidas com a Lei Geral de Proteção de Dados para promover um ambiente seguro e mitigar riscos cibernéticos, envolvendo ações capazes de comprovar a máxima executada a fim de manter a integridade, ética e segurança dos dados e todos os sistemas que os compõem.

PALAVRAS-CHAVE: Proteção de Dados. *Compliance*. Crimes cibernéticos. Prevenção.

187 Advogada. Bacharel em Direito pela PUC MINAS. Membro Colaboradora da Comissão de Proteção de Dados e da Comissão de *Compliance* da Ordem dos Advogados de Minas Gerais. Técnica em Administração e Logística pelo SENAC Minas com qualificação em Controle de Qualidade Industrial pelo SENAI.

188 Advogado especialista em análises de conformidade e requisitos legais relacionados a Riscos, Governança e *Compliance*. Especialista em Governança, Riscos e *Compliance* pelo Centro de Estudos em Direito e Negócios - CEDIN. Bacharel em Direito pela PUC MINAS e Membro da Comissão de *Compliance* da Ordem dos Advogados de Minas Gerais. Ampla vivência na implantação e monitoramento de Programas de *Compliance* em empresas atuantes nos setores de Mineração e Construção.

ABSTRACT

The present study focuses on the applicability of compliance programs integrated to the General Data Protection Law (Law No. 13,709/2018, amended by Law No. 13,853/2019), aiming to prevent and mitigate risks related to cybercrimes. Thus, a brief introduction to technological evolution and data protection will be presented. Subsequently, the concept of cybercrime and cyberspace will be addressed, clarifying, in both legal and corporate perspective, which are the typical offenses perpetrated against the assets of organizations, encompassing all their resources, including the personal data of both the direct and indirect segments of an organizational production chain. Therefore, it will be discussed how the LGPD can contribute to safeguarding personal data through preventive measures, such as data mapping, a diligence committee for proactive and reactive responses to potential security incidents, training, among others. Furthermore, compliance programs will be showcased to ensure the maintenance and adherence of actions in accordance with the General Data Protection Law, in order to promote a secure environment and mitigate cyber risks. This involves actions capable of substantiating the executed dictum with the aim of preserving the integrity, ethics, and the data security of all systems comprising them.

KEYWORDS: Data Protection. Compliance. Cybercrimes. Prevention.

1. INTRODUÇÃO

Com a evolução do mundo globalizado e acesso à informação, as legislações em torno da proteção de dados passaram a ter um papel de destaque, obrigando a todos, principalmente às empresas, a se adaptarem a uma nova cultura, em que a forma de tratamento e conscientização sobre os dados pessoais adviesse de uma relevância sistemática entre todos os envolvidos no processo, originando ações capazes de desenvolver o pensamento crítico sobre a segurança da

informação e consequentemente um novo modo de agir perante a implementação de práticas de *compliance* relacionadas à proteção de dados.

Além disso, com a dependência das organizações em tecnologia e a quantidade de dados armazenados digitalmente, os crimes cibernéticos estão se tornando cada vez mais comuns. Sendo clara a utilização do ciberespaço para aprimorar e desenvolver novos meios capazes de invadir sistemas empresariais para difundir novos crimes, tais como sequestro de dados e compartilhamento não autorizado de informações confidenciais, o que inevitavelmente resulta em danos, tanto para os titulares de dados pessoais como para a empresa. Um exemplo comum de crime cibernético são os vírus, também conhecidos como *malware*.

Nesse contexto, este artigo explora pontos importantes relativos aos crimes cibernéticos conceituando os mais comuns, o papel da LGPD na prevenção e combate, bem como a utilização de programas de compliance para garantia da conformidade da Lei Geral de Proteção de Dados aplicada nas empresas.

2. A ERA DA INFORMAÇÃO E O PAPEL DA LGPD

A Era da Informação trouxe relevantes aspectos para análise jurídica com a criação da internet, suas atribuições e características. De modo que, de acordo com PINHEIRO (2021)[189], "toda mudança tecnológica é uma mudança social, comportamental, portanto jurídica."

Desse modo, antes de abordarmos os assuntos relacionados aos crimes cibernéticos com enfoque em ambientes empresariais, é preciso reforçar que não resta dúvidas de que os dados são considerados o novo petróleo, frase icônica do matemático britânico Clive Humby e popularizada por muitos estudiosos e empresários, uma vez que a

189 PINHEIRO, Patrícia P. Direito Digital. Editora Saraiva, 2021. E-book. ISBN 9786555598438.

captação de dados pode gerar capital monetizado, valor econômico e um poder transformador entre as organizações com relação às suas estratégias de negócio. Esta analogia salienta a crescente importância dos dados na economia e na tomada de decisões. Do mesmo modo, a importância desses dados também se tornou foco dos criminosos cibernéticos com interesse em acessar e roubar dados confidenciais, como dados pessoais, informações financeiras e segredos comerciais para lucro próprio.

Assim, de maneira estratégica, proteger os dados, tanto por meio físico quanto digital e todas as estruturas que os envolvem, significa atender a uma obrigação legal, bem como zelar pelo patrimônio dos ativos tangíveis e intangíveis dentro de uma organização.

A LGPD (Lei Geral de Proteção de Dados - Lei 13.709/2018) foi criada no Brasil com base no modelo GDPR - *General Data Protection Regulation*, traduzida livremente como Regulamento Geral de Proteção de Dados da União Europeia. A GDPR provocou mudanças significativas no mercado mundial, fazendo com que aqueles países que não estivessem em conformidade com o regulamento fossem prejudicados em suas relações comerciais, resultando em publicidade negativa, perda econômica, financeira e de stakeholders [190] no comércio internacional.

Neste cenário, é importante destacar a principal finalidade da Lei Geral de Proteção de Dados, que é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, tendo em vista a segurança dos dados pessoais da pessoa física, com o objetivo de transmitir e resguardar as informações de forma clara e inequívoca e com fulcro na autodeterminação do titular, sobre como estes dados estão sendo tratados e reproduzidos durante a necessidade do seu uso por terceiros, principalmente dentro dos ambientes empresariais.

190 Stakeholders: Partes interessadas no negócio.

A Emenda Constitucional 115/2022, de 10 de fevereiro de 2022, também determina a proteção de dados pessoais entre os direitos e garantias fundamentais da Constituição Federal.

Quando falamos sobre dados pessoais, a LGPD nos apresenta duas qualidades de dados, quais sejam os dados pessoais capazes de identificar ou tornar identificável uma pessoa natural, por exemplo, o CPF, o telefone móvel, a data de nascimento, a placa do carro, o endereço residencial, entre outros, e os dados pessoais sensíveis, que, em rol taxativo conforme **art. 5º, II, da LGPD**[191], são aqueles capazes de discriminar uma pessoa por meio de um conjunto de características específicas, tais como: *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 ao titular.*

Partindo deste contexto, é possível analisar a importância da LGPD na prevenção contra crimes cibernéticos.

2.1. CRIMES CIBERNÉTICOS NOS AMBIENTES EMPRESARIAIS E A LEI GERAL DE PROTEÇÃO DE DADOS

A tecnologia da informação é uma realidade na maioria das empresas. Isso significa que grande parte de suas atividades perpassam por guarda e arquivamento de informações e dados sigilosos no ciberespaço, entre esses os dados pessoais.

O ciberespaço conceituado por FIORILLO (2016)[192] diz que "o território está intimamente relacionado a rede, e se caracteriza pela localização da informação. A informação na rede, portanto, passa a ser elemento identificador do território no ciberespaço."

191 BRASIL. Presidência da República. Casa Civil. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: [26 de set. de 2023].

192 FIORILLO, Celso Antônio P.; CONTE, Christiany P. Crimes no meio ambiente digital. Editora Saraiva, 2016. E-book. ISBN 9788547204198.

Nesse sentido, o ciberespaço pode ser compreendido como uma área extraterritorial, podendo ser acessada em qualquer lugar do mundo, bastando apenas que exista uma rede de internet no local. Então, mesmo que o conteúdo esteja registrado em uma rede de dados protegida, esta pode ser transmitida para qualquer lugar do mundo, bastando analisar onde a informação está guardada.

Para CRESPO (2021)[193], "ciberespaço é campo para o cometimento de delitos que já são tipificados em ordenamentos jurídicos, mas, também, é área onde condutas ainda não necessariamente incriminadas no Brasil, mas altamente danosas, ocorrem".

Dito isso, passa-se a se atentar com a cibersegurança e o que circula no ciberespaço com informações e dados de uma empresa, ganhando maior relevância para mitigar e prevenir ações maliciosas relacionadas aos crimes cibernéticos, tais como o sequestro e transferência de dados. Ou seja, com a evolução tecnológica enfrentamos novas realidades quanto às práticas delitivas, de modo que não se pode ignorar a realidade de novos *modus operandi* das condutas altamente danosas, principalmente quando há dados pessoais envolvidos.

Os crimes digitais que ocorrem no ciberespaço podem ser divididos em crimes próprios e crimes impróprios, conforme conceitua CRESPO (2011). Sendo os crimes próprios todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados). E os crimes impróprios são aquelas condutas tipificadas contra bens jurídicos tradicionais com auxílio da tecnologia.

Neste artigo, vamos nos aprofundar nos crimes próprios mais comuns enfrentados pelas organizações e seus impactos com relação à LGPD, tais como:

I. Acesso não autorizado:

A conduta de acessar de forma indevida o sistema de uma empresa pode gerar danos aos titulares de dados pessoais. Por exemplo,

193 CRESPO, Marcelo Xavier de F. Crimes digitais. Editora Saraiva, 2011. E-book. ISBN 9788502136663.

a invasão de um hacker por meio de um link falso acessado por um funcionário pode ocasionar insegurança jurídica e danos aos titulares de dados, colocando em risco a sua autodeterminação, privacidade e transparência sobre as informações sequestradas.

Nesse sentido, o acesso não autorizado terá que ser avaliado como um incidente de segurança, o que pode acarretar sanções administrativas e advertências caso a empresa não consiga comprovar as condutas internas para prevenir e mitigar o ato ilícito básico para a prática de outros tantos crimes possíveis no ambiente virtual.

Assim, torna-se necessário demonstrar todas as ações e boa-fé das organizações, podendo ser sopesadas por meio da apresentação de sua política de privacidade e proteção de dados, a periodicidade de revisão dos documentos de acordo com o grau de risco, o inventário de dados com todo histórico e suas finalidades de acordo com a LGPD, relatórios de auditoria de cibersegurança e sistemas utilizados para identificação de ataques cibernéticos.

II. Obtenção e transferência ilegal de dados:

Atualmente, uma forma muito simples de obtê-los é por meio dos spywares, termo genérico para designar arquivos espiões. Estes podem ser encontrados de diversas maneiras, por exemplo, os cookies, encontrados facilmente em sites de navegação e têm como efeito comum a guarda de dados para futuros acessos. Porém, seguindo a norma da LGPD, os cookies também devem ser autorizados pelo titular para guarda das informações, devendo ser clara e específica a necessidade desses dados, requerendo ainda o consentimento do titular para continuidade do uso do site com a apresentação de sua política de proteção de dados pessoais. Ocorre que os cookies, a depender do site e a necessidade do titular, serão necessários para atender ao legítimo interesse do controlador na prestação do serviço demandado pelo titular de dados.

Estes cookies também servem como ferramentas para conhecer potenciais clientes, uma vez que, rastreando os usuários, inicia-se uma prática secundária com apresentação de propagandas especialmente

relacionadas com os interesses do titular. Entretanto, há spywares negativos que funcionam espionando as práticas do usuário, inclusive quanto a atividades confidenciais ou protegidas pela intimidade e o sigilo empresarial. E quanto a estes, é necessário a aplicação de treinamentos, DDS –Diálogo Diário de Segurança, comunicados internos dentro das organizações e outras iniciativas cabíveis que funcionem como prova em caso de incidente de segurança com pautas relacionadas aos impactos negativos capazes de atingir todos os públicos, internos e externos, caso seja identificado o vazamento de dados por má conduta no uso das informações.

A transferência ilegal dos dados quando comprovada deve ser informada imediatamente a ANPD, bem como a gravidade e a quantidade de dados vazados, podendo sofrer bloqueio dos dados pessoais aos quais se refere a infração até a sua regularização, eliminação dos dados pessoais de acordo com a infração, suspensão parcial do funcionamento do banco de dados pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pela empresa, conforme art. 52, incisos V, VI, X da LGPD.

III. Dano informático:

O dano informático pode advir da disseminação e contaminação de computadores pelos chamados vírus. Estes vírus são capazes de interromper as atividades da empresa, atrasando transações financeiras e causando instabilidade de sistemas necessários para o andamento das atividades organizacionais. Este dano pode afetar a confiança dos stakeholders e dos titulares com relação à proteção dos dados pessoais, sendo necessária a notificação para a Autoridade Nacional de Proteção de Dados sobre a ocorrência do incidente de segurança, bem como dispõe o art. 48 da LGPD.

IV. Dos vírus e sua disseminação:

Um dos vírus mais comuns, conhecido como phishing ou phishing scam, traduzido livremente como “pescaria” ou “golpe de

pescaria", acontece quando ocorre uma simulação, em que a vítima é atraída para acessar um link falso, uma página falsa ou executar algum arquivo para que haja furto de dados, pensando ser um conteúdo legítimo. É o que podemos chamar de técnica de engenharia social. Este é um dos meios mais comuns em que as ocorrências de ataques em ambientes empresariais possuem recorrência. Uma vez que a utilização do e-mail seja uma vertente e uma necessidade no mundo corporativo.

Neste tipo de ataque, existe também o *spear phishing,* conceituado por PINHEIRO (2020)[194], como:

> Um ataque em que o criminoso mira em um funcionário específico de uma organização, buscando alcançar dados corporativos, instalar malware e obter acesso à infraestrutura de TI da empresa, entre outras possibilidades escusas, podendo ser, ainda, uma ferramenta para alcançar dados e acessos de executivos ou informações que exijam escalação de privilégios. (PINHEIRO, 2020).

