doi.org/10.51891/rease.v10i11.17054

CONSEQUÊNCIAS JURÍDICAS DA LGPD PARA OS CRIMES VIRTUAIS

Alisson Santana Damião[1]
Thyara Gonçalves Novais[2]

RESUMO: O presente trabalho discute como a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil tem impactado a investigação e a punição de crimes virtuais, considerando os novos desafios e exigências legais relacionadas à proteção de dados pessoais. Teve como objetivos explorar as implicações desta lei para indivíduos e organizações envolvidos em crimes virtuais, incluindo multas, responsabilidades e ações penais, e, especificamente, avaliar se essa lei proporcionou uma melhor proteção aos dados dos usuários em relação à prevenção e investigação de crimes virtuais, analisar a eficácia das sanções e penalidades da LGPD em relação a indivíduos e organizações envolvidos em atividades criminosas online, identificar lacunas na legislação ou desafios práticos que surgiram na aplicação da Lei de Proteção de Dados para crimes virtuais e propor possíveis soluções, e recomendar as boas práticas para lidar com crimes virtuais dentro do quadro legal da LGPD, visando proteger os direitos individuais, sem comprometer a eficácia das investigações. A metodologia utilizada foi através da pesquisa exploratória, utilizando-se a fonte de informação da pesquisa bibliográfica, com abordagem qualitativa. Os dados foram coletados por meio do levantamento de entendimentos doutrinários, análises de Leis, Normas Gerais e, principalmente, através dos recortes necessários ao balizamento do tema em questão. Tudo isso buscando responder às questões de que, ainda que existam leis, doutrinas e jurisprudências que disciplinam o assunto, na prática há muita controvérsia, pois o assunto é relativamente novo, demandando do ordenamento jurídico brasileiro novas formas de lidar e resolver as questões. Com isso, esperou-se como resultado dessa discussão, a real efetivação dos preceitos trazidos pela norma em destaque, bem como a investigação e resolução dos delitos em sede virtual.

Palavras-chave: Direito Digital. Lei Geral de Proteção de Dados. Crimes Virtuais. Punição.

1 INTRODUÇÃO

O Direito Digital emergiu como uma área essencial do Direito na atualidade, adaptando-se às novas realidades impostas pela crescente digitalização da sociedade. Dessa forma, ele se fragmenta e se especializa em campos específicos, e, em meio a essa evolução, os crimes virtuais se tornaram uma das maiores preocupações, tanto para legisladores quanto para o Judiciário.

Assim, tornou-se necessário enfrentar as condutas ilícitas praticadas no ambiente digital, seja por meio de ações preventivas ou punitivas, além de destacar os direitos de liberdade e privacidade dos usuários desse meio. Não obstante, a legislação atual ainda enfatiza

[1]Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.
[2]Mestre docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia.

os deveres e garantias atribuídos àqueles que têm a responsabilidade de proteger o fluxo de informações e assegurar a segurança contra os violadores da integridade da pessoa humana no espaço cibernético.

Com isso, o Direito passa a concentrar-se no universo virtual, buscando tanto aplicar as leis existentes quanto criar normas que regulam a vida online. Porém, diante das leis, doutrinas e jurisprudências que disciplinam o assunto e o especificam, o presente trabalho visou responder ao seguinte questionamento: a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil tem impactado a investigação e a punição de crimes virtuais, considerando os novos desafios e exigências legais relacionadas à proteção de dados pessoais?

Nesse sentido, ainda que existam leis, doutrinas e jurisprudências que o disciplinam, na prática há muita controvérsia, pois o assunto é relativamente novo, demandando do ordenamento jurídico brasileiro novas formas de lidar e resolver as questões. Evidencia-se que o principal desafio reside na efetivação da Justiça, onde ocorre a classificação de diversos delitos praticados *online*; conquanto, nota-se uma legislação inadequada para coibir essas condutas, não existindo uma lei particular para lidar com o crime virtual no Brasil.

Deste modo, este artigo realizou uma análise teórica sobre a evolução histórica e a aplicação prática do direito no contexto tecnológico, objetivando a avaliação se a LGPD proporcionou uma melhor proteção aos dados dos usuários em relação à prevenção e investigação de crimes virtuais; análise da eficácia das sanções e penalidades dessa lei em relação a indivíduos e organizações envolvidos em atividades criminosas *online*; identificação de lacunas na legislação ou desafios práticos que surgiram na aplicação da Lei de proteção de dados para crimes virtuais e promoção de possíveis soluções; recomendações de boas práticas para lidar com crimes virtuais dentro do quadro legal, visando proteger os direitos individuais, sem comprometer a eficácia das investigações.

Trata-se de um tema de grande atualidade, em vista de que o avanço na tecnologia trouxe problemas que a legislação brasileira precisou se atualizar para poder resolver as celeumas oriundas do meio digital. Além disso, há evidente relevância social, posto que interessa à grande parcela da comunidade o conhecimento dos seus direitos e os limites legais, sob o crivo da proteção do indivíduo.

A revisão bibliográfica foi realizada mediante leitura sistemática, resumos e resenhas, fichamentos, ressaltando os pontos abordados pelos autores que sejam pertinentes ao assunto em questão, tais como: manuais, estudos, críticas jurídicas e materiais didáticos que tratam da

temática, além de consulta a artigos científicos em sítios da *internet*; sempre balizados pelas leis que chancelam o tema em questão, em um lapso temporal dos últimos dez anos, período da efervescência da discussão dessa temática.

O objetivo deste artigo foi analisar, criticamente, as publicações existentes sobre direito digital, com foco específico em como as normas jurídicas têm evoluído para lidar com os desafios impostos pelos crimes virtuais, buscando identificar tendências, lacunas e possíveis soluções.

Este artigo está, didaticamente, dividido em quatro capítulos. No primeiro capítulo, apresenta-se um comentário à Lei nº. 13.709; o segundo, intitulado "Panorama Geral da LGPD" traz um panorama da lei em questão; no capítulo seguinte, aborda-se a temática dos crimes virtuais; no quarto capítulo, cerne desse trabalho, trata das consequências jurídicas da LGPD para os crimes virtuais; e, por fim, nas considerações finais, argumenta-se sobre os desafios sociais do pós-lei.

2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

A Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (com sigla LGPD), é a lei brasileira aprovada no ano de 2018, que disciplina a privacidade e o uso/tratamento de dados pessoais, e que, também, alterou os artigos 7º e 16º do Marco Civil da Internet (Brasil, 2024).

