LORENA LEITE SILVA CROSARA

CRIMES CIBERNÉTICOS: IMPACTOS E DESAFIOS APÓS A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS"

CURSO DE DIREITO-

UniEVANGÉLICA 2024

LORENA LEITE SILVA CROSARA

CRIMES CIBERNÉTICOS: IMPACTOS E DESAFIOS APÓS A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Monografia apresentada ao Núcleo de Trabalho Cientifico do curso de Direito da UniEVANGÉLICA, como exigência parcial para a obtenção d grau de bacharel em Direito, sob orientação do professor (a) Me.**Chrystiano Silva Martins.**

ANÁPOLIS-2024

CRIMES CIBERNÉTICOS: IMPACTOS E DESAFIOS APÓS A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Anápolis, de 2024.

BANCA EXAMINADORA

_____

_____

AGRADECIMENTOS

Agradeço a Deus por me sustentar até este momento e por amparar meus estudos com sabedoria.

Expresso minha gratidão à minha família, que é a fonte de inspiração para meu sucesso profissional.

Agradeço também ao meu professor orientador Chrystiano Silva Martins, por seus valiosos ensinamentos, paciência e incentivo, sem os quais a conclusão deste trabalho não teria sido possível.

Por fim, agradeço a todos que, de alguma forma, colaboraram para que eu chegasse até aqui. Muito obrigada.

RESUMO

O presente Trabalho de Conclusão de Curso realiza uma análise aprofundada sobre a relação entre a legislação vigente e um projeto de lei que aborda os delitos virtuais. O objetivo principal é destacar a fragilidade do sistema legal na interpretação tanto da jurisprudência quanto das leis, ao tipificar condutas criminosas nesse contexto. A pesquisa envolve o exame de casos concretos e suas resoluções à luz do direito penal, decretos, jurisprudência e analogia, evidenciando as dificuldades enfrentadas na judicatura de crimes virtuais.

A abordagem utilizada para resolver conflitos nesse ambiente tem se baseado em jurisprudência e legislação já existentes, que se mostram insuficientes e ineficazes em muitos aspectos. A metodologia adotada foi dedutiva, utilizando-se de pesquisa bibliográfica fundamentada no método positivista, com a análise de legislações e opiniões doutrinárias.

A pesquisa foi desenvolvida em três capítulos, e a conclusão aponta para a carência de uma legislação adequada e específica para lidar com o crescente problema dos delitos virtuais. Essa carência se torna ainda mais evidente à medida que a sociedade se torna cada vez mais dependente do ambiente digital, exigindo uma resposta jurídica mais eficaz e atualizada.

Palavras-chave: Delitos Virtuais. Legislação Vigente. Jurisprudência. Conflitos Digitais. Ambiente Virtual.

SUMÁRIO

INTRODUÇÃO 07

CAPÍTULO I – O AMBIENTE CIBERNÉTICO 08

1.1.Histórico sobre o ambiente cibernético 08
1.2 Conceito de ambiente cibernético 11
1.3 Princípios que regulam o ambiente cibernético 13

CAPÍTULO II – IMPLEMENTAÇÃO DA LEI DE PROTEÇÃO DE DADOS..... 17

2.1 Fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD) 17
2.2 Princípios e Direitos dos Titulares de Dados 20
2.3 Impactos e Desafios da Implementação da LGPD 23

CAPÍTULO III – CRIMES NO AMBIENTE CIBERNÉTICO 28

3.1 Introdução aos Crimes Cibernéticos..... 28
3.2 Tipos de Crimes Cibernéticos..... 30
3.3 Prevenção e Combate aos Crimes Cibernéticos com a LGPD 38

CONCLUSÂO 40

REFERÊNCIAS 41

INTRODUÇÃO

O presente trabalho tem como objetivo analisar e estudar os crimes cibernéticos, os quais ocorrem em mundo virtual, ou seja, rede mundial de computadores, conhecida como world wide web e os crimes no direito brasileiro que protegem este bem jurídico.

Para definir o que se entende por crimes cibernéticos, concerne analisar a aplicabilidade Do Código Penal Brasileiro e da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), bem como o seu marco histórico, os seus institutos protetivos e a atuação dos órgãos estatais, e ainda o impacto na sociedade, mensurado em casos diários registrados nas delegacias.

Na busca de efetivar a presente pesquisa, estudaremos como o crime cibernético praticados na atualidade brasileira vem afetando o ‘’Mundo Real’’ desde o surgimento da internet, posto que, há um crescimento exponencial da utilização de recursos oferecidos pelo mundo virtual.

Ao longo dos anos, devido ao surgimento de vários casos de crimes no ambiente virtual, a legislação brasileira vem introduzindo normas penais na intenção de reforçar a proteção de dados pessoais 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.

Todavia, será que a criação da Lei de proteção geral de dados tem aplicabilidade imediata para evitar que os crimes de maior gravidade sejam cometidos, neste diapasão indagaremos se tais crimes na maioria das vezes decorem da impunidade pelo uso dos recursos da Deep Wep.

Importante ressaltar ainda, quais os principais tipos penais praticados no contexto de cibercrimes, e quais são os crimes virtuais mais sofridos pelos usuários da internet e a aplicação do Código Penal Brasileiro para tais crimes.

Para que esse problema fosse resolvido com maior abrangência possível certas questões de suma relevância devem ser abordadas, a exemplo a definição acerca do local de apuração e competência destes crimes nesta modalidade.

Logo, tal pesquisa será feita tendo como base a melhor doutrina e a mais atualizada jurisprudência sobre o assunto, sem perder o foco dos mais variados pontos de entendimento, buscando uma melhor compreensão da finalidade da norma.

CAPÍTULO I - O AMBIENTE CIBERNÉTICO

O Presente capítulo objetiva conceituar o ambiente cibernético, partindo da definição de ambiente cibernético, que tem trazido ao longo dos tempos grandes problemas e desequilíbrio no mundo virtual e consequentemente para o mundo real, em razão da desinformação e do difícil controle de ações criminosas.

Visa demonstrar as características das normas penais que tratam de questões voltadas para o ambiente cibernético, que é imprescindível para entender como é realizado os atos criminosos dentr zo do ambiente virtual e quais medidas são adotadas para combater tais atos na tentativa de evitar que mais pessoas caiam em golpes.

O desenvolvimento desenfreado perante o campo tecnológico é um dos maiores fatores para o crescimento dos crimes virtuais, onde abrange o ramo da internet de forma genérica onde alguns indivíduos que praticam condutas delituosas de forma virtual, tornam-se difíceis de rastrear.

Desse modo, a Lei n° 13.709/2018, será analisada desde os fatores históricos que ensejam a sua criação até a efetiva vigência, bem como seus institutos protetivos e a atuação dos órgãos estatais, juntamente com a aplicabilidade do Código Penal Brasileiro.

1.1. Histórico sobre o ambiente cibernético

Quando estamos falando de internet, logo analisamos um mundo virtual com vasto e incontável número de informações, podendo estar organizados ou desorganizados em decorrência da quantidade de informações colocadas na rede e que estão à disposição de todos nós, podendo ser utilizados contra ou a favor das pessoas, dependendo claro do ponto de vista, e os meios utilizados por esses recursos (Barreto; Wednt, 2020).

A internet desenvolveu-se na década de 1960, primeiramente para emprego militar, tendo como ideia central a reunião de computadores mundialmente interconectados, comunicando-se através de protocolos, inicialmente TCP/IP considerados organizadores de mensagens de dados que circulavam entre essas maquinas. Este protocolo é composto por um conjunto de regras, no qual se divide em mensagem em pacote que irá trafegar pela internet, podendo assim seguir caminhos diferentes na rede. Com isso ocorreu a possibilidade de troca de informações entre inúmeros computadores e outros dispositivos, utilizando-se várias conexões diferentes. (Bomfati; Kolbe Junior, 2020).

As origens da internet podem ser encontradas na Advanced Research Projects Agency Network (ARPANET), uma rede de computadores criada em setembro de 1969, foi formada em 1958 pelo Departamento de Defesa dos Estados

Unidos, como missão e objetivo de superioridade teológica frente a União Soviética. A ARPANET não passava de um pequeno programa fundado em 1962 com base em uma unidade preexistente, tinha como objetivo definido estimulação da pesquisa e por justificativa a concentração de vários centros de computadores e também grupos de pesquisas que trabalhavam para agência, reunindo como compartilhar tempo de computação online (Castells, 2003).

A criação e o desenvolvimento do computador estavam diretamente vinculados as atividades bélicas das forças armadas e dos departamentos de defesas dos países desenvolvidos como Estados Unidos, Rússia e a Inglaterra, em razão da militarização demorou algum tempo para popularização dessa máquina, que veio à mão dos civis apenas em meados dos anos 1960, com finalidade de executar tarefas de cálculos pesados e gerenciamento de grandes empresas. A população em geral estava fora do uso dos computadores, até a invenção dos microprocessadores, conseguindo operar com números maiores de operações, diante da evolutiva, também do desenvolvimento dessas técnicas, e da popularização e elevado capital gerado com a venda desses computadores, no final dos anos 1970, foi desenvolvido por um grupo de estudantes californianos anonimamente resultando no projeto do primeiro computador de cunho pessoal, dando o passo inicial para ascensão da cultura da informação (Ribeiro, 2013).

A internet é conhecida no mundo todo, devido ao fato do desenvolvimento do www, esta aplicação de compartilhamento de informação foi desenvolvida na década de 1990, por um programador inglês Tim Berners-Lee (Castells, 2003).

Com isso ainda na década de 1990, a internet popularizou-se ainda mais entre as universidades norte-americanas e logo para o mundo todo, revolucionando as trocas de conhecimentos e informações, criando um ambiente virtual, paralelo ao real, sendo chamado de ciberespaço (Barreto; Wednt; Caselli, 2017, p. 58).

Tendo assim, uma troca de informações, e-mails, noticiais, implementado no Brasil em meados de 1991, com transmissão de alguns pacotes TCP/ITP para os Estados Unidos, considerado revolução da época. A evolução da comunicação contribui com muita celeridade dos dados, aonde estes devem chegar (Barreto; Wednt; Caselli, 2017).

No Brasil, o IBGE (Instituto Brasileiro de Geografia e Estatística), passou a utilizar um computador no ano de 1964, foi criado o Centro Eletrônico de Processamento de Dados do Estado do Paraná. Em 1965 foi criado o serviço Federal de Processamento de Dados, e com isso o Brasil associou-se ao consórcio internacional de telecomunicação via satélite, estava vinculado ao Ministério das 12 Comunicações. No ano de 1972 foi fabricado o primeiro computador brasileiro pela Universidade Federal de São Paulo (USP), sendo dois anos depois criados o Computadores S.A, 1979 criou-se a Secretaria Especial de Informática, sendo um passo importante da consolidação da internet brasileira em 1988 com a conexão à bitnet da Fundação de Amparo à pesquisa do Estado de São Paulo (FAPESP), Laboratório Nacional de Computação Cientifica (LNCC), e da Universidade Federal do Rio de Janeiro (Wednt; Jorge, 2013).

Já em meados de 1998, surge a Google Inc. foi fundada e revolucionou os sites e formas de pesquisas na web, fundadores da Google Sergey Brin e Larry Page, priorizava nas pesquisas buscas pela quantidade de links, no qual o termo buscado possuía, ou seja, se determinada palavra tinha sido buscava mais vezes por determinados sites, seriam colocados como prioridade, trazendo dados úteis e mais precisos, foi a revolução de internet, tornando a Google a maior empresa do

setor, inovando e trazendo a busca mais atrativa para o público (Barreto; Wednt, 2020).

> O uso da internet como sistema de comunicação e forma de organização explodiu nos últimos anos do segundo milênio. De acordo com a Internet World Stats, em junho de 2019 chegamos ao impressionante volume de 4,536 bilhões de pessoas com acesso à Internet (Barreto; Wednt, 2020, p. 13).

A conexão entre os inúmeros dispositivos pode dar-se por diferentes tecnologias, antigamente essas conexões utilizavam-se do uso de modens, foram substituídos pelo uso da banda larga, que tem como principal forma a conexão A DSL, o cabo, o rádio, 3G, 4G, o satélite e recentemente a fibra ótica. Para que ocorra o envio, requisição para a internet devemos ter instalado no computador um browser ou aplicativo de acesso, podendo ser feito através de um modem ligado a linha telefônica ou a um cabo, também temos conexões via Wi-Fi, e Bluetooth, que acessarão um provedor, e com isso entrar nos servidores de todos os lugares do mundo conectados entre cabos ou satélites. (Bomfati; Kolbe Junior, 2020).