O *ransomware* é um *malware* utilizado para o sequestro dos dados e possuem duas formas de atuação, classificadas como concomitantes e não concomitantes.

De acordo com PINHEIRO (2020):

> Na primeira modalidade, é infectada a máquina e os dados do dispositivo são criptografados, sendo gerado um arquivo acessível, geralmente na área de trabalho ou apresentado em um navegador web em que o criminoso pede um resgate –geralmente a ser pago em criptomoedas –prometendo o envio de um código que possibilite que os dados sejam descriptografados, o que muitas vezes não acontece, ainda que seja

194 PINHEIRO, Patrícia P. **Segurança Digital - Proteção de Dados nas Empresas**: Grupo GEN, 2020. *E-book.* ISBN 9788597026405.

> efetivado o pagamento do "resgate". Na segunda modalidade, ocorre o mesmo processo supracitado, porém, o criminoso envia os dados da vítima –e da empresa inteira em algumas oportunidades –para servidores remotos, podendo ou não os criptografar, exigindo o resgate para não revelar informações sigilosas que a empresa possua. (PINHEIRO, 2020).

De acordo com Bússola, em artigo disponibilizado no site (EXAME, 2022)[195], nos últimos anos, empresas brasileiras foram grandes vítimas do *ransomware*. Em pesquisa realizada pela *Apura Cyber Intelligence,* as áreas mais visadas são as instituições governamentais e a indústria, que empatam em primeiro lugar, com 17,4%. Os prejuízos desses ataques são sequestro, exposição e/ ou destruição de dados, invasão a conteúdos sigilosos, fraudes financeiras, queda de ativos, paralisação das operações, etc.

Outros meios de ataques cibernéticos são os golpes do falso boleto, troca do Simcard de telefones corporativos, furto de dados por funcionários terceirizados, espionagem industrial e comercial por meio de vírus ocultos na base de dados das empresas, funcionando como um parasita coletando dados privados.

São diversos os meios de ataques aos ambientes corporativos, e estes citados foram apenas para sinalizar e alertar, sobre os crimes mais comuns, principalmente, com a LGPD sendo meio de confrontar as empresas sobre suas medidas de cibersegurança.

Válido ressaltar que LGPD não contém artigos específicos que tratam exclusivamente da segurança da informação, no entanto, é um tema latente e implícito em diversos artigos da lei. Alguns artigos relevantes que se relacionam com a segurança da informação incluem:

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

195 Bussola. (11 de 02 de 2022). EXAME. Acesso em 25 de set. de 2023, disponível em www.exame.com: https://exame.com/bussola/ransomware-e-uma-forte-ameaca-para-asempresas-brasileiras-em-2022/

> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> **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.
> **Art. 47.** Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
> **Art. 48.** O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> **Art. 49.** Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (Lei Geral de Proteção de Dados nº 13.709, de 14 de agosto de 2018)

Outros artigos da LGPD, como o Art. 50, também estabelece que o controlador deve adotar medidas para mitigar riscos associados ao tratamento de dados pessoais, incluindo riscos de segurança.

Ou seja, esta Lei se apresenta como uma norma de caráter orientativo, fiscalizatório e punitivo, arrecadatório, uma vez que permeia entre medidas de conscientização e boas práticas, assim como a aplicação de sanções administrativas com multas pecuniárias, advertências, publicização de fatos capazes ofuscarem a confiança das empresas nas relações de mercado. Essas sanções administrativas, são aplicadas pela ANPD –Autoridade Nacional de Proteção de Dados, órgão que tem por objetivo fiscalizar e garantir a ampla e correta observância da Lei Geral de Proteção de Dados, presente nos artigos 52, 53 e 54.

Assim, algumas medidas como a adoção de políticas de segurança da informação e, privacidade e proteção de dados; a compreensão sobre os atores responsáveis pela proteção de dados; a execução dos direitos dos titulares de dados; a anonimização por meio de criptografia de dados quando possível; a criação de relatórios de impacto de proteção de dados (RIPD) de forma periódica como medida de prevenção e análise de riscos; a implementação de um comitê de proteção de dados visando a táticas de ação e reação perante um incidente de segurança para tomada de decisão são atitudes que evidenciam o preparo e a conscientização sobre como as empresas devem se monitorar tendo como suporte a própria Lei Geral de Proteção de Dados.

E uma maneira de garantir que estas práticas não se percam com o tempo, principalmente porque o mercado é rotativo com relação às pessoas que a compõem, o *compliance* surge de maneira a colaborar com a manutenção das razões necessárias para a conformidade de todas as ações envolvidas dentro de uma organização.

3. PROGRAMAS DE *COMPLIANCE* COMO MECANISMOS DE CONTROLE E PREVENÇÃO

O termo *Compliance* (*to comply)*[196] é compreendido de forma literal como o *"estar em conformidade com as normas*", no sentido de que seria uma forma de se fazer cumprir o que está na lei e regulamentos estatais (VERISSIMO, 2017).

A abrangência do instituto alcança diferentes esferas da atividade empresarial, vai dos códigos de prevenção em matéria ambiental ou em defesa do consumidor a um arsenal de medidas preventivas e marcos regulatórios do exercício de atividades laborais, criando uma estrutura que tende a adotar medidas para prevenir sanções e evitar aplicação de punições mais severa por parte do Estado, além da garantir medidas e controles internos para prevenir e mitigar o cometimento de irregularidades e ameaças.

Para Lothar Kuhlen[197] (2013), são chamados de *compliance* as medidas pelas quais as empresas pretendem assegurar que as regras vigentes para elas e para seus funcionários sejam cumpridas, que as infrações se descubram e eventualmente sejam punidas.

Além dos conceitos iniciais, vale destacar o que menciona o autor Ivó Coca Vila (2013):

> Segundo o autor, *compliance* é o conjunto de medidas tendentes a garantir que todos e cada um dos membros de uma empresa, desde o presidente do conselho de administração, até o último empregado, cumpram com os mandados e as proibições jurídico-

196 To comply, em inglês, é um verbo que significa agir de acordo com as regras. O significado da palavra tem relação com a conduta da empresa e sua adequação às normas legais e administrativas.

197 KUHLEN, Lothar. **Cuestiones fundamentales de comlpliance y derecho penal**. Madrid: Marcial Pons, 2013, p. 51

> penais, e que, em caso de infração, seja possível suas descobertas e adequada sanção (VILA, 2013).[198]

Contudo, a origem do *compliance* está relacionada com diferentes fatores nacionais e internacionais que se fizeram, progressivamente, presentes nas últimas décadas. Entre eles, podem ser citados os escândalos empresariais ocorridos nos diversos países, expondo riscos e desestimulando as atividades econômicas (MOREIRA, 2019).

No âmbito dos crimes cibernéticos, isso implica adotar ações para evitar invasões, identificar possíveis ameaças e agir prontamente e eficientemente diante de incidentes de segurança.

Existem várias razões pelas quais o programa de *compliance* é crucial para a prevenção dos crimes cibernéticos. Primeiramente, ao implementar políticas de segurança da informação robustas e assegurar a conformidade com os padrões estabelecidos, as empresas estão em melhor posição para identificar e tratar vulnerabilidades em seus sistemas.

Além disso, um programa de *compliance* bem estruturado auxilia na criação de uma cultura de segurança digital nas organizações, de modo que as boas práticas de conformidade incluam a conscientização e a capacitação dos colaboradores acerca das melhores práticas de segurança, tal como a utilização de senhas robustas, a identificação de tentativas de *phishing,* a implementação de *backups* periódicos e entre outros diversos pontos.

Com os colaboradores cientes dos riscos e aptos a se protegerem, as possibilidades de sucesso de um ataque cibernético são mitigadas. Outro aspecto importante do programa de *compliance* é a elaboração de políticas de governança de dados. Isso inclui a definição de quem tem

198 COCA VILA, Ivó. ¿Programas de cumplimiento como forma de autorregulación regulada? In: SILVA SÁNCHEZ, Jesús-María (Ed.). *Criminalidad de empresa y compliance*: prevención y reacciones corporativas. Barcelona: Atelier, 2013, p. 55. No original: "por *compliance* hay que se entender aquel conjunto de medidas tendiente a garantizar que todos y cada uno de los membros deuna empresa, desde el consejo de administración hasta el ultimo empleado, cumplan com los mandatos y las prohibiciones jurídico-penales, y a que, em caso de infracción, sea posible su descumprimento y adequada sanción."

acesso a quais informações e sob que circunstâncias. Ao estabelecer controles rigorosos sobre o acesso aos dados e informações da empresa, é possível evitar que sejam obtidos indevidamente ou divulgados por indivíduos não autorizados.

Outrossim, um programa de *compliance* eficaz acompanha as regulamentações em constante evolução relacionadas à segurança cibernética. Com o aumento das leis de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, as empresas estão sob pressão para proteger as informações pessoais.

Um programa de *compliance* robusto e bem implementado permite que as empresas se adaptem às mudanças regulatórias e tomem as medidas necessárias para garantir os devidos atendimentos de conformidade às legislações e regulamentações vigentes.

Assim, o programa de *compliance* é fundamental na prevenção dos crimes cibernéticos, pois ajuda as empresas a identificar, mitigar e responder a ameaças de segurança de forma eficaz. Ao implementar políticas de segurança, promover a conscientização e treinamento dos funcionários, estabelecer políticas de governança de dados e estar atualizadas com as regulamentações, as empresas podem fortalecer sua postura de segurança e minimizar os riscos de crimes cibernéticos.

4. DESAFIOS E LIMITAÇÕES DOS PROGRAMAS DE *COMPLIANCE* EM ATENDIMENTO À LGPD

A implementação de um programa de *compliance* eficiente é essencial para garantir o cumprimento da Lei Geral de Proteção de Dados (LGPD) dentro de uma organização e, assim, prevenir o vazamento de dados e ataques de crimes cibernéticos.

No entanto, essa tarefa apresenta desafios e limitações. Entre os principais obstáculos enfrentados pelas empresas na busca por atender às exigências da LGPD e nas possíveis limitações durante a implementação de programas de *compliance*, destacam-se: em alguns casos *a necessidade de* apoio da alta gestão, a realização do correto

mapeamento de dados e análise de riscos, as mudanças de cultura organizacional, a segurança da informação, as restrições financeiras e tecnológicas e a due diligence de dados. Será explorado cada um deles em detalhes abaixo.

I. Apoio da alta gestão:

Implementar os controles estabelecidos na LGPD e mitigar os crimes de segurança da informação não é uma tarefa simples. Requer esforço e comprometimento de todas as partes envolvidas, principalmente a alta gestão das organizações. O apoio da alta gestão é essencial para garantir que os controles de segurança sejam eficazes e que a LGPD seja cumprida de forma eficaz.

Isso significa que devem demonstrar o compromisso com a proteção dos dados e liderar pelo exemplo. Ao adotar boas práticas de segurança e respeitar as diretrizes da LGPD, a alta gestão mostra que leva a proteção dos dados a sério, incentivando os demais colaboradores a fazer o mesmo.

Além disso, a alta gestão também deve estar envolvida nas estratégias de monitoramento e resposta a incidentes de segurança da informação. Isso implica que devem ser informados sobre as ameaças atualmente existentes, as medidas tomadas para mitigá-las e as ações tomadas em caso de violação de dados. A participação da alta gestão nessas atividades ajuda a garantir uma resposta rápida e eficaz aos incidentes, minimizando possíveis danos.

II. Mapeamento de dados pessoais e análise de riscos:

Identificar onde os dados pessoais são armazenados, como são tratados e compartilhados e suas finalidades, além de documentar adequadamente os processos em conformidade com as leis, é fundamental para realizar um mapeamento completo e detalhado dos dados coletados e processados pela organização.

III. Mudança de cultura organizacional:

Um programa de *compliance* envolve não apenas a implementação de políticas e procedimentos, mas também uma mudança cultural na organização. É necessário promover uma conscientização generalizada sobre a importância da privacidade e proteção de dados em todos os níveis da empresa, isso permitirá que os riscos sejam mitigados e possíveis vazamentos sejam amenizados.

IV. Segurança da informação:

A Lei Geral de Proteção exige a implementação de medidas de segurança para proteger os dados pessoais contra vazamentos, acessos não autorizados e incidentes de segurança. No entanto, garantir a segurança dos dados é um desafio constante devido à evolução tecnológica e às ameaças cibernéticas.

V. Limitações financeiras e recursos tecnológicos:

Para implementar um programa de *compliance* eficiente, é necessário investir em tecnologias, treinamentos, contratação de especialistas e adaptação dos sistemas internos. No entanto, nem sempre as empresas possuem recursos financeiros suficientes para implementar todas as medidas necessárias.

A implementação de um programa de *compliance* em atendimento à LGPD apresenta desafios significativos para as organizações, desde a compreensão da lei até a mudança cultural e a garantia da segurança da informação. Além disso, as limitações financeiras e de recursos tecnológicos podem dificultar a implementação efetiva das medidas necessárias. No entanto, com planejamento adequado, investimento e conscientização, as empresas podem superar esses desafios e garantir o cumprimento da LGPD, protegendo os dados pessoais de seus clientes e expandindo a confiança em seus negócios.

A alta administração tem o dever de alocar recursos apropriados para a implementação e manutenção dos controles de segurança. Tal responsabilidade envolve investir em tecnologias e ferramentas que assegurem a devida proteção das informações. Essa colaboração é

fundamental para garantir que a equipe encarregada da segurança da informação tenha à disposição os recursos necessários para identificar e minimizar as vulnerabilidades e ameaças aos dados da organização.

VI. Due Diligence de dados:

A *due diligence* de dados é um processo fundamental para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD). Trata-se de uma investigação minuciosa realizada por uma organização antes de coletar, utilizar ou transferir dados pessoais, visando identificar possíveis riscos à privacidade e segurança dessas informações.