O Brasil passou a fazer parte dos países que contam com uma legislação específica para a proteção de dados e da privacidade dos seus cidadãos. Outros regramentos similares à LGPD do Brasil são o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia (UE), que passou a ser obrigatório em 25 de maio de 2018 e aplicável a todos os países-membros, e o *California Consumer Privacy Act of* 2018 (CCPA) dos Estados Unidos da América, implementado através de uma iniciativa em âmbito estadual, na Califórnia, aprovado no dia 28 de junho de 2018 (AB 375).

Para Pinheiro (2018), no seu tratado sobre a "Proteção de dados Pessoais: comentários à Lei nº. 13.709/2018" assinala que:

> A legislação se fundamenta em diversos valores, como o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, opinião, informação e, comunicação; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos de liberdade e dignidade das pessoas (Pinheiro, 2018, p. 12).

Essa Lei trouxe consigo um rol de novos conceitos jurídicos, como por exemplo "dados pessoais sensíveis", e suscitou procedimentos para o tratamento de dados pessoais, estabeleceu direitos para os titulares dos dados, gerou deveres para os controladores desses dados e criou uma gama de mecanismos legais para que tivesse um maior cuidado com o tratamento desses dados e, consequentemente, compartilhamento com terceiros. Nesse sentido, toda informação que tenha como temática questões como etnia, religião, opinião política, posicionamento filosófico, filiação a sindicato, referente à saúde, à vida sexual, genética, estarão adstritos a uma pessoa natural (Pinheiro, 2018, p. 13).

A Lei nº. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas, quanto para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Nesse diapasão, Teixeira (2020) discute que essa lei "é uma legislação extremamente técnica, que reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas cujo lastro se funda na proteção dos direitos humanos" e amplia a discussão:

> O prazo inicial estabelecido para adaptação às novas regras foi de dezoito meses, tanto para a iniciativa pública como para a privada, considerando qualquer porte e segmento de mercado e a necessidade de atender às exigências de forma eficiente e sustentável, atingindo um nível de proteção de dados inclusive em âmbito internacional quando há tratamento do dado fora do Brasil. Findo esse prazo, poderão, então, ser aplicadas as penalidades previstas, consideradas elevadas, seguindo a mesma tendência das demais regulamentações sobre a mesma matéria em outros países, inspirada, especialmente, pelo Regulamento Europeu de Proteção de Dados Pessoais, também conhecido como GDPR (Teixeira, 2020, p. 36).

Para os estudiosos nessa temática, o espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis (Pinheiro, 2018, p. 14).

O motivo inspirador do surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma

dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização. Desse modo, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948.

Nos comentários de Pinheiro (2018, p. 14) à Lei nº. 13.709, "a base desse pacto é a liberdade, mas o fiel da balança é a transparência". Sendo assim, as leis sobre proteção de dados pessoais têm uma característica muito peculiar de redação principiológica e de amarração com indicadores mais assertivos, de ordem técnica, que permitam auferir de forma auditável se o compromisso está sendo cumprido, por meio da análise de trilhas de auditoria e da implementação de uma série de itens de controle para uma melhor governança dos dados pessoais.

Quanto ao aspecto histórico desta lei, Pinheiro (2018) assevera:

> A liderança do debate sobre o tema surgiu na União Europeia (UE), em especial com o partido The Greens, e se consolidou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão "free data flow". O Regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades (Pinheiro, 2018, p. 15).

Este Regulamento (GDPR), por sua vez, ocasionou um "efeito dominó", visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar (Pinheiro, 2018, p. 15).

O supradito regulamento tem como objetivo: a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas; b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de

dados pessoais no mercado interno; c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo; d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros (Teixeira, 2020, p. 37).

Destaque-se que a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia; no Brasil, já tinha previsão no Marco Civil da Internet e na Lei do Cadastro Positivo, mas a questão ainda era, muitas vezes, observada de forma difusa e sem objetividade no tocante aos critérios que serão considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizentes.

A Lei nº. 13.709/2018 está dividida em 10 Capítulos, com 65 artigos. Comparativamente, ela é mais enxuta do que a sua referência europeia (GDPR), que possui 11 Capítulos, com 99 artigos. Portanto, a versão nacional é mais enxuta e em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço para subjetividade onde deveria ter sido mais assertiva. Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê "prazo razoável".

Além disso, houve o veto presidencial no tocante à criação da Autoridade Nacional de Proteção de Dados Pessoais e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. O veto à criação da ANPD gera uma lacuna inicial estruturante no projeto de implementação da nova regulamentação no país, além de não permitir que o Brasil receba o reconhecimento por parte da União Europeia de legislação de mesmo nível do GDPR, pois um dos requisitos é a existência de uma autoridade nacional de fiscalização independente, o que pode não apenas dificultar a aplicação e fiscalização das medidas propostas, mas também criar um entrave nas relações comerciais para o Brasil.

Por certo, há a possibilidade de a fiscalização ocorrer por intermédio dos agentes legitimados para tanto, como o Ministério Público; no entanto, isso pode gerar alguns entraves, visto que a matéria é nova e de ordem técnica elevada, e a centralização do diálogo com um

único órgão central fiscalizador facilitaria sobremaneira os avanços na implementação das novas exigências, visto que o órgão foi pensado para garantir o cumprimento e o melhor proveito da regulamentação, por meio de normas complementares, pareceres técnicos e procedimentos de inspeção, devendo concentrar ali uma equipe treinada para tanto.

Ainda que seja por uma boa causa, a implementação da conformidade à LGPD trará um impacto grande nas instituições, podendo contribuir para o aumento do "custo Brasil", especialmente nos setores de Startups, pequenas empresas e no setor público, com especial atenção aos que tratam muitos dados pessoais sensíveis, como os de saúde.

Nesse lamiré, conceitos e terminologias trazidos pela lei são fundamentais e devem ser objeto de harmonização em documentos, com especial atenção às políticas, às normas, aos procedimentos e aos contratos. Consoante Teixeira (2020):

• **Titular**: Pessoa a quem se referem os dados pessoais que são objeto de algum tratamento.

• **Tratamento dos dados**: Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

• **Dados pessoais**: Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

• **Dados pessoais sensíveis**: São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

• **Dados anonimizados**: São os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.

• **Anonimização**: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

• **Consentimento**: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Não é o único motivo que autoriza o tratamento de dados, mas apenas uma das hipóteses.

• **Agentes de tratamento**: O controlador que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal.

• **Encarregado**: Pessoa natural, indicada pelo controlado, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.

