UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE NACIONAL DE DIREITO

DELITOS CIBERNÉTICOS: UMA ANÁLISE DA LEGISLAÇÃO E SEUS SUJEITOS NO CONTEXTO DA PROTEÇÃO DE DADOS NO BRASIL

GUSTAVO DOWSLEY DE SOUSA

Rio de Janeiro

2024

GUSTAVO DOWSLEY DE SOUSA

DELITOS CIBERNÉTICOS: UMA ANÁLISE DA LEGISLAÇÃO E SEUS SUJEITOS NO CONTEXTO DA PROTEÇÃO DE DADOS NO BRASIL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Antônio José Teixeira Martins.

Rio de Janeiro

2024

CIP - Catalogação na Publicação

Dowsley de Sousa, Gustavo
D725d Delitos Cibernéticos: Uma análise da legislação e seus sujeitos no contexto da proteção de dados no Brasil / Gustavo Dowsley de Sousa. -- Rio de Janeiro, 2024.
53 f.

Orientador: Antônio José Teixeira Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2024.

1. Lei Geral de Proteção de Dados. 2. Crimes Cibernéticos. 3. Legislação. 4. Compliance. I. Teixeira Martins, Antônio José, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

GUSTAVO DOWSLEY DE SOUSA

DELITOS CIBERNÉTICOS: UMA ANÁLISE DA LEGISLAÇÃO E SEUS SUJEITOS NO CONTEXTO DA PROTEÇÃO DE DADOS NO BRASIL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Antônio José Teixeira Martins.

Data da Aprovação: 13 / 12 /2024 .
Banca Examinadora:

Antônio José Teixeira Martins
Orientador

Co-orientador (Opcional)

Tiago Joffily
Membro da Banca

Membro da Banca

Rio de Janeiro

2024

AGRADECIMENTOS

Primeiramente ao acaso do destino, que, de um encontro entre dois adolescentes, formou um bacharel na Faculdade Nacional de Direito. Mãe e pai, obrigado por tanto.

À Mônica, talvez - ou com certeza - a maior responsável pela minha educação e capacidade inventiva.

Aos avós, Paulo César, Luiz Claudio, Sandra Maria e Maria Adenice, obrigado pelo apoio e por serem pais e mães duas vezes. Tudo seria diferente sem vocês.

Aos tios e tia, que contribuem um pouco a cada dia para a formação de um jurista calmo e educado.

Ao meu pai, Márcio, que me inspira todos os dias e mostra que a palavra “paizão” nunca será superlativa quando a ele se referir.

À minha mãe, Ligia, obrigado por me mostrar que, além das dificuldades, a vida pode ser leve quando se tem o apoio da família.

À minha madrasta, Jaqueline, pela paciência em conviver com um jovem em formação, que ainda se descobre todos os dias.

À Maria Luisa, Beatriz e Rebeca, por, sem mesmo saber, me inspirarem a ser o melhor exemplo que eu posso ser. Nunca imaginei ter a admiração de alguém.

À Paula, minha alma gêmea, que todos os dias me surpreende com Mutirão de Amor e prova que nós realmente somos feitos um pro outro, de encomenda.

Aos meus amigos mais antigos, em especial os do Colégio Bahiense Vaz Lobo, por descobrirem a vida, as dificuldades e - sobretudo - as risadas comigo.

Ao Clube do Vinho, por inúmeras vezes, sem titubear, dizer e mostrar o que eu precisava ver e ouvir.

Aos meus cachorros e gatos, que, na inocência que só a eles pertence, me dizem que está tudo bem, todos os dias.

Ao colossal e centenário Clube de Regatas do Flamengo, que me acompanha do berço à eternidade.

A todos que - positivamente ou não - contribuíram de alguma forma à minha trajetória. Muito obrigado.

RESUMO

O presente trabalho tem como objeto a análise da evolução da legislação brasileira referente à internet e à proteção de dados pessoais, com ênfase nas Leis nº 12.737/2012 (Lei Carolina Dieckmann), nº 12.965/2014 (Marco Civil da Internet) e nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). O estudo inicia-se com a contextualização do crescimento exponencial da internet e o consequente aumento de crimes cibernéticos, fenômenos que exigem uma contínua adaptação do ordenamento jurídico com vistas à proteção da privacidade e à garantia de segurança no ambiente digital. Primeiramente, a Lei nº 12.737/2012 é examinada como resposta legislativa à vulnerabilidade dos usuários na internet, especificamente no que tange aos crimes cibernéticos, ao passo que a Lei nº 12.965/2014 é apresentada como um marco normativo que visa equilibrar os direitos fundamentais dos usuários da rede, como a liberdade de expressão e a proteção da privacidade, ao mesmo tempo em que impõe responsabilidades aos provedores de serviços de internet. Em sequência, com a promulgação da Lei nº 13.709/2018, a qual estabelece diretrizes claras para o tratamento de dados pessoais por parte de empresas e organizações, abordam-se os mecanismos de obtenção de consentimento, as exigências quanto à segurança da informação e os direitos dos titulares de dados pessoais. A legislação se insere, assim, em um contexto global de crescente regulamentação da proteção de dados, o que possibilita a comparação entre a LGPD e a *General Data Protection Regulation* (GDPR) da União Europeia, destacando-se as semelhanças e as diferenças entre ambas, bem como a atuação das autoridades competentes na fiscalização e aplicação das normas em seus respectivos territórios. Por fim, buscou-se expor que, apesar dos avanços significativos na legislação brasileira, a normativa ainda apresenta lacunas, especialmente no que se refere à tipificação dos crimes cibernéticos, à criminalização de condutas específicas e à adequada dosimetria das penas. Nesse contexto, enfatiza-se a necessidade de constante aprimoramento do arcabouço legislativo, de modo a assegurar a efetiva proteção dos dados pessoais e a punição adequada dos crimes praticados no ambiente digital, em conformidade com as novas demandas da sociedade digital.

Palavras-chave: legislação; privacidade; consentimento; tipificação; delito; *internet*; entidades; sanções e *compliance*.

ABSTRACT

The present paper aims to analyze the evolution of Brazilian legislation concerning the internet and the protection of personal data, with emphasis on Laws No. 12,737/2012 (Carolina Dieckmann Law), No. 12,965/2014 (Marco Civil da Internet), and No. 13,709/2018 (General Data Protection Law – LGPD). The study begins with the contextualization of the exponential growth of the internet and the consequent rise in cybercrimes, phenomena that require continuous adaptation of the legal framework to ensure privacy protection and security in the digital environment. First, Law No. 12,737/2012 is examined as a legislative response to the vulnerability of internet users, specifically regarding cybercrimes. Law No. 12,965/2014 is then presented as a regulatory milestone designed to balance the fundamental rights of internet users, such as freedom of expression and privacy protection, while imposing responsibilities on internet service providers. Subsequently, with the enactment of Law No. 13,709/2018, which establishes clear guidelines for the processing of personal data by companies and organizations, the mechanisms for obtaining consent, the security requirements for information, and the rights of data subjects are addressed. This legislation is framed within a global context of increasing data protection regulation, allowing for a comparison between the LGPD and the European Union's General Data Protection Regulation (GDPR), highlighting both similarities and differences, as well as the role of the competent authorities in the enforcement and application of these norms within their respective jurisdictions. Finally, the paper seeks to demonstrate that, despite significant advances in Brazilian legislation, gaps still exist, particularly regarding the criminal classification of cybercrimes, the criminalization of specific conducts, and the adequate proportionality of penalties. Therefore, the need for constant improvement of the legal framework is emphasized, so as to ensure effective protection of personal data and the proper punishment of crimes committed in the digital environment, in line with the new demands of the digital society.

Keywords: legislation; privacy; consent; criminal classification; fellony; internet; entities; sanctions and compliance.

SUMÁRIO

1. **HISTÓRICO**

O avanço da internet e o consequente aumento de sistemas, documentos e dados sensíveis armazenados *online* possibilitou, também, o crescimento de delitos praticados nesta esfera. Os crimes cibernéticos - cibercrimes - ganham força na última década com diversas modalidades e meios de ação, impondo desafio crucial no que concerne à sua identificação e contenção.

Plataformas como *Facebook, Twitter* e *Instagram* revolucionaram a comunicação e a interação social, permitindo a criação e o compartilhamento de conteúdo em uma escala sem precedentes. Além disso, essas plataformas desempenham um papel crucial na disseminação de notícias e na mobilização de movimentos sociais. No entanto, elas também enfrentam críticas relacionadas à proteção de dados e à regulamentação de seu conteúdo, inicialmente desregulado.

Dessa forma, a expansão da conectividade resultou em uma ampliação da vulnerabilidade a ataques cibernéticos, tornando a segurança de dados e a cibersegurança prioridades essenciais tanto para pessoas físicas quanto jurídicas.

Nesse contexto, o *phishing* se apresenta como uma nova engenharia social, isto é, um novo método que permite o criminoso enganar a vítima para que ela comprometa seus dados pessoais, seja por e-mail, mensagens sms, criação de sites falsos ou, ainda, por chamadas de voz. Essa técnica possibilita, por intermédio destes *links* falsos, que os criminosos apropriem-se dos dados pessoais das vítimas escolhidas e, uma vez em posse destes, são infinitas as possibilidades de utilização. Assim, a criptografia desempenha papel indiscutível na segurança da comunicação *online*, o que, no entanto, suscita dúvidas quanto à viabilidade de acesso destas informações pelas autoridades, quando necessário.

Numa esfera maior, as técnicas de desinformação e má-informação, construídas a partir da evolução das tecnologias *online*, lançam a crescente preocupação dos poderes legislativo, executivo e judiciário quanto à idoneidade

dos processos democráticos em meio a este turbilhão tecnológico. Desse modo, a edição de regras específicas a fim de conter a utilização destas técnicas, seja no cotidiano com o controle da opinião pública através de ataques maciços a instituições de poder e grupos minoritários resguardados pela Constituição, ou, em um contexto mais recente, na tentativa de manipular pleitos eleitorais por meio de vídeos, imagens e áudios manipulados por inteligências artificiais de maneira inverídica ou retirada de contexto.