A Internet tornou-se a maior ponte para todo o engenho tecnológico, pois ao ligar o mundo de ponta a ponta tornou-se possível levar novas tecnologias de informação e desenvolvimento social a muitas culturas. Por outro lado, também é crescente a utilização desta importante ferramenta tecnológica para a prática de atos ilícitos. (Trentin, 2012).

De acordo com o crescimento da internet temos o entendimento de Jesus e Milagre (2016, p. 15):

> A convergência tecnológica. a dinâmica industria e a queda dos preços dos equipamentos. aliados ao vertiginoso crescimento da internet. São molas propulsoras das recentes transformações sociais locais. • Brasil ultrapassa pela primeira vez 100 milhões de usuários de internet. A evolução rápida eis que duas décadas atrás utilizávamos redes-idonet. Conectando-se com pessoas através de BBS (Bulleting Board Svstems) e modems que nos permitiam o acesso discado. Muitas vezes em não mais que 56kpb (kilobvts por segundo).

A Internet cresce exponencialmente a cada ano, ligada à evolução tecnológica, entrelaçada com dispositivos tecnológicos mais baratos, tornando-se assim mais acessível a grande parte da sociedade (Wednt; Jorge, 2013).

O Brasil integra o grupo de 79 países onde mais de 50% da população tem acesso à Internet. No país, 57,6% das pessoas estão conectadas. A forma de acesso, porém, apresenta variações. A cada 100 brasileiros, apenas 11,5 possuem uma assinatura de banda larga fixa, quando avaliados as assinaturas de banda larga móvel esse valor sobe para 78,1, ainda segundo o relato da UIT, 48% dos domicílios do Brasil não possuem conexões a internet, sendo os resultados da Pesquisa Nacional por Amostra de domicilio de 2013 (PNAD), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE). Segundo a ONU houve avanços referentes a evolução tecnologia nas residências, mas estes avanços foram totalmente desiguais pois em países como Noruega, Dinamarca e Islândia o número de pessoas conectadas ultrapassa os 90%, e em países em desenvolvimento a média de conexão da internet é de apenas 35%, ainda segundo a ONU esses avanços desiguais se deram no ano de 2014 para 2015 em que 300 milhões de

pessoas conquistaram o acesso à rede mundial de computadores somando 3,2 bilhões, sendo que metade da comunidade mundial não está conectada (Nações Unidas Brasil, 2015).

A Internet de hoje é crucial para nossas vidas. A tecnologia da informação de hoje é a eletricidade da era industrial. A Internet tornou-se a base técnica para a forma organizacional (ou seja, rede) da era da informação. Essa rede interligada é uma prática civilizacional muito antiga, mas que ganhou sobrevivência em nosso tempo, transformando-se em uma rede de informações (Castells, 2003).

Porém com o avanço tecnológico os usuários com intenções de causar danos, aproveitando-se destes serviços para suas práticas criminosas (Barreto; Wednt, 2020).

1.2. Conceito de ambiente cibernético

No período mais recente da nossa história passamos por uma grande revolução, a revolução Digital, entendida como “o movimento de inserção na sociedade de novas tecnologias e novos serviços que aproveitam os progressos recentes e que modificam a forma como o cidadão comum avança” (Sydow, 2014).

À medida que a tecnologia passa a fazer parte do cotidiano de uma pessoa, torna-se necessário que o indivíduo passe a ter certos conhecimentos presumidos para lidar com a modernidade. A tecnologia da informação tornou-se um campo independente de estudo tecnológico, exclusivo e necessário aos cidadãos que inclusive fazem cursos para aprender e aprimorar as técnicas utilizadas na Internet. (Sydow, 2014).

Discutir ou mesmo conceituar o ciberespaço (ou Ambiente virtual) não é uma tarefa fácil, pois como definir um espaço que não tem “espaço”, não ocupa espaço, não tem representação física, mas impacta vidas e resultados do mundo real. Mais uma vez, embora difícil, uma vez que não há consenso, é quase em grande parte um espaço reservado à comunicação, mesmo que a localização seja incerta e imperceptível. (Gibson, 2003).

Na perspicaz definição de Gibson sobre o ambiente cibernético:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade. (Gibson, 2003, p.67).

Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Este mundo não é não tangível, no entanto, existe de outra maneira, em outra realidade. O ciberespaço é um espaço indefinido e desconhecido, área cheia de oportunidades. Contudo, não é possível afirmar que o ciberespaço está presente em nossos PCs ou nas redes. Além disso, onde o ciberespaço está localizado? Quando desligamos nossos computadores, aonde vai todo esse "mundo"? É esse caráter fluido do ciberespaço que o torna virtual. (Monteiro; 2004).

O ciberespaço é um novo meio de comunicação criado pela interconexão global de computadores. Além de especificar a estrutura material da comunicação

digital, esta designação também caracteriza o universo da informação armazenada e também os seres humanos que transitam por este sistema. (Levy, 1999, p. 16)

Com a invenção dos computadores, o termo “cibernético” tornou-se cada vez mais popular. A cibernética é “a ciência que estuda não apenas os organismos vivos, mas também os sistemas de comunicação e controle das máquinas”. Agora, todas as “redes” estão diretamente interligadas com o mundo virtual e o “ciberespaço”.

Em outras palavras, buscamos uma definição na doutrina de Luis Monteiro, que ele classificou Internet como:

> A internet (ou a “Rede” como também é conhecida) é um sistema de redes de computadores interconectadas de proporções mundiais, atingindo mais de 150 países e reunindo cerca de 300 milhões de computadores (DIZARD, 2000) e mais de 400 milhões de usuários. Computadores pessoais ou redes locais (em um escritório, por exemplo) se conectam a provedores de acesso, que se ligam a redes regionais que, por sua vez, se unem à redes nacionais e internacionais. A informação pode viajar através de todas essas redes até chegar ao seu destino. Aparelhos chamados “roteadores”, instalados em diversos pontos da Rede, se encarregam de determinar qual a rota mais adequada. (Monteiro, 2011, online).

Com o advento dos computadores e o acesso massivo à Internet, o Brasil passou a se preocupar com esse problema, principalmente nas últimas décadas, com o aumento da popularização dessa inovação tecnológica, que na Constituição Federal de 1988 promulgou leis relativas à competência do Estado sobre questões de informática e automação (Monteiro, 2014).

No Ambiente virtual pode-se comunicar com qualquer computador através da rede de internet, então o ciberespaço inclui a internet que está presente em todas as redes, algumas dessas redes são privadas que são teoricamente separadas e o usuário tem que se conectar a elas, é redes transacionais que fazem coisas como enviar dados de fluxo de caixa, bolsas de valores, dados de cartão de crédito, algumas dessas redes são sistemas que controlam máquinas que só podem se comunicar com outras máquinas, no caso de elevadores, painéis de controle de conferência de bombas hidráulicas, geradores que são controlados desta forma. (Clarke; Knake, 2015).

Isso significa que no ambiente virtual tem-se uma variedade de informações onde todos trafegam pelos e-mails, mensagens que hoje chegam a qualquer parte do mundo com apenas um click, e que estão em circulação, podem ser muito úteis na produção de conhecimento, bem como na tomada de decisões governamentais. (Barreto; Wednt; Caselli, 2017).

O ambiente virtual consiste em um conjunto de regras que se dividem em pacotes de mensagens que trafegarão pela Internet, para que possam seguir diferentes caminhos na rede. Isso permitiu a troca de informações entre inúmeros computadores e outros dispositivos utilizando diversas conexões diferentes como, por exemplo, a conexão A DSL, o cabo, o rádio, 3G, 4G, o satélite e recentemente a fibra ótica e conexões via Wi-Fi, com isso entrar nos servidores de todos os lugares do mundo conectados entre cabos ou satélites surgindo também o lado obscuro do ambiente virtual a DeepWeb (Bomfati;Kolbe Junior,2020).

Lidando com a Deep Web, também conhecida como o lado negro da internet. A informação que impressiona é que esta rede contém 90% das

informações contidas na web, mas não pode ser acessada por meio de um navegador comum. Os usuários que entram nesta rede geralmente não querem ser identificados, ou seja, entre os usuários que nela entram estão traficantes de drogas, terroristas, traficantes de órgãos humanos de crianças e outros criminosos. (Bomfati;Kolbe Junior,2020).

A Deep Web também foi criada com o intuito de ser uma rede independente fora do padrão www que pudesse ser utilizada em caso de desastre global. Como resultado, surgiu a dark web, que é chamada de camada ainda mais obscura, profunda e oculta da rede, originada das análises do Laboratório Naval dos Estados no qual tinha desenvolvido o The Onion Routing –TOR (roteamento em cebola, uma rede em anonimato no qual o acesso está ligado em adentrar as camadas da web, comose fossem uma cebola) (Bomfati;Kolbe Junior,2020).

> A Deep Web é, portanto, composta por redes de computadores que têm como características o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo conteúdo não é "visível" pelas ferramentas de buscas convencionais (Barreto; Santos, 2019, p.17).

Assim, a Deep Web consiste em redes de computadores cujas características são o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo conteúdo não é "visível" pelas ferramentas convencionais de busca.(Barreto; Santos, 2019, 17).

Uma das vulnerabilidades da Internet é o fato de tudo que funciona é aberto, ou seja, sem criptografia. Ao navegar na web, a maior parte das informações é enviada sem a devida proteção, o que significa que não são criptografadas, deixando você vulnerável às consequências dos cibercriminosos. Realmente com o universo da Deep Web e Dark Web, fica de fato evidenciado, o grande avanço tecnológico frente ao nosso Direito, os criminosos utilizam-se desses mecanismos para evadir-se e dificultar as investigações, mostrando perícia e destreza nos crimes praticados na internet. (Clarke; Knake, 2015).

1.3. Princípios que regulam o ambiente cibernético

A sociedade humana há muito tempo desenvolve um modelo harmonioso de coexistência social baseado num sistema de regras comportamentais. Anteriormente, as regras eram transmitidas oralmente e rapidamente evoluíram para a forma escrita e documentada. Esta mudança é importante considerando que quando as normas são claras, objetivas e organizadas, são mais fáceis de aceitar e até mesmo de impor à comunidade (Pinheiro, 2014).

Desde a criação da Internet, um dos maiores debates tem sido sobre a necessidade ou não de regulamentação deste ambiente, que surgiu basicamente sem qualquer controle. (Pinheiro, 2014).

Hoje em dia, a Internet tornou-se um verdadeiro fenómeno que mudou e remodelou empresas em diversas áreas. Por exemplo, a Internet melhora e proporciona novas oportunidades para vários grupos minoritários ganharem determinados espaços de discussão na vida pública. No entanto, à medida que o acesso aumenta, também aumentam as atividades baseadas no discurso de ódio, como referido anteriormente (Wigerfelt; Wigerfelt; Dahlstrand, 2015).

Neste contexto, o Estado Democrático de Direitos, como no Brasil, deve prevalecer sobre os princípios da liberdade de expressão e outros, como o da dignidade da pessoa humana, a fim de possibilitar e preservar o acesso à Internet

como um meio interativo e participativo e decisivo espaço no contexto da atual (Pannain; Pezzella, 2015).

No Brasil, a Lei 9.609, de 19 de fevereiro de 1998, que substituiu a Lei 7.646, de 18 de dezembro de 1987, trouxe para a legislação considerações inovadora sobre tecnologia virtual, garantindo a proteção da propriedade intelectual de programas de computador, sua comercialização no país e outras providências (Siqueira, 2017).

A Lei 9.609/1998 apresenta conceituação de programa de computador nos seguintes termos:

> Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. (Brasil, 1998, *online*).

Além disso, devido à necessidade imediata de aprimorar a legislação relacionada aos crimes cibernéticos ou virtuais, em 2012 o Congresso Nacional aprovou a Lei 12.737, de 30 de novembro de 2012, que estabeleceu a classificação penal dos crimes informáticos e alterou o Código Penal (BARBOSA, 2014).

O princípio da liberdade de expressão foi introduzido pela Constituição Federal de 1988, no artigo 5º, inciso IX, e também inserido no artigo 220, § 1º, o referido princípio dá ênfase às expressões de pensamento, opinião, expressões intelectuais, artísticas, científicas e de comunicação, sem censura. Este princípio desperta a busca pela informação, o que por sua vez cria a liberdade de imprensa, pois inclui o direito de ser informado, o que leva à formação de conhecimentos e ideias conduzindo a um senso crítico, onde segundo Carlos Roberto Siqueira6 “e as pessoas desinformado e privado da capacidade crítica de avaliar o processo social e político, encontram-se excluídos das condições de cidadania que impulsionam o destino das nações” (Muta, Luiz Carlos Hiroki, Elsevier, 2012).

Nesse contexto surge o Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014, que estabelece os princípios, garantias, direitos e obrigações para o uso da Internet no Brasil, bem como diretrizes para a atuação da União, dos Estados, Distrito Federal e Municípios nessas coisas (Brasil, 2014*, online*).