• **Transferência internacional de dados**: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. (Teixeira, 2020, p. 38)

De acordo com Pinheiro (2018), os Princípios que guiam o tratamento de dados pessoais previstos na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) são os seguintes: Princípio da boa-fé, Princípio da finalidade, Princípio da adequação, Princípio da necessidade, Princípio do livre acesso, Princípio da qualidade dos dados, Princípio da transparência, Princípio da segurança, Princípio da prevenção, Princípio da não discriminação, e Princípio da responsabilização e prestação de contas (Pinheiro, 2018, p. 18).

Essa lei traz no seu bojo sanções administrativas para o caso de descumprimento dela e estão previstas no artigo 52. De acordo com a Lei, instalada no sítio do governo, são elas: [1] **Advertência**, com indicação de prazo para adoção de medidas corretivas; [2] **Multa simples**, de até 2% do faturamento líquido da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 por infração; [3] **Multa diária;** [4] **Publicização da infração** após devidamente apurada e confirmada a sua ocorrência; [5] **Bloqueio dos dados pessoais** envolvidos na infração até a sua regularização; [6] **Eliminação dos dados pessoais** envolvidos na infração; [7] **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; [8] **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; e [9] **Proibição parcial ou total** do exercício de atividades relacionadas a tratamento de dados (Brasil, 2024, p. 10).

Se não representa mérito por ser uma obrigação estatal, a LGPD caracterizou-se por ser um avanço na segurança de dados pessoais, pois padronizou procedimentos para a proteção das informações relacionadas à pessoa física. Houve sérias transformações sociais, com a aprovação dessa lei, seja no âmbito organizacional, seja na maneira com que as empresas passaram a tratar os dados pessoais. A partir daí, passou a exigir a forma correta para tal tratamento, urgindo a necessidade da revisão dos processos de administração e segurança das informações.

Para a coleta e tratamento desses dados, é preciso que a pessoa com direitos sobre eles manifeste consentimento sobre a sua utilização. Essa anuência deve ser fornecida somente após esse titular ter sido devidamente informado acerca dos termos de uso, das extensões da autorização e da necessidade da sua aquisição; com exceção das situações em que o uso das informações seja indispensável para o cumprimento de alguma obrigação legal ou execução de políticas públicas baseadas em lei. Para além disso, dá ao cidadão a supervisão sobre os seus dados e a garantia do direito de solicitar que se excluam os seus dados e o cancelamento do consentimento manifestado, dando-lhe o livre arbítrio tanto de controlar seus dados, quanto de punir os responsáveis por uso indevido e nocivo dos seus dados.

Para fiscalizar a segurança dos dados por parte das pessoas jurídicas, foi criada a "Autoridade Nacional de Proteção de Dados (ANPD)", órgão responsável para verificar se a conduta condiz com o que está disciplinado em lei. Ademais, é o órgão responsável pela regulamentação e orientação preventiva sobre como realizar a aplicação da Lei Geral de Proteção de Dados. Então, é essa autoridade quem dispara os alertas e as orientações às organizações antes de aplicar as punições, que serão definidas de acordo com a gravidade do erro cometido (Pinheiro, 2018, p.19).

Ainda nesse tocante, Pinheiro (2018) afirma que:

> Além da ANPD, a lei também conta com os agentes de tratamento de dados, sendo eles: **agente controlador**, responsável pelas decisões sobre o tratamento; **agente operador**, que executa o tratamento conforme definido pelo controlador; e **agente encarregado**, cuja função é a interação com os cidadãos e a autoridade nacional, o qual poderá não existir dependendo do porte organizacional (Pinheiro, 2018, p. 19). [grifo nosso]

Finalmente, existe um trâmite no processo de administração de riscos e falhas, que se caracteriza pela necessidade de definir medidas preventivas de segurança, adotar boas certificações do mercado, realizar auditorias, elaborar planos de contingência, e apresentar resoluções ágeis perante incidente, ao que Pinheiro (2018, p. 19) suscitou que "no caso de

vazamento de dados, a empresa deverá imediatamente informar à ANPD e os titulares afetados".

3 PANORAMA GERAL DA LGPD: AVANÇOS

O Direito Digital constitui a progressão intrínseca do Direito, englobando todas as suas vertentes, sejam elas cível, penal, consumerista, processual, etc. Conforme aponta Patrícia Peck Pinheiro (2021), o Direito Digital é a evolução do próprio Direito e abrange "todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas". Em especial, das complexidades da designada "Era Digital" emergem modalidades delitivas diferentes das presenciadas à época em que a legislação visou combater - urgindo um novo *modus operandi*.

No contexto do aumento exponencial da utilização dos meios informáticos e dispositivos conectados, surge uma multiplicidade de disputas que a lei precisa resolver, além de ocorrências criminais cometidas através da *internet*. Dessa forma, há de se conceituar crimes cibernéticos, conforme descrito por Kunrath (2017), "caracterizado como uma ação na qual o infrator é aquele que pratica uma conduta ilícita com uma intenção negligente, ou realiza uma transgressão dolosa dentro do âmbito de um delito virtual". Os transgressores digitais podem ser delinquentes motivados, *hackers* coordenados, colaboradores insatisfeitos, ou terroristas digitais.

Nesse ensejo, muitas nações enfrentam a obrigação de criar legislação para controlar o manuseio, disponibilidade, e acessibilidade dos ativos considerados hoje como valiosos e alvo da ação criminosa: os dados individuais e as informações; surgindo, assim, no Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018). Com a promulgação das diretrizes estabelecidas pela LGPD, empresas e/ou entidades encontraram-se confrontadas com a necessidade de se conformar com precisão às regulamentações para a concretização do processamento de dados, visando salvaguardar os direitos essenciais de confidencialidade, moralidade, autonomia e transparência.

No entanto, as instituições (tanto públicas quanto privadas), em certo ponto, necessitam da adoção de um plano que esteja em conformidade com a lei, fato este que se apresenta de forma ineficaz na atualidade, advindo a problemática. No tocante à implementação e à interpretação da Lei nº 13.709/18 - LGPD, visando prevenir a discriminação,

certos registros necessitam de um maior nível de proteção, especialmente no que concerne aos dados delicados. Estes dados são especificados como aqueles contendo informações e/ou categorias que possibilitam a identificação do indivíduo, conforme estipulado no artigo 5º, parágrafo 1º, da referida lei, tais como "origem étnica ou racial, crença religiosa, visão política, filiação sindical ou a grupo religioso, filosófico ou político, dados relacionados à saúde ou vida sexual, informação genética ou biométrica, quando ligada a uma pessoa física".