A LGPD estabelece diretrizes claras sobre a coleta, uso, armazenamento e compartilhamento de dados pessoais no Brasil. Para cumprir os requisitos da lei, as empresas devem adotar medidas de segurança adequadas e serem transparentes sobre como os dados são tratados.

Ao realizar uma due diligence de dados, é necessário considerar alguns aspectos essenciais:

a) Identificação dos dados: É importante ter uma visão abrangente dos tipos de dados pessoais que a organização lida. Isso inclui informações como nome, endereço, número de CPF, dados de saúde, dados bancários, orientação sexual, preferência política, entre diversas outras. Identificar e categorizar os dados ajudará a entender quais riscos estão associados a eles.

b) Finalidade da coleta[199]: É necessário identificar claramente por que a empresa está coletando os dados pessoais. Isso pode incluir a prestação de serviços, o cumprimento de obrigações contratuais, o marketing, entre outros. A finalidade da coleta deve ser legítima e estar em conformidade com a LGPD.

199 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (Lei nº 13.709/2018).

c) Consentimento: Considerado como um dos pilares legais da LGPD, a base legal do consentimento estabelece que a coleta, o processamento e a compartilhamento de informações pessoais só são viáveis mediante a obtenção do consentimento explícito do indivíduo titular dos dados ou de seu representante legal. Nesse sentido, a avaliação de *due diligence* deve examinar de que maneira a empresa obtém o consentimento, assegurando que seja de forma explícita e direcionada a propósitos específicos. É crucial garantir que o consentimento possa ser revogado a qualquer momento.

d) Medidas de segurança: A due diligence também deve avaliar as medidas de segurança implementadas pela organização para proteger os dados pessoais. Isso pode incluir a criptografia de dados, o acesso restrito às informações, o uso de firewalls e a implementação de políticas internas de segurança da informação.

VII. Políticas e procedimentos: É fundamental que a empresa tenha políticas e procedimentos claros relacionados à proteção de dados pessoais. A due diligence deve avaliar a existência e eficácia dessas políticas, bem como a capacidade da organização em implementá-las e monitorá-las adequadamente.

A due diligence de dados é um processo essencial para garantir a conformidade com a LGPD. Ao realizar essa investigação minuciosa, as organizações podem identificar e mitigar riscos relacionados à proteção de dados pessoais, garantindo o cumprimento à privacidade e segurança das informações dos titulares dos dados.

Apesar dos diversos desafios e limitações apresentados, os programas de *compliance* representam poderosas ferramentas para mitigar e eliminar os riscos de não atendimento à Lei Geral de Proteção de Dados (LGPD). A implementação de um programa de *compliance* efetivo implica estabelecer diversos controles preventivos, garantindo assim a privacidade e proteção dos dados pessoais. Além disso, tais programas visam educar e engajar os colaboradores em relação

às melhores práticas de proteção de dados, criando uma cultura de *compliance* dentro da empresa.

Dessa forma, ainda que existam desafios e limitações, os programas de *compliance* se mostram como estratégias fundamentais para o cumprimento da LGPD e para a construção de uma relação de confiança com os indivíduos cujos dados são tratados pela organização.

5. CONCLUSÃO

Neste sentido, não há razão para não assistir às novas tecnologias como meios de ressignificar e facilitar as atividades operacionais de uma organização, fazendo com que o uso consciente dos sistemas promova alta produtividade e qualidade de serviço.

Em contrapartida, uma vez que se utiliza destes recursos tecnológicos, é correto afirmar que a integração e conformidade com as leis deve prevalecer acima de qualquer ação. Isso envolve todas as partes interessadas de uma empresa, de forma direta e indireta, moldando a cultura para uma visão sistemática e holística, em que a informação passa a ser um dos maiores ativos da empresa, principalmente, quando o assunto envolve dados pessoais.

E por que mitigar e prevenir? O ciberespaço, conforme dito neste artigo, é um ambiente extraterritorial, onde as informações circulam o tempo todo. Isso significa que não há fórmula perfeita para o combate aos crimes cibernéticos, até porque a evolução tecnológica é um fato e diante de cada inovação um novo tipo de crime pode ser desenvolvido com objetivo claro de quebrar as barreiras de segurança causando danos graves aos envolvidos.

No entanto, com o uso de ferramentas de controle e a busca contínua de conformidade com a Lei Geral de Proteção de Dados por meio de programas de *compliance* propicia um relevante mecanismo de defesa contra estes ataques uma vez que os processos estão alinhados e parametrizados.

REFERÊNCIAS

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

Bussola. (11 de 02 de 2022). EXAME. Acesso em 25 de set. de 2023, disponível em www.exame.com: https://exame.com/bussola/ransomware-e-uma-forte-ameaca-para-asempresas-brasileiras-em-2022/

COCA VILA, Ivó. **¿Programas de cumplimiento como forma de autorregulación regulada?** In: SILVA SÁNCHEZ, Jesús-María (Ed.). *Criminalidad de empresa y compliance*: prevención y reacciones corporativas. Barcelona: Atelier, 2013

CRESPO, Marcelo Xavier de F. **Crimes digitais**. Editora Saraiva, 2011. E-book. ISBN 9788502136663

FIORILLO, Celso Antônio P.; CONTE, Christiany P. **Crimes no meio ambiente digital**. Editora Saraiva, 2016. E-book. ISBN 9788547204198.

KUHLEN, Lothar. **Cuestiones fundamentales de comlpliance y derecho penal**. Madrid: Marcial Pons, 2013, p. 51.

PINHEIRO, Patricia P. **Segurança Digital - Proteção de Dados nas Empresas**: Grupo GEN, 2020. *E-book.* ISBN 9788597026405.

PINHEIRO, Patrícia P. **Direito Digital**. Editora Saraiva, 2021. E-book. ISBN 9786555598438.

VERÍSSIMO, Carla. ***Compliance*: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.

PRIVACY OPS: COMO UMA FERRAMENTA DE GOVERNANÇA NO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Poliane Almeida Silva Dias
Rafael Marques Silva

Poliane Almeida Silva Dias[200]
Rafael Marques Silva[201]

RESUMO: O presente artigo fornece uma visão das práticas e estratégias necessárias para garantir a privacidade e a proteção de dados pessoais em um mundo onde as regulamentações estão em constante evolução. Ele destaca a importância da conformidade e do gerenciamento de riscos por intermédio de métricas e *reports*, além de oferecer orientações práticas para profissionais e organizações que desejam implementar programas de Privacidade com controles eficazes.

PALAVRAS-CHAVE: Privacidade - LGPD - Privacy Ops - Frameworks e Metodologias - Métricas do programa de privacidade

ABSTRACT: This article provides an insight into the practices and strategies necessary to ensure privacy and protection of personal data in a world where regulations are constantly evolving. It highlights the importance of compliance and risk management through metrics and reports, in addition to offering practical guidance for professionals and organizations that want to implement Privacy programs with effective controls.

200 Poliane Almeida Silva Dias: Advogada e bacharel em Direito pela PUC/MG, Palestrante e Analista Sênior em Privacidade/Proteção de Dados. Pós-graduada em Direito Civil pela PUC/MG e Pós-graduada em Direito Digital e Proteção de Dados pela Ebradi. Com certificações internacionais em Privacidade e Proteção de Dados (CIPM e CDPO/BR) pela IAPP - (International Association of Privacy Professionals). Presidente da Comissão de Proteção de Dados da OAB/MG Subseção de Betim, e Membro da Comissão de Proteção de Dados da OAB/MG.

201 Rafael Marque Silva: Rafael Marques Silva: Advogado e bacharel em Direito pela Universidade Paulista, cursando especialização em Data Science e Analytics na USP/ESALQ. Pós-graduado em Direito Empresarial pela FGV/RJ, com certificações internacionais (CIPM e CDPO/BR), IAPP - (International Association of Privacy Professionals). Atuante no ramo de Direito Empresarial, Direito Digital e Privacidade e Proteção de Dados Pessoais, especificamente no segmento de Tecnologia da Informação, Internet e Hospedagem. Membro da Comissão de Inteligência Artificial da OAB/SP Subseção de Santo Amaro, e Membro da Comissão de Proteção de Dados da OAB/SP.

KEYWORDS: Privacy - LGPD - Privacy Ops - Frameworks and Methodologies - Privacy program metrics

1. INTRODUÇÃO

Com a crescente preocupação mundial sobre o tema da privacidade e proteção de dados pessoais, com o surgimento, significativo, de novas leis de privacidade em vários países, e inúmeras etapas a serem vencidas para que uma empresa esteja adequada, muitos projetos foram colocados em prática, inclusive aqui no Brasil. Em conformidade com a *Lei Geral de Proteção de Dados (LGPD)*[202] nasce também a necessidade de definições estratégicas funcionais que auxiliarão os profissionais de privacidade na implementação de requisitos de privacidade em suas organizações.

À medida que as regras, definições de papéis e responsabilidades, bem como os níveis de maturidade e aderência à LGPD são compreendidos, a presença de pessoas comprometidas com os elementos de "Conhecimento, Habilidade e Atitudes" é fundamental para assegurar o funcionamento eficaz deste programa de privacidade.

A depender do tamanho, a localização, e setor empresarial que uma organização se encontra, a adoção estratégica de proteção de dados pessoais será diferenciada e segmentada por jurisdição que os seus titulares estejam. Assim, talvez, uma única metodologia "local" de privacidade não surta o efeito desejado.

Portanto, tornar a abordagem de privacidade "híbrida" para que atenda aos diversos mecanismos ao redor do mundo, potencialmente, seja o mais eficiente. Daí poderíamos nos questionar: Qual o melhor *framework* a ser utilizado pela minha organização? Bom, o *Privacy Ops* surge como medida proposta para auxílio na definição interna

202 LGPD –Lei 13.709/2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2023.

de privacidade da empresa, cujo fundamento é destacar os requisitos estabelecidos no *artigo 50 da LGPD*[203].

Em outras palavras, após todo o processo de adequação e durante a implementação das iniciativas de privacidade, torna-se necessário definir metodologias alcançáveis, estabelecer uma metodologia de trabalho e designar os responsáveis por indicar cada uma dessas evoluções. Isso ajuda a avaliar tanto os pontos fortes quanto as fraquezas apresentadas no projeto de governança da LGPD.

O presente trabalho procura contribuir, ainda que de modo breve, para a construção de alternativas e construção de hipóteses que levarão a organização ao aumento de capacidade de cumprir com uma infinidade de regulamentações de privacidade globais de modo eficaz e ágil.

Dessa forma, este artigo será dividido em três partes. A primeira parte abordará os conceitos e os primeiros passos para a implementação do *Privacy Ops*. O segundo tópico se concentrará na apresentação de metodologias aplicáveis ao *Privacy Ops*, baseadas em conceitos já conhecidos, mas estruturadas para as iniciativas de privacidade e proteção de dados pessoais. Por fim, na conclusão, será resumido o processo metodológico e será feita uma avaliação das perspectivas sobre o tema.

2. *PRIVACY OPS*: CONCEITO E IMPLEMENTAÇÃO

Privacy Ops (abreviação de *Privacy Operations*) nada mais é que um compilado de metodologias, filosofias, experiências práticas, colaboração multidisciplinar e automação em prol do aumento da capacidade que uma organização possua no cumprimento de uma infinidade de regulamentos de privacidade, de maneira rápida e eficiente.

203 LGPD –Lei 13.709/2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2023.

Se antes uma organização lidava com métodos tradicionais e manuais, com o *Privacy Ops* surge a possibilidade da utilização de ferramentas de automação, métricas e estrutura colaborativa multidisciplinar, que resultará em maior conformidade com a privacidade.

A implementação de um programa de *Privacy Operations* oportuniza a identificação de vulnerabilidades, diretamente, relacionadas às atividades de privacidade e proteção de dados no momento de sua ocorrência, em tempo real. Resultando, assim, a apuração de métricas que ajudam a identificar tendências e fluxos em casos concretos.

Um estudo realizado em 2019 pela organização IAPP em parceria com a TrustArc[204] constatou que muitas organizações - 79% - estão cumprindo duas ou mais leis de privacidade, enquanto apenas 16% se concentram em apenas uma. De fato, enquanto o maior segmento de entrevistados (43%) relata trabalhar ativamente para cumprir entre duas e cinco leis de privacidade, sólidos 13% estão trabalhando em seis a dez leis, outros 13% estão lutando com 11 a 49 leis, e 10 % relatam trabalhar ativamente para cumprir 50 ou mais leis de privacidade ao mesmo tempo.

Portanto, metodologias diferenciadas e abrangentes trazem aos programas de governança em privacidade maior aderência e resultados, fazendo com que os profissionais de privacidade consigam lidar com diversas legislações e requisitos de proteção de dados aos direitos dos titulares. Ademais, as organizações precisam ver a privacidade não apenas como "estar conformidade", mas, sim, como um impulsionador da eficiência dos negócios.

Uma das maneiras de garantir o sucesso dessa iniciativa são os chamados *KPIs2 (Key Performance Indicators)*[205], conforme cisão

204 MCGLADE, Rob. "Measuring privacy programs: The role of metrics." *International Association of Privacy Professionals*, 24 March 2022, Disponível em: https://iapp.org/news/a/measuring-privacy-programs-the-role-of-metrics/. Acesso em: 30 set. 2023.

205 TEBALDI, Pedro César. "KPI | O que é um KPI e como utilizar? Conceito e Significado do termo!" *OpServices*, 22 Dezembro 2016, Disponível em: https://www.opservices.com.br/kpi/. Acesso em: 30 set. 2023.

de Pedro César Tebaldi, que se traduzem como Indicadores-chave de Desempenho. Estes indicadores devem ser cuidadosamente monitorados e mensurados. Com base nesses indicadores, são delineadas todas as estratégias a serem seguidas para manter e aprimorar o programa de governança em privacidade e proteção de dados pessoais.

Ademais, a construção desse programa de governança não se limita apenas a isso. Além de garantir o conhecimento, habilidades e atitudes necessários para cumprir as demandas, é imperativo incluir uma matriz de responsabilidades, como a conhecida *"matriz RACI" sugerida pelo Ministério dos Transportes*[206], para assegurar a execução das demandas e o avanço do projeto, atribuindo responsabilidades específicas a cada área envolvida. Isso aumenta a maturidade da empresa e assegura sua competitividade em um mercado em constante mudança.