Em seus artigos introdutórios, a Lei 12.965/2014 aponta os fundamentos, princípios, objetivos e conceitos básicos aplicáveis na matéria em questão (Brasil, 2014*, online*).

O Marco Civil da Internet estabelece princípios fundamentais que podem ser interpretados como a base do direito digital no Brasil. Esses princípios incluem a garantia da liberdade de expressão, comunicação e manifestação de pensamento, a proteção da privacidade e dos dados pessoais, a preservação da neutralidade de rede, a estabilidade e segurança da rede, a responsabilidade dos agentes de acordo com suas atividades, e a promoção da natureza participativa da rede. Além disso, o Marco Civil permite a liberdade nos modelos de negócios online, desde que estejam em conformidade com os demais princípios estabelecidos. Essas diretrizes refletem a preocupação em equilibrar a inovação digital com a proteção dos direitos individuais e a integridade da infraestrutura da internet (Walmar Andrade, Direito Digital, Online).

Vale destacar os princípios que são mencionados em seu art. 3ºque orientam o espaço cibernético, a saber:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. (Brasil, 2014, *online*).

Entre os conceitos destacados no art. 5° os itens relevantes são internet, terminal, endereço de protocolo de internet (endereço IP), conexão de internet, gerenciador de sistema autônomo, registro de conexão, aplicação de internet e registros de acesso a aplicações de internet. (Brasil, 2014, online)

De acordo com os princípios estabelecidos no artigo 5º, o Marco Civil da Internet aponta os direitos e garantias dos usuários (Capítulo II), o fornecimento de conexão e aplicativos à Internet (Capítulo III), que inclui a neutralidade da rede (Seção I), a proteção de registros, Dados pessoais e comunicações privadas (Seção II), Manter registros de conexões (Subseção I), Manter registros de acesso a aplicativos de Internet ao fornecer conexões (Seção II) e Manter registros de acesso a aplicativos de Internet ao fornecer aplicativos (Subseção III), Responsabilidade por Danos Resultantes de Conteúdo criado por terceiros (Seção III) e solicitação judicial de registros (Seção IV) e, por fim, estabelece diretrizes para atuação do poder público (Brasil, 2014, online).

O artigo 15 do Marco Civil trata da guarda e preservação dos registros de conexão à internet, que devem ser confidenciais e em ambiente controlado e seguro pelo prazo de um ano, podendo o Ministério Público ou as autoridades policiais e administrativas requerer medida preliminar para garantir que a guarda e preservação estejam em andamento há mais de um ano, cabendo à autoridade requerente a autorização judicial para acesso aos dados no prazo de 60 dias (Brasil, online).

Neste ponto, vale ressaltar que o Regulamento do Marco do Direito Civil na Internet, Decreto nº 8.771, de 11 de maio de 2016, define dados cadastrais como filiação, endereço e qualificações pessoais (nome, sobrenome, estado civil e profissão). Embora as informações financeiras não estejam incluídas nesta lista, a jurisprudência é consistente no sentido de que os detalhes de pagamento de serviços, seja por conta bancária ou cartão de crédito ou outros meios, não são confidenciais, pelo que tanto os fornecedores de ligação como os fornecedores de aplicações devem informar as autoridades requerentes (polícia, público Ministério Público e autoridade administrativa), independentemente de ordem judicial. Na verdade, conforme já estabelecido no artigo 17 B da Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro) alterada pela Lei nº 12.683/2012 (Brasil, online).

Um aspecto notável da Lei 12.965/2014 é o contraste entre seu objetivo padronizado de oferecer maior segurança e respaldo jurídico à Internet, bem como às relações criadas em seu âmbito, e a intenção clara e visível do legislador de evitar qualquer impressão de censura. e a intervenção estatal nas relações neste ambiente, neste sentido o legislador apontou os direitos garantidos constitucionalmente como garantia da liberdade de expressão, comunicação e manifestação de pensamento (Tomas, 2016).

Nesse sentido, o art. 22 do Marco dos Direitos Civil da Internet busca oferecer suporte normativo individual adequado ao solicitar o armazenamento de informações que possam servir como prova em processos judiciais (Brasil, 2014, online).

CAPÍTULO II - IMPLEMENTAÇÃO DA LEI DE PROTEÇÃO DE DADOS

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, estabeleceu um marco significativo no cenário jurídico brasileiro e internacional, estabelecendo diretrizes fundamentais para o tratamento de dados pessoais e reforçando os direitos dos titulares desses dados. Esta legislação surge em resposta à crescente preocupação com a privacidade e a proteção de informações pessoais em um mundo digital cada vez mais interconectado e dependente de tecnologias de informação.

O presente capítulo busca realizar uma análise abrangente da LGPD, explorando suas diferentes facetas e implicações. Inicialmente, será realizada uma contextualização da legislação, destacando sua origem, evolução e importância no contexto nacional e internacional. Serão abordados aspectos históricos e motivadores que culminaram na criação da LGPD, bem como sua relação com outras normativas internacionais de proteção de dados.

Em seguida, será explorada a base filosófica e legal da LGPD, examinando seus princípios e direitos dos titulares de dados. Serão detalhados os princípios que regem o tratamento de dados pessoais, tais como finalidade, adequação, necessidade, consentimento, transparência, segurança e prestação de contas, destacando-se o papel central do indivíduo na proteção de sua própria privacidade e no controle sobre suas informações pessoais.

Por fim, serão discutidos os impactos e desafios da implementação da LGPD, tanto para as organizações quanto para a sociedade como um todo. Serão analisadas as mudanças necessárias nos processos internos das empresas, os investimentos em segurança da informação e o papel dos órgãos reguladores na fiscalização e aplicação da legislação. Além disso, serão exploradas as implicações sociais e econômicas da LGPD, bem como os desafios enfrentados na adaptação às novas exigências legais em um mundo digital em constante evolução.

2.1. Fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD)

A coesão social é um elemento crucial em qualquer sociedade, pois é o que viabiliza a convivência pacífica entre os indivíduos. O Direito desempenha um papel fundamental ao promover relações mais harmoniosas entre as pessoas e os diversos grupos sociais, constituindo-se assim em uma das bases essenciais para o progresso da sociedade. (Nader, 2004).

As comodidades proporcionadas por esses avanços tecnológicos são tão ubíquas em nossas vidas diárias que muitas vezes não percebemos claramente que estamos imersos em uma sociedade informatizada. Neste contexto, os dados fluem em velocidades antes inimagináveis, exercendo influência significativa sobre os valores sociais e econômicos. (Lisboa, 2016).

O ciberespaço representa o emergente meio de comunicação resultante da interconexão global dos computadores. Esta terminologia, além de descrever a infraestrutura material da comunicação digital, delineia igualmente o vasto repositório de informações nele contido, bem como os indivíduos que o exploram. (Levy, 1999).

O Direito desempenha um papel fundamental na promoção da coexistência social, visto que sua principal função é contribuir para a manutenção de um mínimo de ordem, direção e solidariedade. Em consonância com o antigo provérbio "ubi societas, ibi jus" (onde está a sociedade, está o Direito), a relação é recíproca, de modo que é inconcebível imaginar qualquer forma de convivência social sem regras, assim como não há sociedade sem Direito. (Reale, 2002).

A informação desempenha um papel crucial em um mundo cada vez mais globalizado e interconectado. Nesse contexto, os sistemas de segurança devem se dedicar a assegurar autenticação, controle de acesso, confidencialidade dos dados e integridade. (Starllings, 2008).

No ambiente cibernético, os tipos de dados são variados e abrangentes, refletindo a diversidade das interações e transações digitais que ocorrem diariamente. Desde dados estruturados, como informações em bancos de dados relacionais, até dados não estruturados, como texto livre em redes sociais e e-mails, o ecossistema digital é rico em uma infinidade de tipos de dados. (Wendt, 2013).

Com a crescente preocupação com a proteção da privacidade e dos dados pessoais em um mundo digitalizado e interconectado foi criada a Lei Geral de Proteção de Dados Pessoais (LGPD), tendo como principal motivação uma série de fatores que evidenciaram a necessidade de uma legislação específica para regular o tratamento de dados pessoais. (Garcia, 2020).

A Lei nº 13.709/2018 foi criada para estabelecer regras claras e abrangentes sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, visando garantir a privacidade e a proteção dos direitos fundamentais dos cidadãos em um cenário de constante evolução tecnológica. (Brasil, 2018).

O avanço tecnológico e a expansão da internet trouxeram consigo uma crescente preocupação com a privacidade dos dados pessoais dos cidadãos. O aumento da coleta e do compartilhamento de informações pessoais por empresas e governos gerou uma demanda por regulamentações mais rigorosas para proteger os indivíduos contra possíveis abusos e violações de privacidade. (Brasil, 2018).

A criação da LGPD foi motivada, em parte, pelo desejo de alinhar o Brasil às melhores práticas internacionais em proteção de dados. A União Europeia, por exemplo, já havia implementado o Regulamento Geral de Proteção de Dados (GDPR), estabelecendo um novo padrão global para a proteção da privacidade dos cidadãos europeus. A LGPD busca seguir essa tendência global, promovendo a conformidade com os princípios e diretrizes estabelecidos pelo GDPR e outras legislações similares. (Regulation of the European Parliament, 2016).

> A LGPD representa um marco regulatório importante para o Brasil, trazendo consigo desafios e oportunidades para as organizações se adaptarem às novas exigências legais e garantirem a conformidade com os princípios e diretrizes estabelecidos pela legislação.(Doneda, 2019).

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia teve um papel significativo na elaboração da LGPD, servindo como referência para muitos dos princípios e diretrizes adotados na legislação brasileira. (Regulation of the European Parliament, 2016).

A existência de uma legislação robusta de proteção de dados é fundamental para fomentar a confiança dos cidadãos no uso de serviços digitais e no compartilhamento de informações pessoais. Ao estabelecer regras claras e transparentes para o tratamento de dados, a LGPD contribui para o desenvolvimento de um ambiente de negócios mais seguro e favorável à inovação, incentivando empresas a investirem em tecnologias e práticas que promovam a proteção da privacidade dos usuários. (Gov.br, Online).

A LGPD tem como objetivo fortalecer os direitos individuais dos cidadãos em relação aos seus dados pessoais, garantindo maior controle e autonomia sobre suas informações. Ao estabelecer direitos como o acesso, retificação, exclusão e portabilidade dos dados, a legislação empodera os titulares dos dados, permitindo-lhes tomar decisões informadas sobre o uso de suas informações pessoais por parte das empresas e organizações. (Garcia, 2020).

A Lei estabelece uma série de princípios incluindo os princípios da Finalidade, Adequação, Necessidade, Livre Acesso, Qualidade dos Dados, Transparência e Segurança. Que devem ser observados no tratamento de dados pessoais, visando assegurar a proteção dos direitos fundamentais dos titulares dos dados. Os dados pessoais devem ser tratados para finalidades legítimas, específicas e explícitas, sendo vedado o tratamento posterior para finalidades incompatíveis com aquelas previamente informadas ao titular. (Brasil, 2018).

O tratamento de dados deve ser adequado, relevante e limitado ao mínimo necessário para o cumprimento das finalidades informadas ao titular. Devendo limitar-se ao mínimo necessário para a realização de suas finalidades, abrangendo apenas os dados estritamente relevantes e indispensáveis para o cumprimento da finalidade pretendida. (Brasil, 2018).

Deve-se realizar o tratamento de dados pessoais com o consentimento do titular, exceto nos casos previstos em lei ou em situações de exceção previstas na própria LGPD, devendo os controladores de dados adotar medidas transparentes, claras e acessíveis para informar os titulares sobre o tratamento de seus dados, incluindo a finalidade, a forma e a duração do tratamento, bem como os direitos do titular em relação aos seus dados. (Brasil, 2018).

No contexto da Lei Geral de Proteção de Dados (LGPD), o tratamento de dados pessoais é conduzido por dois agentes principais - o Controlador e o Operador. Além deles, a legislação estabelece a figura do Encarregado, designado pelo Controlador para atuar como intermediário entre este, o Operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (Gov.br, Online).

Um aspecto fundamental abordado pela LGPD é o tratamento de dados, que abrange qualquer atividade que envolva dados pessoais em sua execução, incluindo coleta, produção, acesso, armazenamento, eliminação e compartilhamento, entre outros. (Gov.br, Online).

Antes de iniciar qualquer tipo de tratamento de dados pessoais, é imperativo que o agente responsável assegure que a finalidade da operação esteja claramente registrada e explícita, e que os propósitos sejam informados devidamente aos titulares dos dados. No caso do setor público, a finalidade principal do tratamento está relacionada à execução de políticas públicas, conforme estabelecido por lei, regulamentos ou acordos contratuais. (Garcia, 2020).