Por outro lado, a gradativa conscientização da sociedade civil acerca da privacidade e segurança *online* vem norteando o comportamento dos usuários e, concomitantemente, exigindo maior transparência e responsabilização das empresas no tratamento destes dados.

Isso porque, com o advento da Lei Geral de Proteção de Dados (Lei 13.709/2018), as empresas ganham novos parâmetros de coleta, armazenamento e descarte de dados pessoais dos usuários que, caso não observados, podem acarretar em multas sobre o faturamento da empresa e, ainda, na publicação da infração cometida, que pode impactar significativamente na reputação da empresa com o consumidor, dificultando, por consequência, na retenção e captação de novos clientes e, dessa forma, no futuro da Companhia. Além disso, há também o risco de litígios judiciais com os titulares dos dados e, nos casos mais graves, a ação civil pública, como no caso de vazamento de dados mantidos pela Caixa, União e Dataprev em 2022, que rendeu a cerca de 4 milhões de pessoas R$ 15.000 (quinze mil reais) cada a título de indenização, totalizando aproximadamente R$ 60.000.000.000 (sessenta bilhões de reais) de condenação[1].

No Brasil, a ANPD - Autoridade Nacional de Proteção de Dados - é a autarquia, criada pela Lei 13.853/2019, que tem por objetivo garantir a efetiva aplicação das leis de proteção de dados no ordenamento jurídico brasileiro. Nesse sentido, à ANPD compete definir e regulamentar as normas para o

[1] MINISTÉRIO PÚBLICO FEDERAL (MPF). **Justiça determina indenização de R$ 15 mil a cidadãos que tiveram dados pessoais vazados em 2022**. São Paulo, 20 set. 2023. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias/justica-determina-indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais-vazados-em-2022. Acesso em: 29/08/2024.

tratamento de dados pessoais, fornecendo orientações e diretrizes para ajudar empresas e organizações a cumprir a LGPD, além da realização de auditorias e inspeções para verificar o cumprimento da norma por parte de empresas e entidades públicas e privadas, sendo estas sujeitas a sanções aplicáveis pela própria autarquia em caso de descumprimento à legislação, nos termos do Art. 55-J, IV, da Lei 13.853/2019.

Ainda, a Carta de Serviços da ANPD dispõe dos meios de acesso à legislação pertinente ao tema, direcionamento para ouvidoria e esclarecimento de dúvidas sobre sua atuação e sobre os normativos, orientações ou materiais emitidos pelo órgão, reforçando a importância do tema na sociedade civil.

De outra parte, tem sido discutido por especialistas da área a utilização da tecnologia *blockchain* na administração pública, com a compatibilização desta tecnologia com a LGPD. A ideia é que a imutabilidade dos registros em *blockchain* possa contribuir para a prevenção de fraudes e corrupção, fortalecendo a integridade dos sistemas e das instituições públicas.

Criada em 2022 através de parceria do Tribunal de Contas da União (TCU) e do Banco Nacional de Desenvolvimento Econômico e Social (BNDES), a Rede Blockchain Brasil surge com este objetivo. Desse modo, a tecnologia permitirá, além da inovação para o setor financeiro, o aumento da confiabilidade na administração pública e a segurança no âmbito cibernético, uma vez que deverá gerir dados sensíveis e identidades digitais, garantindo maior controle das informações pessoais.

2. A INTERNET E O DIREITO

2.1. Crimes Cibernéticos e a Legislação Brasileira

2.1.1 Lei Carolina Dieckmann

A Lei Carolina Dieckmann (Lei n° 12.737/2012) surge a partir da necessidade de resposta da legislação brasileira ao avanço dos crimes cibernéticos e à vulnerabilidade de usuários da internet, uma vez que, antes da sua promulgação, a legislação não tutelava especificamente a proteção contra invasões e crimes digitais.

A promulgação da Lei em questão guarda relação com o caso concreto que comoveu a opinião pública em 2011, quando a atriz global Carolina Dieckmann teve seu computador invadido e mais de 30 fotos íntimas vazadas. Os *hackers* responsáveis pelo vazamento tentaram, ainda, extorquir a atriz, exigindo o pagamento de quantia exorbitante para que as imagens não fossem publicadas, o que foi prontamente recusado pela vítima, que teve as imagens divulgadas na internet.

Nesse sentido, a referida Lei alterou o Código Penal Brasileiro, fazendo constar duas novas disposições: os artigos 154-A e 154-B, sendo o primeiro a tipificação geral e o segundo a regra procedimental deste tipo. Vejamos:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> [...]
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a

> administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Assim, a lei também considera crime a obtenção de dados sem autorização, assim como a utilização desses dados de forma indevida, estendendo a tutela a informações que, caso divulgadas, possam causar dano à honra ou à imagem da pessoa.

Além disso, inseriu alterou também os artigos 266 e 298 do Código Penal:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de um a três anos, e multa.
>
> [...]
>
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

De outra parte, a promulgação da Lei 12.737 teve um impacto significativo no modo como a sociedade civil percebe a segurança digital e a privacidade, ampliando o debate acerca da privacidade digital e da necessidade de regulamentação do tratamento destes dados pelas empresas responsáveis.

Nessa égide, em que pese as críticas sofridas pelo dispositivo por parte da doutrina penal, sendo este considerado vago ou genérico para alguns juristas, é seguro afirmar que a Lei Carolina Dieckmann representa importante avanço no combate aos crimes cibernéticos no Brasil. Isto porque, apesar de tardia e

precisar ser combinada com outros tipos penais, é a primeira Lei a tipificar delitos cibernéticos na legislação nacional, dando impulso à criação de uma série de outras normas que viriam a seguir.

2.1.2. Marco Civil da Internet

A Lei nº 12.965/2014, batizada de Marco Civil da Internet, representa um marco histórico na regulamentação do uso da internet no Brasil. Este conjunto de normas surge como uma maneira inovadora de garantir a proteção dos direitos dos usuários, estabelecer diretrizes para o uso da rede e definir as responsabilidades dos provedores de serviço. No entanto, uma década após a sua aprovação, seu texto é tido como obsoleto ou pouco eficaz, entrando em conflito com outras normas aprovadas posteriormente, além daquelas que ainda não receberam a aprovação necessária.

No contexto de sua criação, o Marco Civil preocupa-se em assegurar direitos tidos como fundamentais aos usuários da internet: privacidade, proteção de dados pessoais e liberdade de expressão. Assim, pela leitura de seu texto observa-se o zelo do legislador com questões atinentes à liberdade de expressão e o combate à censura no meio virtual.

Tal preocupação manifesta-se prontamente no artigo 2º, caput, que, numa interpretação lógica, denota o fundamento maior da Lei a que se passa a editar e, ainda, posto como o primeiro princípio a ser citado na redação do artigo 3º. Vejamos:

> Art. 2º A disciplina do uso da internet no Brasil **tem como fundamento o respeito à liberdade de expressão**, bem como:
>
> I - o reconhecimento da escala mundial da rede;
>
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
>
> III - a pluralidade e a diversidade;

> IV - a abertura e a colaboração;
>
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VI - a finalidade social da rede.

> 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;

Não obstante, o artigo 19 - que mais tarde viria a ser objeto de discussão acerca de sua constitucionalidade[2] -, por sua vez, ainda que debruce-se sobre matéria tão importante quanto a responsabilidade civil do provedor de internet pelos danos causados por terceiros no meio virtual, também é ressalvado com a demonstração da garantia da liberdade de expressão e combate à censura:

> 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.

Ademais, os demais direitos fundamentais para o Marco Civil da Internet (privacidade e proteção de dados pessoais) são demonstrados, também nos artigos 8º e 11, sendo este último, em especial, importante na relação de

[2] BRASIL. Supremo Tribunal Federal. Tema 987 - **Discussão sobre a constitucionalidade do art. 19 da Lei n. 12.965/2014 que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros**. Brasília, DF. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5871934. Acesso em: 02/10/2024.

qualquer empresa estrangeira que, mesmo não tendo filial ou estabelecida no Brasil, participe de qualquer operação que envolva os dados pessoais do cidadão brasileiro:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, **deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais** e ao sigilo das comunicações privadas e dos registros.

No entanto, o dispositivo criado, principalmente, para coibir a censura e assegurar a liberdade de expressão, acabou por isentar as empresas de tecnologia da responsabilidade do conteúdo divulgado por terceiros, salvo em caso de descumprimento de ordem judicial. Tal fato levou a série de descumprimento de decisões judiciais por parte dessas empresas e, dessa forma, pôs em xeque a soberania nacional frente às *big techs*.

Passado o ponto explicativo dos fundamentos basilares da Lei em questão, chega-se ao ponto fundamental do presente trabalho: a evolução da legislação no meio virtual, os choques normativos e as lacunas apresentadas ao caso concreto.

O Marco Civil da Internet, ao passo que representa edição legislativa inovadora e importante no ordenamento jurídico brasileiro, também flexibiliza a exigência do dever de vigilância das empresas (provedores de internet) em relação ao conteúdo que é propagado no ambiente virtual a que se propõem a criar. Isto porque, de acordo com o artigo 19 - já abordado anteriormente - da referida Lei, 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 providências para remover o conteúdo classificado como infringente.

Ou seja, além de não impor o dever de vigilância próprio das empresas para atender os preceitos constitucionais de dignidade e eventuais disposições legais pertinentes, o texto condiciona a atuação efetiva à prévia decisão judicial, impossibilitando, por exemplo, a possibilidade de resolução extrajudicial com denúncias à plataforma e afetando diretamente a celeridade do trâmite em questão.

Ainda, o conceito de celeridade mostra-se fundamental para a resolução do caso em tela, uma vez que, tratando-se do crescimento exponencial dos discursos de ódio e assédio *online*, o período em que o conteúdo ofensivo permanece à disposição do público é crucial para o dimensionamento do dano causado.