Diante das narrativas acima, destacamos alguns princípios fundamentais que a *Privacy Ops* possui para sua implementação, tais como automação, transparência, responsabilidade e multidisciplinariedade.

3. *FRAMEWORKS* E METODOLOGIAS APLICÁVEIS

Dentro do planejamento estratégico da empresa, é necessário definir metas com base nas quais um plano de ação pode ser indicado. Além disso, dentro de todos esses controles internos, o *artigo 50 da LGPD*[207] estabelece alguns elementos mínimos que podem ser considerados como componentes de governança, tais como:

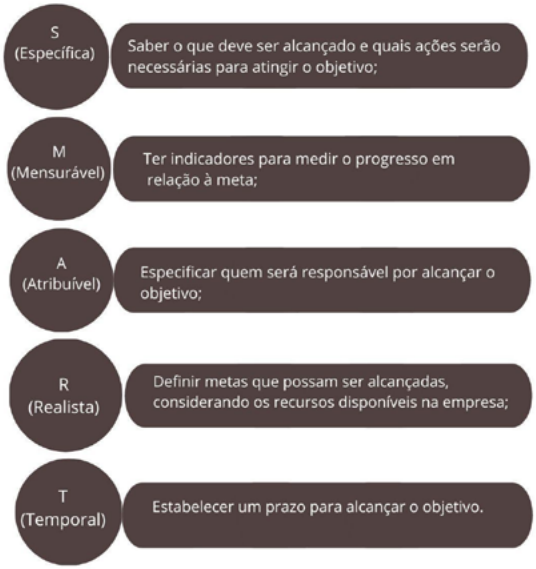
206 MINISTÉRIO DOS TRANSPORTES. "Como implementar a matriz RACI?" *Governo Federal*, 20 June 2018, Disponível em: https://www.gov.br/transportes/pt-br/assuntos/portal-da-estrategia/artigos-gestao-estrategica/como-implementar-a-matriz-raci. Acesso em: 30 set. 2023.

207 LGPD –Lei 13.709/2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2023.

> [...]" I - Implementar um programa de governança em privacidade que, no mínimo: a) Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento abrangente de normas e boas práticas relativas à proteção de dados pessoais; b) Seja aplicável a todos os dados pessoais sob seu controle, independentemente do modo como foram coletados; c) Seja adaptado à estrutura, escala e volume de suas operações, bem como à sensibilidade dos dados tratados; d) Estabeleça políticas e salvaguardas apropriadas com base em uma avaliação sistemática de impactos e riscos à privacidade; e) Tenha o objetivo de estabelecer uma relação de confiança com o titular dos dados, por meio de uma atuação transparente que assegure mecanismos de participação do titular; f) Esteja integrado à estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) Conte com planos de resposta a incidentes e remediação; e h) Seja constantemente atualizado com base em informações obtidas por meio de monitoramento contínuo e avaliações periódicas; II - Demonstrar a efetividade do programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei."

Antes de estabelecer qualquer mudança e ou metodologia, é fundamental compreender a importância e a aplicabilidade de todos os controles e gerenciamento aplicados ao *Privacy Ops*, que neste contexto se refere à garantia da governança dos elementos de privacidade dentro da empresa. Com base nessas diretrizes, é possível obter uma visão otimizada dos resultados esperados neste programa de governança de privacidade e proteção de dados. Entre os elementos buscados, é

fundamental considerar no *Privacy Ops*, o *acrónimo SMART*[208], como uma ferramenta para ajudar na formulação de objetivos mais eficazes. Dessa maneira, o *Privacy Ops* será entendido, conforme organograma abaixo:



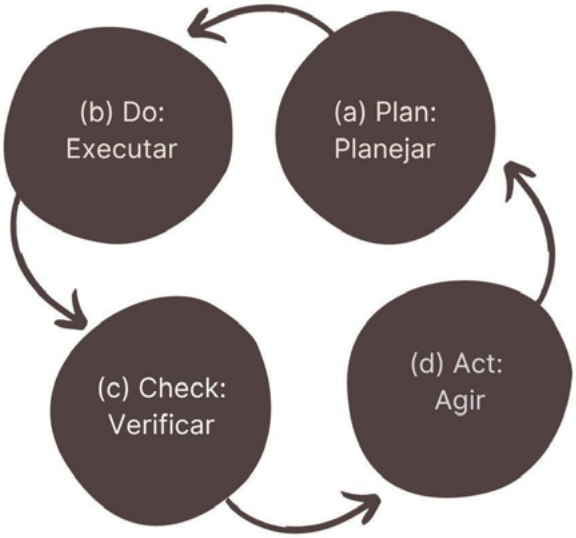
Fonte: desenho elaborado pela Autora Poliane Almeida

Já em condições de estrutura alguns modelos podem ser adequados para inspirar um Projeto de governança, consequentemente, poderá auxiliar na construção de métricas, baseadas em metodologias que demonstrará um habilitador baseado na estratégia da empresa, para facilitar a maneira de desenvolvimento do programa de governança em privacidade e proteção de dados pessoais, tais como: *Ciclo PDCA (Plan, Do, Check e Act)*[209]*: O PDCA*, cujo

208 SMART. Disponível em: https://www.researchgate.net/profile/Zdravko-Sergo-2/publication/317258825_SHADOW_ECONOMY_AND_TOURISM_RECEIPTS_EVIDENCE_FROM_EUROPE/links/592e91800f7e9beee73cf754/SHADOW-ECONOMY-AND-TOURISM-RECEIPTS-EVIDENCE-FROM-EUROPE.pdf#page=281. Acesso em: 30 set. 2023.

209 CARDOSO, Domingos Lopes e Cardoso, Thiago. Adequação da LGPD via "Projetos Ágeis Scrum". Disponível em: https://nppg.org.br/revistas/boletimdogerenciamento/article/view/731. Acesso em: 25 set. 2023.

nome vem do inglês, representa quatro etapas essenciais na gestão de um projeto, neste caso adotaremos para o programa de governança de Privacidade e proteção de dados pessoais da seguinte forma, conforme organograma abaixo:



Fonte: desenho elaborado pela Autora Poliane Almeida

Após a definição dessas métricas com base no plano de ação, torna-se necessário submetê-las a uma validação de resultados, de modo que os níveis estratégicos possam reportar de forma clara a evolução do projeto de governança de privacidade e proteção de dados pessoais em seus relatórios. Isso ocorre porque essas informações passam a ser relevantes para os relatórios da alta administração, podendo tais indicadores serem introduzidos em um ***"book de report"*** da empresa.

Ainda no contexto de metodologias, conforme observado por *Rob McGlade*[210], em um contexto sobre métricas de privacidade: "As métricas de privacidade podem ser usadas para indicar uma ampla variedade de pontos de dados. As métricas básicas de conformidade e operacionais medem as atividades realizadas por uma organização, como o número de transferências de titulares de dados e avaliações de impacto na proteção de dados, permitindo a rastreabilidade e, consequentemente a melhoria na eficiência dos processos organizacionais. com base nos tipos de dados que medem:

- **Direitos individuais**: essas métricas medem as taxas de consentimento para compartilhamento de dados e marketing por e-mail, proteção de titulares de dados e quantos clientes estão satisfeitos com o resultado, além do número de notificações de privacidade e de clientes impactados por eles. Esses dados são úteis para medir até que ponto o programa de privacidade protege os dados pessoais dos clientes e quanta confiança eles depositam no programa.
- **Treinamento e conscientização**: Este conjunto de análises compila o número de treinamentos sobre privacidade oferecido aos funcionários e o número de funcionários treinados, bem como o envolvimento dos funcionários com o programa de privacidade. Ao ter uma equipe mais envolvida com questões de privacidade, as empresas podem garantir o melhor cumprimento das leis, ao mesmo tempo que melhoram a sua imagem pública e criam excelência operacional em matéria de privacidade. Estas pesquisas também podem mostrar lacunas no conhecimento da privacidade organizacional que podem ser preenchidas por formações futuras.

210 MCGLADE, Rob. "Measuring privacy programs: The role of metrics." *International Association of Privacy Professionals*, 24 March 2022, Disponível em: https://iapp.org/news/a/measuring-privacy-programs-the-role-of-metrics/. Acesso em: 30 set. 2023.

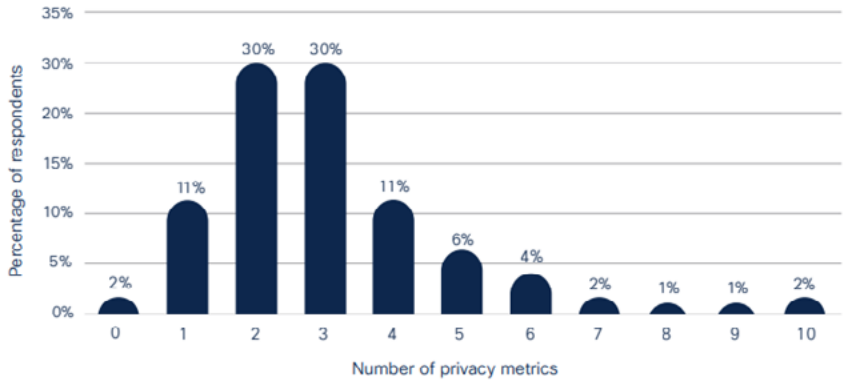
- **Comercial:** As análises comerciais medem o número de acordos de processamento de dados firmados com clientes, análises de fornecedores externos do programa de privacidade da organização e o número de atestados de conformidade de privacidade concluídos. Estas medições centram-se no envolvimento dos clientes e dos negócios e monitoram a capacidade de um programa de privacidade apoiando as prioridades dos negócios ao mesmo tempo que adotam novas tecnologias. Essas análises podem estimular novos investimentos por parte das partes interessadas, aumentando o valor do negócio.
- **Responsabilidade**: Ao realizar avaliações de privacidade, proteção de dados e impacto de transferência, acompanhando o número de projetos recebidos aconselhamento sobre privacidade e mantendo as políticas e procedimentos de privacidade atualizados, à medida que as organizações podem demonstrar sua capacidade de cumprimento das leis relevantes, aumentando ao mesmo tempo a vantagem competitiva e de consultoria da organização.
- **Administradores de privacidade:** essas métricas medem a extensão dos produtos de privacidade de uma organização. Isso inclui o número de sistemas de gerenciamento de informações pessoais, avaliações de impacto na privacidade de dados e perguntas frequentes sobre privacidade de dados criados. A administração da privacidade é responsável por transformar as políticas de dados em uma prática comum dentro de uma organização.
- **Política:** Uma organização pode monitorar de perto a sua conformidade com uma potencial legislação de privacidade enquanto trabalha para melhorar sua classificação Ambiental, Social e de Governança. Isso aumenta a confiança do público de que a organização tratará os dados de forma ética, ao mesmo tempo que aumenta a consciência de quaisquer possíveis alterações políticas.

Vale ressaltar que os critérios definidos com os objetivos são desenvolvidos em conjunto com as métricas. Os objetivos podem representar as condições conceituais buscadas com a melhor abordagem para a gestão estratégica do plano de ação. As métricas devem ser interpretadas por meio de indicadores quantitativos específicos para atingir o que chamamos de *Privacy Ops* por meio dos *KPI*.

As métricas de privacidade passam a ser uma das principais preocupações da alta administração. De acordo com *Cisco Data Privacy Benchmark Study*[211], 98% das empresas pontuaram uma ou mais métricas relacionadas à privacidade e proteção de dados pessoais. Isso evidencia a importância crítica dessas informações como fatores que não apenas promovem a confiança, mas também impulsionam a atração das empresas. Abaixo representamos este estudo e a quantidade de controles adotados:

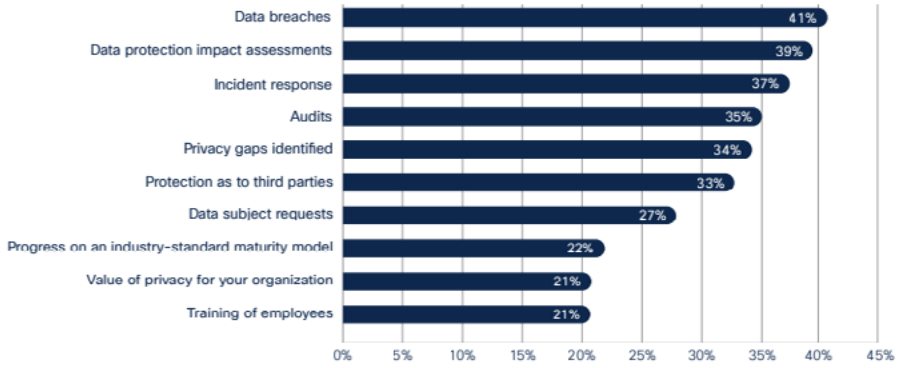
No contexto do estudo conduzido pela Cisco, é importante destacar que as observações mais frequentemente relacionadas incluem o acompanhamento do status de qualquer violação de dados (41%), a realização de avaliações de impacto de proteção de dados (39%) e a capacidade de resposta a incidentes (37%) ("Cisco 2023 *Data Privacy Benchmark Study*"). Essas informações são demonstrações de forma mais detalhadas na imagem abaixo:

Figure 8: Number of privacy metrics reported to the Board



Source: Cisco 2023 Data Privacy Benchmark Study

Figure 9: Privacy metrics reported to the Board



Source: Cisco 2023 Data Privacy Benchmark Study

Para fins práticos, aconselha-se que seja adotado, no cenário da organização, um método que permita alcançar métricas passíveis de serem reportadas e que indiquem os fatores relacionados à alocação de recursos, bem como a exposição ao risco caso essas métricas não sejam implementadas. Portanto, o principal aspecto a ser observado em relação ao risco ocorrerá no contexto de impacto versus probabilidade, ou seja, o impacto que a ausência dessas métricas representa em relação à probabilidade da ocorrência destas.

