UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

ANA LETÍCIA DE ANDRADE MARTINS

CONDUTAS ILÍCITAS NA INTERNET E PROTEÇÃO PENAL

São Luís
2024

ANA LETÍCIA DE ANDRADE MARTINS

CONDUTAS ILÍCITAS NA INTERNET E PROTEÇÃO PENAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Estadual do Maranhão, para o grau de Bacharel em Direito.

Orientador: Prof. Dr. Adriano Antunes Damasceno

São Luís
2024

FICHA CATALOGRÁFICA

ANA LETÍCIA DE ANDRADE MARTINS

CONDUTAS ILÍCITAS NA INTERNET E PROTEÇÃO PENAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Estadual do Maranhão, para o grau de Bacharel em Direito.

Aprovado em: ____ /____ / ____

BANCA EXAMINADORA

_____

Prof. Dr. Adriano Antunes Damasceno
Universidade Estadual do Maranhão

_____

Prof. Me. José Caldas Góis Junior
Universidade Estadual do Maranhão

_____

Prof. Me. Francisco Ferreira de Lima
Universidade Estadual do Maranhão

À Deus, meu porto seguro, ao meu marido, por todo cuidado e felicidade que proporciona ao meu coração, aos meus pais e irmão pelo apoio incondicional.

AGRADECIMENTOS

Gostaria de expressar minha mais profunda gratidão a Deus. Desde o momento em que compreendi a magnitude e a profundidade da Sua Graça, minha vida mudou irrevogavelmente. Sua Graça inundou o meu coração de maneira abundante e transformadora. Sem a Sua presença, minha existência não seria a mesma.

Agradeço ao meu marido Márvio. Obrigada por compartilhar a vida comigo. Por ter me escolhido como sua esposa. Por tornar os piores momentos da vida, os mais leves. Por nunca ter deixado (e nem mesmo me deixar) de ver bondade, honestidade e sinceridade nas pessoas. Obrigada por segurar minha mão, e me ajudar a chegar até aqui.

Aos meus pais, João Batista e Cristiane, por sempre prezarem por minha educação. Pelo apoio e amor incondicional. Por terem me mostrado na prática como o estudo e o trabalho mudam a vida das pessoas. Por sempre terem prezado pela minha educação. Pelas vezes em que cansada e desanimada, me disseram “filha, não desiste! Você vai conseguir”. E eu consegui. Agradeço ao meu irmão João Lucas pela amizade e compreensão. Por entender meus momentos de ausência - às vezes tudo que eu precisava era das palavras que você me dizia: "irmã, você consegue" e "vai dar tudo certo”.

Aos meus avós, Marilde, Marlene e Djalma por todo o carinho, conversas e ensinamentos. Ao meu avô Luiz (in memoriam), que esteve comigo no início dessa jornada, mas infelizmente não pôde estar no fim, minha gratidão: ele sempre me fez acreditar que eu sou capaz. E a toda a minha família — tanto a Andrade quanto a Martins, assim como a Oliveira e a Ribeiro que eu ganhei através do meu casamento —, agradeço profundamente pelo apoio e pela presença constante em minha vida.

Às minhas amigas de faculdade Angélica, Laura e Camila, por tornar a jornada universitária mais leve e enriquecedora. Aos meus amigos Jhefane, Géssica e Matheus por toda força que sempre deram em todos os momentos.

Meu reconhecimento se estende ao meu orientador, Adriano Antunes Damasceno, pela ajuda e dedicação ao longo destes meses. Sua disposição para ouvir, debater e compartilhar seu conhecimento foram fundamentais para mim.

Finalmente, expresso minha gratidão à Universidade Estadual do Maranhão, uma instituição essencial para minha formação acadêmica. Encontrei nas nossas salas um ambiente repleto de oportunidades. A todos que fazem parte da UEMA, meu sincero agradecimento por ter sido uma peça tão significativa na construção do meu futuro.

RESUMO

O trabalho tem como objetivo analisar as condutas ilícitas na internet e a eficácia das medidas de proteção penal existentes para combatê-las. Diante da crescente digitalização e da complexidade dos crimes cibernéticos, a pesquisa busca compreender a natureza das infrações cometidas no ambiente virtual e avaliar as respostas legais implementadas para a sua repressão. A metodologia adotada inclui uma revisão bibliográfica e uma análise crítica da legislação vigente. Os principais resultados revelam que, embora haja uma evolução significativa na legislação penal voltada para a internet, ainda existem lacunas e desafios na aplicação das normas e na adequação das leis às novas modalidades de delitos virtuais. A pesquisa evidencia que a tecnologia e a internet estão se desenvolvendo rapidamente, levando ao surgimento de novas formas de crimes. Em resposta, o Código Penal tem enfrentado dificuldades para acompanhar essas mudanças, por isso recorrer a medidas administrativas e cíveis para lidar com a problemática é uma opção, uma vez que outros marcos regulatórios têm se mostrado mais eficazes. Sendo assim, embora a legislação atual represente avanços, ainda é necessário aprimorá-la para assegurar uma proteção mais eficaz contra as ameaças cibernéticas.

Palavras-chave: condutas ilícitas; internet; proteção penal; crimes cibernéticos.

ABSTRACT

The aim of this study is to analyze illicit conduct on the internet and the effectiveness of existing criminal protection measures to combat it. Given the increasing digitalization and the complexity of cybercrimes, the research seeks to understand the nature of offenses committed in the virtual environment and evaluate the legal responses implemented to address them. The methodology employed includes a bibliographic review and a critical analysis of current legislation. The main findings reveal that, although there has been significant progress in criminal legislation related to the internet, there are still gaps and challenges in applying the norms and adapting the laws to new forms of virtual crimes. The research highlights that technology and the internet are rapidly evolving, leading to the emergence of new types of crimes. In response, the Penal Code has struggled to keep up with these changes, making it necessary to consider administrative and civil measures to address the issue, as other regulatory frameworks have proven to be more effective. Therefore, although the current legislation represents advancements, it still needs to be improved to ensure more effective protection against cyber threats.

Keywords: illicit conduct; internet; criminal protection; cybercrimes.

SUMÁRIO

1 INTRODUÇÃO

Os crimes digitais emergem como uma nova e complexa dimensão do direito penal no cenário contemporâneo. A revolução tecnológica e a crescente integração da internet nas atividades cotidianas têm exposto fragilidades nas legislações penais tradicionais, incluindo o Código Penal Brasileiro. Este código, que foi estabelecido há décadas, enfrenta desafios significativos para acompanhar a rápida evolução das tecnologias e das práticas criminosas associadas. Portanto, compreender sua adequação às novas formas de criminalidade digital é crucial para avaliar sua eficácia e propor possíveis melhorias.

O estudo dos crimes cibernéticos é particularmente relevante para o direito penal moderno devido ao impacto substancial dessas infrações na segurança, privacidade e economia. Com o crescimento das atividades online, novas modalidades de crimes surgem, muitas vezes não contempladas pelas legislações vigentes. Essa relevância é acentuada pela necessidade de atualizar e adaptar o Código Penal para proteger adequadamente os direitos e interesses dos indivíduos e instituições. Assim, a análise do tratamento dado aos crimes cibernéticos é vital para garantir uma resposta jurídica eficaz e atualizada.

Esta pesquisa tem como objetivo geral analisar a adequação e a eficácia das normas do Código Penal no enfrentamento dos crimes cibernéticos, identificando lacunas e propondo melhorias. Para atingir esse objetivo, serão examinadas as disposições aplicáveis aos crimes virtuais, identificados os principais tipos e características desses delitos, avaliada a prática judicial e a aplicação das normas existentes.

A pesquisa enfrentou o problema principal da dificuldade em identificar deficiências no que diz respeito à definição e punição dos crimes cibernéticos, dada a evolução rápida das tecnologias e a diversificação das práticas criminosas. Destacam-se a também a falta de clareza e especificidade em algumas disposições legais, o que dificulta a aplicação eficaz no contexto digital, e a necessidade de constante atualização das leis para acompanhar as novas formas de criminalidade.

A hipótese principal é que o Código Penal, em sua forma atual, apresenta lacunas que dificultam a abordagem e a solução eficaz dos crimes cibernéticos. Hipóteses secundárias incluem a possibilidade de que a aplicação das normas existentes seja limitada pela falta de especificidade e que uma legislação mais detalhada e atualizada poderia melhorar a resposta do sistema jurídico. Além disso, é possível que o Código Penal não consiga acompanhar a evolução das práticas criminosas digitais, tornando necessárias medidas cíveis e administrativas como

alternativas para enfrentar essas infrações. Para responder a problemática proposta, será empregada uma metodologia de análise descritivo-analítica, bem como argumentos baseados em um desenvolvimento pautado em pesquisas bibliográficas.

Essa abordagem possibilitou organizar o trabalho em três pontos. No primeiro capítulo procura-se entender como a sociedade tem reagido à ampla e acessível disseminação de dados, que está reformulando economias, interações sociais e culturais, e a forma na qual o emergir dessa "sociedade da informação" tem se comportado perante o Direito.