Nesse âmbito da avaliação de proteção de dados dos usuários, a esfera digital oferece uma variedade de recursos destinados a garantir esse procedimento de aquisição de informações em conformidade com os regulamentos estabelecidos pela LGPD. Então, garantindo através de práticas internas e diretrizes de confidencialidade todas e quaisquer operações que requeiram a utilização de dados. Este é o período em que as corporações e entidades precisam estar em consonância com os princípios da lei, sendo esta conformidade em breve uma exigência.

Esta legislação apresenta vantagens para as corporações e organizações, ao contemplar a previsão, atualização e eventualmente a revisão de suas práticas dentro da Lei Geral de Proteção de Dados Pessoais - LGPD, a fim de sugerir alterações visando à confiabilidade e ao reforço de suas iniciativas.

Entretanto, conforme se percebe, atualmente, os dados dos usuários ainda se encontram à mercê das vulnerabilidades. A título de exemplo, no campo do Direito, percebe-se até um aumento nos volumes de processos envolvendo essa seara:

> APELAÇÃO. VAZAMENTO DE DADOS PESSOAIS. RELAÇÃO DE CONSUMO. RISCO DO EMPREENDIMENTO. LEI GERAL DE PROTEÇÃO DE DADOS. DANOS MORAIS. A sentença condenou a ré a pagar R$10.000,00 de indenização por danos morais. Apelo do réu. Falha do serviço comprovada. Dever de proteção dos dados pessoais. Lei 13.709/18. Ataque de hacker que se insere no risco do empreendimento. Dano moral configurado. Verba que não comporta redução. Acesso aos dados que não poderão ser revertidos. Dados pessoais não anonimizados. Súmula 343 desta Corte. Recurso desprovido.
>
> (TJ-RJ - APL: XXXXX20208190002, Relator: Des(a). NATACHA NASCIMENTO GOMES TOSTES GONÇALVES DE OLIVEIRA, Data de Julgamento: 03/02/2022, VIGÉSIMA SEXTA CÂMARA CÍVEL, Data de Publicação: 04/02/2022)

Apesar da importância em encontrar um equilíbrio entre preservar a privacidade das pessoas e combater de forma eficaz os delitos virtuais; garantir a aplicação das leis por meio de supervisão e fiscalização competentes; e promover a educação e sensibilização para fortalecer a segurança na era digital, a transgressão da LGPD pode acarretar sérias ramificações legais. No

que tange às sanções, a norma exibe uma série de penalidades como meio de garantir potenciais infrações das normas estipuladas na seção I do capítulo VIII, conforme o artigo 52, tais como: advertência; multa; bloqueio e eliminação dos dados; suspensão e proibição da atividade; entre outros (Teixeira, 2020, p. 11).

Logo, com o objetivo de garantir a integridade dessas informações, a LGPD estabeleceu medidas legais e penalidades que devem ser impostas pela distorção de seu propósito ou pela sua má utilização na oferta de serviços, sejam eles educacionais ou comerciais. Isso evidencia a importância de ser preciso ao lidar com a segurança e o manuseio de dados conforme delineado pelas diretrizes da Lei. Não obstante, a legislação concede aos indivíduos o direito de entender de que maneira seus dados estão sendo coletados e processados, assim como o direito de requerer a exclusão ou retificação dos mesmos. Contudo, sem a adequada conformidade com a LGPD, as pessoas podem ter seus dados coletados sem autorização ou empregados para finalidades não legalmente autorizadas (Teixeira, 2023, p. 12).

Ademais, sob a égide dos desafios e lacunas que permeiam a aplicação das diretrizes da referida lei, apesar das diretrizes contidas na LGPD serem cruciais para resguardar informações individuais, identificar os perpetradores de delitos *online* apresenta um desafio monumental. Somados a isso, os embates potenciais entre a LGPD e outras legislações voltadas aos crimes cibernéticos ampliam a complexidade na contenção dessas transgressões, no que tange ao conflito de competência das normas. Por último, a constante atualização da LGPD e a incorporação de tecnologias emergentes são imprescindíveis para assegurar a eficácia na proteção dos dados pessoais.

Assim, é imprescindível implementar medidas que incorporem uma avaliação sistemática e direcionada à constante atualização da legislação para enfrentar novas tecnologias, ao mesmo tempo que esclarece os desafios presentes em sua execução. As orientações para a execução eficiente da LGPD e a asseguração da privacidade e segurança tornam-se ainda mais pertinentes diante do aumento dos delitos cibernéticos.

Com base nesses aprendizados, pode-se inferir que o manejo de informações demanda uma abordagem cautelosa e diligente. É vital assegurar que todas as fases envolvidas na coleta, retenção, utilização, compartilhamento e remoção dos dados sejam executadas de maneira apropriada. Igualmente crucial é a necessidade de que os usuários sejam devidamente informados sobre o destino de suas informações pessoais, e que possam consentir previamente à coleta.

Além disso, é um direito dos usuários acessar, retificar ou eliminar seus dados pessoais, assim como requerer a transferência de seus dados para outro serviço. Por conseguinte, para salvaguardar a privacidade dos usuários e cumprir integralmente as normativas da LGPD, é essencial que as corporações compreendam e assumam responsabilidade pela gestão de informações.

Por fim, há de se propor recomendações e boas práticas. Para atingir essa meta, é indispensável empregar medidas de segurança digital, como criptografia, autenticação e gestão de acesso. Essas precauções evitam a entrada não autorizada a informações pessoais sensíveis e contribuem para mitigar os perigos de divulgação de dados e potenciais atividades fraudulentas. Quanto à responsabilidade civil na Lei Geral de Proteção de Dados (LGPD), seu artigo 42 determina o dever de o controlador ou o executor compensar o possuidor de informações individuais, se resultar em qualquer prejuízo financeiro, psicológico, particular ou coletivo, devido a uma manipulação ilícita de dados pessoais (Teixeira, 2020, p. 13).

Consequentemente, o manuseio indevido de informações se define quando não está em conformidade com a LGPD, como, a título de exemplo, o envio de promoções por *e-mail* sem a autorização do titular, que exige como fundamento legal o consentimento dele, conforme estipulado no Artigo 7, parágrafo II da LGPD. Outro exemplo de manuseio ilegítimo é utilizar as informações do titular para propósitos diferentes daqueles divulgados, já que o tratamento das informações deve ser feito exclusivamente para os fins comunicados ao titular. Dessa maneira, se os dados forem utilizados com alteração dos objetivos estabelecidos, isso configura um manuseio ilícito.

Em síntese, tem-se o Direito Digital como uma extensão do Direito tradicional, que abrange diversas áreas. Destaca-se a necessidade de lidar com crimes cibernéticos, que surgem com o avanço tecnológico e a expansão da *internet*. No Brasil, a Lei Geral de Proteção de Dados (LGPD) foi criada para regulamentar a manipulação de dados pessoais, impondo obrigações às empresas e entidades para proteger a privacidade dos usuários.