Essas métricas são capazes de auxiliar a empresa na identificação de vulnerabilidades e ameaças que podem ser mitigadas de diversas formas. Isso pode envolver a transferência de risco, como a contratação de seguro. Além disso, é importante considerar os riscos associados à imagem comercial da empresa em decorrência dessa ação.

Outra abordagem eficaz para mitigar esses riscos é por meio do acompanhamento do *Privacy Ops* e da adequação dos processos internos, conforme descrito no *artigo 46 da LGPD*[212]. Isso inclui a adoção de medidas de segurança técnicas e administrativas que protejam os

212 LGPD – Lei 13.709/2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2023.

dados pessoais contra qualquer forma de tratamento inadequado ou ilícito.

Por fim, ao abordar as iniciativas de *Privacy Ops*, é importante considerar uma estrutura amplamente utilizada por organizações. Alguns exemplos que podem ser incorporados nessa metodologia incluem:

1. Número de projetos já estabelecidos com base na Metodologia de *Privacy by Design*[213], incorporando práticas de privacidade desde a concepção de projetos que envolvem dados pessoais;

2. Taxa de conformidade com regulamentações, avaliando a porcentagem de conformidade com a LGPD e o número de regulamentações aplicáveis ao negócio;

3. Taxa de resposta a solicitações de titulares de dados;

4. Taxa de incidentes de privacidade resolvidos;

5. Taxa de treinamento e conscientização;

6. Nível de satisfação do cliente/usuário, avaliando a satisfação em relação à proteção de dados pessoais;

7. Número total de violações de dados relatadas em um período específico;

8. Tempo médio de resposta a incidentes de privacidade;

9. Taxa de adoção de políticas de privacidade;

10. Taxa de auditorias concluídas com êxito, representando a porcentagem de auditorias de privacidade bem-sucedidas, sem descobertas de não conformidade;

11. Taxa de uso eficaz de tecnologias de privacidade;

12. Taxa de documentação e registros completos;

13. Taxa de conformidade de terceiros;

14. Avaliação do retorno financeiro relacionado à implementação de práticas de privacidade e ao cumprimento das regulamentações;

15. Nível de adequação a LGPD dos parceiros, criando um score interno de adequação.

213 CAVOUKIAN, A., & Jonas, J. (2017). Privacy by Design in the Age of Big Data. Springer.
https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf

Essas métricas desempenham um papel fundamental na continuidade do programa de governança de privacidade e proteção de dados pessoais, fornecendo visibilidade e orientação para manter e melhorar as atividades implementadas e gerenciar eficazmente os riscos ao longo do monitoramento contínuo do projeto.

4. CONCLUSÃO

É preciso ter em mente que a governança no programa de programa de privacidade e proteção de dados pessoais não fluirá sem as ferramentas certas, ou seja, será necessário que o gestor de privacidade e/ou o Comitê de privacidade utilizem de automação, métricas e estrutura colaborativa multidisciplinar e uma infinidade de metodologias ágeis de trabalho.

A implementação de um programa de *Privacy Operations* abre espaço, internamente, para que a gerência identifique vulnerabilidades relacionadas às atividades de privacidade e proteção de dados. Assim, as medidas mitigadoras serão mais eficazes e rápidas, seja com a utilização de métricas (permitindo a rastreabilidade e, consequentemente a melhoria na eficiência dos processos organizacionais), metodologia SMART, KPIs2 (Key Performance Indicators), planilhas, Ciclo *PDCA (Plan, Do, Check e Act),* dentre inúmeras outras.

Dessa forma, o uso de ferramentas de *Privacy Ops* no programa de programa de privacidade e proteção de dados pessoais resultará na identificação de tendências e fluxos em casos concretos e tomada de decisão da melhor forma possível pelo gestor e/ou Comitê de Privacidade.

5. REFERÊNCIAS

CAVOUKIAN, A., & Jonas, J. (2017). Privacy by Design in the Age of Big Data. Springer. Disponível em: https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf. Acesso em: 20 ago. 2023.

CARDOSO, Domingos Lopes e Cardoso, Thiago. Adequação da LGPD via "Projetos Ágeis Scrum". Disponível em: https://nppg.org.br/revistas/boletimdogerenciamento/article/view/731. Acesso em: 25 set. 2023.

CISCO 2023 Data Privacy Benchmark Study." *Cisco*, 2023, Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf?CCID=cc000160&DTID=odicdc000016&OID=rptsc030828. Acesso em: 30 set. 2023.

LGPD –Lei 13.709/2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2023.

MCGLADE, Rob. "Measuring privacy programs: The role of metrics." *International Association of Privacy Professionals*, 24 March 2022, Disponível em: https://iapp.org/news/a/measuring-privacy-programs-the-role-of-metrics/. Acesso em: 30 set. 2023.

MINISTÉRIO dos Transportes. "Como implementar a matriz RACI?" *Governo Federal*, 20 June 2018, Disponível em: https://www.gov.br/transportes/pt-br/assuntos/portal-da-estrategia/artigos-gestao-estrategica/como-implementar-a-matriz-raci. Acesso em: 30 set. 2023.

SMART. Disponível em: https://www.researchgate.net/profile/Zdravko-Sergo-2/publication/317258825_SHADOW_ECONOMY_AND_TOURISM_RECEIPTS_EVIDENCE_FROM_EUROPE/

links/592e9SHADOW-ECONOMY-AND-TOURISM-RECEIPTS-EVIDENCE-FROM-EUROPE.pdf#page=281. Acesso em: 30 set. 2023.

TEBALDI, Pedro César. “KPI | O que é um KPI e como utilizar? Conceito e Significado do termo!” *OpServices,* 22 Dezembro 2016, Disponível em: https://www.opservices.com.br/kpi/. Acesso em: 30 set. 2023.

ANÁLISE DA FIGURA DO ENCARREGADO PELO TRATAMENTO DE DADOS (DPO)

ANALYSIS OF THE DATA PROTECTION OFFICER (DPO) ROLE

Claudio Nunes dos Santos Maulais.

Claudio Nunes dos Santos Maulais.[214]

RESUMO

Em cumprimento das disposições da Lei nº 13.709/2018 –Lei Geral de Proteção de Dados Pessoais ("LGPD"), toda organização precisa indicar um Encarregado pelo tratamento de dados pessoais, mitigando o risco para a não aplicação de conflito de interesse. Diante do contexto, indaga-se quais são as referências legais e melhores diretrizes jurídicas para a definição da pessoa a ser o Encarregado, conhecido também como *DPO*, ou seja, *Data Protection Officer*, autoridade dentro das empresas, responsável pelo tratamento de dados pessoais. Este artigo discute o papel do Encarregado de Proteção de Dados, de acordo com a Lei Geral de Proteção de Dados. Explora a relevância dessa figura na intermediação entre os controladores de dados, os titulares de informações pessoais e a Autoridade Nacional de Proteção de Dados (ANPD). A ênfase recai sobre a necessidade de independência e integridade do Encarregado, bem como a importância de seu conhecimento em áreas como a privacidade e governança. Destaca que o Encarregado não deve acumular funções que possam prejudicar sua autonomia e a importância da sua disponibilidade para cumprir suas obrigações e contribuir ativamente na formulação de políticas de proteção e privacidade de dados e governança, conforme a LGPD.

PALAVRAS-CHAVE: Proteção de dados. Encarregado. Tratamento de Dados. *Data Protection Officer.*

ABSTRACT

In compliance with the provisions of Law No. 13.709/2018 – General Personal Data Protection Law (LGPD), every organization must appoint a person responsible for the processing of personal data, mitigating the risk of non-application of conflict of interests.

214 Claudio Nunes dos Santos Maulais. Universidade FUMEC. Mestre em Sistemas de Informação e Gestão do Conhecimento. Segurança da Informação e Gestão do Conhecimento; Inteligência Artificial; Proteção de Dados

Given the context, we asked what are the legal references and the best legal guidelines to define the person as responsible, also known as DPO, that is, Data Protection Officer, authority within companies, responsible for the processing of personal data. This article discusses the role of the Data Protection Officer, in accordance with the General Data Protection Law. It explores the relevance of this figure in the intermediation between data controllers, holders of personal information and the National Data Protection Authority (ANPD). The emphasis is on the need for the Guardian's independence and integrity, as well as the importance of their knowledge in areas such as privacy and governance. It highlights that the person responsible should not accumulate functions that could harm their autonomy and the importance of their availability to fulfill their obligations and actively contribute to the formulation of data protection, privacy and governance policies, in accordance with the LGPD.

KEYWORDS: *Data protection. DPO. Data processing. Data Protection Officer.*

1. INTRODUÇÃO

A temática proteção e privacidade de dados pessoais não é primário no mundo e no Brasil, uma vez que em países da União Europeia iniciou-se em 2012 o projeto para proteção e privacidade de dados pessoais, sendo aprovado em 2016, criando assim o Regulamento Geral sobre a Proteção de Dados (GDPR).

A lei europeia para tratamento de dados tem grande impacto para LGDP, como fonte inspiradora para a formulação da Lei 13.709, entretanto uma das obrigações comuns entre as duas leis é a denominação de um profissional responsável pelo tratamento de dados pessoais, denominado pela GDPR como DPO, e, na LGPD, como Oficial de Proteção de Dados Pessoais, cargo regulamentado no Brasil

pelo Ministério do Trabalho, sob o CBO[215] –1421-35, não regulamentado ainda sob a ótica de conflito de interesse, o qual será tratado também neste artigo.

2. O ENCARREGADO PELO TRATAMENTO DE DADOS NA LGPD.

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 41, trata da obrigatoriedade de indicação do Encarregado por todos os controladores de dados pessoais, salvo aqueles expressamente dispensados, como é o caso das microempresas e empresas de pequeno porte empresarial.

O Encarregado pelo tratamento de dados pessoais passou por uma atualização, conforme o Decreto nº 10.474/2020, que versa sobre a definição e as atribuições. Esse documento inclui as hipóteses de dispensa da necessidade da indicação Encarregado, de acordo com a natureza e o porte da organização, bem como o volume de dados tratados.

Para melhor compreensão da figura do Encarregado, que necessariamente deve ser designado, tem-se, pelo artigo 5º, inciso VIII, da mesma lei, que o Encarregado será a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Além de centralizar a comunicação entre o controlador e operador, os titulares dos dados e a ANPD, são atividades do Encarregado, conforme estabelece o citado art. 41, parágrafo 2º, da LGPD:

> § 2º As atividades do encarregado consistem em: (...) III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em

215 Código brasileiro de ocupação acessado em 29/10/2023 https://empregabrasil.mte.gov.br/76/cbo/

> relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Embora a ANPD tenha competência normativa para melhor regulamentar o cargo de Encarregado, até a presente data não houve materialização de nenhuma resolução nesse sentido. Na ausência de normatização específica, tem-se que os requisitos acerca do Encarregado devem ser extraídos das previsões da LGPD e eventual *benchmarking*[216].

Contudo, para a interpretação da LGPD quanto ao Encarregado, é necessário buscar a norma por detrás do simples texto da lei, a fim de extrair o comando pretendido pelo legislador. Logo, é preciso ter uma visão sistêmica da LGPD, em compasso com as demais legislações pátrias.

Com isso, para mitigar riscos, é preciso ir além da objetividade do texto legal, para buscar uma interpretação jurídica que melhor aproxime a pretensão do legislador, conforme o Guia Orientador da ANPD, sobre a figura do Encarregado. Para tanto, existe a importante referência do chamado *Data Protection Officer* – DPO ("DPO"), previsto no *General Data Protection Regulation* ("GDPR").

O GDPR é o regulamento europeu aplicado aos países da União Europeia, proveniente de um esforço internacional do respectivo bloco para se trazer harmonia em matéria de proteção de dados aos países signatários. Assim, a principal preocupação foi possuir um denominador comum mínimo em proteção de dados, com requisitos legais essenciais a todos os países abrangidos pelo GDPR.

A LGPD, embora possua suas particularidades e distinções do GDPR, possui forte inspiração, daí porque o presente comparativo é relevante de ser feito. Importante frisar que o GDPR está em vigor desde 24 de maio de 2016, ou seja, há mais sete anos, o que demonstra

216 Acessado em 29/10/2023 https://pt.wikipedia.org/wiki/Benchmarking

como a cultura jurídica estrangeira está muito mais familiarizada com a temática do que a brasileira.

Em um breve resgate histórico, a figura do DPO existe desde a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24/10/1995 (há mais de 25 anos, portanto). Sem nos aprofundarmos na evolução do DPO ao longo dos anos, tem-se que, atualmente, é o responsável por verificar a conformidade do GDPR e das legislações especiais dos Estados-Membros com as políticas de proteção de dados do controlador ou do operador, conforme artigo 37 do guia geral da GDPR[217].

Nessa tarefa, é dever do DPO a repartição de responsabilidades, a sensibilização e formação das pessoas que tratarão dos dados pessoais e das auditorias correspondentes[218].

Com isso, na sua escolha devem ser levados em consideração a sua experiência, conhecimento, credenciais e habilidade para desempenhar sua função, mas, acima de tudo, a integridade e elevado nível de ética profissional diante da sua posição de imparcialidade opinativa e conscientizador de princípios no tratamento de dados pessoais que envolvem direitos e garantias fundamentais, como privacidade, intimidade, direitos da personalidade, entre outros.[219]

Apesar da ausência de regulamentação mais detalhada do Encarregado, é relevante destacar que o Governo Federal, ao editar a Medida Provisória nº 869/2020, pretendeu incluir na Lei Geral de Proteção de Dados, na seção relativa ao Encarregado, requisitos quanto à sua qualificação e autonomia profissional:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. (...) § 4º Com

217 Acessado em 29/10/2023 https://gdpr-info.eu/art-37-gdpr/

218 BLUM, Renato Ópice, VAINZOF, Rony, MORAES, Henrique Fabretti (coord.). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 27.

