UNIVERSIDADE DE SANTA CRUZ DO SUL
CURSO DE DIREITO

Victória Corrêa da Conceição

A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL E OS POSSÍVEIS CRIMES CIBERNÉTICOS

Capão da Canoa
2024

Victória Corrêa da Conceição

A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL E OS POSSÍVEIS CRIMES CIBERNÉTICOS

Trabalho de Conclusão apresentado ao Curso de Direito da Universidade de Santa Cruz do Sul para obtenção do título de Bacharel em Direito.

Orientadora: Profa. Ms. Aline Burin Cella

Capão da Canoa

2024

AGRADECIMENTOS

Agradeço primeiramente à Deus, por guiar-me e protegei-me ao longo de toda trajetória acadêmica.

Ao meu querido pai, por despertar-me o amor pelo Direito e fazer com que este sonho se concretizasse. À minha mãe, pelo zelo e preocupação. Agradeço por serem meu alicerce durante toda minha vida e principalmente por nunca terem medido esforços para que eu chegasse até aqui.

Às minhas irmãs, pelas palavras carinho e apoio.

Ao meu namorado, pelo incentivo e suporte constante.

Às minhas avós, por serem sinônimos de força e amor.

Este trabalho não seria possível sem o suporte e contribuição da minha orientadora, Profa. Ms. Aline Burin Cella, que agradeço profundamente pelo apoio e disponibilidade durante todo o percurso deste projeto. Obrigada por compartilhar seu conhecimento, essencial para a realização do presente trabalho.

Por fim, agradeço ao meu avô (*in memorian*), que sempre incentivou-me aos estudos. Dedico a conclusão desse trabalho a realização de seu sonho de me ver formar.

RESUMO

O presente trabalho propõe uma análise abrangente sobre a interseção entre a Lei Geral de Proteção de Dados (LGPD) no Brasil e os desafios enfrentados no combate aos crimes cibernéticos. Por meio de uma investigação detalhada sobre a LGPD, incluindo suas origens, princípios e aplicabilidade, juntamente com uma análise dos tipos de crimes cibernéticos, estatísticas e tendências, busca-se compreender os impactos sociais e econômicos dessas questões. Além disso, são examinadas as regulamentações específicas para proteção de dados em incidentes de segurança cibernética, juntamente com estudos de caso sobre as penalidades aplicadas tanto no Brasil quanto em outras jurisdições. Para alcançar os objetivos específicos propostos, será analisado os princípios gerais da LGPD frente ao Direito Civil e/ou Penal para chegar a conclusões específicas sobre a influência da LGPD na proteção de dados e no combate aos crimes cibernéticos. Esse método permitirá uma análise lógica das relações entre a legislação de proteção de dados e a criminalidade cibernética. Serão utilizadas fontes de pesquisa acadêmica, legislação vigente, jurisprudência de tribunais, documentos normativos e relatórios internacionais. Por fim, são propostas reflexões sobre a evolução da LGPD para enfrentar os novos desafios em segurança cibernética, visando contribuir para a compreensão e o aprimoramento do quadro legal e regulatório nessa área em constante transformação.

Palavras-chave: Cibernéticos. Crimes. Dados. *Internet*. Lei Geral de Proteção de Dados.

ABSTRACT

This academic work proposes a comprehensive analysis of the intersection between the General Data Protection Law (LGPD) in Brazil and the challenges faced in combating cybercrimes. Through a detailed investigation into the LGPD, including its origins, principles and applicability, together with an analysis of the types of cyber crimes, statistics and trends, we seek to understand the social and economic impacts of these issues. Additionally, specific regulations for data protection in cybersecurity incidents are examined, along with case studies on penalties applied both in Brazil and in other jurisdictions. To achieve the proposed specific objectives, the deductive method will be used, starting from general principles of the LGPD and Civil and/or Criminal Law to reach specific conclusions about the influence of the LGPD on data protection and the fight against cybercrime. This method will allow a logical analysis of the relationships between data protection legislation and cybercrime. Sources of academic research, current legislation, court jurisprudence, normative documents and international reports will be used. Finally, reflections are proposed on the evolution of the LGPD to face new challenges in cybersecurity, aiming to contribute to the understanding and improvement of the legal and regulatory framework in this constantly changing area.

Keywords: Crimes. Cybernetics. Data. General Data Protection Law. Internet.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
COE	Conselho da Europa
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
OCDE	Organização para a Cooperação e o Desenvolvimento Econômico
PEC	Proposta de Emenda à Constituição
STF	Supremo Tribunal Federal
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

A crescente digitalização da sociedade moderna tem sido acompanhada pelo surgimento de novos desafios jurídicos, especialmente no que diz respeito à proteção dos dados pessoais e à prevenção de crimes cibernéticos. Nesse contexto, a promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil representa um marco significativo na busca por garantir a privacidade e a segurança dos cidadãos em meio ao ambiente virtual.

A presente monografia visa abordar a interseção entre a Lei Geral de Proteção de Dados no Brasil e os crimes cibernéticos, investigando tanto a estrutura normativa quanto as práticas relacionadas à proteção de dados e à prevenção desses delitos. Para tanto, o estudo se propõe a analisar diversos aspectos, desde os fundamentos da LGPD até as implicações das infrações cibernéticas, com o intuito de fornecer uma compreensão abrangente e aprofundada sobre o tema.

O problema central deste reside na necessidade de compreender como a implementação da Lei Geral de Proteção de Dados no Brasil impacta a ocorrência e o tratamento dos crimes cibernéticos. Diante do atual panorama jurídico e tecnológico, surge a indagação “qual a influência da LGPD na proteção de dados e no combate aos crimes cibernéticos?”.

O objetivo primordial deste trabalho consiste em investigar e analisar de forma crítica e sistematizada a relação entre a Lei Geral de Proteção de Dados no Brasil e os crimes cibernéticos, buscando identificar lacunas, desafios e possíveis soluções para a proteção efetiva dos dados pessoais e a prevenção dos delitos virtuais. Para alcançar esse desiderato, a pesquisa se propõe a realizar uma abordagem multidisciplinar, que englobe aspectos jurídicos, tecnológicos e sociais pertinentes ao tema.

A fim de responder ao problema de pesquisa delineado, o presente estudo foi estruturado em diversas etapas que visam explorar diferentes aspectos relacionados à proteção de dados e aos crimes cibernéticos. Inicialmente, serão abordados os fundamentos teóricos da Lei Geral de Proteção de Dados, contextualizando sua origem e antecedentes tanto no cenário nacional quanto internacional. Posteriormente, serão analisados os tipos de crimes cibernéticos, suas estatísticas e tendências, bem como os impactos sociais e econômicos decorrentes dessas práticas ilícitas.

Além disso, serão examinadas as regulamentações específicas para a proteção de dados em incidentes de segurança cibernética, com ênfase na análise das penalidades aplicadas de acordo com a LGPD em casos de violações de dados e crimes cibernéticos no Brasil e no mundo. Por fim, será realizada uma comparação entre as penalidades civis e penais previstas na LGPD e aquelas aplicadas em diferentes jurisdições, bem como uma reflexão sobre a evolução necessária da legislação para enfrentar os novos desafios em segurança cibernética.

2 A LEI GERAL DE PROTEÇÃO DE DADOS

Com crescente aumento no número de usuários nas plataformas digitais, abrangendo tanto pessoas físicas como empresas públicas e privadas, surgiu uma crescente preocupação em estabelecer regulamentações que proporcionem segurança jurídica máxima aos usuários nesse ambiente digital. A Lei Geral de Proteção de Dados (LGPD) veio à tona com o propósito de promover um tratamento legal adequado das informações pessoais no contexto da utilização de ferramentas digitais, visando normatizar todas as operações que envolvem dados pessoais.

A proteção de dados se configura como uma das principais estratégias para salvaguardar a privacidade das pessoas. Este direito à proteção de dados é, na verdade, uma parte integrante do direito à privacidade, um princípio consagrado da Constituição. É relevante destacar que, em 2020, o Supremo Tribunal Federal (STF) emitiu um posicionamento que afirmava ser o direito à proteção de dados um direito fundamental. Além disso, no final de 2021, a Proposta de Emenda à Constituição (PEC) n. 17/2019 incluiu expressamente esse direito no artigo 5º da Constituição Federal, reconhecendo sua importância e visando sanar a ausência de menção direta a ele no texto constitucional.

Observa-se como essa legislação representa um marco fundamental na proteção da privacidade digital, alinhando-se aos princípios constitucionais de garantia de direitos fundamentais. A LGPD não apenas regula o tratamento de dados pessoais, mas também fortalece a segurança jurídica necessária para as operações digitais, estabelecendo um novo paradigma de responsabilidade e transparência. A análise das origens e antecedentes da LGPD no contexto brasileiro revela uma evolução contínua em resposta aos avanços tecnológicos e à crescente importância da privacidade como um direito essencial na era digital.

2.1 Origens e antecedentes da LGPD no contexto brasileiro

Muito antes de especular-se sobre a criação da LGPD devido os avanços tecnológicos e criação de novas tecnologias, a proteção à privacidade e aos dados pessoais já eram protegidos, legislados e tendo suas evoluções graduais conforme a evolução da necessidade. Podemos ver que em 1948, na Declaração Universal dos Direitos Humanos, o direito à privacidade veio como um direito fundamental do ser

humano, dando origem, assim, às diversas legislações, a respeito do tema. A Declaração Universal dos Direitos Humanos, em seu artigo 12, ainda válida para os dias de hoje, ressalta que: “Ninguém será sujeito a interferências na sua vida privada, família, lar ou na sua correspondência, nem a ataque à sua honra e reputação. Toda Pessoa tem direito à proteção da lei contra tais interferências ou ataques” (Declaração Universal Dos Direitos Humanos, 1948).

Partindo para momentos mais atuais, obteve-se a evolução e garantias no Brasil, começando pelo artigo 5º da Constituição Federal de 1988 que coloca “todos iguais perante a lei” e demonstra que o direito à privacidade é um direito fundamental conforme inciso X, XI e XII:

> [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Brasil, 1988).

Porém, devido a evolução tecnológica e digital, tornou-se insuficiente somente o exposto na Constituição, necessitando de uma complementação:

> Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada. (Mulholland, 2012, p. 3).

Desta forma começaram a ser criados instrumentos legais que buscam a proteção de dados pessoais e alteravam a visão sobre a importância desses dados. Em 1990 o Código de Defesa do Consumidor regulou direitos ao consumidor sobre seus dados em posse de outros (Brasil, 1990). Em 1996, a Lei de Interceptação Telefônica e Telemática impôs a utilização desse meio a somente casos específicos

e sempre com a devida autorização judicial (Brasil, 1996), também como a Lei do Habeas Data, que regulou o rito de acesso e a correção de informações pessoais e se tornou um direito constitucional (Brasil, 1997). Ainda se destaca o direito à vida privada, o qual é reconhecido no art. 21 do Código Civil: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (Brasil, 2002).

Em 2014, com o Marco Civil da Internet, veio a regulamentação dos direitos aos usuários da Internet, os incisos I e II do artigo 7º asseguram, respetivamente, o direito à “inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação” e à “inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei” (Brasil, 2014).

Continuando com o Marco Civil da Internet, há outros incisos do artigo 7º da referida lei que tutelam a proteção de dados, destacando-se o inciso VII, que veda o fornecimento de dados pessoais sem que haja autorização do internauta, o inciso IX, que exige consentimento expresso para o armazenamento de dados, e o inciso X, que determina a exclusão definitiva dos dados ao término da relação entre as partes (Brasil, 2014). Entre outros artigos estes não tão específicos, mas que auxiliam a proteção, como a necessidade de consentimento para utilização de dados, sendo um grande marco a proteção e tratamento de dados.

A proteção à privacidade e aos dados pessoais no Brasil teve suas raízes históricas enraizadas muito antes da concepção da LGPD. Desde a Declaração Universal dos Direitos Humanos de 1948, que consagrou o direito à privacidade como fundamental, diversas legislações evoluíram em resposta às necessidades emergentes. Esta evolução culminou na promulgação da Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, após um incidente de violação de privacidade que impactou profundamente a opinião pública brasileira. A partir desse marco, novas discussões e exigências legislativas foram iniciadas, pavimentando o caminho para a promulgação da Lei Geral de Proteção de Dados (LGPD).

2.2 Lei 12.737/2012 – Lei Carolina Dieckmann

A Lei 12.737/2012, ficou assim nomeada devido a um evento envolvendo a atriz Carolina Dieckmann. Ela foi vítima de uma invasão em seu dispositivo pessoal,

na qual criminosos acessaram seu conteúdo, incluindo conversas e fotos íntimas, e divulgaram esses dados na internet sem a autorização da atriz. Essa lei trata da tipificação de crimes cibernéticos e introduziu modificações no Código Penal Brasileiro de 1940.

A Lei de invasão de dispositivo informático incluiu os artigos 154-A e 154-B ao Código Penal, além de alterar a redação dos artigos 266 e 298. Essa legislação visa a combater as ações criminosas no ambiente digital, proporcionando uma base legal sólida para lidar com invasões de dispositivos e a divulgação não autorizada de informações pessoais na internet:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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.
> Art. 266 - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - Pena - detenção, de um a três anos, e multa.
> Art. 298 - Falsificação de documento particular/cartão - Pena - reclusão, de um a cinco anos e multa (Brasil, 2012).

Antes da existência desta Lei, acessar dispositivos privados não era considerado um crime, mas sim atos preparatórios, ou seja, práticas que não eram puníveis. Com a promulgação desta Lei, essa ação passou a ser tratada como um crime.

Portanto, essa legislação foi fundamental para proteger a segurança e a privacidade online. Além disso, ela representou um marco importante para o avanço das regulamentações nesse sentido, influenciando leis como a Lei Geral de Proteção de Dados e o Marco Civil da Internet.

A disseminação da tecnologia da informação trouxe uma otimização significativa na abordagem das necessidades da sociedade contemporânea, levando os indivíduos a adotar cada vez mais o mundo virtual para se adaptar ao novo contexto. Um amplo espectro de atividades é atualmente conduzido através da internet, que vai desde a utilização para fins profissionais e educacionais até o

comércio e a prestação de serviços, bem como a facilitação da comunicação e interação social.

A evolução dessas práticas também trouxe desafios relacionados à privacidade e à segurança dos dados pessoais dos usuários. Nesse sentido, o Marco Civil da Internet, instituído pela Lei nº 12.965/2014, representa um marco regulatório fundamental no Brasil. Esta legislação visa estabelecer princípios, garantias, direitos e deveres para o uso da internet no país, promovendo a proteção dos dados pessoais e a neutralidade da rede, além de estabelecer diretrizes para a atuação do Estado, do setor privado e da sociedade civil na gestão e regulamentação da internet brasileira.

2.3 Marco Civil da Internet

A disseminação da tecnologia da informação trouxe uma otimização significativa na abordagem das necessidades da sociedade contemporânea, levando os indivíduos a adotar cada vez mais o mundo virtual para se adaptar ao novo contexto. Um amplo espectro de atividades é atualmente conduzido através da internet, que vai desde a utilização para fins profissionais e educacionais até o comércio e a prestação de serviços, bem como a facilitação da comunicação e interação social. Segundo Bonfati e Kolbe (2020, p.66):

> A rapidez do avanço tecnológico trouxe aos indivíduos uma gama enorme de formas de agir dentro de uma sociedade e, por consequência, exigiu do direito uma nova linha de pensar e atuar, de modo que se adaptasse a essa nova realidade.

Essa conjuntura tem impelido o campo do direito a seguir um caminho que permita uma adaptação mais eficaz às demandas atuais, culminando na necessidade de regulamentação jurídica no espaço virtual. Dessa evolução, emerge uma nova esfera de garantias conhecida como o direito digital. Como resposta a essa dinâmica, foi promulgada a Lei nº 12.965/2014, amplamente reconhecida como o Marco Civil da Internet.

> Assim, surgiu o direito digital, que busca a regularização desse mundo tecnológico, definindo direitos e deveres. Para tanto, surgiu a ideia do Marco Civil da Internet, que trata da construção dos direitos dos cidadãos dentro dessa rede, ou seja, não se fala apenas de crimes na internet, mas de tudo

> que for necessário ser discutido e regulamentado em todas as áreas em que a tecnologia da informação se faça presença (Bonfati; Kolbe, 2020, p.67).