Apesar das vantagens da LGPD, como a atualização das práticas das organizações e a proteção dos direitos individuais, ainda há desafios, como a falta de conformidade e as vulnerabilidades dos sistemas. A transgressão da LGPD pode resultar em sanções, incluindo multas e suspensão das atividades. Portanto, é essencial implementar medidas de segurança digital e seguir boas práticas para garantir a integridade e a privacidade dos dados.

4 DOS CRIMES VIRTUAIS E OUTRAS DENOMINAÇÕES

O mundo vem sofrendo grandes transformações, no que se refere ao avanço da tecnologia. Com ela, vieram facilidades, comodidades e agilidades que, até então, eram inimagináveis. A interação humana se intensificou de forma significativa, reorganizando a forma de acesso à informação, o modo e, até, a velocidade de comunicação entre as pessoas, estabelecendo novos desafios e impondo oportunidades que atingiram todos os setores da sociedade; incluindo o ramo do Direito, que, também, não ficou alheio a essas mudanças.

Essas mudanças e adequações legislativas não acompanharam a escalada digital, proporcionando segurança e proteção aos seus milhões de usuários, que se tornaram vítimas dos mais variados tipos de crimes virtuais. Assim, dentro do Direito Digital nasceu um novo ramo que envolve uma série de normas, relações jurídicas e conhecimentos que estão no foco, entretanto, com uma grande carência de profissionais especializados (Mendes & Paz, 2024).

Crime virtual, cibercrime, crime eletrônico, crime informático, crime digital e e-crime são algumas nomenclaturas atribuídas aos "crimes cibernéticos". No país, ainda não há uma lei específica para esses delitos, entretanto, há normas e regramentos que tipificam tais atos criminosos e preveem suas penalidades (Kaspersky, 2024).

O Ministério da Justiça e Segurança Pública afirma que publicar ofensas em redes sociais não equivale ao exercício do direito à liberdade de expressão. A ilusória sensação de anonimato tem levado centenas de internautas a divulgarem conteúdos ofensivos de diversas naturezas, atingindo milhares de pessoas, sejam elas famosas ou anônimas. Assim,

> Sem contar os casos de roubos de senhas, de sequestro de servidores, invasão de páginas e outros cybercrimes. Todas as pessoas que são atingidas podem recorrer à Justiça para garantir o seu direito de reparação. Apesar de ser um assunto relativamente novo, a legislação tem avançado com textos específicos para cada propósito (Brasil, 2024).

Assim, o MJSP destaca, ao abordar a Legislação, que em 2012 foram sancionadas duas leis que tipificam crimes na internet, promovendo alterações no Código Penal e estabelecendo punições para delitos como invasão de computadores, disseminação de vírus ou códigos maliciosos para roubo de senhas, bem como o uso não autorizado de dados de cartões de crédito e débito. Essas leis são:

> A primeira delas é a **Lei dos Crimes Cibernéticos** (12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica atos como invadir computadores, violar dados de usuários ou "derrubar" sites. Apesar de ganhar espaço na mídia com o caso da atriz, o

> texto já era reivindicado pelo sistema financeiro diante do grande volume de golpes e roubos de senhas pela *internet*.
>
> Os crimes menos graves, como "invasão de dispositivo informático", podem ser punidos com prisão de três meses a um ano e multa. Condutas mais danosas, como obter, pela invasão, conteúdo de "comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas" podem ter pena de seis meses a dois anos de prisão, além de multa.
>
> O mesmo ocorre se o delito envolver a divulgação, comercialização ou transmissão a terceiros, por meio de venda ou repasse gratuito, do material obtido com a invasão da privacidade. Nesse caso, a pena poderá ser aumentada em um a dois terços. Já a **Lei 12.735/12** tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares que sejam praticadas contra sistemas informatizados. Essa é a lei que determina a instalação de delegacias especializadas (Brasil, 2024). [grifo nosso]

A Lei nº. 12.965/2014, também conhecida como "Marco Civil da Internet", sancionada em 2014, desde então, regula os direitos e deveres dos internautas, protege os dados pessoais e a privacidade dos usuários. Essa lei, no seu artigo 1º "estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria". No artigo 3º dessa Lei, assevera que a disciplina do uso da *internet* tem os seguintes Princípios:

> [...]
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (Brasil, 2024)

No âmbito da Competência Civil, o Marco Civil da Internet estabelece que os Juizados Especiais são responsáveis por decidir sobre a legalidade ou ilegalidade de conteúdo. Essa regra se aplica a casos de ofensa à honra ou injúria, sendo tratados da mesma forma que ocorrências fora do ambiente virtual. De acordo com o artigo 70 do Código de Processo Penal, o local competente para julgamento é o da consumação do delito. Por outro lado, crimes como violação de privacidade ou aqueles que envolvam bens, interesses ou serviços da União, de suas autarquias ou empresas públicas, são de competência da Justiça Federal, assim como delitos previstos em convenções internacionais, tais como tráfico, tortura, falsificação de moeda, entre outros.

A sensação de impunidade e o anonimato que o meio virtual proporciona é o que incita a ação criminosa, pois, além de ser mais difícil a identificação, o agente dispõe, ainda, de tempo para se organizar. Além disso, o meio virtual é um campo propício para o acesso, a criação, a dissimulação e a indução de situações e pessoas.

Importa, aqui, distinguir os delitos que são cometidos por meio virtual, de outros que somente são possíveis por meio da tecnologia: os primeiros sempre existiram, ampliando e/ou facilitando apenas o acesso das ações criminosas, tais como: estelionato, fraudes, desvios, chantagem, assédio, extorsão, pornografia infantil (vídeos/ imagens), discriminação, crimes contra a honra, dentre outros, que passaram a ser praticados de forma mais elaborada, sofisticada, evoluída e potencializada; já o segundo, passou a existir em razão da tecnologia, como por exemplo, a invasão de dispositivos informáticos ou qualquer móvel eletrônico (Mendes & Paz, 2024).

As consequências desses crimes são gravíssimas, ocasionando prejuízos incalculáveis, não somente para a vítima, mas também para a segurança dos sistemas de informações e banco de dados. Seja por motivos pessoais, seja por motivos políticos, os crimes virtuais costumam ser cometidos por pessoas demoninadas "cibercriminosos" ou "hackers". Eles infestam computadores e dispositivos digitais com vírus e *malware* com o objetivo de danificar determinados serviços ou, simplesmente, impedir o seu funcionamento, disseminar informações falsas, as chamadas "fake news", bem como roubar ou excluir dados.