219 BLUM, Renato Ópice, VAINZOF, Rony, MORAES, Henrique Fabretti (coord.). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 33.

> relação ao encarregado, o qual deverá ser detentor de conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados, além do disposto neste artigo, a autoridade regulamentará: I - os casos em que o operador deverá indicar encarregado; II - a indicação de um único encarregado, desde que facilitado o seu acesso, por empresas ou entidades de um mesmo grupo econômico; III - a garantia da autonomia técnica e profissional no exercício do cargo.

O parágrafo 4º foi, ao final, vetado, não tendo sido incluído no art. 41 da LGPD. Pelas razões do veto, A propositura legislativa, ao dispor que o encarregado seja detentor de conhecimento jurídico regulatório, contraria o interesse público, na medida em que se constitui em uma exigência com rigor excessivo que se reflete na interferência desnecessária por parte do Estado na discricionariedade para a seleção dos quadros do setor produtivo.

Por meio da Instrução Normativa DEGDI nº 100/2020[220], a Secretaria de Governo Digital do Ministério da Economia estabeleceu que os Encarregados indicados pelos Sistema Integrado de Segurança Pública (SISP) detenham, no mínimo, conhecimentos multidisciplinares essenciais a sua atribuição, incluindo as áreas de gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção da privacidade e governança de dados, entre outros (art. 1º, parágrafo 1º, inciso II).

Em resumo, portanto, quis o legislador exigir a qualificação mínima do Encarregado, o que foi ao final vetado. Para tanto, porém, não houve qualquer ressalva à independência e autonomia técnica e profissional do cargo. Por sua vez, na nomeação de seus Encarregados, a Administração Pública determinou a necessidade de conhecimentos multidisciplinares para suas atribuições.

220 Acessado em 27/10/2023 https://www.in.gov.br/en/web/dou/-/instrucao-normativa-degdi-n-100-de-19-de-outubro-de-2020-284432280

Feitas essas considerações e resgatando as premissas iniciais deste tópico, tem-se que a LGPD fixou expressamente como funções do Encarregado, além de aceitar reclamações de titulares e comunicar-se com a ANPD, a atividade de orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (art. 41).

Todavia, para se entender a extensão da referida função, é preciso recorrer aos critérios de interpretação legal mencionados anteriormente. O art. 50 da LGPD estabelece genericamente que os controladores e operadores poderão formular:

> "a) 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.
> b) Normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento.
> c) Ações educativas.
> d) Mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

Ainda, dispõe a lei que o controlador deverá implementar programa de governança em privacidade que, no mínimo, (i) demonstre seu comprometimento em cumprir normas e boas práticas em proteção de dados, (ii) seja aplicável a todo conjunto de dados sob seu controle, (iii) seja adaptado à estrutura, escale e volume de suas operações, e (iv) seja atualizado constantemente com informações obtidas a partir de monitoramento contínuo e avaliações periódicas, dentre outros (art. 50, parágrafo 2º). Deverá ser demonstrada também a efetividade do programa de governança em privacidade.

Tais previsões legais são, naturalmente, direcionadas ao próprio agente de tratamento de dados (sobretudo ao controlador). Contudo, entendemos ser praticamente impossível dissociar a idealização,

aprovação, execução e melhoria contínua de todas essas políticas, programas e regras de governança da informação, sem a participação ativa do Encarregado.

De fato, não é responsabilidade deste (Encarregado), pela lei, editar tais procedimentos de boas práticas e adequação à LGPD, mas é impossível pensar na implantação genuína de governança da informação nas atividades empresariais e governamentais sem a contribuição do Encarregado.

É importante se fazer essa ressalva porque a LGPD, em uma rápida leitura, leva a crer que o Encarregado seria apenas um "representante comunicativo" dos agentes de tratamento (sobretudo o controlador), pois centralizaria o contato entre os titulares e a ANPD.

Entretanto, ao estabelecer ser atividade do Encarregado a "orientação dos funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados", a LGPD compartilhou diretamente com este a responsabilidade pelas boas práticas e governança ao Encarregado.

Essas (boas práticas e governança) estão listadas nos princípios norteadores do tratamento de dados, previstos no art. 6º da LGPD, dos quais destaco os princípios da segurança e prevenção:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> (...)
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Por essas razões, não há como se conceber um papel meramente reativo do Encarregado. Mais do que "repassar" informações

ou simplesmente promover treinamentos e outras medidas de aculturamento, a LGPD pretende do Encarregado um comportamento de liderança na construção de tais procedimentos e manuais de boas práticas e governança.

Seja na conscientização dos indivíduos que dentro da operação tratam dados sob sua responsabilidade, mas também no acompanhamento contínuo da conformidade da tecnologia da informação (adesão aos programas já editados) e em possíveis revisões e aperfeiçoamentos (gestão do comportamento humano).[221]

Neste contexto, para que o Encarregado possa exercitar todas essas incumbências, é preciso que detenha certo nível de conhecimento (i) jurídico em privacidade e proteção de dados, (ii) de gestão de programas de governança corporativa, (iii) de segurança e sistemas de informação, (iv) da operação de tratamento de dados na atividade empresarial, e, por fim, (v) detenha independência ou ausência de conflito de interesses.

No mesmo sentido, e mais uma vez recorrendo às disposições europeias em matéria de proteção de dados, tem-se que o *Data Protection Working Party*, responsável por editar diretrizes no assunto em questão, consolidou o *Article 29 (Guidelines on Data Protection Officers),* em 13/12/2016[222], no qual reconhece a possibilidade de o DPO possuir outras funções na organização, desde que não resultem em conflito de interesses, para garantir sua atuação independente. Dessa forma, o DPO não deve determinar os meios e propósitos de tratamento de dados em qualquer processo, por exemplo[223].

221 BLUM, Renato Ópice, VAINZOF, Rony, MORAES, Henrique Fabretti (coord.). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 52.

222 Disponível em: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44100>, acesso em 05/11/2020.

223 Trecho do Article 29 no original: 3.5. Conflict of interests Article 38(6) allows DPOs to 'fulfil other tasks and duties'. It requires, however, that the organization ensure that 'any such tasks and duties do not result in a conflict of interests'. The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organization

A preocupação com a independência de atividades (e ausência de conflito de interesses) não é apenas uma formalidade.

Ao se considerar que o controlador tem a obrigação de comunicar à ANPD a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48 da LGPD) e que a comunicação entre controlador e ANPD é centralizada no Encarregado, estar-se-ia diante do risco de autoincriminação deste, acaso o incidente tenha ocorrido em alguma área ou processo interno da qual o Encarregado participava, a título de atividades cumuladas com sua função de Encarregado.

Nesse tocante, é preciso ressaltar que o art. 5º, inciso LXIII, da CF/1988, garante o direito à não autoincriminação. Assim, como se poderia exigir do Encarregado uma comunicação transparente e clara com a ANPD, mas que poderia resultar na produção de provas contra si mesmo pelo exercício de outras atribuições? Há evidente conflito de interesse nesta situação hipotética.

Por essas razões, entende-se que a medida de segurança jurídica e mitigação de riscos a adoção de uma interpretação abrangente sobre as limitações do cargo de Encarregado (ainda que no silêncio da literalidade da LGPD), para evitar a cumulação de funções e cargos. Agregar ao Encarregado outras atividades poderá sujeitar ao Controlador/Operador, futuramente, ao conflito de interesses ou comprometimento da autonomia e independência de seu Encarregado, gerando um possível passivo para ambos, controlador e Encarregado.

3. DA INDICAÇÃO DE UM CARGO DE CONFIANÇA COMO ENCARREGADO

Vencidas as considerações jurídicas iniciais sobre o Encarregado, cumpre analisar a regência interna do Direito, para compreender suas funções e o seu papel na rotina do Controlador/Operador. A partir dos

that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organizational structure in each organization, this has to be considered case by case. (Grifamos).

estudos apresentados, conduz-se ao final considerações sobre sua conformidade à LGPD no que diz respeito ao conflito de interesses.

Ato contínuo, resgatando-se o quanto tratado no tópico anterior, sobre as funções esperadas do Encarregado e o *benchmarking* europeu do *Data Protection Working Party, Article 29 (Guidelines on Data Protection Officers)*, tem-se que há possibilidade do DPO possuir outras funções na organização quando não resultarem em conflito de interesses, a fim de garantir sua independência e autonomia técnica e profissional (termos estes adotadas pela Medida Provisória nº 869/2019, posteriormente objeto de veto pela Presidência da República).

Entre as funções que poderiam gerar a incompatibilidade de atuação e conflito de interesses, estão aquelas em que o DPO participe, de qualquer modo, nos meios e propósitos de tratamento de dados em qualquer processo. Com base no exposto anteriormente, o gerenciamento de riscos estaria ligado ao tratamento de dados e, por consequência, comprometeria a independência da função de Encarregado.

Diversos aspectos podem influenciar tal decisão, desde desavenças pessoais à mudança de composição do Conselho de Administração, além da perda de confiança ou mesmo desinteresse do próprio mandatário em sua recondução.

Por decerto que se deve estabelecer um programa que permita a preservação dos trabalhos e que combata a perda de informação. Mas é também inevitável pensar na ruptura de visões entre os diferentes cargos de confiança que vierem a ocupar o cargo de Oficial de tratamento de dados pessoais, o que poderá alterar o direcionamento, o foco e as prioridades das políticas de proteção de dados.

Além disso, é importante que o Encarregado esteja amparado por estrutura suficiente para atender às demandas dos titulares, conforme o tamanho do controlador e o segmento de atividade. Assim, seria necessário que o profissional indicado fosse dotado de equipe razoável para exercício de suas funções, o que poderia acarretar algum impasse quanto à verba orçamentária prevista para o núcleo de governança e proteção de dados pessoais.

É improvável cogitar que um Encarregado consiga gerenciar suas atribuições em um momento crucial e sensível de implantação da governança de dados, ao mesmo tempo em que exerce outras funções (as quais ainda podem lhe comprometer a independência de interesses). É preciso, senão, disponibilidade para a função.[224]

Afinal, não obstante a responsabilidade jurídica sobre o cumprimento das obrigações previstas na LGPD recair sobre o controlador e/ou o operador dos dados, o DPO é o pilar da governança em privacidade e proteção de dados nas organizações que buscam a jornada permanente de conformidade.[225] Portanto, é preciso que o Encarregado aprecie todos os elementos e planos de ação qualitativamente para identificar pontos de melhoria na governança, a fim de manter um processo "permanente de conformidade".

4. CONCLUSÃO

Em conclusão, fica evidente que a figura do Oficial pelo Tratamento de Dados Pessoais desempenha um papel crucial na aplicação eficaz da Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro. Sua função de atuar como um intermediário entre as organizações, os titulares de dados e a Autoridade Nacional de Proteção de Dados (APND) é de suma importância para garantir o cumprimento das diretrizes da LGPD. A independência e a capacidade

224 Como enfrentam Pedro Nachbar Sanches e Tiago F. Campanholi dos Santos: (...) mesmo que não se considere a disponibilidade como uma habilidade, certamente é um fator que deverá ser observado quando da procura de um profissional para o cargo de Encarregado, ainda mais se considerarmos o cenário atual onde se coloca tanto peso e importância nesta função, esperando que este profissional, assim que nomeado, "arrumará toda a casa". Assim, em especial até dois anos após a entrada em vigor da LGPD, é de se esperar que o profissional designado ou companhias que sejam nomeadas como encarregado tenham um árduo trabalho pela frente, exigindo tempo disponível para conseguir lidar com todas as questões que se apresentarem no decorrer da jornada. In BLUM, Renato Ópice, VAINZOF, Rony, MORAES, Henrique Fabretti (coord.). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 447.

225 BLUM, Renato Ópice, VAINZOF, Rony, MORAES, Henrique Fabretti (coord.). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 54

de contribuir ativamente na formulação de políticas são atributos essenciais para um encarregado bem-sucedido. No entanto, é fundamental que as organizações compreendam a relevância dessa função e a designem adequadamente, evitando conflitos de interesse que possam comprometer a eficácia da proteção de dados pessoais. A LGPD representa um marco significativo na garantia da proteção e privacidade de dados no Brasil, e o Encarregado desempenha um papel fundamental nesse processo, auxiliando as empresas a navegar com sucesso nesse novo paradigma de proteção e privacidade de dados. Portanto, a nomeação e o compromisso com os Encarregados qualificados e independentes são passos essenciais para garantir a conformidade contínua com a LGPD e para promover a confiança dos titulares de dados pessoais.

REFERÊNCIAS

ALCASSA, F. DPO: Atividade inscrita no CBO, pelo Ministério do Trabalho. Migalhas. 2022. Disponível em: https://www.migalhas.com.br/depeso/362444/dpo-atividade-inscrita-no-cbo-pelo-ministerio-do-trabalho. Acesso em: 31 out. 2023.

ALECRIM, E. O que é GDPR e que diferença isso faz para quem é brasileiro. Tecnoblog. 2018. Disponível em: https://tecnoblog.net/responde/gdpr-privacidade-protecao-dados. Acesso em: 31 out. 2023.

BENCHMARKING. In: Wikipedia, a enciclopédia livre. Flórida: Wikimedia Fundation, ano. Disponível em: https://pt.wikipedia.org/wiki/Benchmarking. Acesso em: 30 out. 2023.

BLUM, R. O.; LÓPEZ, N. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 171-177, Janeiro-Março/2020. Disponível em: https://observatoriolgpd.com/wp-content/uploads/2020/05/ii_7_cadernos_juridicos_epm.pdf. Acesso em: 30 out. 2023.

BLUM, R. O.; VAINZOF, R.; MORAES, H. F. (coord.). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 54.

BLUM, R. O. DPO (ENCARREGADO) E-BOOK AGOSTO 2021 Gestão dos programas de privacidade e proteção de dados. Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/EBOOK-DPO-ENCARREGADO-3.pdf. Acesso em: 30 out. 2023.