O segundo visa compreender como esses crimes, que surgem em um novo ambiente: o digital, tem interferido na população a nível global, bem como suas classificações e competências. Finalmente, o último capítulo busca avaliar a adequação das disposições do Código Penal Brasileiro frente às práticas e técnicas em constante evolução dos crimes cibernéticos, além de explorar possíveis medidas cíveis e administrativas para a resolução do problema.

2 A SOCIEDADE DA INFORMAÇÃO

O advento da Primeira Revolução Industrial, que teve início no século XVIII, introduziu a automação da produção e catalisou a transição de comunidades agrárias para economias urbanas e industriais. Assim, o mundo passou por uma marcante transformação no processo produtivo: o domínio global do sistema capitalista como modo predominante de organização. Nesse contexto, o mercado emergiu como a principal relação entre indivíduos e natureza, entre pessoas e entre nações.

Segundo Oliveira (2017), o avanço nas técnicas de produção, combinado com o progresso tecnológico, não afetou apenas os setores econômico e tecnológico, mas também teve um impacto significativo na esfera social. Esse desenvolvimento provocou uma migração em massa das áreas rurais para as urbanas, resultando em um crescimento populacional nas cidades, que ofereciam condições de vida bastante precárias para os mais desfavorecidos.

Da introdução da máquina a vapor e da mecanização na Primeira Revolução Industrial, até a automação e a ascensão das tecnologias da informação na Terceira Revolução Industrial, essas transições não apenas remodelaram profundamente as economias agrárias em economias industriais, mas também catalisaram mudanças culturais e políticas significativas.

Dathein (2003) menciona que a partir da segunda metade do século XIX, é possível afirmar que ocorreu uma Segunda Revolução Industrial. Diferente da Primeira Revolução, que se fundamentou na energia a vapor derivada do carvão e no ferro, a Segunda Revolução se baseou na eletricidade e no aço. Esse período trouxe avanços significativos nas áreas da química, das comunicações e no uso do petróleo. Inicialmente, essas novas inovações não substituíram completamente as anteriores, mas começaram a se destacar, com sua plena consolidação ocorrendo apenas no século XX.

Desde o início da Primeira Revolução Industrial, com a adoção da máquina a vapor e a mecanização da produção têxtil, à Segunda, marcada pelo surgimento de novas indústrias como a elétrica, química e de aço, até a Terceira Revolução Industrial, caracterizada pela automação e pela ascensão da tecnologia da informação, cada fase impulsionou sociedades agrárias em direção a economias industriais e, posteriormente, para economias baseadas em serviços e na disseminação de informações.

Desse modo, tais revoluções engendraram mudanças em todos os setores sociais, estilo de vida, hábitos e modo de relacionar, implicando com o decorrer do tempo na aplicação

direta dos meios de produção, seus produtos e serviços nas atividades cotidianas de toda uma sociedade.

Segundo Candau (2008) nos dias atuais, há uma crescente percepção de que estamos experimentando transformações profundas que ainda não conseguimos compreender completamente. Muitos intelectuais e agentes sociais não veem apenas um período de mudanças rápidas e significativas, mas sim uma transição de eras em curso.

A evolução da humanidade deu um grande passo com a transição da Revolução Industrial para a era da sociedade da informação. No século XX, especialmente com o avanço da Terceira Revolução Industrial, testemunhamos avanços rápidos em tecnologias de informação e comunicação (TICs), como dispositivos informáticos, que de acordo com Beserra (2020), podem ser qualquer equipamento capaz de armazenar dados, como computadores, tablets, celulares comuns, memórias externas, pendrives e smartphones. Esses dispositivos oferecem acesso ao mundo virtual, proporcionando entretenimento, conveniência e facilidades.

Essas inovações não só automatizaram operações industriais, mas também estabeleceram uma rede global para comunicação instantânea e troca de informações em uma escala sem precedentes. Assim, com base em Ottoboni (2021), é evidente que a sociedade moderna está passando por um processo de transformação, evolução e disrupção, caracterizado pela integração de tecnologias digitais, físicas e biológicas. Estamos vivenciando, de forma cada vez mais acelerada, uma era de informação e conhecimento, na qual tecnologias como inteligência artificial, robótica, diversos avanços em comunicação e informação, realidade aumentada, big data e internet das coisas, desempenham papeis centrais, provocando profundas mudanças na sociedade, bem como em esferas política e econômica.

A Revolução Industrial tinha como foco principal o avanço na produção de bens tangíveis ou materiais, enquanto à Revolução da Informação coube a missão de promover o desenvolvimento das tecnologias de produção através da acumulação de conhecimento e da democratização do seu acesso para todos. “A revolução informacional cuida, pois, do acesso aos bens intangíveis ou incorpóreos. E como, por meio deles, se torna possível o acesso aos bens tangíveis e corpóreos.” (Lisboa, 2006, p. 85).

A expressão "sociedade da informação" emergiu como um substituto para o conceito intrincado de "sociedade pós-industrial", buscando transmitir o conteúdo particular do "novo paradigma técnico-econômico". Sinônimo este que destaca a complexidade da expressão, indicando que as transformações ultrapassam simplesmente o uso de computadores ou da conectividade digital. Hoffmann (2009) em linhas gerais define informação como uma

mensagem contendo dados compreensíveis tanto para o emissor quanto para o receptor, podendo ser apresentada de forma audível ou visual. Na sociedade da informação, o progresso é baseado em ativos intangíveis, como dados, informações e conhecimento. Este conceito é abrangente e vai além da tecnologia, incluindo todas as formas de processamento e comunicação da informação, que adquirem valor econômico (Oliveira; Siqueira, 2007).

Como forma de defini-la, Castells (1999) menciona que o termo 'informacional' denota os atributos de uma forma específica de organização social, na qual a geração, processamento e transmissão de informações se transformam em fundamentais fontes de produtividade e poder, impulsionadas pelas novas condições tecnológicas emergentes neste período histórico. Essa mudança não apenas redefine as bases econômicas e sociais, mas também reconfigura as dinâmicas de poder e influência dentro da sociedade contemporânea.

Lisboa (2006) enfatiza que a ‘sociedade da informação’, também referida como ‘sociedade do conhecimento', representa um estágio histórico onde a primazia da informação sobre os meios de produção e distribuição de bens se torna evidente. Este período é caracterizado pela ampla adoção de tecnologias de comunicação, que facilitam a rápida disseminação e acesso a dados. Além disso, a utilização dessas informações, tanto pessoais quanto objetivas, desempenha um papel crucial na realização de transações comerciais, jurídicas e sociais, moldando profundamente as dinâmicas econômicas e sociais contemporâneas.

Gonçalves e Oliveira (2023) acrescentam que a sociedade da informação representa, entre outros aspectos, a entrada da sociedade em uma nova fase histórica de produção, onde a informação assume um papel fundamental em termos de riqueza e valores. Além de simplesmente confirmar a predominância das regras de mercado, redefine identidades e relações entre os usuários. A informação não é apenas um recurso adicional em um ambiente estável, mas um processo dinâmico com mudanças imprevisíveis em curso.

Ou seja, a era da sociedade da informação se destaca pela difusão generalizada e acessível de dados, que redefine economias, interações sociais e culturais, além de ser caracterizada pelo uso extensivo de dados, conhecimento e tecnologias de informação e comunicação no cotidiano dos indivíduos e da coletividade, em diversas áreas de atuação. A interligação global e a capacidade de processamento de informações têm facilitado a emergência de novos modelos de negócios, educação remota, cooperação internacional e transformações significativas no dia a dia das pessoas.

Bittar (2019) afirma que a ascensão da era digital apresenta novos obstáculos ao campo do Direito. Com o avanço tecnológico, o surgimento da inteligência artificial e a aceleração do ritmo de vida, estamos realmente adentrando em uma 'nova era' - a era da revolução digital, um estágio inédito no desenvolvimento do capitalismo e, consequentemente, do mundo contemporâneo. A expansão da informação somam-se aspectos como complexidade, globalização e interdependência, demandando uma análise mais aprofundada e abrangente de tal fenômeno.

A sociedade da informação está inserida em um cenário de globalização. A transnacionalização e a formação de novos blocos socioeconômicos, junto com a interdependência das esferas produtivas e financeiras, bem como os novos métodos de resolução de conflitos que surgiram desse novo contexto social, impactaram profundamente o pensamento jurídico estabelecido em torno de conceitos e princípios tradicionalmente associados à modernidade, como soberania, legalidade, direitos individuais, território, segurança e cidadania (Ottoboni, 2021).

Dessa forma, é possível observar que a sociedade da informação implica, entre outros aspectos, a transição da sociedade para um novo estágio histórico de produção, marcado por um conjunto de riquezas e valores, onde a informação desempenha um papel crucial. Mais do que apenas validar a primazia das regras de mercado, ela reestrutura identidades e relações entre os usuários.

2. 1 A sociedade da informação e o Direito

A transformação contemporânea na vida das pessoas é um fenômeno inegável, permeando amplamente todos os setores da sociedade atual. Sua importância é tamanha que é possível dispor que a digitalização da sociedade é uma realidade incontestável e irreversível. Não se trata mais de uma fantasia futurista ou de uma preocupação exagerada de alguns; é uma condição presente e atual. Devemos enfrentar essa realidade, que já faz parte do cotidiano de muitas pessoas. A interrupção de todas as redes de computadores atualmente causaria uma paralisia quase total do mundo. Os sistemas essenciais para o funcionamento da sociedade moderna, como os setores energético, de comunicações e financeiro, entre outros, estão fundamentados na tecnologia digital e não podem operar sem ela (Rodrigues, 2020).