A Lei nº 12.965/2014, amplamente reconhecida como a "Constituição da Internet" foi promulgada com o propósito de estabelecer normas para o uso da internet no Brasil. Ela faz parte do conjunto de regulamentações informáticas, e desempenha um papel fundamental na definição de garantias e na criação de um alicerce para a regulamentação do mundo digital em nosso país. O seu artigo 1º é esclarecedor nesse sentido, ao afirmar: "Esta Lei 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" (BRASIL, 2014).

> É válido destacar que o Marco Civil, apesar de visar primordialmente a tutela dos direitos civis na internet, também tem aplicação no Direito Penal e Processual Penal, uma vez que estabelece conceitos fundamentais, bem como disciplina formas de obtenção de provas quanto à materialidade e à identificação da autoria delitiva. (Barreto; Brasil, 2016, p.18).

O Marco Civil da internet tem como objetivo garantir a privacidade e a proteção de dados dos usuários, a referida Lei disciplina o uso do espaço virtual no Brasil destacando em seu art. 3º os princípios que conduzem o uso adequado das redes, tais como: a garantia da liberdade de expressão, comunicação e manifestação em conformidade com a Constituição Federal; resguardar a privacidade; proteger os dados individuais, entretanto disponibiliza dados pessoais por meio de ordem judicial; neutralidade ou a imparcialidade nas redes; estabilidade, segurança e melhor funcionamento; responsabilização dos atuantes conforme suas atividades; entre outros.

2.4 Origens e antecedentes da LGPD no contexto internacional

Em 1970, a Alemanha foi pioneira ao promulgar a primeira lei global destinada a proteger dados pessoais. Schertel (2011, p. 37) enfatizou a necessidade de elevar o nível de proteção dos dados pessoais, argumentando que a salvaguarda desses dados é uma extensão da personalidade individual do ser humano e, portanto, deve ser uma preocupação da jurisdição.

Em 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) estabeleceu um comitê de ministros e publicou diretrizes que delinearam princípios fundamentais para a proteção de dados e o fluxo de informações entre países com leis próprias, em conformidade com essas diretrizes. No entanto, essas diretrizes inicialmente não tinham o poder de estabelecer um padrão definitivo, o que levou a interpretações variadas e resultou na promulgação de várias leis em diferentes países, cada um interpretando os princípios de maneira distinta (OCDE, 2002).

Em 1981, a Comissão Europeia ratificou a *Data Protection Convention* (Convenção de Proteção de Dados, Tratado nº 108), tornando-se o principal instrumento legal internacional destinado a proteger os indivíduos contra o uso indevido e a coleta abusiva de dados pessoais. Esta convenção proibia o processamento de dados confidenciais, como raça, orientação política, saúde, religião, vida sexual e antecedentes criminais de uma pessoa, entre outras informações sensíveis. Além disso, garantia o direito dos indivíduos de saber quais informações eram armazenadas a seu respeito e, quando necessário, corrigi-las (COE, 1981).

Uma decisão de grande relevância ocorreu em 1983, quando o Tribunal Constitucional Alemão reconheceu o direito à autodeterminação da informação, declarando que a Lei do Censo era inconstitucional em relação às obrigações dos cidadãos de fornecerem dados, impondo multas e permitindo o compartilhamento de informações entre órgãos públicos federais. Nas palavras de Laura Schertel (2088, p.50):

> A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subsequentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais se baseia em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação.

Na Europa, a Diretiva nº 46 da União Europeia foi aprovada e sancionada em 1995, representando um marco abrangente na proteção de dados pessoais e atraindo a atenção em todo o mundo até a implementação do Regulamento Geral de

Proteção de Dados (GDPR). Embora a diretiva não possuísse força legal direta nos países membros, ela serviu como referência para a elaboração de legislações nacionais e, em grande medida, seus princípios essenciais foram mantidos no GDPR. A ideia subjacente é que os princípios de proteção de dados devem ser aplicados a todas as atividades de tratamento de dados pessoais, e as atividades do responsável pelo tratamento devem obedecer ao Direito Comunitário. Um ponto importante a ser observado é o princípio de que o tratamento de dados realizado por uma pessoa física no exercício de atividades exclusivamente pessoais ou domésticas, como correspondência ou listas de endereços, deve ser excluído (DIRETIVA 46/95, p. 2).

Destaca-se a influência significativa da Regulamentação Geral de Proteção de Dados da União Europeia (GDPR), promulgada em 2016. Este marco regulatório estabeleceu padrões rigorosos para a proteção de dados pessoais, reforçando os direitos individuais no tratamento e na circulação livre dessas informações dentro da União Europeia. A implementação bem-sucedida do GDPR serviu de inspiração para legislações similares em outras partes do mundo, incluindo o Brasil com a promulgação da Lei Geral de Proteção de Dados (LGPD).

2.4.1 A Regulamentação Geral de Proteção de Dados da União Europeia

Em 2016, a União Europeia testemunhou debates que culminaram na criação do Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), numerado como 679, sancionado em 27 de abril de 2016. Esse regulamento concentrou-se na definição de normas e diretrizes para a proteção dos direitos das pessoas físicas em relação ao tratamento e livre circulação de seus dados pessoais. Dentre os vários objetivos da GDPR pode-se citar:

> 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. (GDPR, 2016)

Com a implementação desse regulamento, tornou-se necessário que os países envolvidos em transações comerciais com a Europa também possuíssem leis equivalentes. Caso contrário, poderiam enfrentar obstáculos adicionais na condução de negócios. (EU, 2016).

Diante disso, apesar da existência de leis isoladas que visavam proteger dados pessoais em certos casos, foi preciso criar uma norma que pudesse seguir os princípios internacionalmente aceitos.

A Regulamentação Geral de Proteção de Dados da União Europeia (GDPR) representou um marco significativo na proteção de dados pessoais, estabelecendo normas rigorosas para o tratamento e circulação dessas informações dentro do bloco europeu. No contexto global, iniciativas semelhantes surgiram, como a Lei Geral de Proteção de Dados do Brasil (LGPD), promulgada em 2018. A LGPD compartilha objetivos comuns com a GDPR, buscando assegurar a privacidade e o controle sobre dados pessoais, refletindo uma tendência internacional rumo à regulamentação mais robusta e unificada nesta área.

2.5 Objetivos da LGPD

A Lei Geral de Proteção de Dados do Brasil (LGPD - Lei nº 13.709/18) surgiu em resposta à necessidade de estabelecer uma base legal clara para o tratamento de dados. (Teffé; Viola, 2019).

A LGPD foi promulgada pelo presidente Michel Temer em 14 de agosto de 2018, e o prazo inicial para a adaptação às novas regras foi de dezoito meses, aplicando-se tanto à iniciativa pública quanto à privada, independentemente do porte ou segmento de mercado (Pinheiro, 2020).

Esta regulamentação estabelece princípios, direitos e obrigações relacionadas ao uso de um dos ativos mais valiosos na sociedade digital, que são as bases de dados que contêm informações pessoais (Pinheiro, 2020).

A LGPD parte do pressuposto de que todos os dados pessoais são importantes e valiosos. Como regra geral, determina que qualquer entidade, seja pessoa física

ou jurídica, de direito público ou privado, inclusive na atividade realizada em meios digitais, deve ter uma base legal para fundamentar o tratamento de dados pessoais que realiza (Teffé; Viola, 2019).

O artigo 1º da LGPD estabelece que:

> Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (Brasil, 2018)

É importante ressaltar que a lei se aplica a qualquer sistema que utilize dados de pessoas naturais, mas não inclui os dados de pessoas jurídicas (Garcia *et al.*, 2020).

A LGPD é composta por dez capítulos com sessenta e cinco artigos e, em alguns aspectos, gera incertezas legais, pois permite margens para interpretações subjetivas onde deveria ser mais precisa. Por exemplo, no que diz respeito aos prazos, enquanto o regulamento europeu (GDPR) estabelece prazos específicos, como setenta e duas horas, a LGPD utiliza o termo "prazo razoável" (Pinheiro, 2020).

Conforme estabelecido no artigo 2º da Lei Geral de Proteção de Dados (LGPD), os fundamentos da proteção de dados pessoais são:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

Com isso posto, há uma clara relação com o texto constitucional no que tange à garantia dos direitos fundamentais, assegurando a privacidade, intimidade, honra, imagem e dignidade.

É esclarecido por Cots e Oliveira (2019, p.49) que:

> [...] o respeito à privacidade está vinculado à oportunidade de a pessoa controlar o que permite em sua vida privada e decidir sobre a inclusão ou

> não de terceiros. Para determinar o acesso de terceiros, é essencial garantir, por exemplo, a autodeterminação informativa.

Portanto, "o princípio da autodeterminação informada envolve a capacidade de expressão de vontade do titular, que não deve ser impedida por terceiros, junto com a obrigação de fornecer informações sobre seus dados" (Cots; Oliveira, 2019, p. 49).

Além disso, se a liberdade de expressão infringir os direitos de terceiros, especialmente no que diz respeito a atividades não autorizadas com dados pessoais, é necessário priorizar a proteção da privacidade.

A inviolabilidade da intimidade, honra e imagem decorre da proteção à privacidade. Todos esses direitos estão relacionados à personalidade. No entanto, a privacidade abrange um conceito mais amplo, envolvendo a exteriorização das ações humanas (Cots; Oliveira, 2019).

Assim, nas palavras de Alonso e Cots (2005, p.52):

> A intimidade é o âmbito interior da pessoa mais profundo, mais recôndito, secreto ou escondido dentro dela. É, assim, algo inacessível, invisível, que só ela conhece, onde ela só elabora ou constrói livremente seu próprio agir e onde se processa sua via interior. Na intimidade a pessoa constrói-se e descobre-se a si mesma.

Além disso, a LGPD estabeleceu que o Estado deve atuar em prol do desenvolvimento econômico, tecnológico, inovação, incentivando e promovendo o avanço científico, a pesquisa e a capacitação tecnológica (Alonso; Cots; Oliveira, 2019).

Por último, a livre iniciativa é assegurada como um dos fundamentos da República Federativa do Brasil, assim como a livre concorrência, decorrente do princípio da ordem econômica.

A LGPD estabelece princípios fundamentais que orientam o tratamento de dados pessoais no país, visando garantir a proteção dessas informações em conformidade com padrões éticos e legais, refletindo uma abordagem alinhada com iniciativas globais, como o GDPR da União Europeia. Esses princípios fornecem uma estrutura sólida para assegurar a privacidade e a segurança dos dados, promovendo a transparência e o controle por parte dos indivíduos sobre suas informações pessoais.

2.6 Princípios da LGPD

Os princípios são regras fundamentais que servem como base teórica ou alicerce para algo. Eles representam o conjunto de normas ou preceitos que se aplicam como referência para todas as operações jurídicas, delineando, assim, a conduta a ser adotada em qualquer atividade desse campo (Cots; Oliveira, 2019).

No contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), o artigo 6º estabelece que, nas atividades de tratamento de dados, devem ser considerados princípios como a boa-fé, bem como os princípios da finalidade, adequação, necessidade, qualidade dos dados, transparência, livre acesso, segurança, prevenção, não discriminação, responsabilização e prestação de contas (Brasil, 2018).

A boa-fé implica fidelidade no cumprimento das expectativas alheias, honestidade, lealdade e confiança. Em outras palavras, requer uma conduta que respeite os interesses legítimos e direitos de forma leal, sem causar abuso, obstrução ou lesão a terceiros (Cots; Oliveira, 2019).

O princípio da finalidade estipula que o tratamento de dados pessoais deve ter propósitos legítimos, explícitos, específicos e informados ao titular, sendo inviável realizar tratamentos posteriores incompatíveis com as finalidades inicialmente definidas (Brasil, 2018).

Assim, há violação desse princípio quando se informa que a coleta de dados servirá para faturamento de produtos ou serviços, mas se utilizam os dados para campanhas de marketing, ou quando se promete compartilhar dados com a empresa X, mas compartilha-se com a empresa Y (Cots; Oliveira, 2019).

O princípio da adequação refere-se à compatibilidade do tratamento de dados com as finalidades comunicadas ao titular (Brasil, 2018). Ou seja, o procedimento utilizado) deve estar em conformidade com a finalidade pretendida. No entanto, há descumprimento desse princípio quando se informa que os dados serão eliminados, mas mantém-se cópias dos mesmos (Cots; Oliveira, 2019).

O princípio da necessidade relaciona-se com a finalidade pretendida, permitindo o tratamento apenas dos dados necessários para atingir essa finalidade (Brasil, 2018). Desse modo, viola-se esse princípio ao solicitar informações excessivas ou desnecessárias, como orientação sexual para admissão de

empregados ou cor da pele para faturamento de produtos ou serviços (Cots; Oliveira, 2019).

O princípio da qualidade dos dados assegura aos titulares a clareza, exatidão, relevância e atualização dos dados, de acordo com a necessidade e para cumprimento da finalidade do seu tratamento (Pinheiro, 2018).

A transparência garante aos titulares acesso claro, preciso e fácil às informações sobre o tratamento e seus responsáveis, levando em consideração segredos industriais e comerciais (Brasil, 2018). Assim, dificultar o acesso do titular às informações de tratamento ou omitir a identificação completa do controlador ou operador contraria esse princípio (Cots; Oliveira, 2019).

O princípio do livre acesso permite aos titulares consultar facilmente e de forma gratuita a duração e forma do tratamento, assim como a integralidade de seus dados (Brasil, 2018).

A segurança implica o uso de medidas técnicas e administrativas para proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de perda, destruição, alteração, divulgação ou acesso (Brasil, 2018).

A prevenção, relacionada à segurança, envolve a adoção de medidas para evitar danos devido a um tratamento inadequado dos dados pessoais (Oliveira; Lopes, 2019).

O princípio da não discriminação proíbe o tratamento de dados para finalidades discriminatórias abusivas ou ilícitas. Portanto, ocorre violação desse princípio ao oferecer produtos ou serviços apenas para pessoas de determinada nacionalidade ou ao negar o acesso a usuários com base no sexo (Cots; Oliveira, 2019).

Por fim, o princípio da responsabilização e prestação de contas exige que os agentes de tratamento demonstrem o uso de medidas eficazes para garantir a proteção de dados, não bastando apenas a existência de um programa de proteção, sendo necessário comprovar sua efetividade (Brasil, 2018).

A LGPD visa proteger os direitos fundamentais de privacidade e autodeterminação informativa dos indivíduos, promovendo a responsabilidade das entidades que lidam com dados pessoais em conformidade com os princípios estabelecidos na legislação.

2.7 Aplicabilidade da LGPD

O artigo 3º da Lei Geral de Proteção de Dados Pessoais determina os limites da sua aplicação, os quais incluem:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. (Brasil, 2018).

Considerando isso, a LGPD tem uma abrangência significativa quanto aos seus destinatários, pois “se aplica a qualquer operação de tratamento de dados realizada por pessoa física ou jurídica, tanto de direito privado quanto público, atuando como controladora ou operadora” (Menezes; Colaço, 2019, p. 192).

Além disso, a sua aplicação é válida independentemente do meio em que esses dados estejam sendo processados. Ou seja, a lei é aplicável não apenas a operações digitais, mas também a operações físicas, off-line, diferentemente do escopo do Marco Civil da Internet. (Menezes; Colaço, 2019)

Em relação à legislação aplicável ao tratamento de dados realizados na internet, entende-se que a LGPD é uma lei específica, enquanto o Marco Civil da Internet é uma lei geral. No entanto, é importante ressaltar que não houve a revogação implícita do Marco Civil da Internet, pois ele trata de outros temas, fundamentos e princípios relacionados ao uso da internet no Brasil, além de estabelecer diretrizes para a atuação do Poder Público (Cots; Oliveira, 2019).

Portanto, é necessário haver uma integração entre as leis envolvidas, como o Código de Defesa do Consumidor, o Marco Civil da Internet, a LGPD e a Lei de Acesso à Informação, garantindo uma ampla proteção aos titulares de dados submetidos a processamento no ambiente virtual. (Menezes; Colaço, 2019).

Além disso, a aplicação da LGPD não depende da localização da sede da empresa ou da origem dos dados, desde que alguma etapa do processo ocorra no Brasil. Assim, se qualquer fase do tratamento for realizada no território nacional,

tanto a coleta quanto o processamento estarão sujeitos à LGPD (Menezes; Colaço, 2019).

Da mesma forma, a lei é aplicável a atividades que visem oferecer bens ou serviços ou tratar dados de pessoas localizadas no território nacional. Portanto, "os dados pessoais tratados por uma empresa de serviços de computação em nuvem que armazena dados fora do país terão que cumprir as exigências da LGPD" (Menezes; Colaço, 2019).