Nos estudos de Mendes & Paz (2024), são considerados "crimes cibernéticos":

- **Invasão de dispositivos informáticos para disseminação de vírus e *malware*** que coleta dados (e-mail, telefone, dados bancários e etc.), como é o caso do *Trojan Horse*, também conhecido por Cavalo de Tróia.

- **Distribuição de material pornográfico e pedofilia**.

- **Violação de propriedade intelectual** (fraudes de identidades).

- **Falsificação de dados financeiros**, documentos particulares ou cartões de crédito.

- **Extorsão cibernética** (quando se exige dinheiro para impedir o ataque ameaçado).

- **Ataques de *ransomware***, que restringe/ bloqueia o acesso ao sistema infectado e cobra resgate em criptomoedas para liberação do acesso.

- ***Cryptojacking***, invasão de computadores para mineração de criptomoedas.

- **Interrupção ou perturbação em sites ou perfis** para disseminar mensagens difamatórias ou insultos dirigidos a empresas ou pessoas.

- **Golpes e fraudes** perpetuados por meios de redes sociais, anúncios falsos, *WhatsApp*, entre outros.

Em razão do aumento significativo de delitos/crimes praticados pela *internet* e visando coibir as ações criminosas neste universo virtual, foi publicada A Lei nº 14.155, de 27 de maio de 2021, que alterou o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto qualificado e estelionato cometidos de forma eletrônica ou pela *internet*, com duras penas que podem chegar até 8 anos.

Por isso, com o intuito de combater a escalada criminosa, o Estado implementou as Delegacias Especializadas em Crimes Digitais, com centros de inteligência e laboratórios técnicos, a fim de prevenir e coibir os crimes praticados pela *internet* e identificar os criminosos por meio de técnicas, materiais, instrumentos e ferramentas inteligentes. Assim, qualquer pessoa física ou jurídica que tenha sofrido qualquer ação criminosa, podem proceder a uma denúncia ou registrar um boletim de ocorrência.

Tratando-se desse contexto jurídico em que estamos inseridos, destaca-se como importante a atuação de um profissional que seja especializado na área criminal frente a essa nova demanda social. O advogado criminalista precisa acompanhar as tendências sociais, o avanças da tecnologia, para realizar investigações, fazer requerimentos, juntar provas para instruir o inquérito, tomar ciência de resultados periciais e respostas de ofícios, seja na representação do acusado ou da vítima; e isso se faz com a busca incessante do conhecimento.

5 CONSEQUÊNCIAS JURÍDICAS DA LGPD PARA OS CRIMES VIRTUAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) e as leis que combatem os crimes virtuais têm consequências jurídicas para as empresas e para os indivíduos. Tanto para um quanto para outro, o impacto pode ser enorme, ocasionando desde danos financeiros, mas, principalmente, perda de confiança e danos à imagem de alguém. Por isso, impõe-se ao Poder Público a tutela de proteger os cidadãos e organizações, através de instrumentos coercitivos, que podem funcionar como forma pedagógica, ou mesmo, como punição (Duarte, 2022, p. 5).

Nesse tipo de delito, é difícil comprovar de quem foi a autoria, devido à ausência física do agente; entretanto, tem-se investido bastante na tentativa de neutralizar as ações dos criminosos, bem como identificá-lo para que este responda, criminalmente, pelos atos cometidos. Mundialmente, tem-se ampliado os golpes ocorridos por meio digital, numa evolução de mecanismos para subtrair de outrem vantagens e privilégios. Incorporou-se,

destarte, ao cotidiano dos crimes presenciais e ataques físicos essa nova modalidade de crimes virtuais (Lopes, 2021, p. 32).

A ineficiência da LGPD nesse cenário pode ser explicada por vários fatores. Inicialmente, o crescimento exponencial de crimes cibernéticos, como fraudes digitais, ataques de phishing, roubo de identidade e vazamentos de dados, demonstrou que as medidas previstas na lei, embora robustas no papel, não são suficientes para mitigar os riscos no ambiente digital. *Hackers* e grupos criminosos continuam a encontrar brechas nos sistemas de segurança, aproveitando-se das vulnerabilidades tecnológicas e das falhas na aplicação da legislação.

Outro fator importante é a falta de estrutura e preparo de muitas organizações para garantir o cumprimento efetivo da LGPD. Empresas de pequeno e médio porte, em especial, têm dificuldades para implementar todas as exigências da lei, como a necessidade de nomear um encarregado de dados, realizar auditorias frequentes e adotar medidas de segurança cibernética adequadas. Isso resulta em um cenário em que, mesmo que a legislação esteja em vigor, muitos dados pessoais continuam expostos a ataques, já que as empresas não conseguem proteger suas informações de forma adequada (Duarte, 2022, p. 9).

Além disso, a LGPD enfrenta desafios relacionados à fiscalização e à aplicação de sanções. A Autoridade Nacional de Proteção de Dados (ANPD), responsável pela supervisão do cumprimento da lei, ainda está em fase de consolidação e carece de recursos e pessoal suficiente para monitorar e punir efetivamente as infrações. Como resultado, muitos incidentes de violação de dados continuam a ocorrer sem que haja uma resposta rápida ou punição adequada, o que enfraquece a força coercitiva da LGPD.

Outro ponto crucial é a rápida evolução das técnicas de crimes virtuais. A LGPD, embora abrangente, não foi projetada especificamente para lidar com a sofisticação e a velocidade com que os ataques cibernéticos evoluem. A lei possui dispositivos que tratam do tratamento seguro de dados, mas muitos crimes virtuais envolvem técnicas que vão além do simples vazamento de informações, como ataques direcionados, ransomware e espionagem digital, que exigem respostas mais dinâmicas e coordenadas entre as autoridades de segurança e a legislação.

A subjetividade em algumas disposições da LGPD também contribui para a insegurança jurídica, dificultando a definição clara de responsabilidades em casos de crimes cibernéticos. Isso cria um ambiente onde, em vez de prevenir e combater de maneira eficaz o uso indevido

de dados, as organizações, em muitos casos, ficam sem orientação precisa, o que fragiliza a proteção dos dados.