Esta revolução digital, que teve um impacto significativo desde seu início, redefine de maneira marcante a maneira como as pessoas interagem coletivamente, remodelando os

fundamentos tradicionais e, até mesmo, o campo jurídico, uma vez que "[...] o direito não se resume ao fato social normativo, mas inclui também a dinâmica da sociedade, sendo que as normas e os princípios jurídicos tornam balizas jurídicas para resolver os casos concretos." (Siqueira Júnior, 2007, p. 167), requerendo uma adaptação contínua para lidar com as complexidades emergentes. Essas transformações e seus impactos constituem o novo campo de atuação do Direito.

Na era digital, o Direito enfrenta desafios significativos devido à rápida transformação das tecnologias. De acordo com Rodrigues (2020) o que está se observando através da internet e das novas tecnologias digitais, que continuam a se expandir no mundo moderno, é um aumento progressivo do controle disperso na sociedade - a instauração de um controle social imperceptível. A internet, como um centro de informações centralizado, possui a capacidade de exercer controle com alta eficácia. Esse controle é difuso, praticamente invisível e imperceptível, não gerando violência direta. A dominação que ela viabiliza é velada, o que a torna mais sutil e eficaz. Em certa medida, a internet pode ser vista como o panóptico contemporâneo.

A disseminação generalizada da informação promoveu profundas mudanças na sociedade, cujos impactos ainda não são completamente compreendidos. Essas mudanças não se restringiram apenas aos usuários de computadores, mas afetaram todos os aspectos da vida. Temáticas como a proteção de dados, regulação da propriedade intelectual, responsabilidade por conteúdos online, combate aos crimes cibernéticos e governança global da internet são assuntos que passam a ser discutidos com cada vez mais frequência, uma vez que:

A internet e os vários dispositivos eletrônicos, embora proporcionem um acesso sem precedentes à informação, também facilitam a concentração de dados e, consequentemente, se configuram como locais de poder. No entanto, esses meios por si só não seriam capazes de exercer esse poder. Junto a eles, há um componente simbólico de importância crucial: a tecnociência (união de tecnologia e ciência) como uma ideologia predominante na era contemporânea (Rodrigues, 2020).

Com isso, a adaptação jurídica é fundamental para assegurar direitos e garantir um ambiente digital seguro e justo, refletindo as mudanças profundas na sociedade contemporânea, uma vez que é inegável que a sociedade da informação promoveu mudanças profundas nas dinâmicas sociais, econômicas e de poder em um mundo globalizado, influenciando significativamente as concepções tradicionais do Direito.

A evolução da criminalidade digital não apenas resultou no surgimento de novos tipos de comportamentos ilegais, além dos já previstos na legislação brasileira, cometidos com o uso de computadores. Segundo Ramos (2017, p. 20): “outras particularidades foram trazidas com o advento da internet, já que as novas condutas atingem aos mais variados bens e interesses da sociedade tais como a violação de bens jurídicos até então não atingidos com a prática de um crime.”

Isso é um fato, trazendo como parâmetro que os direitos são fruto de uma construção da modernidade por meio de valores, processos e lutas que a mesma propõe, permitindo a uma pessoa afirmar sua condição como ser humano, uma vez que todos os ter reconhecidos. Assim, vale mencionar que a dignidade humana está em risco quando não são garantidas condições básicas para uma vida digna, quando não há controle sobre o poder e quando liberdade, autonomia, igualdade em direitos e dignidade, assim como direitos fundamentais, não são reconhecidos e assegurados. Nessas circunstâncias, não há espaço para a dignidade humana, e a pessoa pode ser reduzida a um objeto de arbitrariedade e injustiças (Sarlet, 2006).

Além disso, o compromisso com o respeito, a asseguração e a promoção da dignidade humana é um processo marcado por avanços e conquistas, porém também sujeito a retrocessos e desafios. Por isso, é fundamental que a questão da dignidade humana seja constantemente abordada em todos os aspectos da sociedade, seja como tema para reflexão e debate, seja como motivação para a prática do respeito aos direitos alheios (Pequeno, 2001).

Dessa maneira, considerando que a dignidade da pessoa humana deve ser respeitada, independente do período histórico a que se refira, parafraseando a autora Ottoboni (2021), o Direito, diante da sociedade da informação, requer uma abordagem renovada dos vários institutos jurídicos, levando seus praticantes a reconsiderar e revisar conceitos tradicionais, pois a necessidade agora é de se adaptar à nova realidade digital.

Lisboa (2006) acrescenta que a informática revolucionou o mundo, contudo, sua transformação não invalidou o que foi feito anteriormente: os sistemas de produção não apenas se mecanizaram, mas também se eletronizaram, utilizando programas de dados; a maioria dos contratos jurídicos são agora realizados através de processamento computacional, mesmo que não sejam formalizados virtualmente. Em outras palavras, a Sociedade da Informação melhorou as interações sociais, contribuindo para o avanço e facilitando o acesso à informação, inclusive para a celebração de atos jurídicos e negócios. Portanto, todas as áreas do direito devem ser reexaminadas à luz da Sociedade da Informação: Direito Civil, Direito Empresarial, Direito do

Consumidor, Direito Processual, Direito do Trabalho, Direito Tributário, Direito Administrativo, entre outros.

Rousseau (1985) já tratava em suas obras que todos os homens nascem livres e iguais, e Locke (1978), que todo homem naturalmente tem direito à igualdade. Desse modo, é válido destacar também os pensamentos de Bobbio (1982), que menciona que “o problema grave do nosso tempo, com relação aos direitos humanos, não é mais o de fundamentá-los e sim o de protegêlos”. Nesse sentido, torna-se essencial que o Direito e a era da informação caminhem juntos, tendo em vista que o aumento das plataformas e tecnologias de comunicação instantânea, traz consigo um risco de violações dos direitos individuais. Regulações apropriadas são necessárias para garantir transparência, veracidade das informações compartilhadas e proteção contra práticas abusivas.

3 CRIMES CIBERNÉTICOS

Como mencionado no capítulo anterior, a sociedade atual vem sofrendo diversas transformações em razão do avanço da tecnologia da informação. Couri (2009) enfatiza que as tecnologias virtuais constituem um avanço social de grande importância, pois são amplamente utilizadas em todos os países, sem distinção de estágio econômico, social ou cultural. Da mesma forma, pessoas de diferentes origens econômicas, culturais e sociais têm acesso aos produtos tecnológicos, evidenciando a presença generalizada da informática em todos os setores públicos e privados globalmente.

Segundo Colli (2009), embora a internet e essa nova era proporcionem um grande avanço e facilitem e promovam a comunicação entre pessoas, sua utilidade pode ser desviada para facilitar a prática e a coordenação de atividades criminosas. Entre essas, destacam-se os crimes digitais, conhecidos como cibercrimes. A emergência dessas práticas criminosas decorre do avanço contínuo da tecnologia e da disseminação da internet, que facilitaram o desenvolvimento de métodos e ferramentas para a realização de delitos virtuais.

O aumento de novas práticas ilegais realizadas por meio da internet, com o uso de computadores, é cada vez mais abrangente e segue o ritmo do desenvolvimento das novas realidades tecnológicas e sociais. Antes de conceituá-los é de suma importância observar o que dispõe no atual Código Penal brasileiro, que conceitua crime, conforme estabelecido pela Lei de Introdução ao Código Penal (Brasil, 1940), como toda violação penal que acarreta pena de reclusão ou detenção, seja de forma isolada, alternativa ou cumulativa com multa.

Malaquias (2012) menciona que embora não haja um consenso absoluto quanto à classificação dos crimes cibernéticos, geralmente são divididos entre aqueles em que a informática é utilizada como meio e outros tipos de conduta. Para essa categorização, é fundamental considerar não apenas as práticas já tipificadas na legislação, agora facilitadas pela tecnologia (onde o computador é utilizado como ferramenta para a prática do crime), mas também aquelas ações consideradas perigosas e ainda não penalizadas no Brasil, que afetam exclusivamente os sistemas informatizados.

Com isso, podemos observar que a expansão da criminalidade digital não apenas resultou no surgimento de novos comportamentos ilícitos, além dos já tipificados na legislação brasileira e executados com a ajuda de computadores. Outras características distintas surgiram com o avanço da internet, já que esses novos comportamentos afetam uma ampla gama de

interesses e bens jurídicos da sociedade, incluindo a violação de áreas anteriormente não contempladas pela legislação penal.

Os crimes cibernéticos são infrações cometidas através da tecnologia da informação e comunicação, utilizando computadores, redes digitais e sistemas informatizados. Roque (2005) define os crimes cibernéticos como qualquer ação, estabelecida por lei como delito, na qual o computador tenha sido empregado como meio para sua realização ou constitua seu alvo principal.