Para Ingo Sarlet e Andressa de Bittencourt Siqueira[3], a busca pelo equilíbrio entre a liberdade de expressão e a garantia de proteção de direitos fundamentais e de personalidade segue sendo um dos principais desafios, na perspectiva do Direito, para a manutenção da democracia. Neste contexto, os autores classificam as informações online e seu potencial dano em diferentes tipos, dada sua origem e finalidade:

> Note-se que a desordem informacional (information disorder) pode ser tanto falsa, incluindo a mis-information e a dis-information, quanto danosa, neste caso incluindo a mal-information e a dis-information. A mis-information, essencialmente falsa, envolve a dissimulada conexão entre fatos e o conteúdo enganoso, enquanto a mal-information, essencialmente danosa, envolve vazamentos, assédio, discurso de ódio e situações similares. A dis-information, por sua vez, abarca tanto as informações falsas quanto danosas, envolvendo o falseamento do contexto, o conteúdo impostor, a manipulação de conteúdo e a fabricação de conteúdo (WARDLE, 2017). No caso específico das assim designadas fake news, cuida-se da imbricação entre falsidade e danosidade (LAZER; BAUM; BENKLER, 2018, p. 1094).

---

[3] SARLET, Ingo Wolfgang; Bittencourt Siqueira de, Andressa. **Liberdade de expressão e seus limites numa democracia: o caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil**. REVISTA ESTUDOS INSTITUCIONAIS, v. 6, n. 2, p. 545, 2020.

Assim, seguindo o conceito de mal-information apresentado, o combate aos discursos de ódio no meio virtual passam pelo controle da circulação e eventual proibição e descontinuamento de informações - sendo estas especificamente caluniosas -, o que representa um choque à liberdade de expressão e coibição da censura, preceitos tidos como fundamentais no âmbito da Lei 12.965/2014. No entanto, tal regulação não passa apenas pelo Estado, mas por uma espécie de autorregulação regulada pelos veículos de comunicação que abarcam tais informações[4].

Ademais, uma questão crucial no caso das informações propagadas no âmbito cibernético é que, caso eventual conflito e infringência de regra não seja solucionado com a celeridade necessária, o conteúdo em análise continua sendo amplamente exibido, o que pode levar à discussão sobre a extensão do dano e o dano continuado.

Em consonância com o disposto no Código Civil, a indenização é medida pela extensão do dano causado[5]. Nesse sentido, como a busca por justa indenização - tutelada coletiva ou individualmente - é medida recorrente perante o judiciário nacional, há que se falar, também, na extensão do dano sofrido por quem busca este direito.

Em caso julgado no ano de 2022 pelo Tribunal de Justiça de São Paulo, a parte autora alega que, no período em que estudava no Colégio Estadual Professor José Scamarelli, era motivo de gozações e chacotas de alunos da instituição de ensino, inclusive dos requeridos, e que, em uma oportunidade, teve sua imagem publicada no *Facebook*, em página denominada "Ridículos Anônimos". Assim, com a referida imagem amplamente divulgada entre alunos do colégio, aduziu o autor que, em decorrência dos danos psíquicos, não foi mais capaz de estudar e, por isso, requereu a condenação dos réus ao pagamento de danos morais.

---

[4] SARLET, Ingo Wolfgang; Bittencourt Siqueira de, Andressa. Liberdade de expressão e seus limites numa democracia: o caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil. **REVISTA ESTUDOS INSTITUCIONAIS**, v. 6, n. 2, p. 545, 2020.

[5] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

Ao final regular do feito, o juízo da 2ª Vara Cível do TJSP condenou os réus ao pagamento de R$15.000,00 (quinze mil reais) em caráter indenizatório, com juros de mora de 1% (um por cento) ao mês, contados a partir do evento danoso, que ocorreu em 2014. Da sentença em questão, destaca-se a definição utilizada pelo magistrado para fundamentar o *quantum* indenizatório determinado:

> O dano moral é evidente, pois **a imagem em questão tem o condão de macular a honra do demandante** e no âmbito infraconstitucional, aplicável o disposto no artigo 953 do Código Civil, segundo o qual: "A indenização por injúria, difamação ou calúnia consistirá na reparação do dano que dela resulte ao ofendido". Enfim, presentes provas da certeza da publicação realizada com **imagem do autor em montagem de conteúdo obsceno** e de sua respectiva repercussão e autoria, é o caso de acolhimento da pretensão.
>
> O dano moral encerra justamente um **prejuízo decorrente da dor ou constrangimento imputado a uma pessoa, em razão de atos que, indevidamente, ofendem seus sentimentos de honra e dignidade, provocando mágoa e atribulações na esfera pertinente à sua sensibilidade moral**.
>
> À vista disso, **necessário se faz fixar a indenização levando-se em conta critérios compensatórios e punitivos**; vale dizer, impõem-se a concessão de lenitivo ao lesado e agravo patrimonial ao responsável pela lesão de tal forma que se impeça a reiteração de atos danosos.
>
> (SÃO PAULO. Processo nº 1017477-41.2014.8.26.0224. **Indenização por Dano Moral**. Autor: Enrique Teixeira Garcia. Réu: Leonardo Alexandre Braga da Silva e outros. Juíza: Larissa Boni Valieris. Guarulhos, 09 de agosto de 2022.)

Desta feita, demonstrado o caráter imprescindível da indenização em ações deste tipo, há que se discutir, conforme exposto, a extensão da discussão até a efetiva prestação jurisdicional. Isto porque, como os fatos narrados no caso em questão ocorreram em 2014 e a sentença acima colacionada foi publicada em

2022, 8 longos anos se passaram com a imagem da vítima - e autor da ação - continuamente violada.

Além disso, a sentença condenou os réus ao pagamento do valor indenizatório acrescidos de juros de mora de 1% (um por cento) ao mês, contados a partir do evento danoso. Ou seja, além da mácula da vítima perdurar por mais tempo do que o necessário, os réus terão que desembolsar quase o dobro do valor arbitrado (R$ 15.000,00), totalizando a quantia de, pelo menos, R$ 29.400,00 (vinte e nove mil e quatrocentos reais), representando vultoso dispêndio financeiro que poderia ser evitado com uma maior vigilância e regulação interna do *Facebook*, que é a rede em questão.

Ademais, o crescimento das produções de *deep fakes* no cenário virtual obriga o poder judiciário a buscar amparo em tipos penais já existentes, em razão da ausência de legislação acerca do tema.

Deep Fake é, em sua essência, uma técnica que utiliza inteligência artificial para criar imagens, vídeos ou áudios falsos, em que a imagem ou voz de uma pessoa é alterada de forma a parecer que ela está dizendo ou fazendo algo que, na realidade, nunca ocorreu. Nesse sentido, discussões acerca do potencial lesivo de materiais produzidos a partir desta técnica estão em ebulição no universo jurídico e político nacional, haja vista as infinitas possibilidades que a ferramenta traz, desde danos à imagem de particular à manipulação da opinião pública.

A importância do assunto é tamanha, por exemplo, que, no contexto das Eleições Municipais de 2024, o Tribunal Superior Eleitoral viu-se obrigado a editar novo conteúdo normativo com preocupação específica sobre a utilização indevida da tecnologia[6]. A Resolução TSE Nº 23.732/2024 altera a Resolução TSE Nº 23.610/2019, que dispõe sobre propaganda eleitoral, fazendo constar uma série de novas regras eleitorais, com destaque àquelas previstas no artigo 9º,

[6] BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Deepfake e inteligência artificial: saiba o que pode e o que é proibido nas campanhas eleitorais**. Brasília, DF, 20 jun. 2024. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr2/2024/deepfake-e-inteligencia-artificial-saiba-o-que-pode-e-o-que-e-proibido-nas-campanhas-eleitorais. Acesso em: 10/10/2024.

9º-B, 9º-C, 9º-D, 9º-E, 9º-F, 9º-G e 9º-H, que versam sobre a desinformação na campanha eleitoral.

Retornando ao conceito de *dis-information*, introduzido aqui por Ingo Sarlet e Andressa Siqueira, tem-se que esta abarca tanto as informações falsas quanto danosas, revelando a particularidade e periculosidade deste tipo[7]. As disposições trazidas nesta nova Resolução, portanto, preocupam-se em[8]: (i) pressupor que o conteúdo eleitoral divulgado por candidato, partido, federação ou coligação tenha sido verificado, com a fidedignidade da informação atestada; (ii) o dever de informar que eventual propaganda eleitoral tenha sido fabricada ou manipulada através do uso de inteligência artificial; (iii) vedar a utilização de conteúdos fabricados ou manipulados para difundir fatos inverídicos ou descontextualizados, a fim de causar danos à integridade do processo eleitoral; (iv) vincular o provedor de aplicação de internet à adoção e publicização de medidas para impedir ou diminuir a circulação destes fatos inverídicos ou descontextualizados; (v) prever a responsabilização solidária dos provedores, civil e administrativamente, quando não promoverem a indisponibilização de conteúdos terminantemente proibidos por esta Lei e (vi) prever que a propaganda eleitoral que veicule fatos inverídicos ou descontextualizados sobre o sistema eletrônico de votação, o processo eleitoral e à Justiça Eleitoral estará vinculada às decisões colegiadas do TSE sobre a mesma matéria.

Assim, tem-se que o crescimento das *deep fakes* é matéria de extrema importância nos cenários jurídico e político nacionais e, com a iminente crescente e atualização destas tecnologias, a legislação civil carece de atualizações mais específicas, a exemplo da recente atualização na Resolução publicada pelo Tribunal Superior Eleitoral.

---

[7] SARLET, Ingo Wolfgang; Bittencourt Siqueira de, Andressa. **Liberdade de expressão e seus limites numa democracia: o caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil**. REVISTA ESTUDOS INSTITUCIONAIS, v. 6, n. 2, p. 545, 2020.

[8] BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 27 de fevereiro de 2024. **Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral**. Diário da Justiça Eletrônico do Tribunal Superior Eleitoral, Brasília, DF, v. 29, p. 132-145, 4 mar. 2024. Seção de Legislação.

Em uma instância superior, ao falar de críticas à Lei 12.965/2014, é indispensável mencionar o grave problema que a norma, ao eximir, em primeiro plano, os provedores de responsabilização pelos danos já explanados, trouxe à soberania nacional.

O caso do aplicativo Telegram, por exemplo, reflete diretamente este ponto. Em investigação que teve início a partir do massacre ocorrido em duas escolas de Aracruz (ES), em novembro de 2022, a Polícia Federal apontou que dados do celular do autor do massacre mostravam que ele integrava grupos extremistas no aplicativo, onde eram divulgados tutoriais de assassinato e fabricação de explosivos, vídeos de mortes violentas, ódio a minorias e ideias neonazistas, o que resultou no pedido de quebra de sigilo dos dados cadastrais destes usuários.