O compartilhamento de dados dentro da administração pública, para a execução de políticas públicas, é previsto pela lei e dispensa consentimento específico. No entanto, o órgão coletor deve fornecer transparência sobre quais dados serão compartilhados e com quem, enquanto o órgão receptor deve justificar a solicitação com base na execução de uma política pública específica, descrevendo o motivo e o uso pretendido dos dados. Informações sigilosas permanecem protegidas e estão sujeitas a regulamentos específicos. (Gov.br, Online).

A estrutura legal de direitos dos titulares de dados pessoais é estabelecida pela LGPD, que devem ser garantidos ao longo de todo o processo de tratamento de dados pelo órgão ou entidade. Para o exercício desses direitos, a legislação prevê ferramentas que reforçam as obrigações de transparência e criam meios processuais para envolver a Administração Pública. (Gov.br, Online).

> A LGPD representa um avanço significativo para a proteção da privacidade e dos dados pessoais no Brasil, alinhando o país às melhores práticas internacionais nessa área e estabelecendo regras claras para o tratamento de informações pessoais por parte das organizações.(Wimmer,2012)

Torna-se evidente a importância crucial da Lei Geral de Proteção de Dados (LGPD) como um marco legislativo fundamental para a garantia da privacidade e segurança dos dados pessoais dos cidadãos. A LGPD não apenas estabelece diretrizes claras para o tratamento de informações pessoais, mas também promove uma cultura de responsabilidade e transparência entre as organizações que lidam com tais dados. Através da implementação efetiva da LGPD, é possível assegurar a proteção dos direitos individuais e promover a confiança dos usuários nas atividades de processamento de dados. (Gov.br, Online).

2.2. Princípios e Direitos dos Titulares de Dados

Nos últimos anos, com o avanço da tecnologia e a proliferação de dados digitais, o tema da proteção de dados pessoais ganhou destaque significativo. É fundamental compreender os princípios e direitos dos titulares de dados, que são fundamentais para garantir a privacidade e a segurança das informações pessoais dos indivíduos. (Anpd, 2019).

> Os princípios da Lei Geral de Proteção de Dados (LGPD) são o coração da legislação, norteando toda a interpretação e aplicação das normas. Eles representam os valores fundamentais que devem guiar o tratamento de dados pessoais, como a finalidade, a necessidade, a transparência, entre outros (Blum, 2021).

A proteção de dados pessoais, no contexto da Lei Geral de Proteção de Dados (LGPD), não se limita apenas a estabelecer regras para o tratamento dessas informações pelas organizações, mas também visa garantir direitos fundamentais aos indivíduos, conhecidos como titulares de dados. (Anpd, 2019).

Os princípios estabelecidos pela LGPD servem como diretrizes fundamentais para o tratamento de dados pessoais, orientando as organizações na coleta, uso, armazenamento e compartilhamento dessas informações. (Bussola, 2019).

> Os princípios e direitos dos titulares de dados refletem uma mudança de paradigma na relação entre as organizações e os indivíduos. Eles promovem uma cultura de respeito à privacidade e transparência, incentivando a responsabilidade e a accountability no tratamento de dados pessoais (Bioni,2022).

O princípio da finalidade, conforme estabelecido no Regulamento Geral de Proteção de Dados (RGPD), destaca que a coleta de dados deve ter propósitos determinados, explícitos e legítimos. É crucial que esses dados não sejam posteriormente tratados de maneira incompatível com essas finalidades, assegurando assim a transparência e a confiança dos titulares. (Rgpd, 2024).

Em harmonia com o princípio da finalidade, o da necessidade ressalta a importância de limitar o tratamento de dados pessoais ao mínimo necessário para alcançar as finalidades estabelecidas. Esta restrição visa proteger a privacidade dos titulares, evitando a coleta excessiva ou o uso indiscriminado de informações pessoais. (Wimmer,2012).

O princípio da transparência garante aos titulares o direito fundamental de serem informados de maneira clara, transparente e acessível sobre como seus dados estão sendo tratados. Esse direito não apenas fortalece a confiança entre as partes envolvidas, mas também permite que os titulares exerçam seus direitos de maneira eficaz. (Doneda, 2019).

Além dos princípios, os titulares de dados possuem uma série de direitos, incluindo o direito de acesso, retificação e apagamento. Esses direitos, estabelecidos pelo RGPD, visam garantir que os titulares tenham controle sobre suas informações pessoais, possibilitando-lhes verificar a precisão dos dados, corrigir informações incorretas e até mesmo solicitar a exclusão de seus dados quando necessário. (Rgpd, 2024).

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I - confirmação da existência de tratamento;
>
> II - acesso aos dados;
>
> III - correção de dados incompletos, inexatos ou desatualizados;
>
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (Brasil, 2024, *online*)

Em síntese, a conformidade com os princípios e direitos dos titulares de dados não apenas é uma obrigação legal para as organizações que tratam dados pessoais, mas também é essencial para preservar a confiança do público e evitar possíveis repercussões negativas, tanto financeiras quanto reputacional. Garantir a proteção e o respeito à privacidade dos dados contribui para a construção de uma sociedade mais justa e transparente, onde os direitos individuais são valorizados e protegidos. (Garcia, 2020).

A Lei nº 13.709, estabelece direitos fundamentais para os titulares de dados pessoais, visando assegurar sua privacidade e liberdade. De acordo com o Artigo 17 desta lei, toda pessoa natural possui a titularidade de seus dados pessoais, garantindo-se os direitos essenciais de liberdade, intimidade e privacidade. (Trt5, online).

Dentre os direitos conferidos aos titulares de dados, o Artigo 18 destaca uma série de prerrogativas que podem ser exercidas mediante requisição ao controlador. Esses direitos incluem a confirmação da existência de tratamento, o acesso aos dados, a correção de informações incompletas ou incorretas, bem como a possibilidade de anonimização, bloqueio ou eliminação de dados desnecessários ou tratados de forma inadequada. (Trt5, online).

Além disso, o titular tem o direito à portabilidade dos seus dados, podendo solicitar a transferência para outro fornecedor de serviço ou produto. O controle sobre o consentimento também é assegurado, com o direito de revogação, conforme estipulado no § 5º do artigo 8º da LGPD. É importante ressaltar que o titular também tem o direito de ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa negativa. (Trt5, online).

O acesso facilitado às informações sobre o tratamento de dados é garantido pelo Artigo 9º da LGPD, o qual estabelece que tais informações devem ser disponibilizadas de forma clara e ostensiva. Isso inclui a finalidade específica do tratamento, a identificação do controlador, informações de contato, além das responsabilidades dos agentes envolvidos no tratamento e os direitos explícitos do titular, conforme previsto no Artigo 18. (trt5, online).

Por fim, o Artigo 20 da LGPD confere ao titular o direito de solicitar a revisão de decisões baseadas unicamente em tratamento automatizado de seus dados pessoais. Isso abrange decisões que impactem seus interesses, incluindo definições de perfil pessoal, profissional, de consumo e crédito, bem como outros aspectos de sua personalidade. Esses direitos garantem um maior controle e proteção aos titulares de dados, promovendo assim uma relação mais equilibrada e transparente no tratamento de informações pessoais. (trt5, online).

Em suma, os princípios e direitos dos titulares de dados são fundamentais em qualquer cenário de tratamento de informações pessoais. Esses princípios, como finalidade, necessidade e transparência, orientam as organizações no manejo ético e responsável dos dados, desde sua coleta até o armazenamento. Paralelamente,

os direitos concedidos aos titulares, como acesso, retificação, portabilidade e o direito ao esquecimento, objetivam garantir a proteção e o controle sobre seus dados pessoais. O respeito e entendimento desses princípios e direitos não apenas são requisitos legais, mas também são cruciais para estabelecer uma relação de confiança entre as organizações e os titulares, fomentando uma cultura de privacidade e transparência no meio digital. (Garcia,2020).

2.3. Impactos e Desafios da Implementação da LGPD

A implementação da Lei Geral de Proteção de Dados no contexto brasileiro tem gerado diversos impactos e desafios tanto para as organizações quanto para os próprios titulares de dados. Neste capítulo, serão abordados os principais impactos e desafios enfrentados durante o processo de adequação à LGPD. (Peck, 2023).

No âmbito cultural, a LGPD impõe uma mudança essencial, promovendo uma maior conscientização sobre a proteção de dados pessoais. Essa mudança demanda um esforço conjunto entre gestores e colaboradores para promover uma cultura de privacidade e segurança da informação. (Blum, 2021).

Do ponto de vista operacional, a adequação à LGPD requer ajustes nos processos operacionais, desde a coleta até o armazenamento de dados pessoais. Tais ajustes envolvem a implementação de medidas técnicas e organizacionais para garantir a conformidade com a legislação. No entanto, essas mudanças podem impactar diretamente nos custos e na eficiência dos processos. (Blum, 2021).

Juridicamente, a LGPD estabelece uma série de obrigações legais para as organizações. Isso inclui a revisão e elaboração de políticas de privacidade, a realização de avaliações de impacto à proteção de dados e a comunicação de incidentes de segurança. O não cumprimento dessas obrigações pode resultar em sanções administrativas e financeiras significativas. (Blum, 2021).”A implementação da LGPD requer uma mudança cultural nas organizações, que precisam adotar medidas efetivas para garantir a conformidade com a legislação e proteger os direitos dos titulares dos dados”. (Bioni,2022).

Os impactos da LGPD são abrangentes e afetam aspectos culturais, operacionais e jurídicos das organizações, exigindo um esforço conjunto para garantir a conformidade e proteção dos dados pessoais. (Blum, 2021).

No âmbito cultural e organizacional, enfrenta-se a resistência interna à mudança de cultura e práticas em relação à proteção de dados. A falta de conscientização e comprometimento por parte dos colaboradores pode dificultar o processo de implementação da LGPD, tornando essencial um trabalho contínuo de sensibilização e educação sobre a importância da proteção de dados pessoais. (Bioni,2022).

No campo tecnológico, destaca-se o desafio da adaptação dos sistemas e tecnologias existentes para atender às exigências da LGPD. Essa adaptação pode ser complexa e custosa, demandando investimentos em infraestrutura e soluções tecnológicas que assegurem a segurança e conformidade no tratamento de dados pessoais. (Bioni,2022).

Juridicamente, a interpretação e aplicação da LGPD têm suscitado debates e dúvidas no meio jurídico e empresarial. Questões como o tratamento de dados sensíveis, o consentimento dos titulares e as responsabilidades dos agentes envolvidos no processamento de dados têm sido temas de análise detalhada e interpretação das normas. (Peck, 2023).

A implementação da LGPD tem sido um desafio multifacetado para as organizações, abrangendo aspectos culturais, tecnológicos, jurídicos e regulatórios.

É crucial que as empresas estejam preparadas para enfrentar esses desafios de forma estratégica e proativa, garantindo a conformidade com a legislação e a proteção efetiva dos dados pessoais dos indivíduos. (Bioni,2022).

A conscientização sobre a importância da Lei Geral de Proteção de Dados (LGPD) ainda não atingiu todas as empresas de forma plena, e muitas delas ainda não compreendem totalmente os requisitos que ela impõe. A adaptação à LGPD requer mudanças organizacionais significativas, o que pode representar um desafio considerável para instituições de diferentes portes e segmentos. Esse processo envolve desde a revisão de políticas internas até a implementação de novos procedimentos para garantir a conformidade com a legislação. (Damasio, online).

A falta de recursos financeiros e capacitação adequada também se apresentam como um obstáculo na implementação da LGPD. A adequação à lei demanda investimentos em tecnologia, treinamento de funcionários e, em muitos casos, a contratação de especialistas em proteção de dados. Esse cenário pode ser especialmente desafiador para pequenas e médias empresas, que podem enfrentar dificuldades em alocar os recursos necessários para atender a todas as exigências da lei. (Damasio, online).

Além disso, a efetividade da LGPD depende em grande parte da fiscalização e aplicação de sanções adequadas para as empresas que não cumprirem a legislação. Entretanto, no Brasil, ainda não há uma estrutura consolidada de fiscalização, o que pode comprometer a aplicação da lei. As penalidades previstas para o descumprimento da LGPD são substanciais e podem impactar severamente as organizações. No entanto, é crucial que essas sanções sejam aplicadas de forma justa e consistente para garantir a eficácia da legislação. (Damasio, online). "A LGPD é uma oportunidade para as organizações repensarem suas práticas de coleta, armazenamento e compartilhamento de dados, adotando medidas proativas de proteção da privacidade desde a concepção de seus produtos e serviços." (Peck, 2023).