De acordo com Rosa (2002), a conduta que compromete o estado original dos dados e recursos oferecidos por um sistema de processamento pode ocorrer em várias formas, como na compilação, armazenamento ou transmissão desses dados. O chamado ‘crime de informática’ se refere a qualquer ato que afete a integridade dos dados, seja na forma em que estão armazenados, compilados ou transmitidos. Esse tipo de crime envolve dois elementos principais: a violação dos dados preparados para operações computacionais e a realização dessa violação utilizando software e hardware. Em termos gerais, os crimes de informática englobam ações típicas, ilícitas e passíveis de punição que ocorrem contra ou por meio do processamento automático e/ou eletrônico de dados ou sua transmissão. Assim, esses crimes envolvem o uso de sistemas de informática para atacar bens ou interesses juridicamente protegidos, abrangendo áreas como a ordem econômica, integridade física, liberdade individual, privacidade, honra, patrimônio público ou privado, e administração pública.

Ou seja, segundo a autora conceitua o crime cibernético como aquele que se refere a qualquer atividade que interfira com o fluxo normal de transferência de dados e recursos em um sistema de processamento de informações, incluindo a transmissão, armazenamento ou manipulação de dados, conforme definido pelos componentes do sistema de transmissão, armazenamento e processamento de informações.

A complexidade dos crimes cibernéticos se manifesta em diferentes níveis, desde ataques dirigidos a indivíduos para o roubo de informações pessoais e financeiras, até operações criminosas em larga escala que visam comprometer a infraestrutura crítica de nações inteiras. A interligação global e a onipresença da internet facilitam esses ataques, permitindo que os criminosos operem de forma virtual e transnacional, o que torna desafiadora a identificação e a responsabilização dos culpados. Assim, torna-se imprescindível discutir os mesmos, uma vez que sua caracterização se dá pelo uso da rede mundial de computadores, atingindo toda a população a nível global.

3.1 Classificação

Segundo Vianna (*apud* Rossini, 2004), os crimes virtuais podem ser categorizados em quatro grupos distintos: Crimes informáticos impróprios, nos quais o computador é utilizado como ferramenta para cometer o delito, mas sem violar diretamente a inviolabilidade dos dados. Crimes informáticos próprios, que visam diretamente proteger a inviolabilidade das informações armazenadas em sistemas automatizados. Crimes informáticos mistos, que são complexos e protegem não apenas a inviolabilidade dos dados, mas também outros interesses jurídicos relevantes. Estes são derivados do acesso não autorizado a sistemas computacionais e são considerados crimes "sui generis" devido à importância dos bens jurídicos tutelados. Crime informático mediato ou indireto, onde um crime não informático é cometido utilizando um crime informático como meio para sua realização.

Ou seja, é importante observar que os crimes cibernéticos podem ser próprios são aqueles que só podem ser cometidos no ambiente digital, onde tanto a execução quanto a consumação do crime ocorrem exclusivamente nesse meio. São tipos novos de crime em que o bem jurídico protegido é a informática. Por outro lado, os crimes cibernéticos impróprios estão tipificados no Código Penal, pois violam bens jurídicos comuns e podem afetar a dignidade da pessoa humana.

3.2 Tipos penais no meio cibernético

O meio virtual acaba proporcionando aos usuários uma sensação ilusória de liberdade absoluta, atraindo indivíduos que buscam ocultar sua identidade ao realizar atividades ou interações, com o intuito de resguardar sua privacidade, prevenir consequências adversas ou possibilitar a expressão de opiniões sem medo de retaliação ou julgamentos, o que acaba e proporcionando um ambiente sem “limites geográficos”, incentivando a prática de crimes.

Atualmente, muito se ouve falar sobre crimes cibernéticos como phishing e ransomware, por exemplo. O phishing envolve tentativas de enganar indivíduos para divulgar informações pessoais ou financeiras através de e-mails falsos, mensagens de texto ou sites fraudulentos, frequentemente imitando instituições legítimas. Já o ransomware é um tipo de malware que criptografa dados de computadores ou sistemas, exigindo pagamento de resgate para restaurar o acesso. Ataques reconhecidos pelo impacto severo que podem causar, incluindo grandes prejuízos financeiros e comprometimento da segurança de dados. Além disso, tais

crimes não impactam apenas pessoas e empresas, mas podem chegar a atingir governos e entidades públicas, causando danos que podem se tornar irreversíveis e ameaçar a segurança nacional.

O artigo 5º da Constituição Federal de 1988 garante a liberdade de expressão, porém proíbe o anonimato, exigindo que qualquer manifestação de pensamento seja identificável, de forma a responsabilizar seus autores pelos conteúdos expressos, dispondo que: "É livre a manifestação do pensamento, sendo vedado o anonimato." (Brasil, 1988) Como forma de tipificar alguns crimes virtuais, temos como exemplos:

Nos crimes que envolvem fraudes virtuais, o perpetrador realiza ações de invasão, alteração, modificação, pagamento ou exclusão de dados eletrônicos ou programas, ou outras formas de manipulação em sistemas de processamento de dados (Lima, 2005). Ou seja, os usuários são manipulados para divulgar seus dados financeiros ou pessoais. Atualmente, muitos desses criminosos utilizam plataformas de redes sociais para persuadir os usuários a fornecer informações pessoais. Além disso, é possível observar que tal crime não exige habilidades avançadas em informática e pode ser realizado por qualquer pessoa que tenha acesso a um computador.

Outro tipo penal que vem sendo cada vez mais comentado é o dano informático. Inicialmente, é válido observar que o Código Penal dispõe acerca do crime de dano: Destruir, inutilizar ou deteriorar coisa alheia (Brasil, 1940). Todavia, na época em que o artigo 163 do Código Penal foi elaborado, o legislador não contemplou o conceito de dano informático. Entretanto, o delito de dano relacionado a programas ou outros dados informáticos está descrito no artigo 4º da Lei nº 109/2009, de 15 de setembro, que prevê que aquele que, sem autorização legal ou sem estar devidamente autorizado pelo proprietário ou outro detentor dos direitos sobre o sistema ou parte dele, eliminar, modificar, destruir, total ou parcialmente, danificar, eliminar ou tornar inutilizáveis ou inacessíveis programas ou outros dados informáticos pertencentes a terceiros, ou de qualquer forma prejudicar sua capacidade de uso, está sujeito a uma pena de prisão de até 3 anos ou multa.

Nos dias atuais tem se falado muito sobre a ‘pornografia da vingança’. De acordo com Lucchesi e Hernandez (2008), a *‘Revenge Porn’* é um termo originado nos Estados Unidos, referindo-se à publicação na internet de imagens ou vídeos de nudez ou sexo sem consentimento da vítima, com o propósito de causar-lhe danos. Normalmente, tais vídeos ou imagens são divulgados por um ex-cônjuge ou ex-parceiro, o que pode causar danos significativos à vítima, expondo sua intimidade e trazendo graves impactos emocionais, psicológicos e sociais.

Com o aumento do uso da internet, indivíduos que já praticavam crimes, intensificaram suas atividades ilícitas. A pornografia infantil é um exemplo disso, que segundo Inellas (2004, p. 46), diferentemente da pedofilia, na qual existe uma distorção sexual caracterizada por sentimentos eróticos advindos de adultos para com crianças, na "pornografia infantil, não é preciso que haja contato sexual entre adultos e menores, mas sim a produção e comercialização de imagens eróticas ou pornográficas envolvendo crianças e adolescentes." O Estatuto da Criança e do Adolescente estabelece sanções para quem fotografa ou publica cena e sexo explícito ou pornográfica envolvendo criança ou adolescente (Brasil, 1990). Além disso, o Supremo Tribunal Federal sustenta que o crime se caracteriza pela simples divulgação, sem depender do meio utilizado, bastando meramente a publicação para que o crime esteja consumado.

O artigo 5º da Constituição Federal de 1988: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (Brasil, 1988). Todavia, consequentemente pela falsa sensação de anonimato proveniente das redes sociais, observa-se uma crescente ascensão de crimes contra a honra, por meio de publicações com conteúdos prejudiciais em redes sociais e aplicativos.

Desse modo, é preciso observar que mesmo quando ocorre através da internet, a calúnia, difamação e injúria possuem os mesmos critérios necessários, todos tutelados pelo Código Penal que prevê que o artigo 138 estabelece que, ao caluniar alguém ao atribuir-lhe falsamente um crime, a pena prevista é de detenção de seis meses a dois anos, além de multa. Já o artigo 139 define que difamar uma pessoa, imputando-lhe um fato que prejudique sua reputação, resulta em detenção de três meses a um ano e multa. Por sua vez, o artigo 140 dispõe que a injúria, caracterizada por ofender a dignidade ou o decoro de alguém, é punida com detenção de um a seis meses ou multa (Brasil, 1940).

Um dos crimes contra a honra mais cometidos nas redes sociais é o racismo, amparado pela Lei nº 7.716/89, em seu artigo 20, que proíbe a prática, indução ou incitação à discriminação ou preconceito baseado em raça, cor, etnia, religião ou origem nacional. Com isso, embora "toda pessoa tem direito à liberdade de opinião e expressão" (Organização das Nações Unidas, 1948), aqueles que as manifestam de maneira preconceituosa ou em conflito com a lei devem enfrentar as consequências de seus atos. Para mais, vale ressaltar que quando existe a prática de racismo pela internet ao mesmo tempo de um crime contra a honra poderá haver o aumento da pena.