Com determinação judicial para que a empresa entregasse as informações em até 24 horas e a resposta, na visão do magistrado da 1ª Vara Federal de Linhares, insuficiente, foi determinada a suspensão do aplicativo até que os dados requeridos fossem efetivamente entregues, além da majoração da multa por descumprimento.

Em sede de Mandado de Segurança, o desembargador Flávio Oliveira Lucas, do Tribunal Regional Federal da 2ª Região, apesar de conceder parcialmente a liminar e cessar qualquer tipo de bloqueio ao aplicativo, manteve a aplicação da multa e destacou a periculosidade da empresa ao operar nas condições de anonimato previstas:

> Ocorre que a proposta de negócio do TELEGRAM por meio da disponibilização de uma plataforma de comunicação de alto alcance com a concepção de **maximizar a privacidade dos usuários e minimizar a coleta de dados, agregando valor ao seu produto**, torna o aplicativo um campo fértil ao anonimato almejado não apenas por aqueles que pretendem preservar sua privacidade, mas também outros que tenham pretensões ilícitas e logicamente desejem realizá-las na mais completa clandestinidade.

> É preciso que as empresas de tecnologia compreendam que o **cyberespaço não pode ser um território livre, um mundo distinto onde vigore um novo contrato social**, com regras próprias criadas e geridas pelos próprios agentes que o exploram comercialmente. As instituições e empresas, tal qual a propriedade privada, devem atender a um fim social, devem servir à evolução e não ao retrocesso.
>
> [...]
>
> Admitindo-se como verdadeira a informação de que seria impossível localizar o grupo pelo seu nome, ou mesmo os usuários, e que para criar uma conta no TELEGRAM basta um número de telefone e mais nenhum outro dado, a plataforma, tal como construída, se eximiria de praticamente qualquer solicitação judicial que buscasse identificar autores da prática de crimes por meio do aplicativo, o que, convenhamos, é inadmissível **ainda mais quando se trata de uma opção consciente da empresa em atuar dessa maneira e que eventualmente lhe serve inclusive como propaganda em relação a seus aplicativos concorrentes**.
>
> Contudo, **a seara penal não é o ambiente adequado para se discutir se há compatibilidade legal para manter o TELEGRAM no Brasil**, no termos em que se propõe a prestar o serviço.
>
> (MANDADO DE SEGURANÇA CRIMINAL (TURMA) Nº 5005459-94.2023.4.02.0000/ES)

Assim, tem-se a problemática: como conter o avanço desses grupos no ambiente virtual nacional, se a própria legislação não fornece meios para a efetiva coibição?

Em contrapartida, em caso mais recente e de maior relevância no debate jurídico nacional, o ministro do STF, Alexandre de Moraes, determinou que a plataforma *X*, anteriormente conhecida como *Twitter*, nomeasse um representante legal da empresa no Brasil, a fim de, nos termos do art. 75, X, do CPC, viabilizar que a empresa pudesse ser corretamente citada e responder judicialmente no Brasil. Como a determinação não foi atendida, o aplicativo foi

bloqueado de todos os servidores nacionais, com previsão de multa diária de R$ 50.000,00 (cinquenta mil reais) para quem o utilizasse, apesar do bloqueio.

O caso teve início, mais uma vez, em investigação acerca de perfis acusados de incitação ao crime e obstrução de justiça nas investigações sobre a procedência destes perfis. Após reiteradas determinações de bloqueio de perfis investigados e sucessivas esquivas do *X* para não cumprir - ou sequer responder - a determinação judicial, o responsável internacional pela rede social, Elon Musk, declarou que manteria o desrespeito às decisões judiciais brasileiras, bem como anunciou que extinguiria a subsidiária brasileira – X BRASIL, com a flagrante finalidade de ocultar-se do ordenamento jurídico brasileiro e das decisões do Poder Judiciário[9].

Assim, o Ministro Alexandre de Moraes, relator do processo, determinou, no dia 30 de agosto de 2024, a suspensão imediata da rede social no Brasil, fundamentando o flagrante descumprimento da empresa à ordem constitucional e, em especial, à Lei 12.965/14.

Nesse sentido, percebe-se que, ainda que a Lei vigente esteja defasada para assuntos mais específicos - o que, com a evolução da internet, pareça o caminho natural a ser seguido -, ela é de extrema importância quando da manutenção da ordem pública e em caso de afronta à soberania nacional. No caso do *Telegram*, por exemplo, foi determinada a suspensão do aplicativo e multa para coibir a empresa a colaborar com as investigações policiais em curso, o que, em sede de Mandado de Segurança, transformaria-se somente na multa por descumprimento, suspendendo o bloqueio imposto. De outra parte, no caso do *X*, com o flagrante descumprimento de determinações judiciais e afrontas à soberania nacional do responsável pela rede, a suspensão do aplicativo foi medida que se impôs, sendo inclusive referendada, por unanimidade, pela Primeira Turma do Supremo Tribunal Federal.

2.1.3. Lei Geral de Proteção de Dados

[9] DISTRITO FEDERAL. **Petição 12.404**. Relator: MIN. ALEXANDRE DE MORAES.

A Lei nº 13.709/2018 - Lei Geral de Proteção de Dados - surge neste contexto de crescente preocupação com a privacidade e a proteção dos dados pessoais dos usuários da internet, com destaque especial no aumento do uso de redes sociais e provedores que facilitam a coleta e o compartilhamento de dados.

Com o objetivo de proteger os direitos fundamentais de liberdade e privacidade dos indivíduos e regular como dados pessoais devem ser tratados, a Lei se aplica a dados pessoais, definidos como informações que podem identificar uma pessoa, e a dados pessoais sensíveis, que incluem informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos, saúde ou vida sexual.

Os princípios fundamentais norteadores da LGPD incluem (i) a finalidade, que exige que os dados sejam coletados para finalidades específicas, legítimas e informadas ao titular; (ii) a adequação, que determina que os dados devem ser compatíveis com a finalidade para a qual foram coletados; a necessidade, que limita a coleta ao mínimo necessário; (iii) a transparência, que impõe às empresas a obrigação de informar claramente sobre o tratamento dos dados e os direitos dos titulares; (iv) a segurança, que requer a adoção de medidas técnicas e administrativas para proteger os dados; e (v) a prevenção, que orienta a adoção de práticas para evitar danos ao titular.

Dessa forma, as empresas de tecnologia - com grande destaque para as chamadas *Big Techs* - possuem diversas responsabilidades sob a LGPD. A conformidade e governança envolvem a criação de políticas de proteção de dados que atendam aos requisitos estabelecidos pela lei, definindo procedimentos para coleta, uso, armazenamento e descarte de dados.

Assim, além da fiscalização do ente público, a LGPD transfere, através do *compliance*[10], parte da responsabilidade de garantir a conformidade com a lei

[10] Sistema de gestão, área ou disciplina dedicados à observância e garantia do cumprimento de normas legais e regulamentares, da conformidade com padrões éticos, políticas e diretrizes estabelecidos para as atividades de determinada instituição ou empresa, bem como à prevenção, detecção e correção de quaisquer desvios, fraudes, atos ilícitos ou irregularidades (geralmente envolvendo casos de corrupção, obrigações trabalhistas, fiscais, regulatórias, concorrenciais, entre outros); conjunto de medidas e

para as próprias empresas, incentivando a implementação de programas robustos de governança de dados, incluindo políticas internas, códigos de conduta, treinamentos e mecanismos de gerenciamento de riscos e estimulando a postura proativa das empresas, tudo em conformidade com o artigo 50 da referida Lei:

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

Nesta toada, o princípio da *accountability*[11], previsto no inciso X, do artigo 6º da Lei 13.709/2018, exige a 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 perante a Autoridade Nacional de Proteção de Dados[12].

Nesse sentido, o *compliance* se torna uma ferramenta essencial da governança de dados, representando um novo passo na relação entre Estado e capital e inaugurando uma era de compartilhamento da tarefa de proteção de dados[13].

Quanto à obtenção de consentimento, subsidiariamente, deve ser assegurado o consentimento explícito dos titulares anteriormente à coleta e processamento de seus dados, garantindo que este seja informado, específico e

---

procedimentos que têm esta finalidade. Fonte: https://www.academia.org.br/nossa-lingua/nova-palavra/compliance

[11] Termo designado às práticas que envolvem responsabilização e prestação de contas.

[12] 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].

[13] GARBACCIO, Grace Ladeira; KISCHELEWSKI, Flávia Lubieska N. **Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da accountability**. Revista Brasileira de Estudos Políticos, v. 128, 2024.

revogável. No entanto, há exceções em que o tratamento de dados pode ocorrer sem consentimento, como para o cumprimento de obrigações legais, execução de contratos, tutela da saúde e execução de políticas públicas. Desse modo, a anonimização de dados é vista como medida essencial para garantir o equilíbrio e a segurança jurídica nestas relações, conciliando o princípio da publicidade com a efetiva proteção de dados, ao remover informações que permitam a identificação do titular.

Exemplificativamente, o Provimento nº 134/2022 do Conselho Nacional de Justiça (CNJ) estabelece uma série de medidas a serem adotadas pelos cartórios extrajudiciais, com o intuito de proteger os dados pessoais dos usuários, sem comprometer a transparência necessária nas atividades extrajudiciais[14]:

> Art. 26. Os registradores e notários remeterão dados com a finalidade da formação de indicadores estatísticos às entidades previstas em lei ou regulamento, garantindo que sejam anonimizados na origem, nos termos da Lei Geral de Proteção de Dados Pessoais.

No que tange à segurança e proteção de dados, as empresas devem adotar medidas técnicas e administrativas para proteger os dados contra acessos não autorizados e vazamentos. Isso inclui práticas como criptografia e controle de acesso, além da necessidade de notificar a ANPD e os usuários afetados em caso de violação de dados.

Os direitos dos titulares incluem o acesso e a correção de dados, eliminação e portabilidade, além do direito de revogar o consentimento previamente concedido. As empresas devem manter uma política de privacidade clara e acessível, que detalhe as práticas de coleta e tratamento de dados, e devem estar preparadas para demonstrar conformidade, o que pode incluir a elaboração de relatórios e auditorias.