Como resultado, a cidadania, nacionalidade ou residência do indivíduo são critérios irrelevantes. Se um estrangeiro estiver no Brasil, mesmo que em trânsito, estará protegido pela legislação brasileira no que diz respeito ao tratamento de dados pessoais.

Ao explorar a aplicabilidade da Lei Geral de Proteção de Dados (LGPD), torna-se evidente a necessidade de compreender não apenas suas diretrizes principais, mas também as exceções que permitem flexibilizações fundamentadas na legislação. Esta análise transita da fase inicial de estabelecer os princípios e direitos garantidos pela LGPD para uma investigação mais detalhada das situações específicas em que essas normas podem não ser integralmente aplicáveis. As exceções não apenas delimitam o escopo da lei, mas também desafiam os aplicadores e os operadores do Direito a interpretar os limites da proteção de dados pessoais frente a interesses contrapostos e circunstâncias específicas.

2.7.1 Exceções da aplicabilidade da LGPD

A Lei Geral de Proteção de Dados Pessoais apresenta exceções no seu artigo 4º em relação à sua aplicabilidade no tratamento de dados pessoais feito por indivíduos para fins estritamente pessoais e não econômicos; para propósitos jornalísticos, artísticos ou acadêmicos exclusivos; em situações de interesse público específico; e para dados tratados fora do território nacional:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;

> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018).

A primeira exceção mencionada na LGPD diz respeito ao tratamento realizado por pessoas naturais para fins estritamente pessoais e não econômicos, ou seja, para uso pessoal. Isso se refere a situações como a agenda telefônica do celular, anotações, fotos, entre outros exemplos. É importante destacar que o objetivo da aplicação da LGPD é proteger a privacidade da pessoa natural em relação às organizações econômicas e ao Estado, especialmente devido ao poder desigual das informações na sociedade contemporânea. Entretanto, não se pode alegar a inaplicabilidade da LGPD para causar danos à privacidade, honra ou imagem do titular dos dados sem resultar em dano moral ou infringir a lei penal (Cots; Oliveira, 2019).

A segunda exceção se refere ao tratamento de dados com finalidade exclusivamente jornalística, artística ou acadêmica. A atividade jornalística pura visa informar, tendo fins sociais e de interesse público, e não deve ser confundida com atividades pessoais ou comerciais que visam atrair público para determinado meio. No entanto, se uma empresa que realiza outras atividades econômicas formar um banco de dados para discriminar informações ou não for clara sobre sua utilização, estará sujeita à LGPD (Menezes; Colaço, 2019).

No âmbito das atividades exclusivamente artísticas, trata-se de obras que expressam o direito de personalidade por meio da criatividade. De acordo com o artigo 7º da Lei de Direito Autoral, as obras artísticas são protegidas pela criatividade humana, incluindo literatura, coreografia, composições musicais, fotografia, desenho, pintura, entre outras formas de expressão (Menezes; Colaço, 2019).

Quanto à finalidade exclusivamente acadêmica, refere-se a atividades desenvolvidas para avançar o conhecimento e a pesquisa científica, especialmente aquelas conduzidas no ambiente acadêmico, como as pesquisas realizadas por universidades (Menezes; Colaço, 2019), respaldadas pela autonomia prevista no artigo 207 da Constituição Federal (Brasil, 1988).

Nesses casos, a fiscalização da pesquisa é conduzida por comitês de ética e por meios convencionais, sem a necessidade de controle direto pela LGPD. No entanto, embora não se aplique completamente, a LGPD menciona a aplicação dos artigos 7º e 11 em relação ao tratamento de dados pessoais e sensíveis, representando uma aplicação reduzida da lei nesses contextos.

Nesse sentido, Cots e Oliveira (2019, p.66) entendem que:

> O Legislador, ao nosso ver, havia pretendido conter o ímpeto da iniciativa privada, que poderia se dedicar ao tratamento de dados pessoais sob o manto da produção acadêmica, mas com finalidades meramente comerciais. Um bom exemplo poderia ser estudos acadêmicos relativos ao desenvolvimento de novos medicamentos ou técnicas em saúde, com formação de banco de dados pessoais que poderia ser utilizado, indevidamente, em detrimento dos titulares.

A terceira situação diz respeito ao uso de informações pessoais em atividades específicas de interesse público, como segurança pública, defesa nacional, proteção do Estado ou investigação e repressão de crimes (Menezes; Colaço, 2019).

Assim, quando há identificação da prática de um crime, o tratamento de dados utilizado exclusivamente para investigação não será mais completamente regulado pela lei mencionada (Menezes; Colaço, 2019).

No entanto, a LGPD será aplicada integralmente a outras operações realizadas pelo Governo.

Portanto, a inaplicabilidade não é total, pois a LGPD determinou que o tratamento de dados referentes às exceções acima mencionadas será regulado por legislação específica. Nesse caso, é necessário observar o processo legal correto, os princípios gerais de proteção e os direitos do indivíduo conforme previsto na Lei (Menezes; Colaço, 2019).

Além disso, foi proibido que entidades privadas realizem esse tipo de tratamento de dados, exceto nos casos em que essas ações estejam sob a responsabilidade de uma entidade pública. Essas situações devem ser especificamente comunicadas à Autoridade Nacional de Proteção de Dados, a menos que não envolvam a totalidade dos dados, a menos que a pessoa jurídica seja totalmente controlada pelo setor público (Brasil, 2018).

Além disso, a Autoridade Nacional de Proteção de Dados emitirá pareceres ou recomendações técnicas e também solicitará aos responsáveis relatórios que avaliem o impacto na proteção dos dados pessoais (Brasil, 2018).

A última situação trata do tratamento de dados realizado no exterior, que não envolvem pessoas localizadas no território nacional. Nesses casos, a lei não se aplica se os dados não forem compartilhados com entidades de processamento no Brasil ou transferidos para outro país que não seja o de origem, desde que o país de origem ofereça um nível de proteção de dados adequado ao estabelecido pela LGPD (Brasil, 2018). A respeito desse tema, Cots e Oliveira (2019, p.68) fornecem a seguinte perspectiva:

> [...] deverá beneficiar as empresas brasileiras, aumentando sua competitividade. Isso porque, ao tratar dados oriundos do exterior, na qualidade de operador, nunca de controlador, desde que os mesmos não sejam relativos às pessoas localizadas no território nacional, não haverá aplicação da LGPD.

Assim, no que diz respeito ao processamento de dados fora do território nacional conforme descrito no item IV do artigo 4º, é necessário interpretá-lo de forma restrita. Isso ocorre porque a regra estabelece que, se qualquer etapa do tratamento de dados acontecer no Brasil, mesmo que os dados sejam originados do exterior, estará sujeita à LGPD (Menezes; Colaço, 2019).

Portanto, fica evidente que as exceções à aplicação da lei conforme previstas no artigo 4º são justificadas por direitos fundamentais, como a liberdade de informação no contexto do jornalismo, ou por um interesse público relevante (Doneda; Mendes, 2018). Além disso, a LGPD protege as pessoas da vigilância governamental e dos agentes do mercado consumidor (Menezes; Colaço, 2019).

Após examinar as exceções que permitem flexibilizações na aplicabilidade da Lei Geral de Proteção de Dados (LGPD), é fundamental direcionar o foco para um campo interligado, porém distinto: os crimes cibernéticos.

3 CRIMES CIBERNÉTICOS

A definição primária distingue os delitos cibernéticos em duas categorias principais: próprios (ou puros) e impróprios (ou impuros). Nesse contexto, é essencial examinar ambas as divisões para identificar as principais diferenças entre elas, especialmente no que diz respeito aos métodos de execução e à sua possível classificação como variações de delitos já existentes.

3.1 Crimes cibernéticos próprios e impróprios

Os crimes cibernéticos puros, também conhecidos como próprios, referem-se àqueles em que os sistemas informatizados, bancos de dados, arquivos ou dispositivos terminais (como computadores, smartphones, tablets, entre outros) são alvo de ataques por parte de criminosos, que exploram vulnerabilidades identificadas. Nesses casos, o foco dos criminosos está nos dispositivos informatizados e/ou nos dados neles contidos (BARRETO; BRASIL, 2016).

Matheus de Araújo Alves (2020, p.43) descreve os crimes digitais próprios da seguinte forma:

> Os crimes digitais próprios são, portanto, aquelas condutas proibidas por lei cujos bens jurídicos infringidos são os sistemas informáticos e as informações automatizadas (dados). Também chamados de crimes digitais puros, essa classificação remete àquelas condutas que recaem sobre o próprio computador físicos e seus componentes (hardware) ou sobre o sistema operacional ou programas (software), prejudicando seu normal funcionamento. Entre os exemplos mais conhecidos de crimes digitais próprios estão: a intrusão informática, o “furto” de identidade virtual, a inserção de malwares, o scamming, o spamming, e a interceptação de emails.

Nesse contexto, os crimes digitais próprios ou puros são aqueles que estão diretamente ligados ao computador, em que o dispositivo é diretamente alvo do crime ou utilizado como meio para acessar conteúdo dentro de seu sistema. Por outro lado, os crimes digitais impróprios se referem a delitos já estabelecidos no ordenamento jurídico, que passaram a ser cometidos com o auxílio das tecnologias modernas, ou seja, são os crimes tradicionais praticados por meio de novos métodos (CRESPO, 2011). Alesandro Gonçalves Barreto e Beatriz Silveira Brasil (2016) explicam que os crimes impróprios são aqueles em que o dispositivo tecnológico é usado como meio para cometer o crime, resultando na execução ou no resultado do delito, enquadrando-se assim em figuras típicas previstas no Código Penal Brasileiro ou em leis penais especiais.

Quanto ao agente ativo, isto é, o autor do delito digital, seja ele próprio (puro) ou impróprio, Alesandro Gonçalves Barreto e Beatriz Silveira Brasil (2016, p. 23) enumeram:

> No ambiente virtual, devem ser bem distinguidas duas figuras: as dos hackers, que possuem grande conhecimento de informática e segurança de

> redes, utilizando-o para proteção e em defesa dos menos favorecidos, também conhecidos como white hats (chapéus brancos), e a dos crackers ou black hats (chapéus pretos), os quais utilizam seus conhecimentos para práticas criminosas ou antiéticas.

A definição mais amplamente aceita considera os *hackers* como pessoas com amplo conhecimento em computadores que realizam invasões. Os *crackers*, por outro lado, são os verdadeiros criminosos da *internet*, divertindo-se com a destruição de *sites* e seu impacto na mídia, usando a *internet* para roubar dinheiro e informações, quebrando sistemas de segurança. Além disso, existem os *carders*, que são descritos como os estelionatários da internet, pois fazem compras online com cartões de crédito de outras pessoas ou gerados por programas de computador; eles invadem os sistemas das administradoras de cartões de crédito e obtêm os números. Os *lammers* se apresentam como *hackers*, afirmam que realizam feitos impressionantes, mas não têm conhecimentos específicos sobre o assunto. Os *wannabes*, embora não sejam especialistas, aprenderam um pouco sobre *hacking*, mas não são capazes de grandes feitos (CRESPO, 2011).

Por fim, Marcelo Xavier de Freitas Crespo (2011) menciona os *phreakers*, especialistas em telefonia, que usam seus conhecimentos para fazer ligações gratuitas (usando computadores para confundir as operadoras com relação à origem das chamadas) ou para interceptar conversas telefônicas (utilizando computadores para fazer com que, ao tocar o telefone da pessoa, o telefone do *phreaker* também toque, permitindo ouvir as conversas).

O sujeito passivo do crime cibernético pode ser qualquer pessoa cujo bem jurídico seja lesado ou ameaçado por ações realizadas por meio do computador, tanto Pessoa Física quanto Pessoa Jurídica (ORRIGO; FILGUEIRA, 2015). Alesandro Gonçalves Barreto e Beatriz Silveira Brasil (2016, p. 23), ao abordarem o sujeito passivo, enumeram:

> No que tange ao sujeito passivo, observa-se que qualquer pessoa pode acabar sendo vítima de crimes cibernéticos, uma vez que os criminosos utilizam técnicas cada vez mais apuradas de engenharia social, aliadas às novas tecnologias, atingindo, assim, muitas pessoas.

Após examinar quem pode ser o sujeito passivo dos *cibercrimes*, é crucial analisar os principais crimes digitais que existem atualmente.

3.2 Tipos de crimes cibernéticos

Com o avanço dos recursos tecnológicos, os crimes cometidos por meio de computadores ou qualquer outro dispositivo com acesso à *internet* se tornaram mais sofisticados ao longo dos anos, resultando na criação de novos métodos para a prática de delitos (REIS, 2021).

Diante desse cenário, é imperativo direcionar a atenção para os demais delitos específicos que permeiam o ambiente digital.

3.2.1 Ameaça

Na perspectiva de Marcelo Xavier de Freitas Crespo (2011), para que um ato seja considerado como crime de ameaça, é necessário que a ameaça feita seja injusta (ou seja, algo que a vítima não está obrigada a tolerar) e grave (capaz de causar um dano significativo). Isso pode ocorrer, por exemplo, ao enviar e-mails ou publicar em redes sociais mensagens como "vou te pegar" ou "pode reservar uma vaga no cemitério", atos que configuram crime de ameaça.

Alesandro Gonçalves Barreto e Beatriz Silveira Brasil (2016, p. 157), ao analisarem o tipo criminal e sua consumação como crime digital, enumeram:

> Comete o crime de ameaça o indivíduo que envia mensagens eletrônicas à vítima, prometendo difamá-la gravemente em redes sociais e, ainda, sugerindo males indeterminados que poderiam acometer sua família.
> É possível identificar o cibercriminoso que ameaçou outrem no ciberespaço mediante uma série de evidências a serem coletadas pelo órgão investigativo, entre elas a coleta do IP e da porta de acesso utilizados pelo suspeito para conectar-se à internet, no dia e na hora dos fatos sob apuração.

Dentro desse contexto, é possível que o crime de ameaça seja perpetrado por meio de computadores ou outros dispositivos conectados à internet, desde que a vítima esteja sujeita a suportar um mal injusto e grave.

3.2.2 Participação em suicídio

Quem auxilia, instiga ou induz outra pessoa a cometer suicídio, seja por meio de palavras, gestos ou facilitando o acesso a ferramentas para que a pessoa tire sua própria vida, é responsável por tal delito. No contexto dos crimes virtuais, aqueles

que criam comunidades em redes sociais com dicas e fóruns sobre como tirar a própria vida, ou que direcionam mensagens à pessoa dizendo que o mundo seria melhor sem ela, também cometem esse delito (CRESPO, 2011).

Um exemplo notório desse fenômeno é o jogo virtual conhecido como "baleia azul", que supostamente envolve o estímulo a mutilações corporais em jovens e até mesmo ao suicídio, através de grupos em redes sociais.

3.2.3 Incitação e apologia ao crime

A prática desse delito ocorre quando uma pessoa incita a prática de um crime, incentivando outras pessoas a cometê-lo, ou faz apologia a um ato criminoso ou ao autor de um delito (CRESPO, 2011). Além disso, pode acontecer quando pessoas participam de comunidades em redes sociais que promovem o preconceito através de agressões a outras pessoas e o consumo ou tráfico de drogas (CRESPO, 2011).

Moisés de Oliveira Cassanti (2014, p. 3), em relação a esse tema, menciona:

> Criminosos estão usando os sites de relacionamentos para propagar fotos com armas, vídeos enaltecendo o crime e incentivando o uso de drogas, fazendo clara apologia a diversos crimes e facções criminosas.
> Na maioria das vezes as imagens postadas servem como prova; e mesmo que as mensagens não sejam suficientes para constatar o delito, elas podem servir de pista para a polícia.

Dessa forma, o crime se caracteriza quando a incitação ou apologia ao delito é feita através de meios virtuais, e a própria manifestação virtual serve como prova da prática do delito.

3.2.4 Violação de direitos autorais

No que diz respeito à violação de direitos autorais, Marcelo Xavier de Freitas Crespo (2011) destaca que sua forma mais evidente é a pirataria, que consiste em copiar ou vender produtos sem a devida autorização do detentor dos direitos. Além disso, o uso não autorizado de marcas e documentos obtidos com o auxílio da internet também pode configurar um crime, uma vez que a legislação brasileira protege a propriedade intelectual (CRESPO, 2011).