BRASIL. ANPD. Autoridade Nacional de Proteção de Dados. [S.l.]. Ministério da Justiça e Segurança Pública, 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 30 out. 2023.

BRASIL. ANPD. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado VERSÃO 2.0 ABR. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 30 out. 2023.

BRASIL. Decreto nº 10.474 de 26 de agosto de 2020 Diário Oficial [da] República Federativa do Brasil. Brasília, DF. Publicado em: 27/08/2020, nº 165, p. 6. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=10474&ano=2020&ato=433gXSU1UMZpWTbae . Acesso em: 30 out. 2023.

BRASIL. Instrução Normativa Degdi nº 100, de 19 de outubro de 2020. Diário Oficial [da] República Federativa do Brasil. Brasília, DF. Publicado em: 22/10/2020, Edição: 203, Seção 1, p. 80. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-degdi-n-100-de-19-de-outubro-de-2020-284432280. Acesso em: 30 out. 2023.

BRASIL. LGPD. Lei Geral de Proteção de Dados - Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/ lei/l13709.htm> Acesso em: 24 out. 2023.

BRASIL. Ministério Do Trabalho - Emprega Brasil - Classificação Brasileira de Ocupações (CBO). Disponível em: https://empregabrasil.mte.gov.br/76/cbo. Acesso em: 31 out. 2023.

CBO. CBO 142135 - Oficial de proteção de dados pessoais (DPO). Disponível em: https://codigocbo.com.br/cbo-142135-oficial-de-protecao-de-dados-pessoais-dpo. Acesso em: 31 out. 2023.

INTERNET CONSULTING. General Data Protection Regulation (GDPR). Art. 37 Gdpr - Designation Of The Data Protection Officer. Disponível em: https://gdpr-info.eu/art-37-gdpr. Acesso em: 31 out. 2023.

PROTEÇÃO DE DADOS E PRIVACIDADE: O PAPEL VITAL DA LGPD NO CENÁRIO BRASILEIRO

DATA PROTECTION AND PRIVACY: THE VITAL ROLE OF LGPD IN THE BRAZILIAN SCENARIO

Cristiane Duarte Ramalho

Cristiane Duarte Ramalho [226]

RESUMO

A Lei Geral de Proteção de Dados (LGPD) representa uma legislação transformadora que estabelece diretrizes sólidas para o tratamento de dados pessoais. Ela vai além da simples regulamentação do universo digital; a LGPD encarna um compromisso em proteger a privacidade e minimizar os riscos relacionados à exposição indevida de informações pessoais. Este artigo explora a importância da LGPD no cenário brasileiro, destacando seu papel essencial na promoção de políticas públicas e práticas organizacionais voltadas para o uso ético e responsável dos dados dos cidadãos. Ao explorar os princípios fundamentais da LGPD e as responsabilidades dos controladores, operadores, agentes de tratamento e processadores de dados, torna-se evidente que essa legislação vai além do mero cumprimento regulatório. Ela impacta cada cidadão e cada organização que lida com dados pessoais, estabelecendo uma cultura de respeito à privacidade e proteção dos direitos individuais. Este artigo examina de perto esses princípios e discute a necessidade de regulamentações eficazes, fiscalização rigorosa e punições adequadas para infrações. Além disso, consideramos a necessidade da criação de um Conselho de Classe da LGPD como um passo crucial para a supervisão e orientação efetiva do tratamento de dados pessoais. A LGPD representa mais do que apenas um marco regulatório; é um lembrete de que, em um mundo digital em constante evolução, a proteção da privacidade e a segurança dos dados pessoais são imperativas. Por meio de políticas públicas sólidas e práticas organizacionais responsáveis, a LGPD está moldando um futuro digital mais seguro e confiável para todos os cidadãos brasileiros.

Palavras Chaves: LGPD, operadores, dados pessoais.

226 Doutorando em Ciência Jurídicas pela UMSA, Mestre em Políticas Públicas pela FLACSO, Pós Graduada em Gestão Pública UEMG, Bacharel em Direito Faminas BH

ABSTRACT

The General Data Protection Law (LGPD) represents transformative legislation that establishes solid guidelines for the processing of personal data. It goes beyond the simple regulation of the digital universe; LGPD embodies a commitment to protecting privacy and minimizing risks related to the undue exposure of personal information. This article explores the importance of LGPD in the Brazilian scenario, highlighting its essential role in promoting public policies and organizational practices aimed at the ethical and responsible use of citizens' data. When exploring the fundamental principles of the LGPD and the responsibilities of controllers, operators, processing agents and data processors, it becomes clear that this legislation goes beyond mere regulatory compliance. It impacts every citizen and every organization that handles personal data, establishing a culture of respect for privacy and protection of individual rights. This article takes a close look at these principles and discusses the need for effective regulations, strict enforcement, and appropriate punishments for infractions. Furthermore, we consider the need to create an LGPD Class Council as a crucial step for the effective supervision and guidance of the processing of personal data. The LGPD represents more than just a regulatory framework; it is a reminder that in an ever-evolving digital world, protecting privacy and securing personal data is imperative. Through solid public policies and responsible organizational practices, the LGPD is shaping a safer and more reliable digital future for all Brazilian citizens.

Keywords: LGPD, data processor, personal data.

INTRODUÇÃO

A revolução digital transformou fundamentalmente a maneira como coletamos, compartilhamos e, acima de tudo, protegemos nossas informações pessoais. À medida que a tecnologia avança rapidamente, surgem preocupações crescentes sobre a privacidade e

a segurança dessas informações sensíveis. Nesse cenário, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, emerge como um farol de proteção dos direitos dos cidadãos brasileiros em relação às suas informações pessoais. Este artigo mergulha profundamente na LGPD e destaca seu papel vital em moldar políticas públicas e práticas organizacionais que visam ao tratamento ético e responsável dos dados dos cidadãos.

No primeiro tópico, que trata sobre o consentimento e Responsabilidade dos Operadores e Processadores de Dados sob a LGPD, exploraremos como o consentimento se interliga com a responsabilidade dos operadores e processadores de dados no tratamento ético e transparente das informações pessoais, enfatizando a necessidade de conformidade e práticas éticas.

No segundo tópico, que trata sobre a Necessidade de Regulamentação de Políticas Públicas de Fiscalização e Punibilidade Solidária, abordaremos a importância das políticas públicas para garantir uma fiscalização rigorosa e punições efetivas em caso de infrações, assegurando que a legislação seja aplicada de maneira justa e responsável.

No terceiro tópico, que trata sobre estabelecimento de Critérios para um Conselho de Classe da LGPD, examinaremos a proposta de criação de um Conselho de Classe composto por especialistas em proteção de dados, juristas e representantes da sociedade civil, destacando seu papel crucial na supervisão e orientação do tratamento de dados pessoais de maneira preventiva.

No quarto tópico, que trata sobre a necessidade do DPO nas Empresas, será abordada a importância da função do Encarregado de Proteção de Dados (DPO) nas empresas, sua responsabilidade no processamento e descarte de dados, a necessidade de formação atrelada ao direito e como o treinamento e conscientização contribuem para a eficácia dessa função.

No quinto tópico, que trata das responsabilidades dos Controladores, Operadores e Agentes de Tratamento de Dados, exploraremos as responsabilidades específicas dos controladores,

operadores e agentes de tratamento de dados sob a LGPD, destacando a importância de garantir o tratamento adequado dos dados e a conformidade com a legislação.

No sexto tópico, que aborda que a LGPD não é apenas um marco regulatório, há um lembrete constante de que, em um mundo digital em constante evolução, a proteção da privacidade e a segurança dos dados pessoais se tornaram imperativas. Por meio de políticas públicas sólidas e práticas organizacionais responsáveis, a LGPD está contribuindo para a construção de um futuro digital mais seguro e confiável para todos os cidadãos brasileiros.

MARCO LEGAL

A era digital trouxe consigo uma revolução em como nossas informações pessoais são coletadas, utilizadas e protegidas. À medida que os avanços tecnológicos aceleram a capacidade de acessar e compartilhar dados, surge uma preocupação cada vez maior sobre a privacidade e a segurança dessas informações sensíveis. No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, emerge como um farol na salvaguarda dos direitos dos cidadãos em relação às suas informações pessoais.

Promulgada em agosto de 2018 e em vigor desde setembro do ano de 2020, a LGPD representa uma legislação transformadora que estabelece diretrizes sólidas para o tratamento de dados pessoais. Vai muito além de simplesmente regular o universo digital, a LGPD encarna o compromisso de proteger a privacidade e minimizar os riscos associados à exposição indevida de informações pessoais. Este artigo mergulha profundamente no cenário da LGPD e destaca seu papel essencial na promoção de políticas públicas e práticas organizacionais voltadas para o uso ético e responsável dos dados dos cidadãos.

À medida que exploramos os princípios fundamentais da LGPD, bem como as responsabilidades dos controladores, operadores, agentes de tratamento e processadores de dados, fica claro que essa

legislação transcende o mero cumprimento regulatório. Ela ressoa em cada cidadão e em cada organização que lida com dados pessoais, estabelecendo uma cultura de respeito à privacidade e proteção dos direitos individuais.

Neste artigo, examinaremos de perto esses princípios, juntamente com a necessidade de regulamentações eficazes, fiscalização rigorosa e punições adequadas para infrações. Além disso, considera-se a criação de um Conselho de Classe da LGPD como um passo crucial para a supervisão e orientação efetiva do tratamento de dados pessoais.

A LGPD é mais do que apenas um marco regulatório; é um lembrete de que, no mundo digital em constante evolução, a proteção da privacidade e a segurança dos dados pessoais são imperativas. Por meio de políticas públicas sólidas e práticas organizacionais responsáveis, a LGPD está moldando um futuro digital mais seguro e confiável para todos os cidadãos brasileiros.

CONSENTIMENTO E RESPONSABILIDADE DOS OPERADORES E PROCESSADORES DE DADOS SOB A LGPD

Dentro do contexto da LGPD, a luz do princípio do consentimento ganha destaque para o tratamento ético e transparente dos dados pessoais, além das diversas bases legais já presentes no ordenamento jurídico. Os operadores e processadores de dados desempenham um papel que excedem ou infringem a lei e podem ser responsabilizados, pois são responsáveis apenas por coletar, processar e armazenar informações em nome das organizações. Esta seção explora como o consentimento se entrelaça com a responsabilidade desses agentes no tratamento de dados, destacando a necessidade de conformidade e práticas éticas.

A LGPD, no artigo 5º, inciso XII, define o consentimento como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma

finalidade determinada. Os controladores, operadores, agentes de tratamento e processadores de dados, ao lidarem com informações pessoais, devem assegurar que o consentimento seja obtido de maneira clara, destacando a finalidade específica para a qual os dados serão utilizados. Esse processo é essencial para garantir que os titulares dos dados tenham controle sobre como suas informações serão tratadas.

Além disso, os controladores, operadores, agentes de tratamento e processadores de dados têm a responsabilidade de respeitar o princípio da finalidade, garantindo que os dados coletados sejam usados somente para os propósitos informados aos titulares. Isso implica que as práticas de tratamento de dados devem ser transparentes e alinhadas com as expectativas dos titulares. Qualquer desvio em relação à finalidade original requer um novo consentimento.

A responsabilidade dos operadores e processadores também abrange a implementação de medidas de segurança adequadas. A LGPD, em seu artigo 46º, estabelece que os agentes de tratamento devem adotar medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados e situações de risco. Isso inclui a implementação de protocolos de segurança, criptografia e restrição de acesso.

Em termos de responsabilidade, atualmente a responsabilidade é da empresa controladora, entretanto o que se pretende discutir neste estudo é a necessidade de criação de mecanismo de fiscalização para que os controladores, operadores, agentes de tratamento e processadores de dados possam ser considerados responsáveis solidários em caso de violações de dados, juntamente com as organizações controladoras. Isso enfatiza a necessidade de parcerias transparentes e contratos sólidos entre todas as partes envolvidas no tratamento de dados pessoais.

Em suma, uma legislação mais apertada, com fiscalização em relação ao consentimento, e a responsabilidade tendem a formar um elo essencial para garantir a conformidade com a LGPD no uso dos controladores, operadores, agentes de tratamento e processadores de dados. O tratamento adequado dos dados pessoais, o respeito aos

limites estabelecidos pelos titulares e a implementação de medidas de segurança sólidas são componentes cruciais para a construção de uma relação de confiança entre todas as partes envolvidas no ecossistema de dados.

A NECESSIDADE DE REGULAMENTAÇÃO DE POLÍTICAS PÚBLICAS DE FISCALIZAÇÃO E PUNIBILIDADE SOLIDÁRIA

No contexto da LGPD, a regulamentação eficaz é um fator determinante para assegurar a proteção dos dados pessoais e a conformidade das organizações. No entanto, a mera existência de regulamentações não é suficiente.

É imperativo que políticas públicas sejam instituídas para garantir a fiscalização rigorosa e punições efetivas em caso de infrações. Uma vez que os dados na atualidade se configuram como o "novo petróleo"[2] Embora a Autoridade Nacional de Proteção de Dados - ANPD, em seu regulamento, contemple a previsão de sanção a descumprimento, inicialmente essa questão contempla a pessoa jurídica, trazendo apenas orientação de conduta aos controladores, operadores, agentes de tratamento e processadores de dados.

POLÍTICAS DE FISCALIZAÇÃO E PUNIBILIDADE

A implementação das políticas de fiscalização e punibilidade mais severas é crucial para garantir que as organizações tratem os dados pessoais com o respeito e a responsabilidade que merecem. A regulamentação deve estabelecer mecanismos de monitoramento contínuo, auditorias regulares e ações corretivas em casos de não conformidade. Além disso, a imposição de multas significativas em proporção às infrações cometidas pode servir como um incentivo forte para que as empresas cumpram estritamente a lei.