---

[14] BRASIL. Conselho Nacional de Justiça. Provimento n. 134, de 24 de agosto de 2022. **Estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à Lei Geral de Proteção de Dados Pessoais**. Brasília, 2022. Disponível em: https://atos.cnj.jus.br/files/original141307202208256307837 3a0892.pdf. Acesso em: 18/10/2024.

A Portaria ANPD nº 35, de 4 de novembro de 2022, que tornou pública a agenda regulatória para o biênio 2023-2024, instituiu o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), um documento que deve ser elaborado por empresas e organizações em todo contexto em que as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, conforme art. 5º, inciso XVII, e art. 55-J, inciso XIII, da LGPD, o que deverá ser avaliado pelo agente de tratamento[15].

Nesse sentido, em atenção ao princípio da *accountability* (art. 6º, X, LGPD), o agente de tratamento deverá elaborar o RIPD sempre que o tratamento a ser realizado puder gerar risco à garantia dos princípios previstos na LGPD e aos direitos fundamentais salvaguardados.

Além disso, a Lei 13.709/2018, permite, com fundamento nos artigos 4º, § 3º, 10, § 3º, 32 e 38, que a Autoridade Nacional de Proteção de Dados (ANPD) exija a elaboração do RIPD em situações de tratamento: (i) para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; (ii) em que o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial; (iii) de dados pessoais pelo Poder Público, incluindo a determinação de sua publicação; e (iv) de controladores em geral, abrangendo todas as suas operações de tratamento, inclusive aquelas que envolvem dados pessoais sensíveis, observados os segredos comercial e industrial.

Ademais, após constatação pelo Tribunal de Contas da União, através do Acórdão nº 1384/2022 (TC 039.606/2020-1), que 76,7% das organizações públicas federais permaneciam nos graus inexpressivo ou inicial de adequação à Lei Geral de Proteção de Dados, foi lançada, no presente ano, nova ação de

---

[15] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 23/10/2024.

controle, em que o TCU, em parceria com TCEs, enviam a cada organização federal, estadual e municipal fiscalizada um questionário para assegurar a conformidade e a implementação de medidas com fim na adequação às normas da LGPD, que depois serão analisadas e encaminhadas às organizações auditadas[16]. Isto porque, em conformidade com a Constituição Federal de 1988 e os princípios vigentes no direito brasileiro, compete ao TCU o controle externo do governo federal, sendo este responsável pela fiscalização contábil, financeira, orçamentária, operacional e patrimonial dos órgãos e entidades públicas do país quanto à legalidade, legitimidade e economicidade[17].

No que concerne à transferência internacional de dados, as empresas devem garantir que o país receptor tenha um nível de proteção adequado ou, em caso de negativa, adotar mecanismos de proteção previstos pela LGPD, como cláusulas contratuais padrão.

O não cumprimento da LGPD pode resultar em sanções e imposição de multa, pela ANPD, de até 2% do faturamento da empresa, sendo este percentual limitado a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Além disso, também podem ser aplicadas advertências, suspensão da atividade de tratamento de dados e, ainda, a exigência de publicização destas infrações, o que pode prejudicar a reputação da empresa e a confiança de clientes e parceiros. Isso porque, em conformidade com o artigo 52 da Lei 13.709/2018, serão aplicadas sanções administrativas em caso de infração às normas previstas no corpo da Lei:

> 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:

---

[16] BRASIL. Tribunal de Contas da União. Secretaria-Geral de Controle Externo. Secretaria de Fiscalização de Governança e Tecnologia da Informação. **Auditoria sobre LGPD**. Brasília: TCU, 2024. Disponível em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd/. Acesso em: 23/10/2024.

[17] BELO, Alcindo Antonio Amorim Batista. **Fiscalizar é preciso**. Revista do Tribunal de Contas da União, Brasília, n. 115, p. 7-16, maio/ago. 2009.

> 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;
>
> 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;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Além das sanções previstas no artigo 52 e dos consequentes danos à reputação da empresa - o que implicaria na perda de confiança em relação a consumidores e parceiros -, as empresas estão sujeitas, também, a potenciais litígios, uma vez que titulares de dados podem exercer em juízo, individual ou coletivamente, a defesa de seus interesses e direitos.

Isso porque o artigo 22 da Lei Geral de Proteção de Dados é claro ao prever expressamente a possibilidade dos titulares de dados postularem seus direitos pela via judicial:

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Ademais, o artigo 42 da mesma Lei, mais especificamente no parágrafo 3°, também prevê o dever de reparar no caso de dano no exercício de atividade de tratamento de dados pessoais:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

Dessa forma, destaca-se, a título de exemplo, a Ação Civil Coletiva movida pelo Instituto Brasileiro de Defesa das Relações de Consumo (IBEDEC) contra a empresa Bytedance Brasil Tecnologia Ltda., responsável pelo aplicativo *TikTok*, por violação de direitos de privacidade e proteção de dados pessoais de seus usuários. Na ocasião, foi alegado que o *TikTok* violou o direito à privacidade de seus consumidores, ao coletar dados faciais dos usuários, armazenando e compartilhando estes dados sem consentimento prévio.

Assim, sobreveio sentença, fundamentada tanto na Lei 12.965/2014 (Marco Civil da Internet) quanto na Lei 13.709/2018 (Lei Geral de Proteção de Dados), que condenou a empresa ré ao pagamento de R$ 23.000.000,00 (vinte e três milhões de reais) a título de dano moral coletivo R$ 500,00 (quinhentos reais) a título de dano moral individual a cada usuário, além da exclusão dos dados coletados ilegalmente, da explicação aos usuários sobre a forma que o consentimento é obtido no processo de adesão ao aplicativo e, ainda, *"Implemente, de forma destacada, com transparência e clareza,ferramenta operacional para obter o consentimento do usuário da plataforma,*

oportunizando ao consumidor que autorize ou não a coleta de dados biométricos"[18].

Em resumo, a LGPD impõe responsabilidades significativas às empresas, e a conformidade não apenas protege dados pessoais, mas também contribui para a construção de confiança na relação entre mercado e consumidor. Portanto, é crucial que as empresas adotem uma abordagem proativa e integrada para a proteção de dados, implementando políticas e práticas robustas para manter uma comunicação transparente com os titulares.

De outra parte, a utilização da tecnologia *blockchain* no âmbito da Administração Pública tem sido discutida por especialista na área, com o objetivo de compatibilizar o uso desta tecnologia com a Lei Geral de Proteção de Dados. Nesse sentido, a *blockchain*, que permite o registro de transações e informações em um sistema seguro e descentralizado, utiliza a criptografia para proteger as informações registradas e validar transações por uma rede descentralizada de participantes.

Dessa forma, ainda que a Lei n° 13.709/2018 seja caracterizada por um modelo centralizador de lidar com a tecnologia e a *blockchain* por um modelo descentralizado, a tecnologia pode ser utilizada a favor do cumprimento da lei, graças à imutabilidade dos registros na rede.

Ainda, de acordo com a empresa BBChain[19] – empresa brasileira especializada em soluções Blockchain para o mercado corporativo –, a utilização da tecnologia também pode auxiliar empresas na adaptação aos padrões exigidos pela LGPD, dando maior transparência ao processo de tratamento de dados e, concomitantemente, facilitando a checagem de dados por auditorias e

---

[18] MARANHÃO. Tribunal de Justiça. **Processo n. 0816292-73.2020.8.10.0001. Ação Civil Coletiva**. Autor: Instituto Brasileiro de Estudo e Defesa das Relações de Consumo - IBEDEC/MA. Réu: Bytedance Brasil Tecnologia Ltda. Juiz: Douglas de Melo Martins. São Luís, 07 mar. 2024. Disponível em: https://pje.tjma.jus.br:443/pje/Processo/ConsultaDocumento/listView.seam. Acesso em: 24/10/2024.

[19] MALAR, João Pedro. **Blockchain pode ajudar empresas na adequação à LGPD e ao ESG; saiba como.** Exame, 20 de março de 2024. Disponível em: https://exame.com/future-of-money/blockchain-pode-ajudar-empresas-na-adequacao-a-lgpd-e-ao-esg-saiba-como/. Acesso em: 31/10/2024.

investidores interessados, com a garantia de que, uma vez inseridos na *blockchain*, as informações seriam imutáveis

Isto posto, o recente estudo divulgado pela *Government Information Quarterly*[20] estabelece que, dentre outros efeitos positivos na sua utilização, a tecnologia *blockchain* contribui para a melhoria da eficácia administrativa, proporcionando o aumento da qualidade dos processos e sistemas, melhor colaboração e comunicação e melhor capacidade de resposta do governo, além da melhor gestão dos recursos públicos.

2.2. Lacunas no Direito

A caracterização de lacunas no direito ultrapassa a mera falta de uma regra jurídica para regular uma situação particular. É crucial examinar a questão da totalidade do sistema legal e as várias visões sobre a presença e o tratamento das falhas, considerando o contexto histórico e social.

A concepção de lacuna como um desafio jurídico emerge da distinção entre o direito e a ciência, intensificando-se no período do direito racional. A partir da Idade Moderna, com a proliferação das normas escritas e a hierarquização das fontes do direito, torna-se imprescindível a elaboração de regras para a integração do ordenamento jurídico. Este problema se consolida com a positivação do direito, a separação dos poderes e a primazia da lei, fatores que contribuem para a compreensão do direito como um sistema normativo estruturado.

---

[20] WAMBA, Samuel Fosso; WAMBA-TAGUIMDJE, Serge-Lopez; LU, Qihui; QUEIROZ, Maciel M. **How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector**. Government Information Quarterly, v. 41, p. 101912, 2024

A teoria do "espaço jurídico vazio", proposta por Bergbohm[21], sustenta que a ausência de norma implica a liberdade de conduta, não configurando uma lacuna, mas sim um limite natural do ordenamento jurídico. Contudo, essa teoria foi objeto de críticas por parte de autores como Norberto Bobbio, que ressaltam a importância da permissão enquanto categoria jurídica relevante.