No contexto dos direitos autorais na internet, conhecido como direito autoral digital, surge a dificuldade em protegê-lo, dada a rapidez e a adaptabilidade das

mídias digitais (MELO; SOUZA, 2019). Considerando que a violação de direitos autorais requer a intenção de obter lucro, sua aplicação pode ser observada tanto através de lucro direto (como na venda de obras não autorizadas) quanto de lucro indireto (como quando um restaurante utiliza música sem autorização para melhorar o ambiente e atrair clientes).

3.2.5 Falsidade ideológica

A falsidade ideológica envolve a inclusão de informações falsas ou a omissão de dados que deveriam constar em documentos públicos ou privados, com o propósito de prejudicar direitos, criar obrigações ou distorcer a verdade sobre fatos legalmente relevantes (CRESPO, 2011). Observa-se que qualquer pessoa que tenha o dever legal de declarar a verdade pode ser considerada autora desse delito (CUNHA, 2016).

Comete esse crime o agente que omite uma declaração que deveria constar em um documento público ou privado, ou que insere ou faz inserir uma declaração falsa ou diferente daquela que deveria ser escrita, com o objetivo de prejudicar direitos, criar obrigações ou distorcer a verdade sobre um fato jurídico considerado relevante.

3.2.6 Falsa identidade

A falsa identidade se configura quando o agente atribui a si mesmo ou a terceiros uma identidade falsa, com o objetivo de obter vantagens para si mesmo ou para outros, ou com o intuito de causar prejuízo a terceiros. Dessa forma, ter um perfil falso de uma pessoa real, viva ou falecida, constitui o crime de falsidade ideológica (ABREU; GOIS, 2021).

O delito de falsa identidade envolve a inclusão de informações falsas ou a omissão de dados que deveriam constar em documentos públicos ou privados, com a intenção de prejudicar direitos, criar obrigações ou distorcer a verdade sobre fatos legalmente relevantes (CRESPO, 2011).

Nesse crime, é importante mencionar que a consumação ocorre no momento em que o agente atribui a si mesmo ou a terceiros a identidade falsa, mesmo que a vantagem pretendida não seja obtida, sendo a tentativa possível no caso de a

execução ser realizada de forma escrita.

3.2.7 Crimes contra a honra

Com relação aos crimes contra a honra, é possível observar a ocorrência de delitos como calúnia, injúria e difamação no ambiente virtual. Moisés de Oliveira Cassanti (2014) menciona que difamar, caluniar e denegrir a imagem das pessoas por meio das redes sociais tornou-se até mesmo uma profissão, fazendo referência à prisão de um criminoso especializado na criação, sob encomenda, de blogs com o intuito de difamar e denegrir a imagem de outras pessoas.

Segundo a definição de Marcelo Xavier de Freitas Crespo (2011), honra refere-se às qualidades físicas, morais e intelectuais de uma pessoa, que a tornam respeitada na sociedade.

Alesandro Gonçalves Barreto e Beatriz Silveira Brasil (2016, p. 159) destacam que:

> As redes sociais, sites, blogs ou e-mails, por exemplo, acabam por se mostrarem, também, instrumentos para a prática dos crimes contra a honra (injúria, calúnia e difamação), previstos nos Arts. 138 a 140 do CP.
> O fato de a publicação em rede social ter veiculado texto que induz os leitores à ocorrência de prática de crimes é suficiente para atingir a esfera íntima das pessoas envolvidas na acusação, configurando evidente abuso àliberdade de informação, passível de responsabilização civil, nos termos do Art. 927 do Código Civil.

A calúnia virtual ocorre quando alguém atribui a outra pessoa a prática de um crime, sabendo que essa acusação é falsa, como publicar em uma rede social que alguém desviou dinheiro de uma empresa (CRESPO, 2011).

Por outro lado, a difamação se configura quando alguém imputa um fato ofensivo à reputação de outra pessoa, desacreditando-a publicamente, mesmo que o conhecimento do crime seja por terceiros, não necessariamente pela própria vítima. Um exemplo de difamação virtual é espalhar na rede social ou por e-mail que é comum ver determinada pessoa se drogando ou se prostituindo (CRESPO, 2011).

Já no crime de injúria, o que se viola é a honra subjetiva da pessoa, por meio de atos de ofensa, difamação ou insulto, sem a necessidade de atribuir um fato específico a alguém. Esse crime se concretiza somente se a vítima toma conhecimento da ofensa. Um exemplo seria chamar alguém de gorda, vaca, imbecil, etc., através das redes sociais.

3.2.8 Racismo

O racismo é definido como a prática, indução ou incitação de discriminação ou preconceito com base em raça, cor, etnia, religião ou origem nacional, sem ser de forma individualizada. Essa conduta pode ocorrer no meio virtual, através de comunidades presentes nas redes sociais que propagam essas ideias (CRESPO, 2011).

Com a popularização crescente da internet, utilizada para uma variedade de propósitos, nem sempre se observa um impacto positivo desse uso na sociedade. Pelo contrário, em muitos casos, a internet é usada para a prática de delitos que prejudicam bens jurídicos amplamente protegidos, como a dignidade da pessoa humana. Condutas lesivas, como o racismo, são frequentemente perpetradas através desse meio eletrônico.

O racismo pode se manifestar de diversas maneiras, incluindo piadas ou comentários que causam ofensa ou mágoa, inflamando a hostilidade em relação ao povo negro (PACHECO, 2020).

Nesse contexto, o racismo se configura como um delito frequente nas redes sociais, especialmente devido à popularização da internet. Nesses casos, a internet, que deveria ser utilizada para propósitos positivos, é desvirtuada e utilizada para disseminar mensagens racistas, causando um impacto significativo no contexto social. Essas ações geram uma profunda sensação de impotência para as vítimas, que são alvo de discriminação e preconceito através desse meio eletrônico.

3.2.9 Intrusão informática

Spencer Toth Sydow (2015) define a intrusão informática, também conhecida como invasão de dispositivo informático ou hacking, como o acesso não autorizado de um usuário a um sistema alheio, com ou sem o objetivo de obter alguma vantagem, utilizando ou não meios ardilosos, violentos ou subterfúgios para enganar o detentor dos direitos a permitir sua entrada, aproveitando-se de algum erro.

O crime de intrusão informática ocorre quando o agente invade um dispositivo informático alheio, esteja ele conectado ou não à rede de computadores, violando indevidamente mecanismos de segurança, com o propósito de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do

dispositivo (COSTA; PACHECO, 2018).

Esse crime pode envolver a instalação de vulnerabilidades ou a busca de vantagem ilícita, independentemente de se alcançar ou não o objetivo pretendido.

3.2.10 “Furto” de identidade virtual

No entendimento de Spencer Toth Sydow (2015), o "furto" de identidade virtual refere-se ao ato de apropriar-se das características e identificações de outra pessoa, assumindo sua identidade sem a devida autorização legal para tal conduta.

Conforme menciona Moisés de Oliveira Cassanti (2014, p. 27), nesse tipo de delito, os criminosos utilizam dados pessoais de terceiros para cometerem golpes, tais como emissão de cartões de crédito, abertura de contas correntes, abertura de empresas, obtenção de empréstimos e compra de bens.

O crime se configura quando há utilização não autorizada de uma identidade virtual alheia, onde o infrator se passa pela pessoa afetada para interagir com indivíduos do círculo social dela, enviar mensagens, persuadir outras pessoas a compartilharem informações pessoais, e assim se apropriar da vida virtual da vítima em benefício próprio, sem necessariamente obter vantagem econômica.

3.2.11Inserção de *malwares*

No âmbito dos métodos desenvolvidos para a prática de delitos digitais, a inserção de *malwares*, que são códigos maliciosos, é considerada a mais popular, uma vez que todos os usuários da internet podem ser alvos desses crimes (ALVES, 2020).

Marcelo Xavier de Freitas Crespo (2011) descreve que os *malwares* incluem os vírus, que são segmentos de código de computação que se anexam a programas ou sistemas com o objetivo de se espalhar pelas máquinas e infectar outros sistemas conectados, muitas vezes através de *e-mails* ou transmissão de dados maliciosos por outros meios. Os *worms*, por sua vez, são uma categoria de vírus que se multiplicam dentro do sistema, causando lentidão, perda de dados e se propagando para outras máquinas, além de possibilitar o controle remoto da máquina infectada em alguns casos.

Um *rootkit* é um tipo de programa utilizado por crackers para manter o controle

sobre um sistema comprometido sem o conhecimento do usuário. Pode ser instalado tanto fisicamente quanto remotamente na máquina (CASSANTI, 2014).

Emerson Wendt e Higor Vinicius Nogueira Jorge (2013, p. 31), definem *keyloggers* como:

> [...] um registrador do teclado, ou seja, realiza a monitoração das informações digitadas pelo usuário do computador.
> A utilização desse tipo de *software* ocorre geralmente com o intuito de permitir a coleta de informações sensíveis sobre o usuário do computador e dessa forma oferecer subsídios para que o *cibercriminoso* cometa seus crimes contra a vítima.

Moisés de Oliveira Cassanti (2014) define os *spywares* como programas projetados para coletar informações sobre o usuário e seus hábitos na internet, podendo fazê-lo com ou sem o consentimento do usuário. Por outro lado, os adwares são programas gratuitos para download que são financiados por anúncios. Ao serem instalados, incluem um componente adicional que exibe publicidade, seja por meio de pop-ups ou baixando barras de ferramentas no navegador do usuário.

3.2.12 Engenharia Social

Engenharia social é caracterizada como qualquer método utilizado para mascarar a realidade, com o objetivo de explorar ou enganar a confiança de uma pessoa detentora de dados importantes que se deseja acessar. Trata-se de um artifício intelectual empregado para obter informações sigilosas, fazendo uso da tecnologia ou de qualquer meio de comunicação disponível (CRESPO, 2011).

Na visão de Emerson Wendt e Higor Vinicius Nogueira Jorge (2012, p. 21), engenharia social:

> É a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo.

Dessa forma, ao distorcer a realidade e recorrer a artifícios com o objetivo de enganar as pessoas, os criminosos conseguem acessar informações essenciais para a realização de seus crimes.

3.2.13 Pornografia infantil

Na visão de Moisés de Oliveira Cassanti (2014), a pornografia infantil, também conhecida como pedofilia, abrange a produção, publicação, venda, aquisição e armazenamento de material pornográfico envolvendo crianças. Essas atividades ocorrem principalmente pela rede mundial de computadores, utilizando páginas da *web*, *e-mails*, grupos de notícias, salas de bate-papo (*chat*) e outros meios digitais. Além disso, também engloba o uso da *internet* para atrair crianças ou adolescentes a participarem de atividades sexuais ou serem expostos de forma pornográfica.

Emerson Wendt e Higor Vinicius Nogueira Jorge (2013, p. 98) ressaltam que:

> A pornografia infantil é uma forma ilegal de pornografia que se caracteriza pela utilização de imagens de cunho erótico de crianças e adolescentes e representa uma das maiores preocupações na internet.
> O suposto anonimato que envolve a utilização da internet muitas vezes representa um campo fértil para inúmeros tipos de comportamentos que o indivíduo não teria coragem de realizar se tivesse que se expor. Nesse contexto, a internet pode propiciar divulgação de pornografia infantil ou prática de crimes contra crianças e adolescentes sob uma conotação sexual.

Nesse contexto, a pornografia infantil é um crime frequentemente perpetrado pela rede mundial de computadores, aproveitando-se da facilidade de troca de dados e da sensação de anonimato proporcionada pela internet. Este tipo de crime pode causar traumas irreversíveis às suas vítimas.

3.2.14 *Cyberbullying*

Cyberbullying é caracterizado pela ação intencional de uma pessoa que utiliza as tecnologias da informação e comunicação para hostilizar, denegrir, diminuir a honra ou reprimir de maneira contínua outra pessoa (CASSANTI, 2014).

Acerca da conceituação do *cyberbullying* e sua origem, Emerson Wendt e Higor Vinicius Nogueira Jorge (2013, p. 102) destacam:

> Independentemente do tipo de agressão, quando esta se torna reiterada, pode tratar-se do denominado *bullying*. Palavra originada da língua inglesa que significa valentão, caracteriza-se pela prática de agressões físicas ou psicológicas de forma habitual, traumática e prejudicial às vítimas.
> Mais recentemente surgiu o termo *cyberbullying,* que consiste no mesmo tipo de agressão, porém praticado por intermédio do computador ou outros recursos tecnológicos. Esse tipo de ofensa pode ser praticado das mais

> variadas formas e tem como característica a rápida disseminação pela rede, ou seja, em pouco tempo a ofensa é disponibilizada em uma infinidade de sites e blogs. Dificilmente a vítima consegue extirpar a informação de todos os locais onde se encontra.

O *cyberbullying* pode ser compreendido como uma forma de intimidação e violência que ocorre na internet, especialmente nas redes sociais. Ele transcende fronteiras e não discrimina vítimas ou perpetradores, trazendo consequências não apenas virtuais, mas também impactos reais para a vítima.

3.2.15 Xenofobia

Como se depreende da visão de Moisés de Oliveira Cassanti (2014, p. 38):

> A xenofobia é uma forma de discriminação social que consiste na aversão a diferentes culturas e nacionalidades. Considerada crime de ódio, a xenofobia mostra-se através de humilhação, constrangimento, agressão física e moral àquele que não é natural do lugar do agressor. Nas redes sociais a xenofobia vem sendo praticada por pessoas que se esquecem ou não sabem que a liberdade de expressão tem limites.

Com o surgimento da Covid-19, observa-se um aumento nos ataques xenofóbicos em várias partes do mundo, especialmente em relação aos chineses e descendentes, que acabam sendo as principais vítimas devido ao primeiro caso da doença ter sido registrado em uma cidade chinesa (LOVISI, 2020).

Essa tendência reflete uma preocupação global com a xenofobia e o racismo, evidenciada pela existência de um Protocolo Adicional à Convenção de Budapeste, que solicita aos países signatários medidas para combater esses crimes.

3.2.16 Vingança pornô *(porn revenge)*

Alesandro Gonçalves Barreto e Beatriz Silveira Brasil (2016) mencionam que o termo "*porn revenge*" tem se popularizado no contexto atual, referindo-se à pornografia de revanche ou vingança pornográfica. Isso ocorre quando fotos e/ou vídeos íntimos de terceiros são divulgados sem o consentimento prévio dessas pessoas. Geralmente, esses vídeos ou fotografias foram consentidos durante o relacionamento, mas, após o término, são expostos em redes sociais ou aplicativos de celular com o objetivo de humilhar uma das partes.

Débora Pricila Silveira (2016) elenca que:

> O nome pode soar estranho no início, mas, o seu significado não é novidade para ninguém. *Revenge porn* ou pornografia de vingança é a expressão usada para denominar o ato de expor, na internet, fotos ou vídeos íntimos de terceiros, sem o consentimento dos mesmos. Casos do tipo costumam acontecer, na maioria das vezes, quando um casal termina o relacionamento e uma das partes divulga as cenas íntimas na rede mundial de computadores, com o objetivo de vingar-se, ao submeter o ex-parceiro a humilhação pública.

Dessa forma, é delineado o tipo penal comumente praticado pela rede mundial de computadores ou por dispositivos com acesso à internet, que resulta na exposição de momentos íntimos de uma pessoa na rede.

3.2.17 Furto Mediante Fraude

No furto mediante fraude, o autor subtrai a "coisa" com o intuito de enganar a vítima, utilizando ações que distraiam a vigilância e atenção dela sobre o bem (OLIVEIRA, 2020).

As três qualificadoras do furto virtual implicam no aproveitamento da boa-fé da vítima. Elas são definidas como furto mediante fraude com uso de dispositivo eletrônico ou informático, furto utilizando programa malicioso e furto por qualquer outro meio fraudulento análogo (BITENCOURT, 2021).

De acordo com a visão de Eduardo Luiz Santos Cabette (2021), o tipo penal descrito no §4º-B aborda a fraude praticada com o emprego de dispositivo eletrônico ou informático, sem exigir conexão à internet, violação de mecanismos de segurança ou utilização de programas maliciosos. Basta o uso da tecnologia eletrônica e/ou informática. O §4º-C, em seu inciso I, prevê aumento de pena entre 1/3 e 2/3 quando o crime é cometido usando servidor mantido fora do território nacional, o que dificulta a investigação. É importante ressaltar que é o servidor que precisa estar fora do país, não necessariamente o agente do crime. O inciso II prevê aumento de pena de 1/3 ao dobro quando o crime é praticado contra idoso ou vulnerável (CABETTE, 2021).