Outro fenômeno em ascensão é o bullying virtual. De acordo com Lucchesi e Hernandez (2008, p. 6) “o cyberbullying trata da forma de agressão virtual, por meio de redes sociais, telefones celulares, entre outras mídias virtuais.” Essa modalidade criminosa pode causar impactos severos na saúde mental e no bem-estar das vítimas. Adolescentes são os principais alvos, decorrente de sua maior interação online e do contínuo desenvolvimento de habilidades sociais e emocionais.

Assim como a honra deve ser respeitada, a Carta Magna dispõe que a intimidade das pessoas deve ser reconhecida. Entretanto, a disseminação ampla de computadores, tornou tal direito ameaço. Segundo Silva (2000) antes da chegada dos computadores, a proteção legal das informações pessoais era bastante restrita. A introdução da informática e o avanço das tecnologias ampliaram significativamente o acesso a dados, gerando novas ameaças à privacidade.

O crime de estelionato é bastante conhecido no sistema legal brasileiro, e está previsto no artigo 171 do Código Penal: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento” (Brasil, 1940) Com o advento de ambientes virtuais, estelionatários se ajustaram de forma precisa, agindo de maneira a enganar vítimas com suas estratégias, e utilizando recursos digitais para alcançar seus objetivos, ou seja, o agente age para induzir ou manter a vítima em erro, visando assim obter vantagem ilícita, seja para si mesmo ou para terceiros, sendo considerado um crime que atenta contra o patrimônio, e em que não há violência ou grave ameaça.

Conforme Martins (2023), na internet, é comum que golpistas empreguem técnicas típicas, como enviar e-mails fraudulentos para usuários, com o objetivo de fazer com que a vítima acredite que, ao clicar no link presente na mensagem, será direcionada a um site confiável para atualizar suas informações pessoais. Dessa forma, o criminoso consegue acessar dados pessoais ou confidenciais da vítima. Frequentemente, essa prática visa a obtenção indevida de informações bancárias.

Nesse sentido, é possível observar que muitos dos crimes que ocorrem na internet têm equivalentes no mundo físico, porém, suas peculiaridades exigem uma adaptação cuidadosa das leis penais.

3.3 Competência

Surge uma problemática envolvendo a competência dos crimes virtuais, tendo em vista que determiná-la é um desafio considerável devido à sua natureza transnacional e à complexidade técnica envolvida. Esses crimes ocorrem de forma online, atravessando fronteiras geográficas e jurisdicionais, o que torna difícil estabelecer o local exato do crime e decidir onde os acusados devem ser julgados. Essa dificuldade é particularmente evidente em casos que envolvem múltiplos países, onde diferentes leis, procedimentos judiciais e interpretações de crimes podem complicar a cooperação internacional e a extradição de criminosos.

A interação entre sistemas legais de diferentes países, juntamente com a crescente globalização das relações comerciais e pessoais, cria uma série de dilemas que afetam diretamente a proteção dos direitos fundamentais das pessoas. Um dos principais desafios envolve o conflito de leis, ou seja, quando casos transnacionais surgem, determinar qual sistema legal deve prevalecer torna-se um problema. Isso pode levar a situações em que a aplicação dos direitos humanos é prejudicada devido a divergências entre as leis de diferentes países. Os direitos fundamentais de um indivíduo podem variar significativamente dependendo de onde uma disputa está sendo julgada. Outrossim, há conflitos ainda no reconhecimento de decisões estrangeiras, uma vez que, nem sempre há reciprocidade na aceitação de sentenças judiciais de um país para outro.

Vale ressaltar que os atos que configuram a infração diversas vezes ocorrem em locais distintos, o que torna mais complexa a definição da competência jurídica. Além disso, a constante evolução das tecnologias e das estratégias de cibercrime apresenta desafios adicionais, muitas vezes superando a capacidade das leis existentes de se manterem atualizadas e eficazes na aplicação da justiça.

Por isso, é importante observar que o Código de Processo Penal Brasileiro versa, em seu artigo 70, que a competência será geralmente determinada pelo local onde a infração for consumada, ou, no caso de tentativa, pelo local onde ocorreu o último ato de execução. Se a execução tiver início no território nacional e a infração se consumar fora dele, a competência será estabelecida pelo local onde o último ato de execução ocorreu no Brasil. Quando o último ato de execução ocorrer fora do território nacional, a competência será do juiz do local onde o crime, mesmo que parcialmente, produziu ou deveria produzir seu resultado. Em casos de incerteza quanto aos limites territoriais entre duas ou mais jurisdições, ou quando a infração for consumada ou tentada nas fronteiras de duas ou mais jurisdições, a competência será determinada pela prevenção (Brasil, 1940).

Além disso, a Lei 7.209 de 11 de julho de 1984, dispõe que o crime é considerado cometido no momento da conduta, mesmo que o resultado ocorra em momento posterior. A legislação brasileira é aplicável aos crimes cometidos em território nacional, respeitando as convenções, tratados e normas de direito internacional.

O Ministério Público Federal (2006) menciona que conforme estabelecido no artigo 109, inciso IV, da Constituição Brasileira, compete aos juízes federais o processo e julgamento de crimes que afetem bens, serviços ou interesses da União, suas autarquias e empresas públicas. Portanto, a Justiça Federal é responsável por julgar os crimes eletrônicos cometidos contra essas entidades da Administração Federal mencionadas no referido inciso. Exemplos incluem estelionato eletrônico, danos ou falsificação de dados presentes em sistemas informatizados mantidos por órgãos ou entidades da administração pública federal.

Assim, nos casos de crimes cometidos via internet, é crucial determinar o local onde ocorreu o delito. Se não for possível identificar esse local, a competência será atribuída ao juízo que iniciou as investigações. Em situações em que o crime virtual apresenta características transnacionais, a competência recairá sobre a Justiça Federal, bem como os crimes internacionais que tiveram início no Brasil, mas que se estenderam para o exterior. Diante disso, destaca-se a necessidade de cooperação internacional, harmonização de leis e regulamentos e esforços contínuos para proteger eficazmente os direitos humanos à medida que o mundo se torna cada vez mais interligado, a resolução dessas questões permanece um desafio crucial no campo do direito internacional.

4 LEGISLAÇÃO EM VIGOR

Uma das missões fundamentais do Código Penal é definir e regulamentar os crimes e as penas correspondentes, oferecendo uma estrutura legal essencial para a justiça. Segundo Vieira (2010), a proteção proporcionada pelo Direito Penal, através de suas sanções específicas, busca garantir a convivência harmoniosa na sociedade e controlar a criminalidade. Dentro do Estado Social e Democrático de Direito, a sanção penal deve ter propósitos preventivos. Estes propósitos incluem a prevenção geral positiva, a prevenção geral negativa e a prevenção especial positiva, todas devendo atuar de forma integrada.

Assim, estabelecendo o que constitui crime e as sanções aplicáveis, visa proteger os direitos individuais, garantir a ordem pública e promover a justiça social. Nesse sentido, o Código Penal deve assegurar uma resposta proporcional aos comportamentos criminosos, tanto realizados de forma física, quanto virtual.

4.1 Análise da adequação das disposições do código penal brasileiro à evolução dos crimes cibernéticos

Como anteriormente citado, o surgimento de novas tecnologias gerou comportamentos e práticas que ainda não eram previstos pela legislação existente. Com o surgimento dessas inovações, a invasão de computadores tornou-se uma ocorrência frequente, evidenciando a necessidade de uma abordagem legal específica. A criação de leis voltadas para a punição desses crimes, como a Lei nº 12.737, a Lei Carolina Dieckmann, surgiu para preencher essa lacuna, estabelecendo penalidades e diretrizes que anteriormente não estavam previstas, tendo como objetivo primordial a tipificação de crimes cibernéticos específicos no Código Penal Brasileiro, com a finalidade de suprir lacunas presentes na legislação anterior e estabelecer uma base jurídica para a punição de algumas condutas digitais prejudiciais.

A Lei Carolina Dieckmann veio com grande relevância no meio jurídico no que diz respeito à punição de crimes cibernéticos, e recebeu esse nome porque, durante o período em que o projeto estava em discussão na Câmara dos Deputados, a atriz brasileira Carolina Dieckmann se tornou vítima de um crime cibernético, com suas fotos pessoais sendo divulgadas sem sua permissão. De acordo com Martins (2017), em março de 2012, a atriz Carolina Dieckmann teve seu computador comprometido após ser enganada por uma fraude virtual ao

abrir um e-mail que parecia ser de uma fonte confiável. Imagens pessoais da atriz foram copiadas do seu dispositivo e, em seguida, ela começou a receber ameaças de extorsão.

Desse modo, diversos crimes semelhantes, que anteriormente versavam-se impunes, passaram a ser amparados pela nova lei. Casos como o da atriz, que frequentemente permaneciam impunes anteriormente, passaram a ser o principal alvo da Lei Carolina Dieckmann. A Lei 12.737/2012 fez uma modificação no Código Penal, adicionando os artigos 154-A e 154-B. Vale ressaltar que os crimes definidos por essa lei são direcionados aos ataques aos dispositivos informáticos da vítima, e não aos equipamentos do agressor.