Para Bobbio[22], a ideia de lacuna é crucial para a compreensão do direito, uma vez que reconhece a dinâmica e a constante necessidade de adaptação do sistema jurídico à complexidade da realidade social. Dessa forma, a existência de mecanismos processuais para suprir a omissão do ordenamento, como a analogia ou os princípios gerais de direito, não nega a existência das lacunas em si. Assim, tem-se que a incompletude constitui uma característica inerente a qualquer ordenamento jurídico. A dinâmica social, caracterizada por suas incessantes transformações e pelo surgimento de novas situações, torna impossível para o legislador prever e regulamentar todas as possíveis relações e conflitos, razão pela qual a utilização da analogia e dos princípios gerais do direito torna-se tão importante para suprir estas lacunas existentes no ordenamento jurídico.

A legislação penal, em especial o Código Penal de 1940, não acompanhou o ritmo acelerado da evolução tecnológica. Essa defasagem resulta em dificuldades na aplicação da lei a crimes digitais, como a falsa identidade virtual, que não se insere de maneira adequada no conceito tradicional de falsa identidade previsto no referido Código. Além disso, crimes informáticos puros, como a interferência em sistemas computacionais, muitas vezes carecem de

---

[21] SOUZA, Luiz Sérgio Fernandes. **Lacunas no direito. Enciclopédia jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Teoria Geral e Filosofia do Direito. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/159/edicao-1/lacunas-no-direito

[22] SOUZA, Luiz Sérgio Fernandes. Lacunas no direito. **Enciclopédia jurídica da PUC-SP.** Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Teoria Geral e Filosofia do Direito. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/159/edicao-1/lacunas-no-direito

tipificação penal apropriada, o que exige uma "subsunção[23] forçada" a tipos penais já existentes, caracterizando as chamadas lacunas ontológicas[24].

No que tange às lacunas axiológicas[25], constata-se que as penas previstas para crimes tradicionais se revelam desproporcionais quando aplicadas aos crimes informáticos, resultando em punições brandas e, por conseguinte, em um cenário de impunidade. A chamada "cifra digital da criminalidade"[26], caracterizada pela subnotificação, agrava ainda mais essa problemática. A ausência de varas especializadas em crimes digitais e a cooperação jurídica internacional, até então limitada, dificultam a efetiva persecução penal.

Para Bitencourt[27], os crimes omissivos – podendo ser próprios ou impróprios – são caracterizados pela conduta do *deixar de fazer*, isto é, o crime comissivo próprio consiste no fato de o agente deixar de realizar determinada conduta, tendo a obrigação jurídica de fazê-lo, enquanto no omissivo impróprio a omissão é o meio pelo qual o agente produz o resultado, no sentido de que, assim, responderá pelo delito que estava obrigado a impedir.

Em contrapartida, os crimes comissivos são caracterizados pelos delitos *de ação*, ou seja, consistem na ação positiva do agente objetivando um resultado ilícito, já previamente tipificado, neste caso, no Código Penal.

Nesse sentido, ainda que a legislação acerca de crimes cibernéticos tenha evoluído e, consequentemente, facilitado a sua persecução, percebe-se que, quando falamos de crimes comissivos, ainda encontramos dificuldade na tipificação destes crimes no ordenamento jurídico brasileiro. Em que pese o

---

[23] GOMES, Milton Carvalho**. O Direito entre fatos e normas: O distanciamento entre a verdade dos fatos e a verdade construída no processo judicial brasileiro**. Revista de Informação Legislativa, Brasília, v. 49, n. 195, p. 231-244, jul./set. 2012.
[24] GARCIA, Gustavo Filipe Barbosa. **Teoria geral do processo**. 3. ed. rev., ampl. e atual. – [S.l.]: Editora Juspodivm, 2023.
[25] GARCIA, Gustavo Filipe Barbosa. **Teoria geral do processo**. 3. ed. rev., ampl. e atual. – [S.l.]: Editora Juspodivm, 2023.
[26] PÁDUA, Vinícius Alexandre. **Edwin H. Sutherland e a Teoria da Associação Diferencia**l Conteudo Juridico, Brasilia-DF: 24 mar 2015, 04:30. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/43623/edwin-h-sutherland-e-a-teoria-da-associacao-diferencial. Acesso em: 31 out 2024.
[27] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. 17. ed. São Paulo: Saraiva, 2012.

advento de leis como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), estas – como aqui demonstrado – se debruçam, em maioria, sobre delitos omissivos.

Dessa maneira, ainda que seja impossível o Direito Penal acompanhar a dinâmica social e, assim, os novos delitos que vão surgindo – como os cibernéticos –, faz-se necessário uma legislação mais robusta e que permita ao operador a melhor aplicação da pena já tipificada, garantindo a eficiência, a celeridade e o devido processo legal.

3. EMPRESAS

3.1. Responsabilidade no tratamento de dados dos usuários

Com o advento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), os preceitos constitucionais de direito à privacidade e à intimidade ganharam materialização, passando a pautar a referida lei e, assim, estabelecer regras de conduta a fim de assegurar os direitos salvaguardados dos usuários da *internet*.

Inspirada na *General Data Protection Regulation* (GDPR), lei europeia correlata e que inspirou a criação da brasileira, a LGPD estabelece diretrizes rigorosas para a coleta, armazenamento e descarte de dados pessoais, impondo novas obrigações às organizações. O descumprimento dessas normas pode resultar em sanções administrativas, inclusive multas, bem como em danos à reputação da empresa.

Em primeiro plano, o *compliance* – que corresponde à adoção de procedimentos internos para estar em conformidade com as leis vigentes no âmbito de atuação da empresa – deve nortear a empresa, em conformidade com o art. 50 da LGPD, à formulação de "*regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos*[28]".

Dessa forma, as empresas devem desenvolver políticas de proteção de dados que estejam em conformidade com os requisitos estabelecidos pela Lei nº 13.709/2018, abrangendo procedimentos específicos para a coleta, utilização, armazenamento e descarte de dados pessoais. Esse processo inclui a implementação de programas de governança de dados que contemplem políticas internas, códigos de conduta, treinamentos e mecanismos de gerenciamento de riscos.

---

[28] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a Proteção de Dados Pessoais. Diário Oficial da União, Brasília-DF, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08/11/2024.

Ademais, as empresas devem adotar medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados e vazamentos, empregando práticas como criptografia e controle de acesso. Em caso de ocorrência de violação de dados, é imperativo que a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados afetados sejam prontamente notificados.

As empresas devem manter, também, uma política de privacidade clara e acessível, especificando detalhadamente as práticas de coleta e tratamento de dados pessoais utilizadas. Além disso, é necessário que estejam aptas a demonstrar conformidade com a LGPD, o que pode envolver a elaboração de relatórios e a realização de auditorias periódicas, nos termos estabelecidos pela mesma norma.

No tocante à relação com os usuários, a obtenção de consentimento é medida que se impõe. O consentimento explícito dos titulares de dados deve ser obtido previamente à coleta e ao processamento de seus dados pessoais, sendo necessário que esse consentimento seja informado, específico e passível de revogação a qualquer momento. Os titulares de dados possuem, por outro lado, direitos assegurados pela legislação, incluindo o acesso, a correção, a eliminação e a portabilidade de seus dados, além do direito de revogar o consentimento concedido.

Ainda, os artigos 42 a 45 da Lei Geral de Proteção de Dados Pessoais (LGPD) constituem um capítulo específico voltado à regulamentação da responsabilidade civil por danos causados aos titulares de dados. Nesse contexto, a disciplina da responsabilidade civil emerge com o propósito de estabelecer fundamentos para situações de lesão imprevista e inevitável, com o objetivo de assegurar a efetiva tutela dos direitos da vítima e a integral reparação dos danos sofridos.

4. REPRESSÃO

4.1. Autoridade Nacional de Proteção de Dados

Criada pela Lei nº 13.853/2019, que alterou a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a Autoridade Nacional de Proteção de Dados surge com o objetivo de garantir a aplicação efetiva das normas de proteção de dados no Brasil, ou seja, compete a ela o dever de zelar pela proteção dos dados pessoais, promover a transparência nas práticas de tratamento de dados e assegurar que as entidades públicas e privadas cumpram as disposições da LGPD.

Nesse sentido, pautada pelos princípios fundamentais norteadores da Lei Geral de Proteção de Dados - finalidade, adequação, transparência, segurança e prevenção -, a ANPD deve publicizar à população as normas e políticas públicas desenvolvidas na matéria de proteção de dados pessoais e as medidas de segurança impostas, além de fiscalizar o correto seguimento, pelas empresas responsáveis pelo tratamento de dados, das normas dispostas na LGPD e aplicar sanções em caso de descumprimento.

O Projeto de Lei nº 53/2018, que deu origem à LGPD, previa a criação da ANPD como uma autarquia em regime especial, vinculada ao Ministério da Justiça e regida pela Lei 9.986/2000 - Lei das Agências Reguladoras, posteriormente revogada devido ao advento da Lei 13.848/2019. No entanto, o presidente da República à época, Michel Temer, vetou a criação do órgão por vício de iniciativa, uma vez que, tratando-se de ente que comporia a estrutura do Poder Executivo, caberia a este poder legislar sobre o tema e criar o referido órgão, tornando o seu texto inconstitucional. Após, a Medida Provisória n° 869/2018, posteriormente convertida na Lei n° 13.853/2019, instituiu a ANPD como um órgão vinculado à Presidência da República, em conformidade com o que estabelecia o artigo 55-A da Lei n° 13.709/2018, mais tarde revogado pela Lei n° 14.460/2022:

> Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República.

Com a transformação da Medida Provisória n° 1.124/2022 na Lei n° 14.460/2022, o artigo 55-A foi revogado, para instituir a natureza jurídica da ANPD, antes de caráter transitório[29], como autarquia em regime especial, conforme disposto no seu corpo legislativo:

> Art. 7º. A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), passa a vigorar com as seguintes alterações:
>
> "Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (...)