Portanto, embora a LGPD tenha estabelecido uma estrutura legal relevante, sua ineficácia no que se refere à proteção de dados pessoais no meio virtual está intrinsecamente ligada ao crescente aumento dos crimes cibernéticos. O aumento da sofisticação dos ataques, aliado à falta de infraestrutura das empresas e à dificuldade de fiscalização, tornam evidente a necessidade de aprimorar não só a aplicação da lei, mas também de desenvolver uma abordagem mais integrada e ágil para enfrentar os desafios de segurança no ambiente digital (Flowti, 2021)

O Objetivo da lei foi "fortalecer os direitos dos indivíduos; capacitar os atores envolvidos no processamento de dados; aumentar a credibilidade da regulamentação por meio de uma cooperação entre as autoridades de proteção de dados (Brasil, 2018). Ademais, a LGPD foi elaborada com o intuito de proporcionar maior autonomia ao titular dos dados e reforçar a salvaguarda de sua privacidade.

O respeito aos direitos dos indivíduos, assim como a garantia de segurança e a transparência no tratamento de suas informações, foram pilares essenciais que orientaram a criação das diretrizes dessa regulamentação. Delegar tarefas de monitoramento e supervisão a profissionais que desconsiderem a perspectiva do usuário pode resultar em decisões divergentes e desalinhadas com os objetivos centrais da lei.

Fica evidente que com essas medidas torna a vida virtual mais segura, pois atualmente vivemos em um mundo em que a maior parte do nosso dia se concentra na *internet*, usamos para trabalhar, estudar, e como a tecnologia vem evidenciando cada vez mais o uso da *internet*, a nova legislação veio para combater atos praticados por meio virtual, exigindo uma melhor maturidade da segurança da informação, tornando as empresas menos vulneráveis aos criminosos digitais e ao vazamento de dados pessoais (Teffé, 2022).

O artigo intitulado "LGPD/Sanções administrativas por descumprimento da lei: como agir para evitar?", alojado no site "Jornal da Advocacia", traz à baila uma importante discussão sobre as formas de punir. Para o artigo, após cinco anos da publicação da lei:

> Em fevereiro de 2023, mais um passo foi dado em relação ao processo de escolha das sanções mais apropriadas para cada caso, também conhecido como dosimetria. Com a publicação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, se tornou possível que a ANPD compreenda a melhor forma de avaliar o grau de gravidade da conduta e pudesse alinhar isso com a sanção escolhida e o seu impacto (São Paulo, OAB, *online*).

Pelo menos a LGPD acena-se como um norte na tentativa de responsabilização dos criminosos, que se utilizam do anonimato do meio virtual, para cometer crimes. A Justiça estará pronta para agir, em consonância com os seus instrumentos. É, pois uma tarefa coletiva dos órgãos de controle, das delegacias especializadas e das leis, que se ajustam para acompanhar esse processo de tecnologia; como aduz Flowti (2021), "o universo virtual pode até parecer oculto e imperceptível, mas não assegura por longo período o anonimato. Deixamos rastros, por onde quer que naveguemos".

6 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados (LGPD), instituída no Brasil em 2018, representa um marco no tratamento de dados pessoais e na proteção da privacidade dos cidadãos em um cenário onde as interações digitais se intensificam e, com elas, os riscos associados aos crimes virtuais. Este trabalho explorou as implicações jurídicas da LGPD no contexto dos delitos cibernéticos, questionando sua efetividade na promoção de um ambiente seguro para os dados dos usuários e analisando os desafios enfrentados em sua implementação e aplicação prática.

Conforme discutido, embora a mesma tenha introduzido uma estrutura robusta e inspirada no modelo europeu do GDPR, ainda há lacunas e dificuldades que impedem uma plena proteção contra crimes virtuais. A legislação brasileira, ao estabelecer princípios como a finalidade, a segurança e a transparência, visa garantir que os dados pessoais sejam utilizados de maneira ética e responsável. Entretanto, a rápida evolução tecnológica e a complexidade dos crimes cibernéticos demandam abordagens mais dinâmicas e adequações contínuas para acompanhar os novos métodos ilícitos de acesso e exploração de dados.

Outro ponto crucial é a capacidade limitada de muitas organizações, especialmente pequenas e médias empresas, de implementar as exigências da norma em questão, como a necessidade de auditorias e medidas de segurança. A carência de estrutura e de recursos técnicos e humanos para uma fiscalização rigorosa agrava a vulnerabilidade dos sistemas de segurança, expondo dados pessoais a riscos. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD), entidade responsável pela supervisão, ainda está em fase de consolidação, o que enfraquece a capacidade de monitoramento e a efetiva aplicação de sanções, contribuindo para uma insegurança jurídica no ambiente digital.

O avanço constante dos crimes cibernéticos exige uma legislação que vá além da proteção dos dados, integrando medidas específicas para coibir ataques sofisticados e proteger

as informações em casos de vazamentos. A LGPD, embora abrangente, não foi desenhada para acompanhar a sofisticação crescente dos delitos cibernéticos, o que evidencia a necessidade de um sistema de atualização constante das normas, alinhado com as inovações tecnológicas.

Portanto, para que a lei atinja seu potencial máximo no combate aos crimes virtuais, é fundamental que haja um aprimoramento contínuo da legislação e o fortalecimento das entidades fiscalizadoras, como a ANPD, de modo a capacitar e prover os recursos necessários para uma atuação eficaz. A conformidade legal deve ser vista não apenas como uma obrigação legal, mas como uma prática essencial para a integridade dos sistemas e a confiança do usuário no ambiente digital.

Esse cenário evidencia a importância de medidas de prevenção e conscientização para que a sociedade se proteja contra o uso indevido de dados pessoais, promovendo uma cultura de privacidade e segurança digital. A criação de diretrizes específicas para crimes cibernéticos e o incentivo a práticas como a criptografia, o controle de acesso e a gestão de vulnerabilidades são essenciais para um ambiente digital mais seguro e confiável. Em suma, o fortalecimento da LGPD e sua adaptação ao dinamismo do ciberespaço são passos imprescindíveis para a proteção dos dados pessoais e a efetiva responsabilização dos agentes que violam a segurança e a privacidade dos cidadãos.

A LGPD representa um avanço significativo na defesa dos direitos fundamentais dos cidadãos, principalmente no que diz respeito à privacidade e à segurança das informações pessoais. No entanto, a efetividade dessa legislação depende de uma aplicação prática que vá além do papel, exigindo um compromisso contínuo de adaptação e evolução. Os desafios encontrados até o momento evidenciam que a proteção de dados no ambiente digital deve ser abordada de forma integrada, considerando não apenas a segurança jurídica, mas também os aspectos técnicos e operacionais que garantam a eficácia das sanções e o respeito aos direitos dos titulares de dados.

É importante destacar que tal regulamento traz implicações tanto para o setor público quanto para o privado, ambos responsáveis por assegurar a conformidade com as normas e os princípios da lei. A implementação de medidas de governança de dados, políticas de privacidade claras e a capacitação de profissionais especializados em proteção de dados são passos essenciais para minimizar os riscos associados aos crimes virtuais. Além disso, a conscientização dos usuários sobre seus direitos e a promoção de uma cultura de segurança digital são vitais para o fortalecimento da proteção de dados no Brasil.