Outro desafio significativo reside nos aspectos tecnológicos. Com a crescente digitalização de serviços e o uso cada vez mais frequente de tecnologias avançadas, a proteção de dados torna-se cada vez mais complexa. Garantir a segurança dos dados em ambientes tecnológicos em constante evolução é um desafio contínuo que as organizações precisam enfrentar. (Damasio, online).

Em suma, a LGPD representa um avanço significativo na proteção da privacidade e dos dados pessoais dos cidadãos brasileiros. No entanto, para que essa legislação seja efetiva, é crucial que tanto as empresas quanto os órgãos fiscalizadores e os próprios cidadãos trabalhem em conjunto para garantir a sua implementação adequada e a proteção dos direitos de privacidade de todos os brasileiros. (Damasio, online).

A compreensão da Lei Geral de Proteção de Dados (LGPD) pode ser desafiadora inicialmente, dada a sua complexidade. Por isso, é fundamental que as organizações contem com profissionais especializados para auxiliá-las na interpretação dos requisitos da lei e na implementação das medidas necessárias para se adequarem. Esses profissionais podem oferecer orientação técnica e jurídica crucial para garantir a conformidade com a legislação e a proteção eficaz dos dados pessoais. (Instituto Rui Barbosa, Online).

A atualização dos processos internos das organizações é uma exigência central da LGPD. Isso requer mudanças significativas nos procedimentos existentes para assegurar a proteção dos dados pessoais em todas as etapas do ciclo de vida

da informação. Desde a coleta até o descarte dos dados, é necessário revisar e adaptar os processos para garantir o cumprimento das disposições legais. (Instituto Rui Barbosa, Online).

Além das mudanças nos procedimentos, a LGPD determina que as organizações implementem medidas de segurança adequadas para proteger os dados pessoais contra diversas ameaças, como acesso não autorizado, destruição, perda, alteração ou divulgação indevida. Essas medidas devem ser proporcionais ao nível de risco enfrentado por cada organização, exigindo uma abordagem personalizada para a segurança da informação. (Instituto Rui Barbosa, Online).

O treinamento dos funcionários é outra dimensão crucial da conformidade com a LGPD. A lei enfatiza a importância de conscientizar todos os membros da organização sobre as boas práticas de proteção de dados e suas responsabilidades individuais. Isso inclui não apenas funcionários permanentes, mas também trainees, colaboradores temporários e prestadores de serviços, que devem ser educados sobre a importância da privacidade e da proteção dos dados pessoais. (Instituto Rui Barbosa, Online).

Por fim, a LGPD estabelece a necessidade de criação de um Programa de Privacidade e Proteção de Dados como parte do compliance das organizações. Esse programa deve incluir políticas e procedimentos específicos para garantir o cumprimento da lei, bem como mecanismos de monitoramento e auditoria para avaliar a eficácia das medidas implementadas. Essa abordagem sistemática é essencial para garantir a conformidade contínua e a proteção adequada dos dados pessoais no ambiente organizacional. (Instituto Rui Barbosa, Online).

Superar os desafios impostos pela Lei Geral de Proteção de Dados (LGPD) é uma jornada necessária para as organizações que lidam com dados pessoais. Apesar dos obstáculos enfrentados, é importante ressaltar que a conformidade com a LGPD traz uma série de benefícios para as empresas, incluindo a melhoria da reputação, a redução do risco de sanções e o aumento da confiança dos clientes e parceiros. Para auxiliar as organizações a enfrentarem os desafios e aproveitarem os benefícios da conformidade com a LGPD, é crucial seguir algumas orientações práticas. (Bioni,2022).

Começar cedo é fundamental, iniciar o processo de adequação à LGPD o mais rapidamente possível proporciona à organização o tempo necessário para compreender a legislação, revisar seus processos de trabalho e implementar as medidas de segurança exigidas. Isso não apenas reduz a pressão do prazo, mas também permite uma implementação mais eficaz. (Bioni,2022).

Contar com profissionais especializados é essencial dada a complexidade da LGPD. Consultorias especializadas, como a LEGRAN, podem oferecer o conhecimento técnico e prático necessário para entender os requisitos da lei e implementar as medidas adequadas. Essa parceria pode garantir uma abordagem mais eficiente e direcionada à conformidade. (Bioni,2022).

Criar um plano de ação detalhado é crucial para o sucesso da adequação à LGPD. Esse plano deve estabelecer as etapas necessárias para se adequar à lei, incluindo revisões de processos, treinamentos de funcionários e implementação de medidas de segurança. Definir recursos e um cronograma claro ajuda a garantir que o processo de conformidade seja gerenciado de forma eficaz e organizado.(Bioni,2022).

Monitorar e otimizar constantemente o Programa de Compliance é fundamental para garantir o cumprimento contínuo da LGPD. Isso pode incluir o uso de indicadores de desempenho para avaliar a eficácia das medidas implementadas,

auditorias regulares para identificar possíveis lacunas de conformidade e treinamentos contínuos para manter os funcionários atualizados sobre as práticas de proteção de dados. Essas atividades garantem que a organização permaneça em conformidade com a legislação e esteja preparada para lidar com quaisquer desafios ou mudanças futuras. (Bioni,2022).

A adequação à LGPD não é apenas um desafio, mas também uma oportunidade para as organizações aprimorarem sua cultura de proteção de dados e fortalecerem a confiança de seus stakeholders. (Blum, 2021).

A conformidade com a Lei Geral de Proteção de Dados (LGPD) é um imperativo que varia de acordo com a categoria da empresa e os tipos de dados que ela trata. Nesse contexto, é crucial que o empresário esteja ciente de que qualquer mudança substancial requer ajustes nas práticas e nos procedimentos adotados pela organização. (Economiasc, 2022).

A relevância dessas mudanças se intensifica quando se considera a possibilidade de imposição de sanções por descumprimento das normas estabelecidas. O desafio primordial para as empresas reside na necessidade de promover uma transformação cultural em sua estrutura organizacional, e simultaneamente conscientizar todos os colaboradores sobre a importância da segurança digital e da proteção da privacidade dos dados. (Economiasc, 2022). "Os impactos da LGPD vão além das questões legais, afetando também a forma como as empresas e instituições lidam com a segurança da informação e a gestão de riscos relacionados à privacidade dos dados." (Mota, 2021).

É imperativo ressaltar que a sociedade como um todo beneficia-se da efetiva aplicação dessa legislação. Atualmente, diversos escritórios de advocacia e empresas especializadas em tecnologia oferecem serviços de consultoria voltados para a adequação à LGPD. Ademais, a disseminação do conhecimento sobre a LGPD está amplamente difundida em grandes associações empresariais do país, contribuindo para a conscientização e a implementação eficaz das diretrizes previstas na legislação. (Damasio, online).

Os impactos e desafios da implementação da LGPD evidenciam a complexidade e a importância desse processo para as organizações. A legislação, embora traga consigo benefícios significativos em termos de proteção de dados e privacidade impõe desafios operacionais, tecnológicos e culturais que demandam uma abordagem estratégica e proativa por parte das empresas. (Damasio, online).

> A LGPD marca um novo paradigma no Brasil em relação à proteção de dados pessoais, impondo a necessidade de empresas e órgãos públicos adotarem uma postura mais responsável e transparente no tratamento das informações dos cidadãos (Cesa, 2020).

É essencial que as organizações compreendam plenamente os requisitos da LGPD, busquem orientação especializada e invistam recursos adequados para garantir a conformidade e, ao mesmo tempo, promover uma cultura de proteção de dados e privacidade. Ao enfrentar esses desafios com diligência e comprometimento, as organizações podem não apenas atender aos requisitos legais, mas também fortalecer a confiança dos consumidores, melhorar sua reputação e mitigar riscos associados ao tratamento inadequado de dados pessoais. (Damasio, online).

CAPÍTULO III – CRIMES NO AMBIENTE CIBERNÉTICO

Atualmente, no mundo altamente conectado em que vivemos, a rede mundial de computadores se transformou em uma ferramenta crucial para comunicação, emprego, diversão e uma variedade de outras tarefas. Infelizmente, essa mesma estrutura também se tornou um ambiente propício para o surgimento de práticas delituosas, os crimes virtuais.

O avanço acelerado da tecnologia digital trouxe consigo um leque ampliado de oportunidades e obstáculos, alterando não só a forma como nos relacionamos e nos expressamos, mas também redesenhando os contornos e os limites do universo jurídico. Diante disso, o mundo virtual se destaca como um ambiente diversificado, no qual a união entre o mundo virtual e o real proporciona um solo fértil para a execução de várias práticas criminosas.

Os delitos virtuais, identificados pelo emprego da tecnologia da informação e comunicação como instrumento, alvo ou modo para cometer ações ilegais, constituem uma séria ameaça para a segurança online, a privacidade dos cidadãos e a solidez das instituições. Desde tentativas de phishing e furto de informações até golpes financeiros e casos de ciberbullying, a ampla gama de crimes praticados no ambiente virtual desafia os aparatos legais e os esquemas regulatórios vigentes, demandando respostas rápidas e flexíveis por parte das autoridades competentes.

Neste cenário, este capítulo explora de maneira ampla e aprofundada o fenômeno dos delitos no mundo virtual. Através de uma análise interdisciplinar que envolve aspectos do direito penal, da tecnologia da informação e da criminologia, será investigado o modo de agir dos criminosos online, os tipos de crimes mais frequentes, os impactos sociais e econômicos dessas atividades ilegais, além dos desafios enfrentados pelas autoridades de segurança e judiciais na prevenção e combate a esses delitos.

Considerando a complicação e movimentação desta área de pesquisa, acredita-se que este estudo possa ajudar no avanço do conhecimento sobre os delitos cibernéticos, oferecendo informações pertinentes para a criação de políticas públicas, melhoria das leis e aplicação de estratégias eficazes para combater a criminalidade online.

3.1. Introdução aos Crimes Cibernéticos

Os crimes cibernéticos são praticados por qualquer pessoa que utilize a tecnologia da informação para causar prejuízos à segurança, reputação ou privacidade alheia. Essas infrações ocorrem principalmente no meio digital e são classificadas como crimes virtuais (Rossini, 2004).

> O conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade,a disponibilidade e a confidencialidade. (Rossini, 2004, p. 110).

Os delitos virtuais são conhecidos por diferentes denominações, não existindo um termo universalmente reconhecido para explicar sua definição. No entanto, o importante não é a forma como esses crimes são chamados, mas sim o uso de tecnologias da informação e comunicação para cometer atos ilícitos, resultando em prejuízos a direitos legais. É imprescindível que a ação seja prevista em lei, contrária à norma e seja realizada de forma consciente (Da Silva, 2015).

Para entender adequadamente esse tipo de ato criminoso, é fundamental compreender que os crimes cibernéticos consistem em condutas criminosas previstas na legislação, praticadas utilizando computadores, contra computadores, sistemas de informação ou dados neles contidos (Castro, 2003).

O termo "crime cibernético" surgiu durante uma reunião do G8 em Lyon, França, em que foram discutidos atos criminosos realizados através de dispositivos eletrônicos ou pela divulgação de dados pela internet. O objetivo desse encontro era analisar questões relacionadas à criminalidade online que surgiram e foram facilitadas pela rede mundial de computadores (Perrin, 2006).

Nesta descrição ampla, a prática do crime informático necessita como fator crucial a utilização de um dispositivo de computação para a realização de várias ações ilegais. Qualquer atividade em que um computador seja empregado como instrumento, ponto de partida de um ataque ou modo de cometer um delito é classificado como cibercrime (Cassanti, 2014).

A ocorrência de crimes cibernéticos acontece no mundo online, onde o computador é utilizado como instrumento, alvo principal ou de maneira conectada. Engloba ações criminosas ligadas ao uso indevido do computador ou da internet, como invasão não autorizada e roubo de informações online, que podem ser utilizadas de diversas formas prejudiciais às vítimas (Agarwall, Kasuhik, 2014).

> Ofensas cometidas contra indivíduos ou grupos de indivíduos com a motivação criminosa de intencionalmente prejudicar a reputação da vítima ou lhe causar sofrimento físico ou mental, direta ou indiretamente, usando redes modernas de telecomunicações como a internet (Salas de Chat, Grupos de notícias) e celulares (Halder, Jaishankar, 2011, online).

As atividades criminosas cibernéticas compreendem ações que são consideradas ilegais, podendo ser classificadas como crimes ou contravenções. Essas práticas podem ser intencionais ou acidentais, realizadas por indivíduos ou empresas, utilizando equipamentos de computação em redes ou fora delas, que interfiram, de forma direta ou indireta, na proteção das informações, incluindo os princípios de confidencialidade, disponibilidade e integridade (Rossini, 2004).

Segundo a OCDE, crime cibernético é caracterizado como toda ação ilegal e antiética não autorizada que englobe a utilização automatizada de informações e/ou a transferência de dados (Reis, 1997).