Atualmente, por força do Decreto n° 11.401/2023, a ANPD passa a ser vinculada ao Ministério da Justiça e Segurança Pública[30]:

> Artigo único. A vinculação das entidades da administração pública federal indireta é a seguinte:
>
> (...)
>
> XV - ao Ministério da Justiça e Segurança Pública:
>
> a) Conselho Administrativo de Defesa Econômica - Cade; e
>
> b) Autoridade Nacional de Proteção de Dados - ANPD;

---

[29] BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD torna-se autarquia de natureza especia**l. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial. Acesso em: 29/10/2024.

[30] BRASIL. Autoridade Nacional de Proteção de Dados. **Base Jurídica da Estrutura Organizacional e das Competências**. [s.d.]. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica-da-estrutura-organizacional-e-das-competencias. Acesso em: 29/10/2024.

Dessa forma, diversamente às autarquias em sentido estrito, à ANPD - como autarquia em regime especial - é conferido maior grau de autonomia e independência.

Ademais, compete também à Autoridade Nacional de Proteção de Dados a edição de procedimentos a serem seguidos pelas empresas, facilitando a participação destas no processo de fiscalização e, consequentemente, o controle e a fiscalização por parte da autarquia.

É nesse contexto que está inserido o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que corresponde à "*documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco*[31]", estabelecido em meio às competências da ANPD pelo artigo 55-J da Lei n° 13.709/2018:

> Art. 55-J. Compete à ANPD:
>
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

Nesse sentido, a edição de estratégias, regulamentos e procedimentos que facilitem a participação das empresas é medida essencial estabelecida à ANPD para o efetivo cumprimento dos preceitos da Lei Geral de Proteção de Dados. Isto porque a flexibilidade metodológica oferecida pela ANPD facilita a participação das instituições no processo de proteção de dados. Na elaboração de perguntas e respostas[32] no *site* da ANPD, por exemplo, direcionam as instituições para uma elaboração segura do RIPD, aumentando, dessa forma, a eficiência na comunicação entre autarquia e empresa e aprimorando a coleta e

[31] Redação dada de acordo com o Art. 5°, inciso XVII, da Lei n° 13.709/2018.
[32] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 29/10/2024.

proteção dos dados. Ainda, dirigindo-se aos órgãos e às entidades da Administração Pública Federal, o Governo Federal, através do Ministério da Gestão e da Inovação em Serviços Públicos e inspirado em publicações da *Information Commissioner's Office* (ICO) e da Autoridade Nacional de Proteção de Dados (ANPD), criou um Guia/Modelo de elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que pode ser facilmente encontrado em seu sítio eletrônico[33], facilitando a difusão de conhecimentos sobre privacidade e segurança da informação.

Outrossim, em consonância com o disposto no artigo 55-K da Lei 13.709/2018, a ANPD representa o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação:

> Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.
>
> Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.

Dessa forma, ela estabelece entendimentos e pareceres acerca do tema de proteção de dados, detendo competência exclusiva para aplicar as sanções previstas na LGPD e possui, também, caráter terminativo quando na deliberação sobre a interpretação da lei, suas respectivas competências e casos omissos.

Prezando pela publicidade das informações e a correta difusão dos preceitos estabelecidos pela LGPD, a ANPD dispõe em seu site todas as suas publicações, que incluem Atos Normativos, Guias para titulares de dados e instituições, Notas Técnicas, Relatórios e, mais recentemente, Consulta à

[33] O Guia/Modelo pode ser acessado através do link https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_template_ripd.docx.

Sociedade acerca da implementação de Inteligência Artificial (IA) e proteção de dados no Brasil[34].

De outra parte, conforme explicitado no artigo 55-K anteriormente colacionado, também compete à ANPD a imposição de sanções e a aplicação de multas. De acordo com o divulgado no *site* da ANPD, em julho de 2023 a Autoridade Nacional de Proteção de Dados aplicou a primeira multa por descumprimento à LGPD.

No caso, a empresa Telekall Infoservice foi denunciada por divulgar listagem de contatos de WhatsApp de eleitores para fins de disseminação de material de campanha eleitoral, em meio à eleição municipal de 2020, em Ubatuba/SP[35]. Após o regular curso do processo, a ANPD entendeu que a empresa infringiu o artigo 7º da Lei nº 13.709/2018 e o artigo 5º do Regulamento de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD, totalizando duas multas simples no valor de R$ 7.200,00 (sete mil e duzentos reais) por infração, além de advertência por infração ao artigo 41, também da LGPD.

Assim, o artigo 52 da LGPD regulamenta as sanções administrativas a serem aplicadas pela ANPD, além dos critérios a serem seguidos quando da dosimetria da pena a ser imposta à instituição infratora, considerando: (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; (ix) a adoção de política de boas práticas e

---

[34]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD); BANCO DE DESENVOLVIMENTO DA AMÉRICA LATINA E CARIBE (CAF). **Consulta à Sociedade: Sandbox Regulatório de Inteligência Artificial e Proteção de Dados no Brasi**l. Brasília, DF: ANPD; CAF, 2023. Disponível em: https://www.anpd.gov.br/uploads/2023/10/anpd-sandbox-regulatorio-consulta-bilingue.pdf. Acesso em: 29/10/2024.

[35] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). A**NPD aplica a primeira multa por descumprimento à LGPD.** Brasília, DF. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 29/10/2024.

governança; (x) a pronta adoção de medidas corretivas; e (xi) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Isso posto, a Autoridade Nacional de Proteção de Dados desempenha um papel essencial na proteção de dados pessoais no Brasil, promovendo a conformidade com a Lei Geral de Proteção de Dados e garantindo que os direitos dos titulares sejam respeitados. Através de suas funções de regulação, orientação, fiscalização e, consequentemente, de aplicação de sanções, a ANPD busca criar um ambiente de proteção de dados robusto e eficaz, tornando-se fundamental para assegurar a privacidade e a segurança dos dados pessoais e promover uma cultura de proteção de dados tanto no setor público quanto no privado.

4.2. Comparação com a atuação em outros países

4.2.1. Legislação Comparada

Na União Europeia, a lei que trata da proteção de dados é a *General Data Protection Regulation* (GDPR). Publicada em 2016 e vigorando desde 2018, a GDPR 2016/679 se assemelha à LGPD, abrangendo todas as pessoas físicas e jurídicas da União Europeia e Espaço Econômico Europeu e, ainda, a exportação dos dados pessoais fora desses territórios.

Em seu corpo normativo, a GDPR pauta a proteção de dados como direito fundamental, baseando-se no disposto no artigo 8º da Carta dos Direitos Fundamentais da União Europeia:

> Artigo 8º
>
> Proteção de dados pessoais
>
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
>
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito

> de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
>
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Dessa forma, percebe-se a preocupação com a proteção de dados no âmbito europeu, de modo que a Carta dos Direitos Fundamentais da União Europeia, adaptação à Convenção Europeia dos Direitos Humanos (CEDH), já estabelece a importância da proteção e do correto tratamento de seus dados pessoais.

Dando ênfase à GDPR, esta representa a norma correlata à LGPD, uma vez que a norma europeia inspirou a criação da lei no Brasil, assim como em diversos países ao redor do globo. De maneira semelhante à LGPD, a GDPR surge com natureza regulatória, abrangendo empresas que operam no território europeu, sediadas ou não na Europa.

Na América Latina, entretanto, o desenvolvimento das leis de proteção de dados não seguiu a uniformidade apresentada na regra europeia. Enquanto alguns países têm normas de proteção de dados de longa data - como é o exemplo da Argentina e do Chile, com leis de proteção de dados que vigoram há mais de vinte anos - outros têm legislação promulgada recentemente, como é o caso do Brasil.

Tomando como exemplo a lei chilena, esta - do mesmo modo da LGPD - mostra-se adequada aos padrões da GDPR, com similitude de princípios norteadores e, para além disso, o direito dos titulares de pleitear indenização por danos em caso de descumprimento.

No que concerne a figura da autoridade supervisora, a GDPR prevê a criação de autoridades supervisoras, que devem agir com total independência no desempenho das suas funções:

Em que pese a presença da figura da autoridade supervisora no ordenamento jurídico brasileiro através da Autoridade Nacional de Proteção de Dados, o chileno não encontra a obrigatoriedade desta figura fiscalizadora, sendo as práticas aqui estabelecidas como de competência da ANPD, descentralizadas em território chileno[36].

4.2.2. Atuação dos órgãos fiscalizadores

Seguindo o exemplo do Chile, como a legislação não estabelece a criação de uma autoridade supervisora responsável pela proteção de dados pessoais e pelo cumprimento das leis de proteção de dados, as competências estabelecidas a estas figuras em outros ordenamentos - como as da ANPD no Brasil - encontram-se descentralizadas.

Desse modo, o SERNAC (*Servicio Nacional del Consumidor*) tem autoridade para supervisionar e auditar instituições que tratam os dados pessoais dos consumidores. Contudo, ao contrário de instituições dotadas de autonomia como a ANPD, o SERNAC não possui autoridade para impor sanções às instituições infratoras, restando para os titulares dos dados pleitearem seus direitos no judiciário, seja na compensação por danos sofridos ou falha no tratamento de dados[37].

No caso europeu, a GDPR prevê, no artigo 51 acima colacionado, a criação de autoridades supervisoras, que deverão funcionar de forma independente, característica esta que se estende a seus membros, não devendo existir quaisquer influências externas ao exercício de suas funções.

---

[36] ALENCAR, Amanda de Sousa. **Proteção de dados pessoais no Brasil e no Chile: Uma análise comparativa sob a perspectiva da decisão de adequação da Comissão Europeia**. Disponível em: https://observatoriolgpd.com/2020/08/15/artigo-protecao-de-dados-pessoais-no-brasil-e-no-chile-uma-analise-comparativa-sob-a-perspectiva-da-decisao-de-adequacao-da-comissao-europeia/. 2020.

[37] LEFOSSE ADVOGADOS. LILLA, Paulo; SEGALA, Carla (Coord.). **What you need to know about data protection in Latin America**. p. 29-37. 2024.

Nesse contexto, as *Data Protection Authorities* (DPA) se estabelecem como autoridades públicas independentes que controlam, através de poderes de investigação e de correção, a aplicação da legislação relativa à proteção de dados[38]. Aliás, foi inspirado no modelo das DPAs, que já existiam muito antes, que se deu a criação da ANPD. Dessa forma, o fortalecimento das DPAs como figuras intervencionistas consolidou um novo modelo no âmbito da proteção de dados.