Outro aspecto relevante é a necessidade de cooperação entre as instituições, especialmente em um cenário globalizado, onde os dados circulam além das fronteiras nacionais. A parceria entre a Autoridade Nacional de Proteção de Dados (ANPD) e outras entidades reguladoras, tanto nacionais quanto internacionais, pode fortalecer a resposta a incidentes de segurança e facilitar a troca de informações e boas práticas para o enfrentamento de crimes cibernéticos.

Em conclusão, o exposto inaugura um novo marco na proteção de dados no Brasil, oferecendo uma base sólida para enfrentar os desafios contemporâneos impostos pela transformação digital. Entretanto, é fundamental que o Brasil continue a aprimorar suas políticas e estruturas, assegurando que a LGPD seja um instrumento efetivo de prevenção e combate aos crimes virtuais. A proteção dos dados dos cidadãos não é apenas uma exigência legal, mas um requisito essencial para a construção de uma sociedade mais segura e transparente, na qual a confiança no ambiente digital seja fortalecida e os direitos individuais sejam devidamente respeitados.

REFERÊNCIAS

ACADEMIA DE FORENSE DIGITAL. **O maior centro de Treinamento de Forense Digital do Brasil**. Disponível em: [https://academiadeforensedigital.com.br/]. Acesso em 04 nov. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm]. Acesso 18 abr. 2024.

_____. Lei nº 12.965, de 23 de abril de 2014.
Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco civil da Internet). Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Acesso em 16 abr. 2024.

_____. **Guia de Boas Práticas. Lei Geral de Proteção de Dados**. V. 2.0. Governo Federal, agosto/2020. Disponível em: [https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf]. Acesso
em: 14 abr. 2024.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Crimes digitais: o que são, como denunciar e quais leis tipificam como crime?**. Disponível em: [https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais#:~:text=O%20Marco%20Civil%20da%20Internet,em%20sites%20ou%20redes%20sociais]. Acesso em 03 nov. 2024.

DUARTE, Karla Lorrany da Silva. **Crimes cibernéticos e os impactos da lei geral de proteção de dados**. Unievangélica, 2022. Disponível em: [http://repositorio.aee.edu.br/bitstream/aee/20048/1/Karla%20Lorrany%20da%20Silva%20Duarte.pdf]. Acesso em 11 nov. 2024.

EDLER, G. O. B. BATISTA, M. S; LINS, I. O, ARGÔLLO, A.C.A. **Regulamento para elaboração do Trabalho de Conclusão do Curso de Direito**. 3 ed. Ilhéus, BA: Faculdade de Ilhéus, 2021.

FIORILLO, Celso Antônio Pacheco. **O Marco Civil da Internet – E o Meio Ambiente Digital na Sociedade da Informação**. 1 ed. São Paulo, Saraiva, 2017. Disponível em: [https://books.google.com.br/books?id=Lj9nDwAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false]. Acesso 15 abr. 2024.

FLOWTI. **A importância da LGPD no combate aos cibercrimes**. Brasil, 12 nov. 2021. Disponível em: [https://flowti.com.br/blog/a-importancia-da-lgpd-no-combateaos-cibercrimes]. Acesso em: 11 nov. 2024. 2022.

KASPERSKY, **O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos.** Disponível em [https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime]. Acesso 03 nov. 2024.

KUNRATH, Cristina. **A expansão da criminalidade no Cyberespaço**. Feira de Santana: Universidade de Feira de Santana, 2017.

LOPES, Alan Moreira. **Direito Digital e LGPD na Prática**. São Paulo: Editora Rumo Jurídico, 2021.

MACHADO, Daniel Dias. **Direito digital e os obstáculos para o meio Judiciário**. Disponível em: [https://www.nucleodoconhecimento.com.br/lei/meio-judiciário]. Acesso em 05 mar. 2024.

OLIVEIRA, Elenilcio Dalto de. **Direito digital no combate a crimes cibernéticos**. Disponível em: [https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos]. Acesso em 05 mar. 2024.

MENDES, Roberto Crunfli; PAZ, Alex Alves Gomes da. **Crimes Cibernéticos no Brasil: conheça os tipos, suas penas e agravantes**. Disponível em: [https://www.pazmendes.com.br/crimes-ciberneticos-no-brasil/#:~:text=Crime%20virtual%2C%20cibercrime%2C%20crime%20eletr%C3%B4nico,criminosos%20e%20prev%C3%AA%20suas%20penas.]. Acesso em 03 nov. 2024.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7 ed. São Paulo: Saraiva, 2021.

_____. **Proteção de Dados Pessoais. Comentários à Lei nº. 13.709/2018 (LGPD)**. São Paulo: Saraiva, 2018.

PRESIDÊNCIA DA REPÚBLICA CASA CIVIL. **Lei nº 12.737, de 30 de novembro de 2012 - "Lei dos Crimes Cibernéticos"**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm]. Acesso em 04 nov. 2024.

SÃO PAULO. Ordem dos Advogados do Brasil. **LGPD/Sanções administrativas por descumprimento da lei: como agir para evitar?** Universo LGPD. Disponível em: [https://jornaldaadvocacia.oabsp.org.br/noticias/lgpd-sancoes-administrativas-por-descumprimento-da-lei-como-agir-para-evitar/#:~:text=Multa%3A%20A%20multa%20pode%20ser,R%24%2050%20milh%C3%B5es%20por%20infra%C3%A7%C3%A3o.]. Acesso em 11 nov. 2024.

TECNOBLOG, **O que é um crime cibernético? 3 casos populares**. Disponível em [https://tecnoblog.net/responde/o-que-e-um-crime-cibernetico-3-casos-populares/]. Acesso em 03 nov. 2024.

TEFFÉ, Chiara Spadaccini de. **A importância da LGPD no contexto da inteligência de dados**. ITS, Rio de Janeiro/RJ, 2022. Disponível em: [https://itsrio.org/pt/artigos/aimportancia-da-lgpd-no-contexto-da-inteligencia-de-dados/]. Acesso em: 10 nov. 2024.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. 7 ed. São Paulo: Saraiva, 2023.

_____; ARMELIN, Ruth. **Lei geral de proteção de dados pessoais: comentada artigo por artigo**. 2 ed. Salvador: Editora JusPodivm, 2020.

_____. **LGPD e E-commerce**. 2 ed. São Paulo: Saraiva, 2023.