No que tange aos dispositivos acrescentados, o artigo 154-A define que invadir um dispositivo informático de terceiros, seja ele conectado ou não à rede, por meio de quebra não autorizada de seus mecanismos de segurança, com o propósito de acessar, alterar ou destruir dados ou informações sem a permissão explícita ou implícita do proprietário do dispositivo, ou instalar vulnerabilidades para obter vantagens ilícitas, constitui crime. A pena para essa conduta é de detenção, variando de 3 (três) meses a 1 (um) ano, além de multa.

Além disso, o § 1º estabelece que a mesma penalidade se aplica àqueles que desenvolvem, oferecem, distribuem, vendem ou divulgam dispositivos ou programas de computador com a intenção de possibilitar a prática da infração descrita no caput. O § 2º prevê que a pena pode ser aumentada de um sexto a um terço se a invasão resultar em danos econômicos para a vítima.

O § 3º especifica que, se a invasão levar à obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais conforme definido por lei, ou ao controle remoto não autorizado do dispositivo invadido, a pena será de reclusão, variando de 6 (seis) meses a 2 (dois) anos, além de multa, desde que o ato não configure um crime mais grave. Por fim, o § 4º estipula que, se houver a divulgação, comercialização ou transmissão a terceiros dos dados ou informações obtidos conforme previsto no § 3º, a pena será aumentada de um a dois terços. O § 5º ainda estabelece que a pena para o crime de invasão de dispositivo informático será aumentada de um terço a metade se o delito for cometido contra determinadas autoridades de alta relevância.

O Art. 154-B estabelece que, para os crimes descritos no Art. 154-A, a ação penal somente se inicia mediante representação da vítima, exceto quando o crime é dirigido contra a administração pública, seja federal, estadual, municipal ou do Distrito Federal, ou contra empresas que prestam serviços públicos. Além disso, o Art. 3º modifica os artigos 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, que é o Código Penal, para incluir a

interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública na sua redação (Brasil, 2012).

Compreende-se que o objeto jurídico do crime está na inviolabilidade da intimidade e vida privada de outrem. O presente delito trata-se de um crime comum, uma vez que pode ser cometido por qualquer indivíduo, e não necessariamente por um "hacker". Assim, o sujeito ativo do crime poderá ser qualquer pessoa que realizar tal invasão. Além disso, não admitindo a modalidade culposa, trata-se de um crime doloso, tendo em vista que apenas é punível no momento em que o sujeito assume o risco de realizá-lo. À vista disso, o elemento subjetivo do delito será o dolo. Já o sujeito passivo será aquele que sofrer danos consequentes da invasão.

Greco (2015) acrescenta que é um crime comissivo, instantâneo e plurissubsistente - uma vez que devem ocorrer os atos dispostos no caput. A consumação se dará na invasão do dispositivo informático ou instalação de vulnerabilidades que o tornem sensíveis à violações. Já a tentativa é possível por consequência do caráter plurissubsistente do delito. Outrossim, com base no texto legal é importante observar que para que o delito descrito seja configurado, é necessário que haja uma violação inadequada de mecanismos de segurança do dispositivo. Se o equipamento em questão não contar com medidas de proteção como antivírus, firewall ou senha, ou se tais programas não estiverem ativos, não se pode considerar que houve uma invasão ou violação inadequada, características essenciais desse crime.

Por isso, a lei nº 12.737/2012 constitui um avanço notável na modernização do sistema jurídico brasileiro, entretanto mesmo sendo um marco importante para a legislação com relação aos crimes virtuais, apresenta lacunas significativas, tendo em vista que segundo Barbosa (2020), apesar de estabelecer punições específicas, essa lei foi alvo de críticas por especialistas por suas penas serem consideradas demasiado brandas.

Além disso, o autor menciona que um problema apontado por especialistas em direito digital é que, para que o crime seja configurado, o infrator deve superar alguma forma de proteção de segurança. Assim, se alguém acessa um computador que não está protegido por senha para roubar dados, essa pessoa não pode ser punida.

Desse modo, entende-se que é inegável a importância do Código Penal para o ordenamento jurídico brasileiro e sua organização. Entretanto, sabe-se que sua criação se deu no ano de 1940, e nesse período, não havia uma preocupação a abordar a complexibilidade dos crimes cibernéticos, presentes na atualidade, embora se possa afirmar que o mesmo pode ser aplicado a certos delitos digitais, como por exemplo: como falsidade ideológica e estelionato.

No entanto, para enfrentar efetivamente os desafios da era digital, é essencial recorrer a leis específicas.

Alguns problemas que anteriormente não estavam tão presentes passaram a causar cada vez mais impactos. Com relação à autoria dos crimes, por exemplo, há um grande desafio devido à tendência dos criminosos de se ocultarem atrás de dispositivos como computadores, tablets e celulares, e até mesmo utilizarem perfis falsos. Outro fator é que a falta de detalhes específicos nas leis pode acabar trazendo diversas interpretações, o que pode ocasionar decisões judiciais desiguais.

Com isso, é possível observar que o Código Penal encontra-se insuficiente para lidar com essas novas modalidades criminosas, sendo um grande desafio para o sistema judicial e para a proteção dos cidadãos. Sendo assim, muitas vezes o sistema judiciário precisa buscar alternativas em outras áreas da legislação e recorrer a vias administrativas e cíveis para resolver questões no ambiente digital. Como por exemplo, a Lei nº 12.965/2014, a Lei de Proteção de Dados e até mesmo o Código de Defesa do Consumidor e o Estatuto da Criança e do Adolescente são frequentemente utilizadas para lidar com aspectos específicos dos delitos virtuais, oferecendo uma abordagem adicional para a proteção de consumidores e jovens contra fraudes, abusos online e outros tipos criminosos.

Assim, a questão a ser colocada, portanto, é determinar se a legislação penal é capaz de acompanhar o surgimento de novas condutas associadas ao uso da internet, e se outros marcos regulatórios poderiam oferecer uma proteção mais eficaz do que o próprio Direito Penal.

4.2 O marco regulatório da internet

O Direito dentre seus princípios busca proteger os cidadãos contra abusos, assim como promover o bem-estar comum. Segundo Podestá (2001), um ponto notável ao longo da história das civilizações é que os seres humanos sempre enfrentaram ameaças à sua existência devido a fatores naturais e à sua vulnerabilidade perante a natureza. Essas circunstâncias evoluíram para situações que colocaram em risco a sobrevivência da espécie humana. Hoje, enfrentamos o avanço tecnológico acelerado, cujos resultados e impactos futuros são incertos e difíceis de prever. Todavia, é fato de maneira incontestável que a intimidade, a vida privada e a imagem das pessoas devem continuar sendo respeitadas, uma vez que se tratam de direitos constitucionalmente amparados.

De acordo com Tormen, (2018) o Marco Civil da Internet foi estabelecido com o objetivo de proteger os consumidores que utilizam a internet para adquirir produtos ou serviços, regulando o comércio eletrônico e promovendo a livre iniciativa e concorrência. Além disso, a legislação também abrange os serviços oferecidos pelas multinacionais provedoras de internet, garantindo funcionalidade e segurança aos usuários. A normativa visa regular as atividades realizadas na internet, definindo direitos e responsabilidades dos usuários, diante da importância crescente da rede como principal fonte de informação na contemporaneidade.

De acordo com Souza e Lemos (2016, p. 18), o Marco Civil da Internet inaugura um novo contexto em que a ideia de uma 'Internet livre' não se refere à ausência de regulamentações, mas sim à presença de leis que assegurem e protejam as liberdades proporcionadas pela tecnologia, especialmente pelo desenvolvimento da mesma.

Desse modo, infere-se que a Lei nº 12.965/2014, fundamenta-se primordialmente no respeito à liberdade de expressão. Além disso, reconhece a escala global da rede, protege os direitos humanos e fomenta o desenvolvimento da personalidade no contexto digital. Valoriza também a pluralidade e diversidade de ideias, promove a abertura e colaboração entre os usuários, e incentiva a livre iniciativa, a concorrência justa e a defesa dos direitos dos consumidores. Adicionalmente, busca alcançar a finalidade social da rede, visando seu uso para o benefício coletivo e o progresso da sociedade, conforme estipulado em seu artigo 2º (Brasil, 2014).

É relevante ressaltar que o artigo 3º traz os princípios norteadores da presente lei, entre esses princípios estão a comunicação e manifestação de pensamento conforme a Constituição Federal, a proteção dos dados pessoais conforme a legislação vigente, a preservação e garantia da neutralidade de rede, a manutenção da estabilidade, segurança e funcionalidade da rede através de medidas técnicas compatíveis com padrões internacionais e a promoção de boas práticas; a responsabilização dos agentes de acordo com suas atividades estabelecidas por lei, a preservação da natureza participativa da internet; e a liberdade dos modelos de negócios na internet, desde que não entrem em conflito com os demais princípios estabelecidos na mesma (Brasil, 2014).