[38] COMISSÃO EUROPEIA. **O que são autoridades de proteção de dados (APD)?**. Disponível em: https://commission.europa.eu/index_pt. Acesso em: 30/10/2024.

5. CONSIDERAÇÕES FINAIS

No presente trabalho, foi objeto de análise a evolução da legislação brasileira relativa à internet e à proteção de dados pessoais, evidenciando-se um avanço substancial na garantia da privacidade e segurança no ambiente digital. A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representou a primeira resposta legislativa à vulnerabilidade dos usuários da internet, ao tipificar crimes cibernéticos. Por sua vez, o Marco Civil da Internet (Lei nº 12.965/2014) procurou assegurar o equilíbrio entre os direitos fundamentais dos usuários, como a liberdade de expressão e a proteção da privacidade, ao mesmo tempo em que impôs responsabilidades aos provedores de serviços de internet. A Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018), em contrapartida, estabeleceu diretrizes claras para o tratamento de dados pessoais, incluindo dispositivos sobre a obtenção de consentimento, requisitos de segurança da informação e direitos dos titulares dos dados pessoais.

No entanto, é possível observar que a legislação brasileira ainda apresenta lacunas significativas, notadamente no que se refere à tipificação dos crimes cibernéticos, à criminalização de condutas específicas e à dosimetria das penas. A defasagem entre a legislação penal e a rápida evolução das tecnologias exige uma atualização contínua do arcabouço legislativo, a fim de assegurar uma efetiva proteção dos dados pessoais e a imposição de punições adequadas aos crimes no ambiente digital.

A crescente utilização de novas tecnologias, como *deepfakes* e *blockchain*, tem gerado desafios adicionais para a legislação brasileira. A ausência de normas específicas para o tratamento das *deepfakes* impõe ao Poder Judiciário a necessidade de recorrer a tipos penais preexistentes, o que pode resultar em punições desproporcionais ou inadequadas. A tecnologia *blockchain*, no entanto, apresenta um potencial significativo para o fortalecimento da segurança e transparência no tratamento de dados pessoais, podendo, inclusive, colaborar para o cumprimento da LGPD.

Neste prisma, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel essencial na proteção de dados pessoais no Brasil, sendo responsável por promover a conformidade com a LGPD e garantir os direitos dos titulares de dados. A atuação da ANPD abrange a emissão de normas e diretrizes, a fiscalização do cumprimento da legislação e a aplicação de sanções em caso de infrações.

A comparação com a legislação e as práticas de fiscalização adotadas por outros países, como a GDPR (Regulamento Geral de Proteção de Dados) da União Europeia e a legislação chilena, revela diferentes abordagens para a proteção de dados pessoais. A GDPR, por exemplo, serviu de inspiração para a criação da LGPD e para a elaboração de legislações semelhantes em outros países. No caso do Chile, a legislação vigente não prevê a criação de uma autoridade supervisora específica, delegando as funções de fiscalização a diferentes órgãos.

Em síntese, a legislação brasileira no âmbito da proteção de dados pessoais evoluiu de forma significativa nos últimos anos, mas ainda enfrenta desafios substanciais para se adaptar à constante evolução tecnológica. Torna-se, portanto, imprescindível a atualização contínua do marco normativo, a atuação eficaz da ANPD e a cooperação internacional, a fim de garantir a proteção dos dados pessoais e enfrentar adequadamente os desafios no ambiente digital.

6. REFERÊNCIAS BIBLIOGRÁFICAS

MINISTÉRIO PÚBLICO FEDERAL (MPF). **Justiça determina indenização de R$ 15 mil a cidadãos que tiveram dados pessoais vazados em 2022**. São Paulo, 20 set. 2023. Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias/justica-determina-indenizacao-de-r-15-mil-a-cidadaos-que-tiveram-dados-pessoais-vazados-em-2022. Acesso em: 29/08/2024.

BRASIL. Supremo Tribunal Federal. Tema 987 - **Discussão sobre a constitucionalidade do art. 19 da Lei n. 12.965/2014 que determina a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros**. Brasília, DF. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5871934. Acesso em: 02/10/2024.

SARLET, Ingo Wolfgang; Bittencourt Siqueira de, Andressa. **Liberdade de expressão e seus limites numa democracia: o caso das assim chamadas "fake news" nas redes sociais em período eleitoral no Brasil**. REVISTA ESTUDOS INSTITUCIONAIS, v. 6, n. 2, p. 545, 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

SÃO PAULO. Processo nº 1017477-41.2014.8.26.0224. **Indenização por Dano Moral**. Autor: Enrique Teixeira Garcia. Réu: Leonardo Alexandre Braga da Silva e outros. Juíza: Larissa Boni Valieris. Guarulhos, 09 de agosto de 2022.

BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Deepfake e inteligência artificial: saiba o que pode e o que é proibido nas campanhas eleitorais**. Brasília, DF, 20 jun. 2024. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr2/2024/deepfake-e-inteligencia-artificial-saiba-o-que-pode-e-o-que-e-proibido-nas-campanhas-eleitorais. Acesso em: 10/10/2024.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 27 de fevereiro de 2024. **Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitora**l. Diário da Justiça Eletrônico do Tribunal Superior Eleitoral, Brasília, DF, v. 29, p. 132-145, 4 mar. 2024. Seção de Legislação.

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].

DISTRITO FEDERAL. **Petição 12.404**. Relator: MIN. ALEXANDRE DE MORAES.

GARBACCIO, Grace Ladeira; KISCHELEWSKI, Flávia Lubieska N. **Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da accountability**. Revista Brasileira de Estudos Políticos, v. 128, 2024.

BRASIL. Conselho Nacional de Justiça. Provimento n. 134, de 24 de agosto de 2022. **Estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à Lei Geral de Proteção de Dados Pessoais**. Brasília, 2022. Disponível em: https://atos.cnj.jus.br/files/original141307202208256307837 3a0892.pdf. Acesso em: 18/10/2024.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 23/10/2024.

BRASIL. Tribunal de Contas da União. Secretaria-Geral de Controle Externo. Secretaria de Fiscalização de Governança e Tecnologia da Informação. **Auditoria sobre LGPD**. Brasília: TCU, 2024. Disponível em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd/. Acesso em: 23/10/2024.

BELO, Alcindo Antonio Amorim Batista. **Fiscalizar é preciso**. Revista do Tribunal de Contas da União, Brasília, n. 115, p. 7-16, maio/ago. 2009.

MARANHÃO. Tribunal de Justiça. **Processo n. 0816292-73.2020.8.10.0001. Ação Civil Coletiva**. Autor: Instituto Brasileiro de Estudo e Defesa das Relações de Consumo - IBEDEC/MA. Réu: Bytedance Brasil Tecnologia Ltda. Juiz: Douglas de Melo Martins. São Luís, 07 mar. 2024. Disponível em: https://pje.tjma.jus.br:443/pje/Processo/ConsultaDocumento/listView.seam. Acesso em: 24/10/2024.

MALAR, João Pedro. **Blockchain pode ajudar empresas na adequação à LGPD e ao ESG; saiba como.** Exame, 20 de março de 2024. Disponível em: https://exame.com/future-of-money/blockchain-pode-ajudar-empresas-na-adequacao-a-lgpd-e-ao-esg-saiba-como/. Acesso em: 31/10/2024.

WAMBA, Samuel Fosso; WAMBA-TAGUIMDJE, Serge-Lopez; LU, Qihui; QUEIROZ, Maciel M. **How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector**. Government Information Quarterly, v. 41, p. 101912, 2024

SOUZA, Luiz Sérgio Fernandes. **Lacunas no direito. Enciclopédia jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Teoria Geral e Filosofia do Direito. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/159/edicao-1/lacunas-no-direito

GOMES, Milton Carvalho**. O Direito entre fatos e normas: O distanciamento entre a verdade dos fatos e a verdade construída no processo judicial brasileiro**. Revista de Informação Legislativa, Brasília, v. 49, n. 195, p. 231-244, jul./set. 2012.

GARCIA, Gustavo Filipe Barbosa. **Teoria geral do processo**. 3. ed. rev., ampl. e atual. – [S.l.]: Editora Juspodivm, 2023.

PÁDUA, Vinícius Alexandre. **Edwin H. Sutherland e a Teoria da Associação Diferencia**l Conteudo Juridico, Brasilia-DF: 24 mar 2015, 04:30. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/43623/edwin-h-sutherland-e-a-teoria-da-associacao-diferencial. Acesso em: 31 out 2024.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. 17. ed. São Paulo: Saraiva, 2012.

BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD torna-se autarquia de natureza especia**l. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial. Acesso em: 29/10/2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Base Jurídica da Estrutura Organizacional e das Competências**. [s.d.]. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica-da-estrutura-organizacional-e-das-competencias. Acesso em: 29/10/2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD); BANCO DE DESENVOLVIMENTO DA AMÉRICA LATINA E CARIBE (CAF). **Consulta à Sociedade: Sandbox Regulatório de Inteligência Artificial e Proteção de Dados no Brasi**l. Brasília, DF: ANPD; CAF, 2023. Disponível em:

https://www.anpd.gov.br/uploads/2023/10/anpd-sandbox-regulatorio-consulta-bilingue.pdf. Acesso em: 29/10/2024.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). A**NPD aplica a primeira multa por descumprimento à LGPD.** Brasília, DF. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 29/10/2024.

ALENCAR, Amanda de Sousa. **Proteção de dados pessoais no Brasil e no Chile: Uma análise comparativa sob a perspectiva da decisão de adequação da Comissão Europeia**. Disponível em: https://observatoriolgpd.com/2020/08/15/artigo-protecao-de-dados-pessoais-no-brasil-e-no-chile-uma-analise-comparativa-sob-a-perspectiva-da-decisao-de-adequacao-da-comissao-europeia/. 2020.

LEFOSSE ADVOGADOS. LILLA, Paulo; SEGALA, Carla (Coord.). **What you need to know about data protection in Latin America**. p. 29-37. 2024.

COMISSÃO EUROPEIA. **O que são autoridades de proteção de dados (APD)?**. Disponível em: https://commission.europa.eu/index_pt. Acesso em: 30/10/2024.