ESTABELECIMENTO DE CRITÉRIO - UM CONSELHO DE CLASSE PARA O OPERADOR DA LGPD

O presente estudo apresenta uma indagação, uma vez que a ANPD apresenta em seu regulamento sanções para casos de descumprimentos, questiona-se por que a sociedade se apresenta insegura diante das novas tecnologias? Um questionamento levantado seria o de que a sanção à pessoa jurídica é tardia, o que impulsiona o operador e processador de dados a poder agir sem responsabilidade, visto não ser solidário com informação que processa.

Nos casos de o operador ou processador de dados serem considerados solidários, percebe-se também que seria um grande fardo para ser suportado, se estes não fossem conhecedores do direito. Diante das questões suscitadas é que o presente estudo apresenta a tese de responsabilidade solidária para o operador ou processador de dados, desde que seja um profissional de direito ou que tenha fácil acesso a um corpo jurídico.

Com todas essas teorias também seria necessário um conselho de classe, composto por especialistas em proteção de dados, juristas e representantes da sociedade civil, pode desempenhar um papel crucial na supervisão e orientação do tratamento de dados pessoais de maneira preventiva.

Além disso, o Conselho de Classe pode colaborar com as autoridades de proteção de dados para aprimorar a eficácia das políticas de fiscalização, compartilhando informações e *insights* sobre as práticas das organizações. Essa cooperação pode resultar em um ambiente de tratamento de dados mais transparente e confiável.

A regulamentação adequada é essencial para a implementação bem-sucedida da LGPD. A combinação de políticas de fiscalização e punibilidade mais severas com o estabelecimento de um Conselho de Classe da LGPD pode criar um ambiente que não apenas garanta a conformidade legal, mas também promova uma cultura de respeito à privacidade e proteção dos dados pessoais. Ações proativas nessa direção têm o potencial de elevar os padrões de tratamento de

dados no Brasil e fortalecer a confiança dos cidadãos no uso de suas informações pessoais.

A NECESSIDADE DO DPO NAS EMPRESAS: RESPONSABILIDADE NO PROCESSAMENTO E DESCARTE DE DADOS, FORMAÇÃO ATRELADA AO DIREITO E A IMPORTÂNCIA DO TREINAMENTO E CONSCIENTIZAÇÃO

No âmbito da LGPD, a designação do Encarregado de Proteção de Dados (DPO) em empresas desempenha um papel de destaque na garantia da conformidade e respeito aos direitos dos titulares. Neste tópico, abordaremos a necessidade da função do DPO, sua responsabilidade no processamento e descarte de dados, a necessidade de formação atrelada ao direito e como o treinamento e conscientização contribuem para a eficácia dessa função.

RESPONSABILIDADE NO PROCESSAMENTO E DESCARTE DE DADOS

O DPO desempenha um papel fundamental, ele deve assegurar que o processamento seja realizado em conformidade com os princípios da LGPD, incluindo a obtenção de consentimento adequado, finalidade legítima e minimização dos dados, conforme art. 5º, VIII e art. 41, §2º da LGPD.

> Art. 5º Para os fins desta Lei, considera-se:
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

> § 2º As atividades do encarregado 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; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. BRASIL (lei 13709/2018);

Além disso, é responsabilidade do DPO garantir que os dados sejam descartados de maneira segura após o término de sua finalidade, evitando riscos de vazamento ou uso indevido.

FORMAÇÃO ATRELADA AO DIREITO

A formação do DPO é essencial para que ele possa desempenhar suas funções com conhecimento e expertise. A LGPD é uma legislação complexa e interdisciplinar, e a formação atrelada ao direito garante que o DPO compreenda as nuances jurídicas das práticas de tratamento de dados. Isso permite que ele oriente a empresa de acordo com as normas legais, reduzindo a possibilidade de não conformidade.

TREINAMENTO E CONSCIENTIZAÇÃO

Além da formação, o treinamento e a conscientização são pilares importantes para a eficácia do DPO. Por meio de programas de treinamento, os funcionários da empresa podem compreender a importância da proteção de dados, suas responsabilidades e ações adequadas em relação ao tratamento de informações e dados pessoais. A conscientização sobre as implicações éticas e legais promove uma cultura organizacional voltada para a privacidade.

A função do DPO é essencial para garantir a conformidade da empresa com a LGPD e o respeito à privacidade dos titulares. Sua responsabilidade no processamento e descarte de dados, a participação em treinamentos e conscientização formam um conjunto de elementos que contribuem para a proteção efetiva dos dados pessoais. Ao investir nesses aspectos, a empresa demonstra seu compromisso com a privacidade e fortalece a confiança de clientes e parceiros.

À medida que empresas e instituições se adaptam às exigências da LGPD, a proteção da privacidade e dos direitos dos cidadãos se fortalece, estabelecendo uma base sólida para um futuro digital mais seguro e confiável.

PONTOS IMPORTANTES DA LGPD

A Lei Geral de Proteção de Dados (LGPD) introduziu uma série de princípios fundamentais que regem o tratamento de dados pessoais no Brasil. Esses princípios foram elaborados para garantir que as informações pessoais sejam tratadas com o devido respeito à privacidade e segurança dos titulares. Abaixo estão os 10 pontos essenciais da LGPD[3]:

1. Consentimento Informado (Artigo 7º): A LGPD estabelece que o tratamento de dados pessoais requer o consentimento livre, informado e inequívoco do titular dos dados. Isso significa que as organizações em tese só deveriam coletar e processar informações pessoais com a permissão explícita e esclarecida do indivíduo

2. Finalidade Legítima (Artigo 6º): Os dados devem ser coletados para finalidades específicas, legítimas e explícitas, não podendo ser utilizados de maneira incompatível com essas finalidades. Isso garante que os dados sejam usados somente para os propósitos para os quais foram obtidos.

3. Necessidade e Minimização (Artigo 6º): A coleta de dados deve ser limitada ao mínimo necessário para atingir a finalidade pretendida.

Isso impede a coleta excessiva e desnecessária de informações pessoais.

4. Acesso dos Titulares (Artigo 18º):* Os titulares dos dados têm o direito de acessar as informações pessoais que estão sendo tratadas. Isso permite que os indivíduos saibam quais informações estão sendo mantidas e como estão sendo utilizadas.

5. Retificação e Correção (Artigo 18º): Os titulares podem solicitar a correção de dados incompletos, inexatos ou desatualizados. Isso garante que as informações pessoais sejam precisas e atualizadas.

6. Portabilidade dos Dados (Artigo 18º): Os titulares podem solicitar a transferência de seus dados para outra empresa ou serviço. Isso promove a portabilidade e controle sobre as próprias informações.

7. Eliminação dos Dados (Artigo 18º): Os dados devem ser excluídos após o cumprimento da finalidade para a qual foram coletados e quando finalizado o prazo legal de retenção Isso evita a retenção desnecessária de informações pessoais.

8. Segurança e Sigilo (Artigo 46º): É necessário implementar medidas de segurança para proteger os dados pessoais de acessos não autorizados. Isso abrange desde a criptografia até o controle de acesso às informações.

9. Responsabilidade e Compliance (Artigo 41º): As organizações são responsáveis pelo tratamento adequado dos dados e pela conformidade com a LGPD. Isso inclui a adoção de práticas que garantam a proteção dos dados.

10. Fiscalização e Sanções (Artigo 52º): A Autoridade Nacional de Proteção de Dados (ANPD) é responsável por fiscalizar e aplicar sanções em casos de não conformidade com a lei. Isso cria um incentivo para que as empresas cumpram as diretrizes da LGPD.

Esses pontos são fundamentais para garantir que o tratamento de dados pessoais seja feito de maneira ética, transparente e segura, protegendo os direitos e a privacidade dos indivíduos.

Certamente, a LGPD (Lei Geral de Proteção de Dados) é uma legislação bem elaborada que estabelece diretrizes claras para o tratamento de dados pessoais no Brasil. Ela não apenas estabelece

direitos e garantias para os titulares dos dados, mas também impõe responsabilidades e prevê sanções para as organizações e indivíduos que manipulam esses dados de forma inadequada. Vamos explorar essa perspectiva em mais detalhes:

RESPONSABILIDADES DOS CONTROLADORES, OPERADORES E AGENTES DE TRATAMENTO DE DADOS

Sob a LGPD, os controladores, operadores e os agentes de tratamento de dados têm responsabilidades específicas.

Controladores de Dados, são as organizações ou indivíduos que determinam as finalidades e os meios de processamento dos dados. Eles são responsáveis por garantir que o tratamento dos dados seja feito de acordo com a lei, obtendo consentimento adequado quando necessário e tomando medidas para proteger os dados.

Operadores de Dados são as organizações ou indivíduos que processam dados em nome dos controladores. Eles também têm responsabilidades significativas para garantir a segurança e a conformidade com a LGPD.

PUNIÇÕES POR USO INADEQUADO

A LGPD prevê sanções significativas para aqueles que não cumprem suas disposições. Isso inclui multas que podem ser aplicadas tanto aos controladores quanto aos processadores de dados, dependendo da gravidade da infração. As multas podem chegar a 2% do faturamento da organização, com um limite de até 50 milhões de reais por infração.

Além das multas, outras sanções podem incluir conforme art. 52 da Lei 13.709 de 2018 diversas sanções a título de exemplificação cita se:

1. Advertências e Multas Diárias: Além da multa única, as autoridades podem impor multas diárias até que a infração seja corrigida.

2. Proibição de Processamento de Dados: Em casos graves, as autoridades podem proibir uma organização de processar dados por um período determinado.

3. Publicização da Infração: As autoridades podem tornar públicas as infrações, expondo a organização ao escrutínio público.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) 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;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> 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; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo

período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)
§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.
§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

> § 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.
> § 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.
> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.
> Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. BRASIL (lei 13709/2018)

É importante destacar que a LGPD tem como objetivo principal proteger os direitos e a privacidade dos titulares dos dados. Portanto, seu foco está em garantir que as organizações tratem as informações pessoais com o devido cuidado e responsabilidade. O cumprimento da LGPD é fundamental para todas as organizações que lidam com dados pessoais, e a legislação fornece os meios para responsabilizar aqueles que não a seguem adequadamente.

CONCLUSÃO

À medida que chegamos ao fim desta exploração sobre a Lei Geral de Proteção de Dados (LGPD) e seu impacto no cenário brasileiro, fica claro que estamos diante de um momento crítico para a proteção da

privacidade e dos direitos dos cidadãos. A LGPD não é apenas uma lei, mas um farol que ilumina o caminho para um futuro digital mais seguro e confiável.

A LGPD estabelece princípios fundamentais que refletem a necessidade de respeitar a privacidade, garantir o consentimento informado e minimizar os riscos associados ao tratamento de dados pessoais. Por meio desses princípios, ela cria uma base sólida para a construção de uma cultura de proteção de dados no Brasil.

No entanto, a LGPD não é apenas sobre princípios; é sobre responsabilidades. Os operadores e processadores de dados desempenham um papel crucial na implementação ética e transparente desses princípios. Eles devem garantir que o consentimento seja obtido de forma clara, que os dados sejam usados apenas para finalidades legítimas e que medidas de segurança adequadas sejam implementadas. A LGPD não deixa margem para descuido ou tratamento inadequado dos dados pessoais.

A regulamentação eficaz é um componente essencial dessa equação. Políticas públicas mais bem elaboradas que incluam fiscalização rigorosa e punições significativas em casos de infração são necessárias para garantir que as organizações cumpram suas obrigações sob a LGPD. Além disso, a criação de um Conselho de Classe da LGPD pode oferecer supervisão e orientação adicionais, fortalecendo a aplicação da lei.

A LGPD não é uma restrição às inovações tecnológicas ou à livre iniciativa. Pelo contrário, ela é uma salvaguarda que promove o desenvolvimento econômico e tecnológico, ao mesmo tempo em que protege os direitos humanos e a liberdade de expressão. Ela incentiva as empresas a adotarem boas práticas de proteção de dados, tornando-se líderes em confiabilidade e respeito à privacidade.

No Brasil, a proteção de dados é uma responsabilidade compartilhada por todos, desde as organizações até os indivíduos. À medida que nos adaptamos às exigências da Lei, estamos construindo um futuro digital em que a privacidade e a segurança dos dados são garantidas. A LGPD não é apenas uma lei, é um compromisso com a

proteção dos direitos fundamentais dos cidadãos e o fortalecimento da confiança em um mundo digital em constante evolução. À medida que seguimos em frente, a LGPD ilumina nosso caminho para um futuro digital mais seguro e confiável para todos.

REFERÊNCIAS BIBLIOGRÁFICAS

BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível https://bdjur.stj.jus.br/jspui/bitstream/2011/142294/lei_geral_protecao_blum.pdf. Acesso em 27 out. 2023.

TRATAMENTO DE DADOS PESSOAIS NA CONSULTA DE JURISPRUDÊNCIA: DESAFIOS E PERSPECTIVAS: COMITÊ DE APOIO PARA ELABORAÇÃO DE ESTUDOS E PARECERES TÉCNICOS SOBRE A SISTEMATIZAÇÃO DO SERVIÇO DE JURISPRUDÊNCIA NO PODER JUDICIÁRIO Disponível https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf . Acesso em 27 out. 2023.

LUCCA, Newton De. LIMA, Cíntia Rosa Pereira de - Polêmicas em torno da vigência da Lei Geral de Proteção de Dados. Disponível em <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/331758/polemicas-em-torno-da-vigencia-da-lei-geral-de-protecao-de-dados > Acesso em 30 de out 2023

Tratamento de dados pessoais na consulta de jurisprudência, desafios e perspectivas, 2020, disponível em <https://www.cnj.jus.br/wp-content/uploads/2022/02/tratamento-dados-pessoais-consulta-jurisprudencia30-11-21.pdf> Acesso em 30 de out 2023

LEI 13.709 de 2018 disponível em < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 30 de out 2023

BOTELHO, Marcos César 1, CAMARGO, Elimei Paleari do Amaral, A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA SAÚDE, R. Dir. sanit., São Paulo v.21, e-0021, 2021 Disponível em < file:///C:/Users/Cristiane/Downloads/168023-Texto%20do%20artigo-538538902-1-10-20220202.pdf> Acesso em 30 de out 2023