3.2.18 Estelionato virtual

O estelionato virtual é caracterizado quando uma pessoa, utilizando

equipamentos tecnológicos e acesso à rede de dados, induz ou mantém a vítima em erro, com o objetivo de obter vantagem ilícita, seja para si própria ou para terceiros, por meio de qualquer artifício fraudulento (OLIVEIRA, 2020).

Para ilustrar a ocorrência do estelionato virtual, Paulo Roberto Silvério Moreira (2022) oferece o seguinte exemplo:

> Nessa toada, criminosos criam páginas falsas, oferecendo oportunidades surreais e, em muitos casos, enviam mensagens por WhatsApp, o que acaba enganando as vítimas mais vulneráveis. Essas fraudes aplicadas caracterizam o crime de estelionato virtual e, alguns exemplos bastantes comuns são: proposta de empréstimo com a taxa de juros baixa ou sem nenhuma taxa; empregos oferecidos na internet com bons salários, entretanto, sendo pedido um valor financeiro para efetuar a inscrição; sites de vendas de produtos que nunca serão entregues; mensagens em massa via WhatsApp, mais conhecidas como correntes; enfim, todos os meios que buscam, de alguma maneira, obter vantagem patrimonial ilícita, induzindo as pessoas ao erro.

Nesse cenário, o estelionato virtual se torna uma prática amplamente difundida na sociedade contemporânea, impulsionada pela rápida disseminação de informações na *internet* e nas redes sociais. Muitas vezes, as pessoas acabam acreditando nessas informações, seja por erro, ganância ou falta de conhecimento sobre o uso seguro da rede.

O estelionato qualificado pelo uso de meio eletrônico ocorre quando a fraude é cometida com o uso de informações fornecidas pela vítima ou terceiros induzidos a erro por meio das redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento ou qualquer outro meio fraudulento similar, conforme previsto no art. 171, §2º-A. O §2º-B estabelece um aumento de pena de 1/3 a 2/3 para essa modalidade de crime, caso os servidores utilizados para sua prática estejam localizados no exterior.

3.2.19 Ciberextorsão

A ciberextorsão é um crime cibernético em que um indivíduo utiliza a internet para exigir dinheiro, outros bens ou determinados comportamentos de outra pessoa, ameaçando causar danos à sua integridade física, reputação ou propriedade (BAPTISTA, 2016). Durante o período da pandemia, o número de ataques cibernéticos aumentou significativamente, sendo o ransomware o mais comum. Trata-se de uma forma de extorsão digital em que os dados ou sistemas de

computador das vítimas são criptografados por meio de um software e só são liberados após o pagamento, geralmente feito por meio de moedas digitais (TIINSIDE, 2021).

É importante ressaltar que a maioria das tentativas de ciberextorsão começa com a distribuição de malware por *e-mail* ou por meio de *downloads* de *sites* comprometidos.

3.2.20 *Typosquatting*

O *typosquatting* é uma prática na qual criminosos registram nomes de domínio que são semelhantes aos de marcas e empresas conhecidas, aproveitando-se de erros de digitação comuns feitos pelos usuários. Esses domínios falsos geralmente têm aparência similar aos originais e podem ser usados para diversos propósitos maliciosos (BARRETO, 2020). Ao induzir os usuários a acessarem esses sites falsos, os criminosos podem tentar roubar informações pessoais ou financeiras, distribuir malware ou realizar outras atividades ilícitas.

Conforme Alesandro Gonçalves Barreto (2020, p. 224-225):

> A disseminação de *fake News* tem sido impulsionada por essa prática. Com o intuito de dar às falsas histórias uma aparência maior de realidade, os infratores registram um endereço semelhante ao de um *site* conhecido para divulgação dos fatos.
> [...]
> Uma das motivações do *typosquatter*, na era da desinformação, visa apenas à monetização de uma página através de clickbait.

O *typosquatting*, conforme descrito por Rofis Elias Filho (2021), envolve a prática de registrar nomes de domínio com pequenas alterações na grafia, como a troca ou remoção de uma letra, para imitar um domínio já registrado. Essas sutis mudanças são feitas com o objetivo de confundir os usuários e levá-los a acessar sites falsos, aproveitando-se dos erros de digitação comuns.

Essa técnica também pode ser aplicada no registro de marcas, onde os infratores tentam imitar marcas comerciais legítimas com grafias semelhantes, induzindo os consumidores ao erro.

3.2.21 *Stalking*

O *stalking*, como descrito por Andrion (2021), envolve a perseguição persistente e incessante de alguém, seja de forma virtual ou presencial, através da monitoração, coleta de informações e contato. Com a promulgação da Lei nº 14.132/21, foi incluído o art. 147-A no Código Penal, que tipifica o crime de perseguição (*stalking*), refletindo a ocorrência desse delito na sociedade contemporânea.

Embora seja uma novidade em termos de legislação penal, o *stalking* sempre ocorreu e era tratado de maneira diversa, inclusive nas Leis das Contravenções Penais. A nova lei trouxe uma definição mais específica e tipificou o *stalking* como crime, estabelecendo um tipo penal próprio para essa conduta.

3.3 Estatística e tendências aos crimes cibernéticos

Diante das vantagens sociais que a internet trouxe, surge o aspecto sombrio do ciberespaço. Com o aumento significativo do número de usuários, a criminalidade online vem se intensificando, o que, por sua vez, demanda uma adaptação do sistema legal para combater os delitos cibernéticos.

> É impossível a existência de um grupo de humanos sem a presença de normas a regularo seu dia a dia; caso isso fosse possível, cada um faria o que bem entendesse, o que traria o caose o fim da humanidade (BONFATI; KOLBE, 2020, p.20).

Em qualquer contexto onde há um grupo de pessoas interagindo, a necessidade de estabelecer regras é evidente. No ambiente virtual, essa necessidade não é diferente. Com a proliferação da internet, tornou-se fundamental a implementação de uma regulamentação jurídica específica para conter os crimes cibernéticos. Conforme definido por Bonfat e Kolbe (2020, p.62), os crimes cibernéticos englobam uma gama de comportamentos nos quais recursos da tecnologia da informação são utilizados como meio para cometer atos ilícitos.

Sobre a evolução dos crimes cibernéticos denota Bertholdi (2020, p.8):

> A história dos cibercrimes é uma narrativa contundente da sua evolução e relevânciano cenário mundial, denotando um ambiente fértil que a internet é para a criminalidade. Como podemos observar, fronteiras nacionais não representam obstáculos para *hackers* e cibercriminosos que se lavram da alta porosidade dos caminhos virtuais e da pluralidade de normas e leis locais sem aplicabilidade no ambiente internacional.

Considerando esses elementos, é claro que a criminalidade na internet tem se expandido para além das fronteiras nacionais. A inclusão digital proporcionou uma acessibilidade ampliada aos usuários, mas também os tornou mais vulneráveis. A popularização do ambiente digital ocorreu de maneira desordenada, inicialmente sem definição de limites claros e sem normas específicas para a punição de crimes cibernéticos em escala global.

Com o crescimento exponencial da criminalidade online refletindo uma nova dinâmica social, torna-se crucial examinar como a legislação e a jurisprudência têm respondido aos desafios dos crimes cibernéticos. Enquanto as estatísticas revelam um aumento alarmante na incidência desses delitos, os tribunais enfrentam o dilema de aplicar leis concebidas para o mundo físico a um ambiente virtual em constante evolução. Essa adaptação jurídica é exemplificada pela jurisprudência do Superior Tribunal de Justiça (STJ), especialmente em casos como a exposição de imagens não autorizadas na internet, onde a interpretação analógica se torna uma ferramenta essencial para a aplicação da justiça.

3.4 Os crimes cibernéticos na visão da jurisprudência

A insuficiência da legislação para lidar com os crimes virtuais tem levado os tribunais a adotar diferentes interpretações. Muitas vezes, recorre-se à analogia para julgar esses delitos, uma vez que a maioria dos crimes cometidos no ambiente digital são essencialmente os mesmos que ocorrem fora dele, variando apenas o meio utilizado para sua realização. Em relação à exposição de imagens não autorizadas na internet, destaca-se a jurisprudência do Superior Tribunal de Justiça (STJ):

> RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. DIVULGAÇÃO DE FOTOGRAFIAS DE NUDEZ (PRODUZIDAS E CEDIDAS COM FINS COMERCIAIS) SEM O CONSENTIMENTO DA MODELO RETRATADA, EM ENDEREÇOS ELETRÔNICOS DA INTERNET. RESPONSABILIDADE DO PROVEDOR PARA PROMOVER A RETIRADA DO CONTEÚDO INDICADO A PARTIR DA DETERMINAÇÃO JUDICIAL PARA TANTO. ART. 21 DO MARCO CIVIL DA INTERNET. INAPLICABILIDADE. RECURSO ESPECIAL PROVIDO DO PROVEDOR DE INTERNET E PREJUDICADO O MANEJADO PELA PARTE DEMANDANTE. (STJ - REsp: 1930256 SP 2021/0093404-0, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 07/12/2021, T3 - TERCEIRA TURMA, Data de Publicação: DJe 17/12/2021)

Em 2017, o Tribunal de Justiça do Piauí proferiu uma decisão sem precedentes relacionada ao Artigo 213 do Código Penal. Esta decisão resultou na prisão de um indivíduo por estupro virtual, em que o acusado utilizou meios virtuais para ameaçar a vítima, exigindo a divulgação de fotos íntimas na internet e solicitando novas imagens pornográficas, prática conhecida como sextorsão. Este caso estabeleceu um importante precedente na jurisprudência:

> Ressalta-se que esse tipo de conduta é denominada pela doutrina moderna como “sextorsão”, a palavra é uma aglutinação da palavra “sexo” com a palavra “extorsão”. Esse neologismo, ainda quase desconhecido no Brasil, que pode ser caracterizada como uma forma de exploração sexual que se dá pelo constrangimento de uma pessoa à prática sexual ou pornográfica, em troca da preservação em sigilo de imagem ou vídeo da vítima em nudez total ou parcial, ou durante relações sexuais, previamente guardadas.

Neste caso, o ministro Rogério Schietti Cruz negou um pedido de Habeas Corpus ao acusado, enfatizando a exploração do anonimato proporcionado pelo ambiente virtual e a vulnerabilidade das vítimas, que são induzidas a extorquir valores cada vez maiores. Essa decisão gerou um amplo debate entre juristas e doutrinadores do país, levantando questões sobre os limites da liberdade sexual, a possibilidade de tipificação no Código Penal e a discussão sobre a definição de estupro sem a conjunção carnal.

Em relação a um conflito de competência, a Terceira Seção estabeleceu que a Justiça Federal tem jurisdição para julgar um caso de ameaça em que o suposto criminoso, residente nos Estados Unidos, teria utilizado o Facebook para intimidar uma mulher no Brasil. Após análise dos autos, a Justiça estadual determinou que a competência para processar e julgar crimes previstos em convenções internacionais, iniciados fora do país e com resultado no Brasil, cabe à Justiça Federal, conforme

estipulado no artigo 109 da Constituição Federal.

De acordo com o entendimento jurisprudencial, o julgamento dos crimes praticados na internet é atribuído ao local da publicação do fato. Se essa localização for incerta, a competência será determinada pelo local onde as investigações foram iniciadas. Normalmente, a competência recai sobre a Justiça Estadual, mas quando a vítima é brasileira e o crime ocorre em outro país, a competência é da Justiça Federal (Bertholdi, 2020).

De acordo com o Recurso Extraordinário n.° 628624 o Superior Tribunal de Justiça (STF):

> Compete a Justiça Federal o processamento e julgamento dos crimes na internet envolvendo divulgação pornográfica de crianças e adolescente, fundamentados na expansão global que esse tipo de conteúdo pode atingir. O recurso abordado trata do crime previsto no art. 241-A do Estatuto da Criança e do Adolescente.
>
> RECURSO EXTRAORDINÁRIO. REPERCUSSÃO GERAL RECONHECIDA. PENAL. PROCESSO PENAL. CRIME PREVISTO NO ARTIGO 241-A DA LEI 8.069/90 (ESTATUTO DA CRIANÇA E DO ADOLESCENTE). COMPETÊNCIA. DIVULGAÇÃO E PUBLICAÇÃO DE IMAGENS COM CONTEÚDO PORNOGRÁFICO ENVOLVENDO CRIANÇA OU ADOLESCENTE. CONVENÇÃO SOBRE DIREITOS DA CRIANÇA. DELITO COMETIDO POR MEIO DA REDE MUNDIAL DE COMPUTADORES (INTERNET). INTERNACIONALIDADE. ARTIGO 109, V, DA CONSTITUIÇÃO FEDERAL. COMPETÊNCIA DA JUSTIÇA FEDERAL RECONHECIDA. RECURSO DESPROVIDO.

Com base no precedente do Superior Tribunal de Justiça (STJ) no Recurso Especial Resp. 617221, onde "o tribunal por unanimidade entendeu que o envio de fotos pornográficas de menores pela internet é crime" (BRASIL, 2017), é evidente que a legislação brasileira reconhece a gravidade dos crimes virtuais, mesmo diante da complexidade e do anonimato proporcionado pelas redes.

Apesar das dificuldades, existe a possibilidade de identificação dos autores dos cibercrimes. A legislação brasileira está em constante evolução para lidar com esses desafios, com a criação de regulamentos específicos destinados a punir os responsáveis pelos delitos virtuais. Além disso, os precedentes jurisprudenciais são utilizados para fortalecer as penalidades contra aqueles que cometem esse tipo de crime.

No mais, a jurisprudência brasileira tem desempenhado um papel crucial na interpretação e aplicação das leis em relação aos crimes cibernéticos. Enquanto a

legislação atual ainda enfrenta desafios na adaptação aos novos cenários digitais, iniciativas como a LGPD surgem com o intuito de fortalecer a proteção dos dados pessoais e mitigar os impactos sociais e econômicos associados aos delitos virtuais. Esses esforços refletem uma resposta contínua e adaptativa do sistema jurídico frente às transformações tecnológicas e às demandas por maior segurança e privacidade dos usuários.

3.5 Impactos sociais e econômicos cibernéticos

Com o propósito de conter o aumento dos crimes virtuais e fortalecer a autonomia e segurança dos usuários sobre seus dados pessoais, a LGPD tem como principal objetivo estabelecer previamente o que pode ou não ser usado com consentimento adequado. Dentro dessa abordagem, as empresas e seus negócios enfrentarão impactos específicos (MAIA, 2019).

Ao considerar os impactos na área de comunicação digital, é necessário também contemplar as mudanças que surgirão a partir disso. Era comum o uso e armazenamento indevido de dados pessoais dos usuários, sujeitando-os a manipulações que poderiam levar a vazamentos e crimes virtuais (MAIA, 2019). Portanto, a nova regulamentação da LGPD tem o potencial de impactar positivamente o tratamento desses dados, permitindo que os usuários recuperem o controle sobre eles. Isso significa que as empresas interessadas em utilizar esses dados devem divulgar claramente o motivo e o método de sua utilização (MAIA, 2019).

A mudança na forma como as empresas lidam com os dados dos usuários influenciará diretamente a apresentação e comercialização da mídia digital. Anteriormente, as empresas podiam usar os dados como desejavam, mas agora há regras a serem seguidas (MAIA, 2019).

As empresas e organizações serão obrigadas a cumprir essas novas regras, que exigem transparência absoluta com os usuários em todas as etapas de coleta e uso de dados, afetando diretamente os investimentos em comunicação digital e a comercialização da mídia (MAIA, 2019).

Além disso, há impactos no processo de análise de dados, com a LGPD estabelecendo novas condutas para a captura, armazenamento e uso de dados pessoais dos usuários. O cuidado com esses dados se torna crucial, pois qualquer

violação ou exposição requer notificação aos usuários dentro de 72 horas, sob pena de multa (MAIA, 2019).

Para implementar a nova regulamentação, as empresas devem cumprir estritamente as diretrizes da LGPD; caso contrário, estarão sujeitas a multas, advertências ou até mesmo ao fechamento das atividades. As multas podem chegar a 2% do faturamento da empresa, limitadas a R$ 50.000.000,00, e podem ser aplicadas diariamente (ARAÚJO, 2020).