O crime online é visto como um perigo para os sistemas de dados, que consistem em elementos conectados entre si responsáveis pela coleta, processamento, armazenamento e distribuição de informações com o objetivo de facilitar a coordenação, controle e decisões tomadas pelas organizações. (Laudon, 2010).

Com o avanço da tecnologia e a popularização da internet, a criminologia passou a se dedicar ao estudo dos crimes virtuais, buscando compreender melhor suas causas e motivações (Jaishankar, 2007).

Segundo Paulo Marco Ferreira Lima, professor, os delitos cibernéticos, que também são denominados crimes cibernéticos, são atos que, do ponto de vista legal, caracterizam-se como sendo típicos, ilícitos e culpáveis. Essas práticas incluem a utilização de equipamentos, como computadores, como forma de facilitar a realização de crimes, causando danos à comunidade, sem considerar se beneficiam ou não o responsável pela ação (Palazzi, 2000).

No Brasil, os delitos online receberam uma designação específica, sendo identificados no âmbito legal como "crimes informáticos", expressão também adotada em nações como a Espanha, demonstrando a preocupação com a proteção dos ativos jurídicos, que podem ser a própria rede ou os dados armazenados nela. Exemplos marcantes de delitos virtuais englobam o golpe, a exploração sexual de menores e, igualmente relevante, as investidas de phishing. Nestes ataques, a pessoa é ludibriada por publicidades online ou mensagens de texto infectadas com software malicioso, que se instala no aparelho do usuário com o propósito primordial de praticar furto de identidade.

Os delitos cibernéticos, além de apresentarem similaridades comuns às transgressões legais tradicionais, são caracterizados por serem praticados através da utilização de aparelhos tecnológicos e recebem diferentes denominações para descrever sua essência (Crespo,2011).

Essas transgressões podem ser divididas em próprias ou impróprias. Os delitos próprios são relacionados a ações ilegais e culpáveis que têm como alvo um sistema de computador ou seus dados, prejudicando sua confiabilidade, integridade e/ou disponibilidade. Por outro lado, os delitos impróprios consistem em ações típicas, ilegais e culpáveis praticadas por meio de dispositivos computacionais, mas que poderiam ser realizadas por outras formas (Sydow, 2014).

Os crimes virtuais podem abranger uma diversidade de participantes. Por exemplo, um especialista em computação contratado para furtar informações confidenciais de um concorrente pode explorar brechas de segurança em um sistema. Ademais, os cyber cafés podem ser utilizados como cenário para táticas de invasão, como o envio de mensagens enganosas para obter acesso não autorizado ao sistema de uma empresa. Nessas situações, há uma variedade de agentes ativos e vítimas envolvidas (Sydow, 2014).

Conforme citado, os crimes virtuais impróprios englobam delitos comumente reconhecidos no Brasil. Um exemplo marcante é o conflito entre a liberdade de expressão e o discurso de ódio. Apesar da liberdade de expressão ser garantida como um princípio constitucional, sua aplicação deve apresentar limites. É fundamental equilibrar o direito à livre expressão com a proteção dos direitos alheios, como a honra, imagem, privacidade e intimidade (Coelho; Branco, 2016).

3.2. Tipos de Crimes Cibernéticos

Considerando que os delitos virtuais abrangem tanto os subtipos próprios quanto os impróprios, iremos analisar alguns crimes com maior destaque, considerando que, ao utilizar a web como meio, com a chance de permanecer anônimo incentivando a quebra das normas, há um aumento expressivo na frequência dessas ocorrências.

3.2.1- Crimes contra honra

A honra é um direito essencial protegido pela Constituição, conforme determinado no artigo 5º, X, da Carta Magna. Os delitos que atentam contra a dignidade são amplamente reconhecidos no âmbito jurídico do Brasil, uma vez que a dignidade é um direito inalienável assegurado pela Constituição, fundamental para preservar a integridade pessoal e a reputação do cidadão (Barroso, 2004).

A doutrina brasileira distingue entre dois elementos da integridade: a integridade objetiva e a integridade subjetiva. A primeira refere-se à reputação e ao prestígio que o indivíduo possui na comunidade em que está inserido, ao passo que a segunda está ligada à dignidade e à autoestima pessoal da vítima, ou seja, a própria percepção que cada indivíduo tem de si mesmo (Cunha, 2014).

Na esfera dos delitos que atentam contra a honra, as leis criminais definem três categorias diferentes de crimes: difamação, calúnia e injúria. Essas transgressões são identificadas de acordo com a natureza do crime e as punições previstas, conforme observa-se:

> **Calúnia**
> Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> **Difamação**
> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> **Injúria**
> Art. 140 Injuriar alguém, ofendendo lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940, *online).*

Caluniar significa atribuir a alguém de maneira falsa um ato que é considerado como crime. Já a difamação consiste em atribuir a alguém um ato que não é criminal, porém que prejudica sua reputação, enquanto a injúria envolve a atribuição de características negativas ou defeitos à vítima (Noronha, 2014).

De acordo com o professor Rogério Sanches Cunha (2014), em relação a esse tema, ele esclarece que, na calúnia e na difamação, ocorre a atribuição de um acontecimento específico e prejudicial, sendo esse fato necessariamente falso na calúnia, condição que não se aplica à difamação. Por outro lado, na injúria, encontramos uma acusação genérica de má qualidade, defeito ou menosprezo em relação à vítima. Nos dois primeiros casos, é essencial que a declaração desonrosa seja conhecida por terceiros, requisito que não é obrigatório no terceiro caso.

A calúnia, com sanção mais rígida, se manifesta quando a alegação criminosa feita nunca aconteceu ou, caso tenha acontecido, a pessoa acusada não teve relação com o ocorrido (Cunha, 2014).

Caluniar ignifica prejudicar a reputação de alguém em seu círculo social, com o propósito claro de denegrir sua imagem, configurando-se a difamação quando a acusação falsa é divulgada para outras pessoas (Nucci, 2017).

O próprio Código Penal estipula as exceções à aplicação da verdade, como no caso da calúnia, onde na difamação protege-se a honra objetiva da vítima,

referindo-se à imputação de fatos que, embora não criminosos, são prejudiciais à reputação da vítima perante terceiros (Cunha, 2014).

Difamar é desacreditar publicamente alguém, imputando-lhe algo desonroso, com intenção específica, consumando-se quando a acusação é conhecida por terceiros (Nucci, 2017).

A exclusão da veracidade é aceita, como no delito anterior, apenas se a vítima for um servidor público e a ofensa estiver ligada ao desempenho de suas atribuições, cabendo ao infrator comprovar a veracidade da acusação, eliminando a ilicitude de seu comportamento (Cunha, 2014).

Na injúria, ao contrário dos crimes anteriores, protege-se o direito à honra subjetiva da vítima, caracterizada pela ofensa à sua dignidade, sem necessariamente haver imputação de fatos específicos, mas uma conceituação negativa É um insulto que mancha a honra subjetiva de alguém, afetando sua dignidade e ferindo sua autoimagem por vontade específica (animus diffamandi), consumando-se no momento em que o insulto é conhecido pelo ofendido, independentemente do conhecimento de terceiros, sem admitir a exceção da verdade (Nucci, 2017).

As diversas possibilidades de uso de computadores e ferramentas online levaram o Estado a perceber que nem sempre estava preparado para julgar e punir usuários potencialmente criminosos, cujas ações atingem a honra, o decoro e a dignidade de terceiros (Santos, 2016).

É imprescindível analisar tais comportamentos levando em consideração a importância da liberdade de expressão. Com base no respeito à individualidade e valor humano, a liberdade de expressão requer a consideração dos direitos básicos de outras pessoas. As inovações tecnológicas trazem à tona uma nova visão sobre essa liberdade, evidenciando de forma positiva o aumento das possibilidades de engajamento social e trocas culturais, ampliando o alcance da verdadeira democracia (Pannain; Pezzella, 2015).

A essência da liberdade de manifestação é vista como um caminho para alcançar soluções apropriadas para os desafios da sociedade, por meio da troca aberta de ideias divergentes, onde aquelas mais assertivas se destacarão (Sarmento, 2018).

A disputa entre a liberdade de comunicação, garantida pela constituição, e as ações que prejudicam a reputação (de forma objetiva ou subjetiva) das vítimas é clara. Mesmo que a liberdade de comunicação não possa ser utilizada sem limitações, é importante equilibrar o direito de comunicação com os direitos de outras pessoas, garantindo que os agressores sejam responsabilizados por seus abusos. Contudo, muitas vezes as ações realizadas online não são punidas judicialmente, seja pela dificuldade em identificar o verdadeiro infrator (anonimato) ou pela falta de competência do Estado em lidar com essa questão (Coelho; Branco, 2016).

Muitas vezes, essas atitudes são fruto de um profundo sentimento de ódio, sem considerar normas sociais. Um exemplo emblemático ocorreu em 2015, com a jornalista Maria Júlia Coutinho, que foi alvo de uma série de comentários racistas após compartilhar uma foto sua em uma rede social (Globo.Com, 2015, online).

Outra conduta criminosa que comumente está relacionada com os delitos mencionados previamente é a prática de ameaça, infringindo a autonomia individual e sendo tipificada no artigo 147 do Código Penal do Brasil.

Para uma análise precisa do crime de ameaça, é fundamental levar em consideração as características individuais da pessoa que foi ameaçada. Sendo

assim, é necessário analisar aspectos como a faixa etária, o gênero, a etnia, a cor da pele, a orientação sexual, e outros, para verificar se de fato ocorreu a ação criminosa, que se caracteriza pela ameaça de causar prejuízo injusto a outra pessoa (Cunha, 2014).

No dia 8 de março de 2018, um seguidor do Palmeiras levantou a bandeira contra a homofobia em suas plataformas digitais. De acordo com informações, o indivíduo foi alvo de diversas ameaças por parte de outros torcedores do Palmeiras, que entenderam a atitude como uma forma de denegrir a reputação do clube (Globo.Com, 2018, online).

Infelizmente, ocorrências como esta são comuns e acontecem frequentemente, muitas vezes motivadas por atitudes machistas, homofóbicas e preconceituosas enraizadas na sociedade. Os atos de intolerância, abarcando questões de raça, religião, cor e identidade de gênero, estão em ascensão na sociedade, principalmente com a disseminação das redes sociais. Ao mesmo tempo, tem se observado um aumento nos casos de cyberbullying, um tipo de violência virtual que tem ganhado notoriedade recentemente e está intimamente ligado aos atos criminosos discutidos nesse contexto.

3.2.2-Crimes de invasão de privacidade e intimidade

Incluído pela Lei nº 12.737 de 2012, mais conhecida como Lei Carolina Dieckmann, o artigo 154-A do Código Penal trata da invasão de dispositivo informático. Os objetos jurídicos protegidos são a intimidade, a vida privada e o direito ao sigilo dos dados armazenados em dispositivos informáticos, in verbis:

> 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. (Brasil, 1940, online).

Os objetos protegidos pela lei são a vida íntima, a privacidade e o direito à confidencialidade de informações contidas em dispositivos eletrônicos, sendo o cerne da primeira parte do delito o ato de "invadir", ou seja, acessar virtualmente sem autorização explícita ou implícita do dono do dispositivo, sem necessariamente envolver a alteração, obtenção ou destruição de dados. Já a segunda parte do crime é caracterizada pela ação de "instalar" e ocorre quando se cria uma vulnerabilidade, independentemente da obtenção efetiva de uma vantagem ilícita, configurando assim um delito formal (Capez, 2016).

A artista Carolina Dieckmann foi alvo de invasão de seu computador e posterior divulgação de documentos pessoais, incluindo suas imagens íntimas, na web. O aspecto legal do delito previsto no artigo 154-A é a proteção da privacidade individual e/ou profissional armazenada em aparelhos eletrônicos, penalizando a ação de invadir dispositivos eletrônicos alheios, através da quebra de seus mecanismos de segurança ou instalação de softwares vulneráveis (Cunha, 2014).

O legislador incluiu no parágrafo 3 uma circunstância agravante relevante para o delito, ligada diretamente à violação da privacidade da vítima. Dessa forma, ao invadir a privacidade, o infrator acaba obtendo acesso a conteúdo de mensagens eletrônicas privadas, dados confidenciais, dentre outros, resultando em um aumento

da pena de seis meses a dois anos, exceto nos casos de crimes mais graves cometidos (Capez, 2016).

De acordo com o parágrafo 4, há um agravante essencial do delito, ligado à qualificação anterior, indicando que a pena será aumentada de um a dois terços caso ocorra a divulgação, venda ou transmissão a terceiros, de qualquer forma, dos dados ou informações adquiridos. (Brasil, 1940, online).