Segundo Martins (2017), a Lei nº 12.965/2014 estabelece que os provedores não podem infringir o direito à intimidade e vida privada dos usuários, proibindo a monitoração dos dados transmitidos pela rede ou sua divulgação, exceto por ordem judicial. Para Ferraz Júnior (2012), a intimidade representa a esfera reservada exclusivamente para si mesmo, sem qualquer influência social, mesmo que seja vivida de forma isolada, ainda assim é uma forma de existir

entre os outros. Por outro lado, a vida privada engloba situações em que a comunicação é inevitável, como em relacionamentos nos quais as mensagens são trocadas entre as partes, excluindo-se terceiros em princípio. Nesse sentido, segundo o autor, assegurar o direito à vida privada por si só inclui a proteção da intimidade, uma vez que esta se encontra intrinsecamente abrangida por aquele direito.

Outro tema relevante tratado pela Lei do Marco Civil é a neutralidade da rede, que segundo Barreto Júnior e César (2007), foi originalmente proposto pelo professor Tim Wu, da Universidade de Columbia. O Chile foi o primeiro país a incorporar essa preocupação em sua legislação nacional, em 2010. Em seguida, em 2012, a Holanda tornou-se o segundo país a incluir na sua legislação a proibição de provedores e prestadores de serviços bloquearem ou reduzirem a velocidade de serviços ou aplicações na Internet. Como forma de defini-la, infere-se que esse princípio implica em tratamento equitativo para todos os usuários, impedindo que os provedores de internet interfiram no conteúdo que os indivíduos podem acessar. Os provedores não devem discriminar ou proibir determinados grupos de utilizar a rede de forma livre e aberta.

É possível observar que a Lei nº 12.965/2014 trouxe significativas melhorias na regulamentação do uso da internet no país. Entretanto, apesar disso e mesmo sendo relativamente recentemente implementada, é considerada controversa por muitos autores devido à necessidade de equilibrar a liberdade de expressão com a regulamentação da rede, especialmente em relação à neutralidade da rede. Além disso, são comuns debates sobre a eficácia das medidas de proteção de dados pessoais e privacidade. A aplicação das orientações também se depara com obstáculos devido ao rápido avanço tecnológico e novas formas de atuação digital.

4.3 Lei geral de proteção de dados

A Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados, visa, principalmente, resguardar os direitos fundamentais à liberdade e à privacidade, bem como promover o pleno desenvolvimento da personalidade dos indivíduos. Além de estabelecer um ambiente de segurança jurídica ao uniformizar regulamentos e práticas, garantindo a proteção dos dados pessoais de todos os cidadãos no Brasil, em conformidade com padrões internacionais.

Embora não seja voltada exclusivamente para crimes cibernéticos, a Lei Geral de Proteção de Dados veio com grande relevância no combate a essas condutas criminosas, tendo em vista que desempenha um papel fundamental ao definir diretrizes precisas para a proteção de dados e delinear as responsabilidades das organizações que lidam com essas informações. Segundo Finkelstein (2019), é essencial compreender que a legislação abrange a coleta, armazenamento e divulgação de dados, tanto no formato físico quanto eletrônico, e por isso tornou-se especialmente relevante devido à crescente facilidade com que dados são capturados e manipulados no ambiente digital.

Um exemplo disso são em situações de vazamento de dados, ataques de ransomware ou outros compromissos à segurança da informação, nos quais a Lei Geral de Proteção de Dados pode desempenhar um papel vital na determinação da responsabilidade das organizações envolvidas. Isso se dá uma vez que a lei estabelece que as empresas devem informar tanto os titulares dos dados quanto a Autoridade Nacional de Proteção de Dados sobre incidentes de segurança causadoras de riscos.

Ademais, a lei oferece diversas garantias aos cidadãos, incluindo o direito de solicitar a exclusão de seus dados pessoais, a possibilidade de revogar o consentimento dado anteriormente e a opção de transferir seus dados para outro prestador de serviços, entre outras prerrogativas. Vale ressaltar que o processamento das informações deve seguir critérios específicos, como a definição clara de propósito e a necessidade, que devem ser previamente acordados e comunicados ao titular dos dados (Brasil, 2018).

4.4 O Código de Defesa do Consumidor e o Estatuto da Criança e do Adolescente no combate aos crimes cibernéticos

No atual cenário contemporâneo, com a ascensão da sociedade digital, a proteção dos direitos dos consumidores e dos jovens no ambiente online deve ser visto com total prioridade. O Código de Defesa do Consumidor e o Estatuto da Criança e do Adolescente surgem como ferramentas fundamentais para enfrentar os desafios dos crimes cibernéticos e garantir a segurança e os direitos desses grupos. Este segmento explora a aplicação dessas leis para lidar com as complexidades da cibercriminalidade.

De acordo com Tormen (2018), devido à praticidade oferecida pela internet para a celebração de contratos, atualmente, muitos acordos são estabelecidos por esse meio, observando princípios fundamentais como publicidade, vinculação, veracidade e não

abusividade, entre outros. No entanto, diante da ausência de legislação específica no ordenamento jurídico brasileiro para crimes em contratos virtuais, o Código Civil e o Código do Consumidor procuram resolver esses conflitos utilizando o princípio da analogia.

A Constituição de 1988 estabeleceu que é dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, direitos como vida, saúde, alimentação, educação, lazer, profissionalização, cultura, dignidade, respeito, liberdade e convivência familiar e comunitária, além de protegê-los contra negligência, discriminação, exploração, violência, crueldade e opressão (Brasil, 1988). Em consonância, o Estatuto da Criança e do Adolescente, promulgado em 1990, estabelece a proteção integral a esse público, visando assegurar seus direitos de forma ampla e abrangente (Brasil, 1990).

A Lei 11.829, também conhecida como Lei da Pornografia Infantil, foi uma disposição de grande importância, tendo em vista que veio para fortalecer as medidas contra a produção, comercialização e disseminação de pornografia infantil, além de criminalizar a aquisição e a posse desse tipo de material e outras atividades associadas à pedofilia na internet.

Entretanto, o que se observa nos dias atuais é que crianças e adolescentes permanecem vulneráveis em ambientes virtuais, pois apesar da existência de normas específicas, como o Estatuto da Criança e do Adolescente, destinadas a proteger os jovens online, a rápida evolução tecnológica e o surgimento de novas formas de criminalidade frequentemente adaptam-se de forma mais rápida que as próprias leis. Além disso, a aplicação e a supervisão dessas leis enfrentam obstáculos, como a carência de recursos e a insuficiência de formação adequada para os profissionais responsáveis pela execução das normas.

5 CONCLUSÃO

A sociedade da informação, impulsionada pelo avanço tecnológico, está remodelando profundamente as interações sociais e profissionais, ao mesmo tempo em que dá origem a novos tipos de crimes, voltados ao ambiente virtual. A análise dos desafios legais na regulamentação dos crimes cibernéticos evidenciou que o Código Penal Brasileiro apresenta limitações consideráveis face às rápidas inovações tecnológicas. O estudo demonstrou que por diversas vezes há a necessidade de explorar alternativas em diferentes esferas legais e utilizar mecanismos administrativos e civis para lidar com desafios no contexto digital, que muitas vezes também deixam lacunas significativas.

Embora a tecnologia e a sociedade tenham evoluído consideravelmente, a legislação ainda se mantém defasada. Portanto, é imperativo revisar e atualizar as normas jurídicas para oferecer definições claras e pertinentes aos crimes cibernéticos. A relevância de outros marcos regulatórios no campo do direito, além do direito penal, não deve ser subestimada, especialmente ao abordar questões emergentes relacionadas ao uso da internet. Muitas vezes, essas normas e regulamentações alternativas demonstram ser mais eficazes do que o direito penal na proteção contra condutas ilícitas digitais. Assim, a análise das disposições legais demonstrou a urgência de atualizações para que o sistema jurídico possa enfrentar de maneira eficaz e adequada às infrações digitais.

É possível inferir que esse estudo proporciona contribuições significativas tanto no âmbito social quanto jurídico. Sob a perspectiva social, a pesquisa oferece uma análise crítica sobre como as deficiências na regulamentação impactam a proteção dos cidadãos contra crimes cibernéticos, sublinhando a urgência de uma legislação mais robusta e atualizada. No campo jurídico, os resultados fornecem uma base para debates sobre a necessidade de reformas no Código Penal e sugerem possíveis direções para o desenvolvimento de novas legislações que possam suprir as lacunas identificadas. O estudo também enfatiza a importância da integração entre as normas legais e as práticas tecnológicas emergentes, visando a criação de um ambiente digital mais seguro e protegido.

Entretanto, o estudo enfrentou desafios significativos, como a dificuldade em acessar dados atualizados e a complexidade de avaliar a eficácia das leis em um cenário em constante mudança. Além disso, o trabalho revelou a necessidade de um aprofundamento adicional sobre como diferentes jurisdições lidam com questões similares. Seria pertinente, inclusive, examinar a aplicação prática das propostas apresentadas, avaliando como as

mudanças sugeridas poderiam influenciar a aplicação da lei e a prevenção de infrações cibernéticas. A comparação com abordagens internacionais também oferece um campo para examinar soluções regulatórias bem-sucedidas em outros contextos, possibilitando a adoção de práticas inovadoras e adaptáveis.

Em resumo, a conclusão é que, embora a legislação vigente represente um avanço significativo, ainda requer aprimoramentos para acompanhar o ritmo acelerado das inovações tecnológicas e garantir uma proteção mais robusta contra as ameaças cibernéticas.