Além das penalidades financeiras, o descumprimento das regulamentações afeta a reputação e a confiabilidade das empresas no mercado. As infrações devem ser expostas publicamente e os infratores podem ser impedidos de acessar bancos de dados ou até mesmo serem excluídos, o que pode prejudicar significativamente a confiança dos usuários na segurança de seus dados (REGINA, 2020).

As empresas devem se adaptar às novas regras da LGPD, avaliando a maturidade de seus processos e os riscos associados. Isso inclui uma revisão cuidadosa dos contratos comerciais e o fortalecimento da cultura interna de proteção de dados (MARKETINGFINNET, 2020).

A implementação da LGPD pode ser desafiadora para as empresas brasileiras, especialmente aquelas que lidam com grandes volumes de dados pessoais. No entanto, os benefícios a longo prazo, como um ambiente de negócios mais seguro e a confiança do consumidor, podem superar os custos iniciais. Portanto, a adesão às regulamentações da LGPD pode promover confiança e segurança tanto para as empresas quanto para os usuários.

4 A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL E OS POSSÍVEIS CRIMES CIBERNÉTICOS

Nos últimos anos, a importância da proteção de dados tem crescido significativamente, tanto no Brasil quanto em todo o mundo. A solicitação de dados pessoais por várias entidades, públicas ou privadas, é uma prática comum. No entanto, apesar de haver propriedade desses dados, muitas vezes há pouco controle sobre como eles são utilizados. Para abordar essa questão, foram estabelecidas marcos regulatórios, como o Regulamento Geral sobre a Proteção de Dados (GDPR), introduzido em agosto de 2018. O principal objetivo do GDPR é oferecer aos usuários controle sobre suas informações pessoais armazenadas por empresas.

A Lei Geral de Proteção de Dados (LGPD) regula o uso, a proteção, o tratamento e a transferência de dados pessoais dentro do território nacional. Anteriormente, as empresas raramente discutiam os riscos, prejuízos e vulnerabilidades associados à expansão dos meios digitais. Em um ambiente digital cada vez mais interconectado, a LGPD aborda especificamente o tratamento de dados pessoais online, seja por indivíduos ou entidades públicas e privadas, com o objetivo de preservar os direitos fundamentais.

Os princípios fundamentais da proteção de dados incluem o respeito à privacidade, a autodeterminação, a liberdade de expressão, informação e comunicação, bem como a preservação da intimidade, honra e imagem. Na era digital, a internet oferece acesso a vasto conhecimento, interação global, facilidades e oportunidades, tudo literalmente ao alcance das mãos. Por isso, a LGPD se aplica a qualquer processo de tratamento de dados realizado por pessoas físicas ou jurídicas, independentemente do meio utilizado ou da localização geográfica, contanto que os dados em questão tenham sido coletados no território nacional. (BRASIL, 2018).

No contexto da Lei Geral de Proteção de Dados, é fundamental destacar o papel dos diferentes agentes envolvidos no processo de proteção de dados: o Titular dos Dados, referindo-se à pessoa natural a quem os dados pessoais se referem e que são objeto de tratamento; o Controlador dos Dados, definido como a pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões relativas ao tratamento desses dados; o Operador dos Dados, que pode ser uma pessoa física ou jurídica, pública ou privada, encarregada de realizar o tratamento dos dados pessoais em nome do controlador, seguindo as diretrizes estabelecidas por este último; e a ANPD (Autoridade Nacional de Proteção de Dados), o órgão do governo federal responsável por supervisionar, implementar e fiscalizar o cumprimento da LGPD no Brasil, com autonomia técnica e decisória garantida por lei.

O acesso à internet pode resultar em abusos e violações dos direitos fundamentais do usuário, como intimidade, privacidade e liberdade, em benefício das instituições. No entanto, o artigo 6º da LGPD estabelece que as atividades de tratamento de dados pessoais devem ser realizadas com base na boa-fé e em conformidade com os princípios da finalidade, adequação, necessidade, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização.

O primeiro passo no tratamento de dados pessoais é obter o consentimento do

titular, conforme exigido pelas obrigações legais, exceto em situações de políticas públicas para proteção da vida e saúde. Esse consentimento pode ser obtido por escrito ou por outros meios que demonstrem a manifestação do titular. É importante observar que o artigo 9º da LGPD confere ao titular o direito de acessar facilmente as informações sobre o tratamento de seus dados, que devem ser disponibilizadas de maneira clara e adequada, conforme previsto na regulamentação (BRASIL, 2018).

O controlador só está autorizado a processar dados pessoais para finalidades legítimas, que são determinadas com base em situações específicas, incluindo o apoio e promoção das atividades do próprio controlador, a proteção do titular e a prestação de serviços em seu benefício, desde que respeitem suas expectativas legítimas, bem como seus direitos e liberdades fundamentais. É importante destacar que o tratamento de dados sensíveis só é permitido em circunstâncias específicas, como o cumprimento de obrigações legais e regulatórias, o compartilhamento com órgãos da administração pública, para fins de pesquisa, desde que os dados sejam anonimizados, para o exercício de direitos, para proteção da vida e garantia de prevenção à fraude e segurança do titular (BRASIL, 2018).

Quanto ao tratamento de dados de crianças e adolescentes, a LGPD estipula que ele deve ocorrer apenas com o consentimento específico dos pais ou responsável legal. Os controladores também são obrigados a disponibilizar publicamente informações sobre os dados coletados e divulgar de forma clara e acessível os detalhes necessários para proporcionar a informação adequada.

A LGPD aborda todo o ciclo de vida dos dados, incluindo o seu término. Conforme descrito nos artigos 15 e 16 da legislação, o tratamento de dados deve cessar quando a finalidade do tratamento for alcançada, quando o titular solicitar o término do tratamento, ou por determinação da Autoridade Nacional de Proteção de Dados. (BRASIL, 2018).

No que diz respeito aos direitos dos titulares dos dados, estes têm o direito de, a qualquer momento, solicitar ao controlador: a confirmação da existência do tratamento, acesso aos dados, correção, anonimização, bloqueio, eliminação e revogação. Além disso, de acordo com os artigos 19 e 20, a confirmação da existência e o acesso aos dados podem ser obtidos por meio de uma solicitação simples, seja eletronicamente ou em formato impresso. Adicionalmente, o titular tem o direito de requerer a revisão de decisões tomadas exclusivamente com base no

tratamento automatizado de dados pessoais, que afetem seus interesses, incluindo decisões relacionadas à definição de seu perfil pessoal, profissional, de consumo, de crédito ou aspectos de sua personalidade. (BRASIL, 2018).

A LGPD também aborda a transferência internacional de dados, estipulando que essa transferência só é permitida em determinadas circunstâncias, tais como para países ou organizações internacionais que garantam um nível adequado de proteção de dados, para outro controlador que ofereça e comprove garantias de conformidade, em casos de cooperação jurídica internacional entre órgãos, para proteção da vida com autorização da autoridade nacional de proteção de dados, cooperação internacional, para necessidades de políticas públicas ou com o consentimento do titular. (BRASIL, 2018).

Em outro aspecto da LGPD, tanto o controlador quanto o operador são obrigados a manter registros das operações de tratamento de dados, e a autoridade nacional de proteção de dados pode exigir que o controlador elabore um relatório de impacto à proteção de dados, inclusive para dados sensíveis. O operador, por sua vez, deve realizar o tratamento de acordo com as instruções fornecidas pelo controlador.

De acordo com as diretrizes da LGPD, o controlador é obrigado a designar um encarregado pelo tratamento dos dados pessoais. O encarregado tem diversas responsabilidades, incluindo: receber reclamações e comunicações dos titulares, prestar esclarecimentos e tomar providências necessárias, receber notificações da autoridade nacional de proteção de dados, orientar os funcionários e contratados sobre práticas de proteção de dados e executar outras ações pertinentes. (BRASIL, 2018).

No que diz respeito às responsabilidades e ao ressarcimento de danos conforme estabelecido pela LGPD, tanto o controlador quanto o operador são responsáveis por reparar danos causados devido a falhas no tratamento de dados, violações da legislação e ações ilícitas. No entanto, os agentes de tratamento não serão responsabilizados caso não estejam de fato realizando o tratamento dos dados atribuídos a eles ou se o dano for exclusivamente causado por culpa do próprio titular.

Quanto à segurança e sigilo dos dados, os agentes de tratamento devem implementar medidas de segurança administrativas e técnicas adequadas para proteger os dados pessoais contra acessos não autorizados, bem como contra

situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

A Autoridade Nacional pode estabelecer padrões técnicos mínimos para garantir a aplicação dos fatores de segurança e sigilo. Além disso, os agentes de tratamento e qualquer pessoa envolvida em qualquer fase do tratamento devem assegurar a segurança da informação conforme previsto na lei, mesmo após o término do tratamento. De acordo com o artigo 48 da LGPD, o controlador é obrigado a comunicar à Autoridade Nacional e ao titular sobre qualquer incidente de segurança que possa representar um risco ou dano relevante aos titulares dos dados. (BRASIL, 2018).

Em relação às boas práticas e governança, a LGPD estabelece no artigo 50 que os controladores e operadores podem desenvolver regras de boas práticas e governança, abordando diversos aspectos como organização, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para diferentes tipos de tratamento, ações educativas, mecanismos de supervisão e mitigação de riscos, entre outros.

Quanto às penalidades e sanções administrativas, a LGPD prevê que, em caso de infração, a Autoridade Nacional pode aplicar diversas sanções, incluindo advertência com prazo para correção, multa simples de até 2% do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil, limitada a R$ 50.000.000,00 por infração, multa diária, publicação da infração, bloqueio ou eliminação dos dados pessoais relacionados à infração, conforme necessário. (BRASIL, 2018).

A LGPD estabelece várias sanções administrativas em caso de infração, incluindo a suspensão parcial do funcionamento do banco de dados relacionado à infração por até 6 meses, prorrogáveis por igual período até a regularização da atividade de tratamento pelo controlador; a suspensão do exercício da atividade de tratamento dos dados pessoais relacionados à infração por até 6 meses, também prorrogáveis; e a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados. (BRASIL, 2018).

A Autoridade Nacional de Proteção de Dados (ANPD) será responsável por definir, por meio de regulamentação, as sanções administrativas e infrações, que serão objeto de consulta pública. Além disso, a ANPD irá estabelecer metodologias para orientar o cálculo do valor-base das multas. O valor da multa diária aplicável às infrações desta lei deve considerar a gravidade da falta e o alcance do dano ou

prejuízo causado, e deve ser fundamentado pela autoridade nacional.

Quanto à Autoridade Nacional de Proteção de Dados (ANPD), esta é um órgão da administração pública federal, integrante da Presidência da República. A ANPD possui autonomia técnica e decisória assegurada, e sua composição inclui um Conselho Diretor, um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, uma Corregedoria, uma Ouvidoria, um órgão de assessoramento jurídico, unidades administrativas e unidades especializadas.

Compete à ANPD: zelar pela proteção de dados pessoais, zelar pela observância dos segredos comercial e industrial observada a proteção de dados pessoais e do sigilo das informações, elaborar diretrizes para a política nacional de proteção de dados pessoais e da privacidade, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, apreciar petições de titular contra controlador após comprovada pelo titular a não solução no prazo estabelecido, promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais (BRASIL, 2018).

Promover ainda ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional, dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; solicitar a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta lei, elaborar relatórios de gestão anuais acerca de suas atividades (BRASIL, 2018).

Além de 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, ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento, arrecadar e aplicar suas receitas e publicar, realizar o detalhamento dos recursos, realizar auditorias, ou determinar sua realização (BRASIL, 2018).

No âmbito da atividade de fiscalização, compete à ela celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, comunicar às autoridades competentes as infrações penais das quais tiver conhecimento, comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal, implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta lei.

A implementação da LGPD não apenas redefine as práticas de tratamento de dados, mas também estabelece um novo paradigma de responsabilidade corporativa e individual na era digital. Em um contexto global onde as violações de dados e os crimes cibernéticos são cada vez mais comuns, a aplicação rigorosa da LGPD destaca-se como um marco essencial na proteção dos direitos individuais e na promoção da confiança nas relações digitais.

4.1 Estudo e análise das penalidades aplicadas de acordo com a LGPD em casos de violações de dados e crimes cibernéticos no Brasil e no mundo

Ao explorar-se exemplos de uso não autorizado de informações, identificam-se cenários nos quais a LGPD desempenhou um papel significativo, evidenciando sua influência no campo jurídico e suas ramificações na abordagem de tais incidentes. Essa análise proporciona uma compreensão valiosa de como a legislação pode impactar diretamente a maneira como as organizações lidam com violações de dados e atividades criminosas online, visando minimizar danos e reforçar a salvaguarda dos direitos individuais.

O episódio envolvendo a *British Airways* está associada a um incidente de grande escala de exposição de informações pessoais. Em setembro de 2018, a *British Airways* anunciou a ocorrência de um ataque cibernético que resultou no acesso não autorizado a dados pessoais de aproximadamente 500.000 clientes. Esses dados comprometidos incluíam informações como nomes, endereços de e-mail, números de cartão de crédito e detalhes de pagamento.

O ataque foi realizado por meio de uma técnica de *skimming* de dados em seu

site e aplicativo móvel, onde os invasores conseguiram redirecionar os clientes para um site fraudulento e capturar suas informações de pagamento durante o processo de reserva de voos.

Após a identificação do vazamento, a *British Airways* prontamente comunicou às autoridades relevantes e adotou medidas para conter o incidente, reforçar sua segurança e auxiliar os clientes afetados. O caso foi objeto de investigação por parte das autoridades competentes, resultando em uma multa proposta pela Autoridade de Proteção de Dados do Reino Unido (ICO, na sigla em inglês) no valor de £20 milhões em 2020, embora esse montante possa ter sofrido alterações em atualizações subsequentes.

É relevante observar que, além das sanções impostas por órgãos reguladores, a *British Airways* também enfrentou processos judiciais movidos por clientes afetados em busca de compensação pelos danos decorrentes do vazamento de dados.

Embora a LGPD seja uma legislação brasileira que entrou em vigor em 2020 e a *British Airways* seja uma empresa do Reino Unido, a LGPD não se aplica diretamente ao caso da *British Airways*. No entanto, é importante ressaltar que a LGPD estabelece princípios e diretrizes para a proteção de dados pessoais no Brasil, com o objetivo de garantir a privacidade e a segurança das informações dos indivíduos. Embora específica para o Brasil, muitos países têm leis semelhantes que visam proteger os dados pessoais de seus cidadãos.

No caso da *British Airways*, foram aplicadas as regulamentações de proteção de dados em vigor no Reino Unido e na União Europeia, como o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês), que é uma legislação abrangente aplicável a empresas que processam dados de cidadãos da UE.

O GDPR compartilha muitos princípios semelhantes à LGPD, incluindo a necessidade de obtenção de consentimento adequado para o processamento de dados pessoais, a implementação de medidas de segurança para proteção dos dados e a obrigação de notificar as autoridades competentes e os indivíduos afetados em caso de violação de dados. Portanto, embora o caso da *British Airways* não esteja diretamente ligado à LGPD, ele está relacionado às questões mais amplas de proteção de dados e privacidade, que várias legislações, como a LGPD e o GDPR, buscam abordar.

Em 2018, surgiu um escândalo envolvendo a *Cambridge Analytica*, uma

empresa de consultoria política, e o *Facebook*. A empresa coletou informações pessoais de cerca de 87 milhões de usuários do *Facebook* sem consentimento adequado. Esses dados foram adquiridos por meio de um aplicativo de teste de personalidade chamado *"This Is Your Digital Life",* instalado por aproximadamente 270.000 pessoas, que também acessou informações dos amigos desses usuários sem sua autorização.

A *Cambridge Analytica* utilizou esses dados para criar perfis psicográficos e direcionar mensagens personalizadas visando influenciar eleições e campanhas políticas, incluindo a eleição presidencial dos Estados Unidos em 2016. Esse incidente gerou preocupações significativas sobre privacidade e manipulação de dados em larga escala, desencadeando debates abrangentes sobre regulamentação e proteção de dados pessoais.

> A Cambridge Analytica teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais The Guardian e The New York Times. [...] (BBC NEWS, 2018).

Apesar de não estar diretamente vinculado à LGPD, já que a *Cambridge Analytica* é uma empresa britânica e o incidente ocorreu antes da entrada em vigor da LGPD em 2020, é crucial destacar seu impacto no debate global sobre proteção de dados pessoais e a necessidade de regulamentação nesse campo. O escândalo revelou vulnerabilidades e abusos relacionados à coleta e uso indevido de dados pessoais de usuários do *Facebook*.