3.2.3- Crimes contra a inviolabilidade do patrimônio

Outra prática criminosa que registrou um aumento significativo com a popularização da internet foram os casos de estelionato. Embora já fosse comum no que diz respeito à segurança do patrimônio, passou a chamar mais atenção com os golpes aplicados virtualmente.

Conforme o artigo 171 do Código Penal, é caracterizado como crime a obtenção de vantagem indevida, em prejuízo de outra pessoa, através de engano, trapaça ou qualquer outro método fraudulento.

O delito se dá quando alguém obtém vantagem de forma injusta, prejudicando outra pessoa, ao enganar ou iludir a vítima. Trata-se de um crime intencional, marcado pela decisão consciente e voluntária de enganar ou iludir alguém (Capez, 2016).

A delimitação entre fraude penal e fraude civil é discutida na literatura especializada, com conotações pejorativas. O conceito de fraude abrange qualquer conduta enganosa, feita de má fé, com a intenção de obter benefícios indevidos e prejudicar terceiros. O Código Penal busca punir a "malícia", a "astúcia" daquele que busca lesar o patrimônio alheio, induzindo a vítima a entregar seus bens voluntariamente (Cunha, 2014).

Como foi destacado anteriormente, a prática fraudulenta está se tornando cada vez mais frequente e se espalhou de maneira mais ampla com o auxílio de recursos online, gadgets tecnológicos e internet. Ela pode se apresentar sob a forma de um e-mail anônimo ou uma comunicação fraudulenta de uma entidade reconhecida, como uma instituição bancária, com o objetivo de persuadir a pessoa lesada a fornecer dados como senhas, informações pessoais e financeiras (Cunha, 2014).

O crime de fraude eletrônica se encaixa de modo preciso na definição do artigo 171 do Código Penal, permitindo sua aplicação sem maiores limitações (Capez, 2016).

A subtração (roubo eletrônico), descrito no art.155 do Código Penal, revelou-se como uma das práticas mais claras, começando com a obtenção e alteração de informações, senhas; com o objetivo de obter alguma vantagem financeira por meio de transferências bancárias ou manipulação de contas bancárias conforme desejado.(E-Gov,online).

Segundo lecionada Damásio de Jesus, “a objetividade jurídica imediata do furto é a tutela da posse; de forma secundária, o estatuto penal protege a propriedade”. Sob este enfoque, o furto virtual se satisfaz com a retirada do bem (dinheiro) da posse de seu titular, já que não há como precisar o instante de sua retirada do campo de visão protecionista do proprietário(E-Gov,online).

Diferente do ponto de vista predominante, acima mencionado, é relevante citar Rogério Greco, que defende a corrente que enxerga a posse como um dos direitos legalmente protegidos, pois há prejuízos tanto para quem possui quanto para o proprietário (E-Gov,online).

Para Gabriel Cesar Zaccaria de Inellas, “o furto mediante fraude; Consiste em um meio enganoso capaz de iludir a vigilância da vítima, para permitir maior facilidade na subtração do objeto material. No estelionato, a fraude é utilizada para induzir a vítima em erro, mediante a utilização de qualquer meio fraudulento, fazendo com que a vítima, voluntariamente, entregue seus bens; no furto mediante fraude, o meio fraudulento utilizando, ilude a vigilância da vítima que não tem conhecimento de que seus bens estão saindo de seu patrimônio.”(Inellas,2009, pág 56).

Desfrutando da mesma linha de pensamento de Inellas, Rogério Greco preleciona: “O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima, que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que iludida, entrega voluntariamente o bem ao agente.” (Greco,2009, pág 378).

Neste ponto de vista, podemos dizer que as etapas internas do crime de furto, ou seja, as fases preparatórias, tem início, por exemplo, com a recepção de uma mensagem e esta pedindo informações da pessoa enganada, que acaba fornecendo o que foi solicitado, como número da conta, senha; o remetente com esses dados segue enviando para um especialista em computação, o qual com essas informações realiza saques e transferências para contas de terceiros, resultando no crime em questão. É evidente que se trata de um procedimento complexo que se desdobra em diversas etapas, ao contrário do roubo previsto no art. 155 do Código Penal, que acontece no mundo físico(E-Gov,online).

O roubo está diretamente ligado ao golpe, confirmado por Agapito Machado e seu filho, que afirmam que os hackers que invadem os sistemas de um banco e transferem valores de terceiros para suas contas podem ser responsabilizados por estelionato (conforme o artigo 171 do Código Penal), enquanto para outros seria considerado roubo mediante fraude (de acordo com o artigo 155, parágrafo 4 do Código Penal).

3.2.4- Crimes contra a liberdade sexual envolvendo menores

É crucial discutir a questão da liberdade sexual, principalmente quando se trata de indivíduos menores de idade. O Estatuto da Criança e do Adolescente é responsável por definir os principais delitos cometidos contra crianças e adolescentes, buscando antecipar diferentes comportamentos que possam ocorrer (Capez, 2016).

Ao contrário das ações mencionadas anteriormente, estas ocorrem de maneira discreta, em sua maioria. Alguns apps de celular permitem a rápida troca de mensagens e dados, levando muitos usuários a compartilhar informações sem notar que estão, de fato, cometendo uma infração (Cunha, 2014).

Adicionalmente, um assunto que não será explorado no projeto - porém merece destaque - é a dark web (rede escura). Amplamente desconhecida pela maioria dos internautas, essa plataforma possibilita a realização de atividades criminosas em sites considerados "invisíveis", por não serem indexados pelos mecanismos de pesquisa convencionais como o Google. Na dark web, é possível encontrar uma ampla variedade de crimes como tráfico de drogas, exploração infantil, tráfico humano, comércio de órgãos, entre outras práticas (Globo.Com, 2016, online).

As ações mais relevantes no ambiente online são aquelas descritas nos artigos 241-A e 241-B do Estatuto da Criança e do Adolescente. O artigo 241-A estabelece punições para condutas ilegais de compartilhamento de qualquer forma de conteúdo sexual explícito ou pornografia envolvendo crianças e adolescentes. Por outro lado, o artigo 241-B penaliza aqueles que obtêm, de qualquer maneira, possuem ou guardam qualquer imagem ou fotografia contendo conteúdo sexual explícito ou pornografia com crianças e adolescentes (Tavares, 2012).

Em casos de crimes virtuais, a jurisprudência costuma ser rigorosa ao impor punições, levando em conta a natureza transnacional/internacional dos delitos praticados por meio da internet.

Os comportamentos considerados como delitos nos artigos mencionados visam proteger a dignidade e a liberdade sexual de menores de idade. São crimes intencionais, sendo necessário o dano potencial, não sendo preciso um dano material concreto para que sejam concretizados (Nucci, 2016).

Com a difusão de aplicativos como o whatsapp, a prática prevista no artigo 241-B está se tornando mais comum. A introdução dos crimes definidos nesse dispositivo facilita a responsabilização do indivíduo que possui em seu poder imagens de menores de 18 anos envolvidos em atos pornográficos. O elemento material consiste na fotografia, no vídeo ou na representação visual contendo pornografia ou ato sexual explícito com crianças ou adolescentes, enquanto o elemento jurídico é a proteção da formação moral da criança ou do adolescente (Nucci, 2016).

Nas palavras de Guilherme de Souza Nucci:

> A maneira pela qual o autor do crime adquire, possui ou armazena o material é livre, valendo-se o tipo da expressão “por qualquer meio”. Comumente, com o avanço da tecnologia e da difusão dos computadores pessoais, dá-se a obtenção de extenso número de fotos e vídeos pela Internet, guardando-se o material no disco rígido do computador, em disquetes, DVDs, CDs, pen drives, entre outros (2016, p. 785).

O dinâmico ambiente virtual e a constante ampliação do acesso aos ambientes virtuais impõe à legislação e aos legisladores o considerável desafio de contemplar as práticas delitivas cometidas no ambiente virtual, notadamente heterogêneas e mutáveis, em tipos penais rígidos com alcance razoável e de assertividade prática.

3.2.5- Crimes Contra a Administração Pública

O artigo 313-A do Código Penal aborda Inserção de Dados Falsos em Sistemas de Informações, para a configuração desse crime, é necessário que a conduta seja praticada por um funcionário autorizado a acessar o sistema. A ação pode ser direta, inserindo dados falsos, ou indiretos, facilitando que outra pessoa o faça. Além disso, a alteração ou exclusão indevida de dados corretos também é punível, desde que realizada com dolo, ou seja, com a intenção de obter vantagem indevida ou causar dano(Brasil, 1940).

A vantagem indevida pode ser de natureza econômica, mas também pode envolver benefícios de outra ordem, como vantagens políticas ou administrativas. O dano causado pode ser tanto patrimonial quanto moral, afetando a credibilidade e a eficiência da administração pública (Brasil, 1940).

Um caso emblemático desse delito seria a inclusão de informações inverídicas em um sistema de seguridade social visando garantir vantagens a pessoas que não preenchem os requisitos. Outra situação pode incluir a adulteração de dados tributários com o intuito de diminuir ou anular tributos devidos por empresas específicas, acarretando em prejuízos consideráveis para os cofres públicos(Brasil, 1940).

As repercussões da inclusão de informações incorretas são amplas e diversas. Além dos prejuízos financeiros diretos, existem impactos na confiança da população na gestão pública, possíveis perturbações em sistemas essenciais e prejuízos à reputação e à confiança nas entidades governamentais. Essas consequências podem perdurar por longos períodos, demandando esforços consideráveis para a correção e recuperação da integridade dos sistemas afetados (Pinheiro, 2020).

O dispositivo legal 313-B do Código Penal do Brasil aborda a prática de modificar ou alterar sistemas de informações ou programas de computador sem autorização por parte de colaboradores. A punição prevista é de prisão de 3 meses a 2 anos, e também está sujeita a multa. A legislação estabelece ainda que a pena pode ser aumentada de um terço até a metade caso a modificação ou alteração resulte em prejuízo para a Administração Pública ou para o cidadão comum (Brasil, 2000).

Ao contrário do artigo 313-A, que exige a inclusão de informações falsas ou a modificação de informações verdadeiras, o artigo 313-B engloba qualquer mudança ou alteração nos sistemas de informação sem consentimento. Isso abrange tanto modificações no código-fonte dos softwares quanto ajustes na configuração dos sistemas que impactam seu desempenho(Brasil, 1940).

A atividade deve ser feita sem a permissão ou pedido de um responsável apropriado, mostrando um desvio de conduta por parte do colaborador. Esse crime costuma estar relacionado a atos de sabotagem, quando o funcionário modifica o sistema para causar danos em seu funcionamento rotineiro. (Garcia , 2020).

Modificações não autorizadas podem danificar o software de gerenciamento de documentos e dificultar o rastreamento e a recuperação de informações. Outro caso infame pode envolver a alteração das configurações de segurança de um sistema para torná-lo vulnerável a ataques externos(Brasil, 1940).

As consequências da modificação não autorizada dos sistemas de informação são igualmente graves. Podem perturbar serviços essenciais ao expor dados sensíveis a terceiros, colocando em risco a segurança e a confidencialidade de informações críticas. Os custos de identificação, correção e prevenção de tais ações podem ser extremamente elevados, além de implicar na perda de confiança pública. (Garcia , 2020).

A inclusão dos artigos 313-A e 313-B pela Lei nº. 9.983 de 2000 do Código Penal Brasileiro foi uma resposta necessária à crescente dependência da administração pública em relação aos sistemas de informática. Estas disposições legais têm como objetivo proteger a integridade dos dados e dos sistemas, garantindo que o tratamento das informações ocorra de forma ética e autorizada. A severidade das sanções impostas a estas práticas reflete as graves consequências que tais atos podem ter no funcionamento e na credibilidade das instituições governamentais. A proteção contra a entrada de dados falsos e a modificação não autorizada de sistemas é essencial para garantir a confiança do público e a eficiência administrativa. (Garcia , 2020).

3.3- Prevenção e Combates aos Crimes Cibernéticos com a LGPD

A Lei Geral de Proteção de Dados Pessoais, também conhecida como LGPD, foi sancionada pelo presidente Michel Temer em 14 de agosto de 2018. Trata-se de uma legislação técnica que visa garantir uma série de direitos fundamentais, incluindo a proteção dos direitos humanos à liberdade e à privacidade. Com impacto tanto no setor privado quanto no público, a LGPD regula qualquer atividade que envolva o tratamento de dados pessoais, estabelecendo princípios, direitos e garantias para uma sociedade digital baseada no uso responsável de informações pessoais (Pinheiro, 2020).