REFERÊNCIAS

ALBAGLI, S. Sociedade da informação e do conhecimento: desafios teóricos e empíricos. 2007. **Liinc em Revista**, Rio de Janeiro, v. 3, n. 1, p. 10-11, 2011. Disponível em: https://revista.ibict.br/liinc/article/view/3112. Acesso em: 22 maio 2024.

BARRETO JUNIOR, Irineu Francisco; CÉSAR, Daniel. Marco civil da internet e neutralidade da rede: aspectos jurídicos e tecnológicos. **Revista Eletrônica do Curso de Direito da Ufsm**, São Paulo, v. 12, n. 8, p. 65-88, semestral, 2017. Disponível em: www.ufsm.br/revistadireito. Acesso em: 7 jul. 2024.

BESERRA, Beatriz Cavalcante; SANTOS, Érika Rocsany Rodrigues dos; AMARAL, Mariana Moreno do. Invasão de dispositivos informáticos no ordenamento jurídico brasileiro. **Revista Eletrônica Interdisciplinar**, Barra dos Graças, v. 12, p. 302-305, 2020. Disponível em: http://revista.sear.com.br/rei/article/view/165/197. Acesso em: 2 jul. 2024.

BEZERRA, Arthur Coêlho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil. **Revista de Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura**, Florianópolis, v.16, 2014.

BITTAR, Eduardo C.B. A teoria do Direito, a era digital e o pós- humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do sujeito pós-humano de direito. **Revista de Direito Práxi**, Rio de Janeiro, v. 10, n. 2, p. 933-961, 2019. Disponível em: https://www.scielo.br/j/rdp/a/5MqNJXcvc9chdXnvPNZsjmk /?lang=pt&format=pdf. Acesso em 20 maio 2024.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Campus, 1992.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2024.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2024.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Brasília, DF: Senado Federal, 1990.

BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 1990.

CANDAU, Vera Maria. **Direitos humanos, educação e interculturalidade**: as tensões entre igualdade e diferença. 2008. 55 f. Tese (Doutorado em Direito e Educação) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008. Disponível em: https://www.scielo.br/j/rbedu/a/5szsvwMvGSVPkGnWc67BjtC/?format=pdf&lang=pt. Acesso em: 20 maio 2024.

CASTELLS, Manuel. **A sociedade em rede, a era da informação**: economia, sociedade e cultura. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999. Capítulo 2. v. 1.

COLLI, Maciel. **Cibercrimes**: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009. 162 f. Tese (Doutorado em Direito) - Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, 2009. Disponível em: https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2009/trabalhos_22009/GustavoFuscaldoCouri.pdf. Acesso em: 10 jul. 2024.

COURI, Gustavo Fuscaldo. **Crimes pela internet**. Rio de Janeiro, 2009. Disponível em: http://tinyurl. com/6khbmqx. Acesso em: 1 ago. 2024.

DATHEIN, Ricardo. Inovação e revoluções industriais: uma apresentação das mudanças tecnológicas determinantes nos séculos XVIII e XIX. **Decon Textos Didáticos**, Porto Alegre, fev. 2003. Disponível em: http://www.ufrgs.br/decon/. Acesso em: 20 maio 2024.

FERRAZ JÙNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Cadernos de Direito Tributário e Finanças Públicas**, São Paulo, v. 1, p. 32, out./dez. 2012.

FINKELSTEIN, Maria Eugenia. Privacidade: lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, Florianópolis, p. 284-301, maio 2019. Semestral. Disponível em: file:///C:/Users/marrv/Downloads/5343-17177-2-PB.pdf. Acesso em: 1 jun. 2024.

GONÇALVES, Andrey Felipe Lacerda. O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. **Revista de Direito Privado**, São Paulo, v. 14, n. 54, p. 49, 2013.

GRECO, Rogério. **Curso de direito penal**: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa. Niterói: Impetus, 2015.

HOBBES, Thomas. **O Leviatã ou matéria, forma e poder de um Estado eclesiástico e civil**. São Paulo: Nova Cultura, 1998.

HOFFMANN, W. A. M. **Gestão do conhecimento**: desafios de aprender. São Carlos: Compacta, 2009.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na internet**. São Paulo: Editora Juarez de Oliveira, 2004.

LÉVY, Pierre. **A inteligência coletiva**: por uma antropologia do ciberespaço. Tradução de Luiz Paulo Rouanet. São Paulo: Loyola, 2007. p. 64-77. Disponível em:

https://www.scielo.br/j/pci/a/qxsGdQ7r46rLdMsGyrYyqXw/?format=pdf&lang=pt. Acesso em: 22 maio 2024.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Editora Millennium, 2005.

LISBOA, Roberto Senise. **Direito na sociedade da informação**. São Paulo: Revista dos Tribunais, 2006.

LOCKE, John. **Segundo tratado sobre o governo civil**. São Paulo: Abril Cultural, 1978.

LUCCHESI, Ângela Tereza; HERNANDEZ, Erika Fernanda Tangerino. Crimes virtuais: ciberbullying, revenge porn, sextortion, estupro virtual. **Revista Officium: estudos de direito,** v.1, n.1, 2018.

MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova**: a investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 60.

OLIVEIRA, Rosane Machado de. Revolução industrial na Inglaterra: um novo cenário na idade moderna. **Revista Científica Multidisciplinar Núcleo do Conhecimento**, v. 1, n. 2, p. 89 – 116, out. 2017. Disponível em: https://https://www.nucleodoconhecimento.com.br/historia/revolucao-industrial-na-inglaterra. Acesso em: 22 maio 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 10 abr. 24.

OTTOBONI, Maria Fernanda Stocco. Direito e Estado sob a perspectiva da sociedade da informação: encontro virtual. **Revista de Movimentos Sociais e Conflitos**, v. 7, p. 83-99, jul. 2021. Semestral. Disponível em: file:///C:/Users/marrv/Downloads/7903-22571-1-PB%20(1).pdf. Acesso em: 20 maio 2024.

PEQUENO, Marconi. **Ética, direitos humanos e cidadania**. Curso de formação de educadores em direitos humanos. João Pessoa: Editora Universitária UFPB, 2001.

PODESTÁ, Fábio Henrique. Direito à intimidade em ambiente da internet. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). **Direito & internet**: aspectos jurídicos relevantes. Bauru: EDIPRO, 2001. p. 155.

RABENHORST, Eduardo. **Dignidade humana e moralidade democrática**. Brasília, DF: Brasília Jurídica, 2001.

RAMOS, André de Carvalho. Direito internacional privado. São Paulo, Saraiva: 2013. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624719/. Acesso em: 5 maio 2024.

REALE, Miguel. **Lições preliminares de direito**. 25. ed. São Paulo: Saraiva, 2001.

RODRIGUES, Horácio Wanderlei. Informática e sociedade: tópicos para reflexão. **Sequência**, Florianópolis, v. 18, p. 74-84, 1989. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/16268/14810. Acesso em: 22 maio 2024.

RODRIGUES, Horácio Wanderlei; BECHARA, Gabriela Natacha; GRUBBA, Leilane Serratine. Era digital e controle da informação. **Revista Em Tempo**, v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3268. Acesso em: 22 maio 2024.

RODRIGUES, Horácio Wanderlei; GRUBBA, Leilane Serratine. Informática, direitos humanos e sociedade: um caminho para a cidadania. **Revista Brasileira de Estudos Políticos**, v. 104, p. 207-228, jan. 2012. Semestral. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/P.0034-7191.2012v104p207. Acesso em: 25 maio 2024.

RODRIGUES JUNIOR, Álvaro. **Liberdade de expressão e liberdade de informação**: Limites e formas de controle. São Paulo: Juruá, 2009.

ROQUE, Sérgio Marcos. **Criminalidade informática**: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2007;000827582. Acesso em: 4 maio 2024.

ROSA, Fabrizio. **Crimes de informática**. Campinas, SP: Bookseller, 2002. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2006;000748363. Acesso em: 4 maio 2024.

SANTOS, Liara Ruff volta; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. **O cibercrime e o direito à segurança jurídica**: uma análise da legislação vigente no cenário brasileiro contemporâneo. 2020.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 4. ed. Porto Alegre: Livraria do Advogado Editora, 2006.

SIQUEIRA JUNIOR, Paulo Hamilton. Habeas data: remédio jurídico da sociedade da informação. *In*: PAESANI, Liliana Minardi (coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

TORMEN, Chalidan Adonai Callegari. **Crimes cibernéticos**: (im)possibilidades de coerção. 2018. 42 f. Tese (Doutorado em Direito) - Universidade Regional Integrada do Alto Uruguai e das Missões, Erechim, 2018. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4078.pdf. Acesso em: 5 abr. 2024.

VIEIRA, Vanderson Roberto. **As funções do direito penal e as finalidades da sanção criminal no estado social democrático de direito**. 2010. 10 f. Tese (Doutorado em Direito) - Unesp, São Paulo, 2010. Disponível em: http://institutoprocessus.com.br/2012/wp-content/uploads/2011/12/4_edicao1.pdf. Acesso em: 5 abr. 2024.