A LGPD, uma legislação brasileira que visa proteger a privacidade e os direitos individuais em relação aos dados pessoais, compartilha objetivos semelhantes aos esforços internacionais de proteção da privacidade dos dados e controle dos indivíduos sobre suas informações pessoais. Embora não tenha sido diretamente aplicada no caso *Cambridge Analytica*, esse incidente enfatizou a importância de leis de proteção de dados, como a LGPD, para garantir a privacidade dos indivíduos e regular as práticas de coleta e uso de dados pessoais por parte das empresas.

Em 2016, veio à tona que a *Uber*, empresa de transporte, foi vítima de um vazamento em massa de dados ocorrido em 2014. Cerca de 57 milhões de usuários e motoristas da *Uber* em todo o mundo tiveram seus dados comprometidos,

incluindo nomes, endereços de e-mail, números de telefone e, em alguns casos, informações da carteira de motorista.

O vazamento ocorreu devido a uma falha nos sistemas de segurança da *Uber*, que permitiu que hackers acessassem e baixassem as informações dos usuários. Além disso, a *Uber* foi criticada por não ter divulgado o incidente imediatamente, mantendo o vazamento em segredo por mais de um ano. O caso resultou em multas e ações legais em vários países, incluindo o Brasil, onde a LGPD entrou em vigor posteriormente.

No Brasil, a *Uber* revelou que dados pessoais de aproximadamente 196 mil usuários brasileiros foram acessados por *hackers* durante o incidente. As informações comprometidas incluíam nomes completos, endereços de *e-mail*, números de telefone e informações de viagens.

Após a descoberta do incidente, a *Uber* notificou as autoridades competentes e os usuários afetados no Brasil, cumprindo as obrigações estabelecidas pela LGPD. A empresa também divulgou a violação por meio de comunicados públicos, demonstrando transparência sobre o ocorrido.

A Autoridade Nacional de Proteção de Dados (ANPD) do Brasil iniciou uma investigação sobre o incidente da *Uber* à luz da LGPD. Em agosto de 2021, a ANPD impôs uma multa de R$1,5 milhão à *Uber* por violações à proteção de dados, considerando o tempo de resposta ao incidente, a comunicação aos usuários afetados e as medidas de segurança implementadas após a violação.

Além da multa, a *Uber* foi orientada pela ANPD a adotar medidas para reforçar a segurança e proteção dos dados pessoais dos usuários, implementando melhores práticas de governança e conformidade com a LGPD.

Esse caso envolvendo a *Uber* destaca a aplicação da LGPD em um incidente de vazamento de dados pessoais. A empresa foi responsabilizada pela violação, notificou as autoridades e os usuários afetados e recebeu uma sanção da ANPD. Essas ações demonstram como a LGPD busca proteger os direitos individuais e garantir a segurança e a privacidade dos dados pessoais no Brasil.

O vazamento de dados da *Equifax*, em 2017, foi um dos maiores incidentes de violação de dados já registrados, expondo informações pessoais confidenciais de milhões de consumidores nos Estados Unidos. Cerca de 147 milhões de consumidores tiveram seus dados comprometidos, incluindo nomes completos, números de Seguro Social, datas de nascimento, endereços residenciais e, em

alguns casos, números de cartões de crédito.

Os *hackers* exploraram uma vulnerabilidade em um aplicativo de *software* utilizado pela *Equifax,* permitindo acesso não autorizado aos sistemas da empresa e expondo uma quantidade massiva de dados pessoais. Embora o vazamento tenha ocorrido entre maio e julho de 2017, a *Equifax* só tornou o incidente público em setembro do mesmo ano, gerando críticas por não agir prontamente para proteger os dados e informar os consumidores afetados.

As repercussões do vazamento foram graves, levando ao aumento do risco de fraudes, roubo de identidade e ataques cibernéticos direcionados. Os consumidores afetados precisaram monitorar suas contas e históricos de crédito, enquanto a Equifax enfrentou múltiplas ações judiciais, investigações regulatórias e multas significativas.

Embora a LGPD não tenha sido diretamente aplicada no caso da *Equifax,* seus princípios de proteção de dados pessoais e privacidade se relacionam com a situação. A LGPD estabelece que o tratamento de dados pessoais requer consentimento adequado dos titulares, o que não ocorreu no caso da *Equifa*x. Além disso, a Lei impõe às empresas a responsabilidade de adotar medidas de segurança para proteger os dados pessoais que possuem, e a *Equifax* falhou nessa obrigação. Outra exigência é que as empresas notifiquem os indivíduos e as autoridades em caso de violação de dados, o que foi criticado no caso da *Equifax* pela falta de transparência e demora na comunicação.

Embora o cenário não esteja diretamente ligado à LGPD, destaca a importância dos princípios de consentimento, segurança, transparência e responsabilização presentes na Lei. Esses princípios visam prevenir a apropriação indevida de dados pessoais, garantir controle aos titulares dos dados e responsabilizar as empresas por violações de segurança e proteção de dados.

A Lei Geral de Proteção de Dados (LGPD) estabelece sanções e penalidades para empresas que negligenciam suas responsabilidades quanto à proteção de dados pessoais. No contexto da *Equifax*, as consequências legais e financeiras incluíram ações judiciais, investigações regulatórias e multas significativas. Embora este caso não esteja diretamente ligado à LGPD, destaca a importância dos princípios de consentimento, segurança, transparência e responsabilização presentes na legislação. Esses princípios têm como objetivo prevenir a apropriação indevida de dados pessoais, garantir que os titulares dos dados tenham controle

sobre suas informações e responsabilizar as empresas por violações de segurança e proteção de dados.

Esses casos práticos demonstram a importância da proteção dos dados pessoais e os riscos associados à violação desses dados. As empresas e órgãos públicos devem adotar medidas de segurança adequadas para proteger os dados pessoais dos usuários e evitar violações. Além disso, é crucial que exista uma legislação abrangente nessa área.

Ao examinar-se casos ocorridos em outros países, podemos destacar incidentes marcantes de violações de dados que resultaram na exposição em larga escala de informações pessoais sensíveis, como mencionado e detalhado anteriormente. Esses casos envolveram grandes empresas e instituições, comprometendo dados críticos e colocando em risco a privacidade e a segurança de milhões de indivíduos.

Em um desses casos, uma violação de segurança significativa resultou na exposição massiva de dados pessoais de consumidores, gerando uma série de problemas, desde riscos de fraudes até a necessidade de monitoramento constante das contas dos afetados. Em outro cenário, uma empresa foi alvo de uma violação de seus sistemas de segurança, expondo informações confidenciais dos usuários e levantando críticas sobre a falta de prontidão da empresa em proteger os dados e informar os afetados.

É relevante considerar como a aplicação da LGPD poderia ter influenciado esses casos. A LGPD, com seus princípios de consentimento, segurança, transparência e responsabilização, busca proteger a privacidade e os direitos dos indivíduos em relação aos seus dados pessoais. Se estivesse em vigor durante esses incidentes, a LGPD teria exigido a notificação imediata das autoridades e dos afetados, bem como a obtenção prévia de consentimento para o tratamento dos dados. Além disso, a imposição de medidas de segurança robustas seria mandatória para garantir a proteção dos dados pessoais.

Esses casos destacam a importância das leis de proteção de dados e evidenciam a necessidade de regulamentações como a LGPD para prevenir a apropriação indevida de dados pessoais e garantir a responsabilidade das empresas diante de violações de segurança e proteção de dados.

A comparação entre a LGPD e as abordagens de outras jurisdições revela não apenas semelhanças na proteção dos direitos individuais, mas também variações

significativas nas sanções aplicadas, refletindo diferentes prioridades e contextos legais em relação à proteção de dados pessoais.

4.2 Comparação entre a LGPD e as penalidades civis e/ou penais aplicadas em diferentes jurisdições

Ao considerar os princípios da LGPD, observa-se que a responsabilidade dos agentes é fundamental na proteção de dados. Com o avanço tecnológico, o mercado de dados está cada vez mais presente no cotidiano e desempenha um papel significativo. Isso implica diretamente na possibilidade de prejudicar o titular dos dados, proporcionalmente à sua relevância econômica e alcance.

A LGPD traz inovações ao estabelecer condições para o tratamento de dados, representando um marco importante para que empresas e instituições que lidam com dados possam se ajustar a essa nova realidade de proteção à privacidade. No entanto, é crucial observar que, como mencionado anteriormente, trata-se de uma atividade com riscos, podendo resultar em danos ao titular, sejam eles de natureza patrimonial ou moral, devido ao descumprimento da lei ou outros fatores.

Para essas situações em que ocorrem danos decorrentes do tratamento de dados, a lei estabelece uma série de regras sobre como deve ser feita a compensação. Nesse contexto, tudo o que foi discutido sobre fundamentos, princípios e normas serve como base para reparar os danos sofridos pelo titular dos dado.

A responsabilidade civil dos agentes de tratamento de dados, sejam controladores ou operadores, em relação ao titular dos dados, é abordada entre os artigos 42 e 45 da Lei. Essa responsabilidade é dividida em dois tipos. O primeiro, descrito no artigo 42, trata da regra geral e reflete o que é estabelecido no Código Civil de 2002 como forma de reparação de danos, ou seja, a responsabilidade subjetiva. A responsabilidade objetiva é a exceção na LGPD, embora isso não signifique que terá menos questionamentos que a responsabilidade subjetiva.

4.2.1 Penalidades civis aplicadas de acordo com a LGPD em casos de violação de dados

No que concerne à responsabilidade civil na LGPD, há uma distinção clara

entre as relações civis e as relações de consumo. No contexto das relações civis, que se baseiam em aspectos contratuais, aplica-se a regra geral do Código Civil, onde a responsabilidade leva em consideração a culpa do agente, já que a responsabilidade objetiva, se aplicável, deveria ser explicitamente indicada.

É importante ressaltar que tanto o controlador quanto o operador são responsáveis, conforme previsto. Embora o operador esteja sujeito às instruções do controlador, ele também está vinculado às disposições legais e deve adotar medidas de segurança de dados, uma vez que se beneficia da atividade e está sujeito a riscos legais.

Outro ponto relevante é que a reparação pode ser realizada tanto em relação a um indivíduo quanto a um grupo. Dada a natureza das atividades de tratamento de dados, que se tornam mais eficientes ao atingir um grande número de pessoas, é mais provável que os danos afetem um grupo.

A seção da LGPD que aborda a responsabilidade detalha normas específicas para o tratamento de dados. Por exemplo, a Lei estabelece solidariedade entre o controlador e o operador na obrigação de reparar os danos. Isso significa que a compensação pode ser exigida de um ou ambos, conforme indicado pelo §1º do artigo 42.

A legislação estipula que existe uma responsabilidade conjunta entre o controlador e o operador na obrigação de reparar os danos, conforme descrito no inciso I, parágrafo 1º, do artigo 4223. Essa disposição reflete a ideia de que o cumprimento da lei e a garantia da segurança das atividades são responsabilidades compartilhadas por todos os agentes envolvidos no processamento, independentemente de qualquer hierarquia entre eles. Portanto, tanto um quanto o outro podem ser responsabilizados pela reparação, como especificado no enunciado do parágrafo 1º, que busca assegurar uma compensação efetiva ao titular dos dados.

O processamento de dados geralmente ocorre em uma rede complexa, onde diversos agentes contribuem para seu funcionamento, e há diferentes arranjos possíveis nessa cadeia produtiva. Portanto, em certas circunstâncias, pode ocorrer uma situação em que uma multiplicidade de agentes, inclusive mais de um controlador, esteja envolvida, como indicado no inciso II do parágrafo 1º. Segundo esse dispositivo, todos os controladores envolvidos serão solidários, o que amplia significativamente a aplicabilidade da regra de reparação a uma variedade de casos,

auxiliando na garantia da compensação adequada.

Essa concepção também abre caminho para a possibilidade de ação regressiva, conforme descrito no parágrafo 4º do mesmo artigo 42. Como a responsabilidade é solidária e a obrigação pode ser cumprida por todos ou por apenas um deles, aquele que arcar com a reparação poderá exigir dos demais o ressarcimento proporcional à sua participação no evento danoso.

Por outro lado, no que se refere à produção de prova para estabelecer a culpa, o legislador optou por adotar as mesmas regras gerais, exceções e teorias que fundamentam a inversão utilizadas no Código de Processo Civil de 2015. De acordo com o artigo 373 desse código, o ônus da prova é geralmente determinado pela posição das partes na demanda: cabe ao autor provar os fatos que fundamentam seu direito, enquanto ao réu cabe provar os fatos que impedem, modificam ou extinguem esse direito. Entretanto, o parágrafo 1º introduz a teoria da distribuição dinâmica do ônus da prova (FILHO, 2018).

Essa teoria estipula que o ônus da prova não é fixo e pode ser invertido em certas situações, visando facilitar a resolução rápida e precisa do mérito da questão. De forma similar, a LGPD também determina no parágrafo 2º do artigo 42.25 essa medida importante, presumindo que os agentes de proteção de dados têm maior facilidade na produção de provas, pois possuem todas as informações sobre a atividade. Essa é uma das razões pelas quais é exigido que eles mantenham registros da atividade de tratamento.

Após, a Lei aborda as excludentes de responsabilidade no artigo 43. Esse dispositivo especifica as circunstâncias em que não há relação entre a conduta do agente e o dano sofrido pelo titular dos dados.

A reparação do dano só pode ser exigida daquele que de fato realizou o tratamento dos dados. Se a demanda é dirigida a um agente que não participou do tratamento, não há base para estabelecer uma ligação causal entre o dano e o suposto ato ilícito, e, portanto, o agente é liberado de sua obrigação de reparação.

Outra situação é quando, mesmo havendo dano, o agente não violou as normas de segurança estabelecidas pela LGPD e pela Autoridade Nacional de Proteção de Dados. Nesse caso, a culpa do agente é descartada, tornando o pleito do titular inviável.

Por fim, a obrigação de reparação é afastada quando o agente prova que o dano foi causado exclusivamente pela culpa do próprio titular dos dados ou de

terceiros. Quando o titular age de maneira negligente em relação à segurança ou subestima os riscos associados a uma determinada medida, ele assume riscos adicionais além dos habitualmente relacionados ao tratamento de dados, escapando assim completamente ao controle do controlador, que não pode ser responsabilizado pelos danos resultantes dessa situação.

Pode-se notar que essas exclusões de responsabilidade dependem da produção de provas por parte dos agentes, tornando o processo mais complexo e detalhado. No entanto, as condições para a produção de prova são mais favoráveis a esses agentes, dada sua capacidade técnica e contexto mais propício.

A ilegalidade dos procedimentos dos agentes é determinada pelo não cumprimento da legislação ou pela não satisfação das expectativas do titular em relação ao procedimento, considerando que se trata de uma relação contratual baseada em transparência e boa-fé. Embora a expectativa do titular seja um critério subjetivo a ser avaliado no caso específico, o legislador detalha nos incisos I a II do artigo 44 essa regra, determinando que o juiz avalie "o modo como o tratamento é realizado", "o resultado e os riscos razoavelmente esperados" e as técnicas disponíveis na época.

Portanto, ao examinar os dispositivos que regem a responsabilidade civil subjetiva dos agentes de tratamento de dados, fica evidente sua grande semelhança com a legislação civil nacional, mostrando-se plenamente capaz de lidar com a necessidade eventual de reparação de danos.

No entanto, considerando que a maioria das atividades de tratamento de dados ocorre no contexto de relações de consumo, a responsabilidade objetiva, que é a exceção, provavelmente será mais frequentemente aplicada. No entanto, essa é uma hipótese que precisará ser confirmada com o tempo e ferramentas específicas.

A responsabilidade civil objetiva é aplicada por determinação legal em casos em que o legislador identifica uma vulnerabilidade estrutural de uma das partes. Essa forma de reparação, que não leva em conta a culpa, é uma disposição especial estabelecida pela lei.

No caso da LGPD, essa responsabilidade está prevista em duas situações: no tratamento de dados no contexto das relações de consumo, conforme o artigo 45 da Lei, e no tratamento de dados pelo poder público, conforme o artigo 37, §6º da Constituição.

Especificamente em relação ao poder público, há um entendimento do

Supremo Tribunal Federal de que a responsabilidade objetiva se aplica a atos comissivos (MALDONADO e BLUM, 2019). No entanto, esse entendimento ainda não abordou especificamente a questão do tratamento de dados, sendo necessário observar em estudos posteriores como essa interpretação se aplica a esse contexto específico.