A LGPD,é uma legislação relativamente nova, que passou por algumas atualizações. Foi basicamente inspirada pela criação da Autoridade Nacional de Proteção de Dados (ANPD), uma entidade que garante a eficácia e aplicação das normas estabelecidas pela regulamentação. A ANPD é responsável pela regulação da proteção de dados no Brasil e pela prorrogação do prazo para a entrada em vigor da lei. Sua criação, apesar das controvérsias, visa proporcionar maior segurança e estabilidade (Pinheiro, 2020).

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (PINHEIRO, 2020, p. 14).

Baseada na legislação europeia de proteção de dados, denominada General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados (LGPD) visa proteger os dados pessoais de indivíduos, sendo estes o alvo principal da regulação, excluindo informações de natureza jurídica e focando nos dados mantidos pelas empresas sobre pessoas físicas, sejam eles colaboradores, fornecedores ou clientes (Garcia , 2020).

A proteção dos dados é uma garantia oferecida pelas plataformas e aplicativos, porém é fato que muitas violações ocorrem devido ao uso indevido de informações pessoais. A Lei 13.709/18 foi criada com o objetivo de proteger e manter em sigilo esses dados em todo o território nacional, garantindo o direito à privacidade e proteção dos dados, inclusive no ambiente digital, tanto por indivíduos quanto por empresas. É proibido publicar informações de terceiros sem sua permissão, violando a nova Lei. Também aborda o tratamento de dados sensíveis, que são aqueles que podem ser utilizados de maneira discriminatória, como informações relacionadas à origem racial, étnica, religiosa, opinião política e dados pessoais de indivíduos. Além disso, a LGPD protege os dados pessoais dos funcionários das empresas e estabelece a responsabilização civil caso haja violação. A fiscalização dessas regras é feita pela ANPD, órgão responsável pela aplicação da legislação e pela mediação de conflitos entre empresas, usuários e a própria lei (Freitas, 2020).

Além da atualização do Marco Civil da Internet, a LGPD se destaca por sua precisão e inovação ao estabelecer sanções específicas e criar um novo órgão de regulação vinculado à presidência da República. Isso obriga tanto empresas públicas quanto privadas a se adaptarem a essa nova realidade, com punições administrativas que podem chegar a até 2% do faturamento da empresa de direito privado (Garcia , 2020).

A legislação de proteção de informações pessoais chega em um momento essencial e crucial em que estamos experimentando, demonstrando ser promissora ao priorizar a defesa e salvaguarda dos direitos individuais dos cidadãos, em meio a tantos incidentes de vazamento de dados e exposição online. A fiscalização e segurança dessas informações são de extrema importância e a nova Lei vem para complementar o Marco Civil da Internet.

CONCLUSÃO

Com os constantes progressos da tecnologia, a Internet se destaca pela ampliação de possibilidades e funcionalidades, trazendo inúmeras vantagens. No entanto, essa evolução também cria oportunidades para indivíduos mal-intencionados utilizarem tais recursos de forma ilícita, prejudicando cidadãos honestos ao ludibriar, roubar dados e dinheiro.

Compreender a importância desse assunto é vital para a legislação brasileira, uma vez que a globalização e o avanço tecnológico são elementos profundamente presentes tanto no ambiente profissional quanto no pessoal. Embora já existam legislações que abrangem e protegem contra crimes cometidos na internet, a fragilidade dessas leis não pode continuar diante do crescente número de casos que exigem uma resposta eficaz para sua classificação.

Portanto, é imperativo que a questão dos delitos virtuais seja destacada e abordada com urgência, levando em consideração os projetos de lei em trâmite. Esse é o caminho necessário para que tais propostas se tornem leis efetivamente sancionadas e divulgadas, proporcionando a proteção necessária para a sociedade como um todo. A atualização e o fortalecimento da legislação são essenciais para enfrentar os desafios impostos pelo avanço tecnológico e garantir a segurança no ambiente digital.

REFERÊNCIAS

ALVES, Fernando Antônio. **O Ativismo Popular nas Redes Sociais Pela Internet e o Marco Constitucional da Multidão, no Estado Democrático de Direito**. Revista Direita Emergentes da Sociedade Global, Santa Maria,2014.

ADMINISTRATIVO,Revista de Direito.**Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa**, Rio de Janeiro, 2004.

BARBOSA, Adriana Silva et al. **Relações Humanas e Privacidade na Internet: implicações Bioéticas.** Rev. Bioética y Derecho, Barcelona Disponível em: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872014000100008, Acesso em : 01 Mai 2024.

BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme.*Investigação **Digital em fontes abertas***. Rio de Janeiro: Brasport, 2017.

BARROSO, LUÍS ROBERTO. **Estado, Sociedade e Direito: Diagnósticos E Propostas para o Brasil**. In: XXII Conferência Nacional dos Advogados. Rio de Janeiro, 2014.

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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 15 Mai 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**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 Mai 2024.

BRASIL.Lei nº 8.069 de 13 de julho de 1990. Dispõe sobre o **Estatuto da Criança e Adolescente.**

BRASIL. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018- **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 Mar 2024.

BUSSOLA, Fernando. "**Lei Geral de Proteção de Dados Pessoais**: Comentários Artigo por Artigo", São Paulo: Revista dos Tribunais, 2019.

BAHIA. Tribunal Regional do Trabalho 5° região. **Direito titular dos dados**. https://www.trt5.jus.br/lgpd-direitos-titular-dados.Acesso em: 23 Fev 2024.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral.** Salvador: Juspodivm, 2014.

Câmara dos Deputados – **CPI dos Crimes Cibernéticos, de 04 de maio de 2016.** Disponível em: EL+4/2016+CPICIBER+%3D%3E+RCP+10/2015> Acesso em: 08 Mai 2024.

CAPEZ, Fernando Prado. **Código Penal Comentado.** São Paulo: Saraiva, 2016.

COMISSÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD) da União Europeia**.https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt. Acesso em: 20 Fev 2024.

CERT.COM. **Incidentes Reportados ao CERT.br Janeiro a Dezembro de 2016.** Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Acesso em: 01 Mai 2024

COELHO, Ivana Pereira; BRANCO, Sérgio. Humor e Ódio na Internet. **Cadernos Adenauer XV,** Rio de Janeiro, 2016. Disponível em: < http://www.kas.de/wf/doc/20595-1442-5-30.pdf>. Acesso em: 04 Mai 2024.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CLARKE, Richard A.; KNAKE, Robert K.**Guerra cibernética***:* a próxima ameaça à segurança e o que fazer a respeito.Rio de Janeiro: Brasport, 2015.

CASTELLS, Manuel. **A Galáxia Internet***:* reflexões sobre a Internet, negócios e a sociedade.Rio de Janeiro: Zahar, 2003.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**.São Paulo: Saraiva, 2016.

DECRETO-LEI nº 2.848 de 7 de dezembro de 1940**. Código Penal Brasileiro.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto- lei/Del2848compilado.htm>.Acesso em: 10 Mai 2024.

DONEDA Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais** São Paulo: Thomson Reuters, 2019.

DAMÁSIO. **Desafios da Implementação da LGPD** https://matriculas.damasio.com.br/blog/lgpd-quais-os-desafios-enfrentados-pelo-brasil-na-sua-aplicacao/. Acesso em: 15 Abr 2024.

E-GOV**, Crime virtual: crime contra o patrimônio no âmbito da internet, suas peculiaridades e controvérsias à luz do Código Penal de 1940.** Disponível em: https://egov.ufsc.br/portal/conteudo/crime-virtual-crime-contra-o-patrim%C3%B4nio-no-%C3%A2mbito-da-internet-suas-peculiaridades-e-controv. Acesso em: 29 Abr 2024.

ESPORTE, Globo.**Torcedor do Palmeiras reclama de homofobia nos estádios e é ofendido** em redes sociais. Disponível em: <https://globoesporte.globo.com/futebol/times/palmeiras/noticia/torcedor-do- palmeiras-

reclama-de-homofobia-nos-estadios-e-e-ofendido-em-redes-sociais.ghtml>. Acesso em: 03 Mai 2024

EUR-LEX. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito **ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados)** (Texto relevante para efeitos do EEE) Disponível em: https://**eur-lex.europa.eu**/eli/reg/2016/679/oj. Acesso em: 23 Fev 2024.

G1**,Globo.Deep Web – O que é e Como Funciona.** 2016. Disponível em:<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e- como-funciona-g1-explica.html>. Acesso em: 12 Mai 2024.

LISBOA, Roberto Senise. **Direito na Sociedade da Informação**, 2016. Disponível em:http://www.egov.ufsc.br/portal/conteudo/direito-na-sociedade-da-informa %C3%A7%C3%A3o. Acesso em: 20 de Fev 2024.

LÉVY, Pierre. **Cibercultura**. 1 ed. São Paulo: 34, 1999

MONTEIRO, Silvana Drumond. **O ciberespaço**: o termo, a definição e o conceito. DataGramaZero, Paraná, v.8, n.3. 2007. Disponível em: < http://www.dgz.org.br/jun07/Art_03.htm>.

TRIBUNAIS, Revista. **Estatuto da Criança e do Adolescente Comentado.** 3 ed. São Paulo, 2016.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital.** 2. ed. São Paulo: Saraiva, 2016

GLOBO.COM. **Maria Júlia Coutinho, a Maju, é vítima de comentários racistas no Facebook.** Disponível em: < http://g1.globo.com/pop-arte/noticia/2015/07/maria-julia-coutinho-maju-e-vitima-de-racismo-no-facebook.html> . Acesso em: 01 Mai 2024.

GARCIA, Lara Rocha *et al.* **Lei Geral de Proteção de Dados (LGPD***):* Guia de implantação. São Paulo: Editora Blucher, 2020.

GOV.BR,Princípios da LGPD. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd Acesso em: 10 Set 2023.

JAISHANKAR, Karuppannan. Establishing a Theory of Cyber Crimes. **International Journal of Cyber Criminology,** 2007.

JESUS, Damasio de Milagre, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

Manual de Direito Penal: Parte Especial. Salvador: Juspodivm, 2014.

MONTEIRO, César Macedo. **Crime Virtual: Os paradigmas apresentados a luz da lei 12.737/2012.** Disponível em: http://pt.slideshare.net/cmacedomonteiro/classificao-dos-crimes-de-informatica-ainda-sem-nota-de-rodap de 2014. Acesso em: 18 de nov. de 2023.

Miriam Wimmer, **Direitos, Democracia E Acesso Aos Meios De Comunição De Massa**: Um Estudo Comparado Sobre Pluralismo Interno Na Televisão,2014

NUCCI, Guilherme de Souza. **Manual do Direito Penal.** 7. ed. São Paulo: Revista dos Tribunais, 2011.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

REALE, Miguel. **Lições preliminares de direito**. 27. ed. São Paulo: Saraiva, 2002.

SILVA, Patrícia Santos da. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

SARMENTO, Daniel. **A Liberdade de Expressão e o Problema do *Hate Speech***. Disponível em: http://www.dsarmento.adv.br/content/3-publicacoes/19-a- liberdade-de-expressao-e-o-problema-do-hate-speech/a-liberdade-de-expressao-e-o-problema-do-hate-speech-daniel-sarmento.pdf. Acesso em: 01 Mai 2024.

STARLLINGS, Willliam. **Criptografia e Segurança de Redes**. - São Paulo: Prentice Hall, 2008.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira.** (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo,2017. Disponível em http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468. Acesso em: 29 Abr 2024

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz**. Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet.** Revista Cesumar Ciências Humanas e Sociais Aplicadas, 2016.

SYDOW,Spencer Toth**.Delitos informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2014.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 01 Mai 2024

Tribunal Regional Federal da 3ª Região. Escola de Magistrados **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017.

ODALIA, Nilo. **A Liberdade Como Meta Coletiva**. In: PINSKY, Jaime; PINSKY, Carla Bassanezi. História da Cidadania. São Paulo: Contexto, 2013.

TAVARES, José de Farias. **Comentários ao Estatuto da Criança e do Adolescente.** Rio de Janeiro: Forense, 2012.

TRENTIN, Taise Rabelo Dutra, **Internet: Publicações Ofensivas em Redes Sociais e o Direito à Indenização por Danos Morais.** Revista Direitos Emergentes da Sociedade Global, Santa Maria, 2012.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo**, São Paulo , 2016.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. **Liberdade de Expressão e Hate Speech na Sociedade da Informação. Revista Direitos Emergentes da Sociedade Global**, Santa Maria, 2015.

PINHEIRO, Patrícia Peck. **Regulamentação da Web**. Cadernos Adenauer XV, Rio de Janeiro,2014

WIGERFELT, Anders S.; WIGERFELT, Berit. DAHLSTRAND, Karl Johan. Online Hate **Crime – Social** Norms And The Legal System. Revista Quaestio Iuris. 2015.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira.**Crimes Cibernéticos** *(2a. ed):* Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.