Por outro lado, o Código de Defesa do Consumidor é um modelo na aplicação da responsabilidade civil objetiva. Ele concretiza um mandamento constitucional de proteção ao consumidor e estabelece diversos direitos que garantem ao consumidor, que é considerado vulnerável, proteção contra danos decorrentes da relação de consumo.

Por isso, a LGPD determina explicitamente que, nas relações de consumo, esse código deve ser aplicado, pois, por ser mais benéfico ao consumidor, é mais adequado para garantir a reparação dos danos causados por agentes que detêm superioridade econômica e informacional na atividade. O defeito do produto ou serviço que causa dano ao consumidor é, portanto, protegido por meio da solidariedade dos agentes, da inversão do ônus da prova e do acesso a informações precisas.

Dessa forma, a LGPD se alinha de forma consistente e segura com toda a legislação em vigor na busca por uma reparação efetiva e justa, levando em consideração as particularidades de todos os contextos envolvidos.

4.2.2 Penalidades penais aplicadas de acordo com a LGPD em casos de violação de dados

A LGPD estabelece a responsabilização penal para empresas e órgãos públicos que não aderirem às normas estabelecidas pela lei. As sanções podem abranger multas, suspensão ou até proibição total do tratamento de dados pessoais.

Além disso, a LGPD também prevê a responsabilização penal de indivíduos que cometam crimes relacionados ao tratamento de dados pessoais, como a obtenção ilegal de informações, divulgação não autorizada e uso indevido de dados pessoais.

A responsabilização penal no tratamento de dados pessoais é crucial para salvaguardar os direitos fundamentais das pessoas e para incentivar conformidade com a LGPD por parte das empresas e órgãos públicos. Contudo, é essencial que a

aplicação da lei seja equitativa e proporcional, evitando abusos e garantindo o devido processo legal.

No entanto, diante do dinamismo do ambiente digital, é crucial considerar como a LGPD pode evoluir para enfrentar novos desafios emergentes em segurança cibernética. A adaptação contínua da legislação é fundamental para garantir que continue eficazmente protegendo os direitos individuais frente às rápidas mudanças tecnológicas e às crescentes ameaças cibernéticas.

4.3 Como a LGPD pode evoluir para lidar com novos desafios em segurança cibernética

A Lei Geral de Proteção de Dados (LGPD) assume um papel central na salvaguarda das informações pessoais em meio ao cenário contemporâneo. Seu propósito reside em estabelecer diretrizes claras para orientar empresas, entidades governamentais e organizações no manejo, tratamento e salvaguarda dos dados pessoais. A constante atualização desta legislação se torna imprescindível diante do incessante avanço tecnológico, visando assegurar sua efetividade.

Conforme preconiza a LGPD, é imperativo que as informações pessoais, sejam elas de cidadãos, colaboradores ou clientes, sejam tratadas de forma a garantir a segurança e o respeito à sua privacidade. Contudo, a implementação efetiva desta lei traz consigo novos desafios decorrentes da rápida evolução tecnológica.

Nesse contexto, a atualização da LGPD adquire uma relevância crucial, uma vez que se faz necessário acompanhar o ritmo dos avanços tecnológicos e suas implicações para assegurar a proteção dos dados. Um exemplo elucidativo é o impacto da inteligência artificial, conforme destacado por um estudo da IBM, que prevê a geração de trilhões de dólares em aplicações globais, evidenciando a importância da inovação e da criatividade na abordagem do tratamento de informações pessoais.

Diante desse panorama, o desafio reside em estabelecer mecanismos robustos para garantir a segurança dessas informações, a fim de prevenir quaisquer formas de abuso ou exploração indevida. A integração da inteligência artificial emerge como uma solução pertinente, exigindo a implementação de medidas de segurança que regulamentem o tratamento de dados para o pleno cumprimento da LGPD.

Em suma, a atualização periódica da Lei Geral de Proteção de Dados, aliada

à adoção de sistemas e processos de segurança avançados, são medidas essenciais não apenas para a conformidade legal, mas também para salvaguardar a privacidade e a integridade dos dados pessoais.

Em linhas gerais, a revisão periódica da Lei Geral de Proteção de Dados, juntamente com a adoção de sistemas e procedimentos de segurança de última geração, são passos cruciais para assegurar a conformidade com os padrões estabelecidos, bem como para proteger efetivamente os dados pessoais.

Investir em tecnologia representa uma das mais significativas estratégias que empresas, entidades governamentais e organizações podem adotar para garantir a segurança das informações pessoais. Como argumenta Kaio Alves (2023, p.6):

> A cada acesso à internet, o usuário deixa registrado vários dados pessoais, o que se torna informação. A informação passou a ser um ativo de grande relevância no ambiente virtual e despertou grande interesse por parte das instituições. Mas o que é feito com essas informações despertou na sociedade a necessidade de proteção aos seus dados. E de uma lei que regulamentasse seus direitos à privacidade e a proteção de dados.

Portanto, no que diz respeito à proteção de dados pessoais, investir continuamente e buscar constantemente melhorias é uma prioridade inegável. Isso se justifica pela importância de garantir que as informações estejam armazenadas de maneira segura, promovendo assim uma experiência de navegação na internet segura e contribuindo para a construção da confiança dos usuários.

Conforme estabelecido no Artigo 1º da Lei, esta legislação define os princípios, garantias, direitos e deveres relacionados ao uso da internet no território brasileiro, além de estipular as diretrizes para a atuação das esferas federal, estadual, distrital e municipal nessa matéria.

A implementação de uma cultura de conformidade contínua emerge como a abordagem mais eficaz para que as organizações operem de acordo com os preceitos da LGPD. Isso implica em manter as equipes constantemente atualizadas e conscientes das mudanças normativas, além de avaliar e atualizar regularmente as ferramentas e processos, a fim de mitigar potenciais não conformidades. Além disso, é fundamental que os usuários da empresa se sintam engajados e responsáveis por identificar e reportar qualquer descumprimento de prazos ou outras formas de não conformidade ao gerenciamento da equipe.

De acordo com a argumentação do autor Kaio Alves (2023, p.30), respaldada

pelo Artigo 50, § 1º da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) tem a prerrogativa de considerar, ao aplicar sanções, mecanismos de minimização de danos, boas práticas, governança e medidas corretivas. Essa abordagem sugere que os princípios de responsabilização e prestação de contas estabelecidos na legislação podem também servir como referência para ações judiciais.

Nessa perspectiva, a internet desempenha um papel essencial na promoção da cidadania, visando garantir tanto a liberdade de expressão quanto a privacidade. Somente assim é possível criar um ambiente onde os direitos fundamentais sejam adequadamente respeitados.

Investir em sistemas avançados de segurança da informação e manter uma atualização contínua da LGPD são medidas fundamentais para aumentar a confiança dos usuários e garantir a segurança de suas informações pessoais. Portanto, é imperativo realizar investimentos adequados para salvaguardar a integridade dos dados.

5 CONCLUSÃO

A proteção contínua dos dados pessoais é uma prioridade incontestável. Ao abordar os antecedentes da LGPD no contexto brasileiro e internacional, juntamente com a análise dos tipos de crimes cibernéticos e suas estatísticas, evidenciou-se a urgência de medidas eficazes para garantir a segurança digital.

A LGPD, ao estabelecer objetivos e princípios claros, busca regular a proteção dos dados pessoais, exigindo conformidade e responsabilidade por parte das organizações que lidam com tais informações. No entanto, diante dos desafios em constante evolução no cenário cibernético, torna-se fundamental a revisão periódica da legislação para acompanhar os avanços tecnológicos e suas implicações.

Além disso, a imposição de penalidades civis e penais em casos de violação de dados, conforme previsto pela LGPD, demonstra a importância de sua aplicação rigorosa para dissuadir práticas negligentes ou maliciosas. A comparação entre as penalidades em diferentes jurisdições ressalta a necessidade de coerência e eficácia na abordagem dos crimes cibernéticos em nível global. A adaptação da LGPD para lidar com desafios emergentes, como o impacto da inteligência artificial, reflete a importância da inovação e da criatividade na proteção dos dados pessoais. É imperativo que tanto as políticas quanto as práticas de segurança de dados sejam constantemente atualizadas e aprimoradas para garantir a confiança dos usuários e a integridade das informações online.

Portanto, a LGPD tem um impacto significativo na proteção de dados e no combate aos crimes cibernéticos. A legislação estabelece um marco regulatório que reforça a segurança dos dados pessoais e impõe obrigações rigorosas aos controladores e operadores de dados.

A adaptação da LGPD para lidar com desafios emergentes, como o impacto da inteligência artificial, reflete a importância da inovação e da criatividade na proteção dos dados pessoais. É imperativo que tanto as políticas quanto as práticas de segurança de dados sejam constantemente atualizadas e aprimoradas para garantir a confiança dos usuários e a integridade das informações online. Assim, a pesquisa contribui para a compreensão abrangente do contexto legal e tecnológico envolvendo a proteção de dados no Brasil e suas implicações na esfera global.

No combate aos crimes cibernéticos, a LGPD contribui ao exigir que as empresas comuniquem violações de dados às autoridades e aos titulares afetados, facilitando uma resposta rápida e coordenada a incidentes de segurança. Além disso, ao estabelecer diretrizes claras para o tratamento de dados, a LGPD ajuda a prevenir a ocorrência de crimes cibernéticos, reduzindo as vulnerabilidades que podem ser exploradas por criminosos.

Portanto, a LGPD não só protege os dados pessoais dos indivíduos, mas também fortalece a infraestrutura de segurança cibernética no Brasil, tornando-se uma ferramenta crucial no combate aos crimes cibernéticos. A evolução contínua da legislação e sua adaptação às novas ameaças tecnológicas são essenciais para manter a eficácia da proteção de dados e a segurança digital.

REFERÊNCIAS

AGNES, Clarice; HAAS, Helga; HELFER, Inácio. **Normas para a apresentação de trabalhos acadêmicos.** 3. ed. Santa Cruz do Sul: EDUNISC, 2019. Disponível em: http://www.unisc.br/editora/e_books_normas.pdf. Acesso em: 30 mar. 2024.

ALVES, Matheus de Araújo. **Crimes digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Criminal e do Instituto da Prova**. 1ª ed. São Paulo: Dialética, 2020.

ANDRION, Roseli. **O que é stalking? Como se proteger?** Canaltech, 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-e-stalking-como-seproteger205060/#:~:text=Nesse%20cen%C3%A1rio%2C%20o%20stalking%20est%C3%A1, persegui%2Dlo%20virtual%20ou%20presencialmente. Acesso em: 30 mar. 2024

BAPTISTA, Ricardo Córdoba. **Crime de participação em suicídio ou automutilação: inovações da Lei 13.968/2020**. Jus.com.br, 2020. Disponível em: https://jus.com.br/artigos/83419/crime-de-participacao-em-suicidio-ou-automutilacaoinovacoes-da-lei-13-968-2020. Acesso em: 30 mar. 2024

BAPTISTA, Ricardo Córdoba. **O que é ciberextorsão?.** My.cybersecurity, 2016. Disponível em: <https://www.mycybersecurity.com.br/o-que-e-ciber-extorsao/>. Acesso em: 30 mar. 2024

BARRETO, Alesandro Gonçalves. **Cibercrimes e seus reflexos no direito brasileiro**. Salvador: Editora JusPodivm, 2020.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do marco civil da internet.** 1ª ed. Rio de Janeiro: Brasport, 2016.

BITENCOURT, Cezar Roberto. **Furto mediante uso de dispositivo eletrônico ou informático**. Consultor Jurídico, 2021. Disponível em: https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivoeletronico-ou-informatico. Acesso em: 30 mar. 2024

BITTENCOURT, R. P. P**. O anonimato, a liberdade, a publicidade e o direito eletrônico**. 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-apublicidade-e-o-direito-eletronico. Acesso em: 30 mar. 2024

BOITEUX, L. **Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual**. Doutrinas Essenciais de Direito Penal. v. 8, 2010.
BRASIL, Decreto – Lei nº 2.848 de 07 de dezembro de 1940. Diário Oficial [da] República Federativa do Brasil, Poder Legislativo, Brasília, DF, 07 dez. 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto lei2848-7-dezembro-1940-412868-norma-pe.html. Acesso em: 30 mar. 2024.

BOMFATI, Cláudio Adriano. KOLBE JUNIOR, Armando. **Crimes Cibernéticos.** Curitiba. Intersabares, 2020.

BRASIL, BBC News. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades, 2018**. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 01 mai. 2024

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 mai. 2024

BRASIL. Decreto-lei n. 2.848, de 7 de dezembro de 1940. **Código Penal.** Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 14 mai. 2024.

BRASIL. Lei nº 8.137/90, de 27 de dezembro de 1990. **Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137.htm. Acesso em: 14 mai. 2024

BRASIL. Lei 10.406, de 10 de janeiro de 2002**. Institui o Código Civil.** Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 14 mai. 2024

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **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. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:
14 mar. 2024

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em:
14 mar. 2024

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709compilado.htm. Acesso em: 26 abr. 2024

BRASIL. Lei nº 13.869, de 5 de setembro de 2019. **Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº**

8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm. Acesso em: 30 mar. 2024

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Full list. Treaty Office**. Disponível em: <https://www.echr.coe.int/Documents/Handbook_data_protection_Por.pdf> Acesso em: 30 mar. 2024

DUFFY, Clara. Meta faz acordo de US$ 725 milhões para encerrar caso sobre Cambridge Analytica. **CNN Brasil**, Nova York, 23 dez. 2022. Disponível em: https://www.cnnbrasil.com.br/economia/meta-faz-acordo-de-us-725-milhoes-para-encerrar-caso-sobre-cambridge-analytica/. Acesso em: 01 mai. 2024.

ECONOMIA, O Globo. Vazamento de dados da Uber em 2016 afetou 196 mil brasileiros. O Globo, 13 abr. 2018. Disponível em: https://oglobo.globo.com/economia/vazamento-de-dados-da-uber-em-2016-afetou-196-mil-brasileiros-22584512. Acesso em: 01 mai. 2024

EFE, agência. Equifax, empresa de crédito dos EUA, sofre ataque hacker e dados de 143 milhões de pessoas são expostos. **G1**, 07 set. 2017. Disponível em: https://g1.globo.com/tecnologia/noticia/equifax-empresa-de-credito-dos-eua-sofre-ataque-hacker-e-dados-de-143-milhoes-de-pessoas-sao-expostos.ghtml. Acesso em: 01 mai. 2024.

EUROPA. Directiva 95/46/CE do parlamento europeu e do conselho. Luxemburgo: 1995

OLIVEIRA JUNIOR, Eudes Quintino Sociedade de Advogados. **A nova lei Carolina Dieckmann.** Disponível em: https://eudesquintino.jusbrasil.com.br/artigos/121823244/anova-lei-carolina-dieckmann. Acesso em: 01 mai. 2024.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários a Lei n.° 13.709/2018.** 2. ed. São Paulo: Saraiva, 2020. 152 p. Disponível em: https://books.google.com.br/books?hl=ptBR&lr=&id=oXPWDwAAQBAJ&oi=fnd&pg=PT1
3&dq=lgpd+lei&ots=k8ZpDxLJZO&sig=DONrdM59uOkg5kMeu8qBgR3DN24#v=onepage&q=lgpd%20lei&f=false. Acesso em: 01 mai. 2024

PRESSE, France. British Airways é multada em US$ 230 milhões por caso de roubo de dados de passageiros. **G1**, 08 jul. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/08/british-airways-e-multada-em-us-230-milhoes-por-caso-de-roubo-de-dados-de-passageiros.ghtml Acesso em: 01 mai. 2024

SILVA, Camila Requião Fernandes. Análise das Leis no 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos. Jus.com.br. Disponível em: <https://jus.com.br/artigos/32265/analise-das-leis-n-12-

735-2012-e-12-737- 2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos>. Acesso em: 01 mar. 2024.

SOUZA, W. I. de. **Proteção de dados pessoais do consumidor online**. 2017. Dissertação (Especialização em Direito do Consumidor e Direitos Fundamentais) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul. Porto Alegre. 2017. Disponível em: <https://lume.ufrgs.br/handle/10183/179003 > Acesso em: 01 mai. 2024

TEFFÉ, C. S. 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: 27 abr. 2024

TEFFÉ, C. S. DE, VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais.** Rio de Janeiro. Civilistica. 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 27 abr. 2024