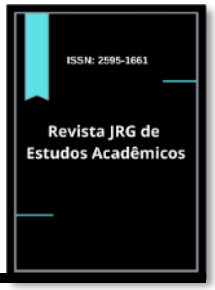
B1 ISSN: 2595-1661

ARTIGO DE REVISÃO

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg



Crimes cibernéticos e os desafios jurídicos na era digital: análise legislativa, doutrinária e jurisprudencial

Cybercrimes and legal challenges in the digital era: a legislative, doctrinal, and jurisprudential analysis

DOI: 10.55892/jrg.v7i15.1662
ARK: 57118/JRG.v7i15.1662

Recebido: 22/11/2024 | Aceito: 28/11/2024 | Publicado *on-line*: 30/11/2024

Carlos Muryllo Rodrigues de Sousa[1]
https://orcid.org/0009-0006-8932-6040
http://lattes.cnpq.br/0895678945350810
Faculdade Serra do Carmo (FASEC), TO, Brasil
E-mail: carmuryllo2010@gmail.com

Guilherme Augusto Martins Santos[2]
https://orcid.org/0000-0002-4714-7558
http://lattes.cnpq.br/5881131138349838
Faculdade Serra do Carmo (FASEC), TO, Brasil
E-mail: guilhermeaugsan@gmail.com

Resumo

Este trabalho analisa os crimes cibernéticos à luz dos avanços legislativos, doutrinários e jurisprudenciais. Discute-se o impacto das inovações tecnológicas no Direito, abordando o surgimento do Direito Eletrônico e a regulamentação do ambiente digital. São apresentados os tipos de crimes cibernéticos, bem como as dificuldades na identificação da autoria e na aplicação da justiça. A pesquisa destaca marcos legais como a Lei nº 12.737/12 e a importância de teorias que sustentam a regulamentação digital, enfatizando a necessidade contínua de adaptações legislativas para acompanhar a evolução tecnológica.

Palavras-chave: Crimes cibernéticos, Direito Eletrônico, Legislação, Tecnologia, Justiça digital.

Abstract

This paper examines cybercrimes in light of legislative, doctrinal, and jurisprudential advancements. It discusses the impact of technological innovations on Law, addressing the emergence of Electronic Law and the regulation of the digital environment. Different types of cybercrimes, challenges in identifying perpetrators, and the application of justice are explored. The research highlights legal milestones such as Law No. 12.737/12 and emphasizes the importance of theories supporting digital regulation, stressing the ongoing need for legislative adaptations to keep pace with technological evolution.

[1] Graduando(a) em Direito pela Faculdade Serra do Carmo (FASEC).
[2] Mestre em Direito pelo Centro Universitário de Brasília. Professor de Direito da Faculdade Serra do Carmo (FASEC). Advogado.

Keywords: *Cybercrimes, Electronic Law, Legislation, Technology, Digital Justice.*

1. Introdução

A era digital transformou a sociedade de forma irreversível, impactando desde relações interpessoais até a dinâmica econômica e jurídica. Com o avanço da tecnologia, surgiram novos desafios para o Direito, principalmente no tocante à proteção de dados e à repressão dos chamados crimes cibernéticos. Esses crimes, que incluem desde invasões de sistemas até fraudes digitais, demandam respostas jurídicas eficazes e atualizadas. Este trabalho propõe uma análise aprofundada sobre o desenvolvimento do Direito Eletrônico, sua regulamentação no Brasil e no mundo, e a tipificação dos crimes virtuais. Destaca-se a evolução legislativa, especialmente com a Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, que trouxe avanços no combate a delitos cibernéticos. Além disso, são discutidas as teorias que fundamentam a regulamentação do ambiente digital e os desafios enfrentados pelo Poder Judiciário na aplicação da justiça em um contexto de rápidas mudanças tecnológicas.

2. Metodologia

A metodologia adotada neste trabalho é de natureza qualitativa e exploratória, com o objetivo de analisar os crimes cibernéticos no contexto brasileiro, à luz dos avanços legislativos, doutrinários e jurisprudenciais. A pesquisa foi desenvolvida, principalmente, por meio de uma revisão bibliográfica e documental, abordando obras teóricas e artigos acadêmicos que discutem o Direito Eletrônico, bem como a evolução do ordenamento jurídico no combate aos delitos digitais.

Foram utilizados autores como Pimentel, Paesani e Pinheiro, que fornecem uma base teórica sólida sobre o Direito Digital e suas implicações legais. Além disso, a análise legislativa focou em marcos legais relevantes, como a Lei nº 12.737/12 (Lei Carolina Dieckmann), o Marco Civil da Internet e a Lei nº 9.609/98, que regula a propriedade intelectual de softwares. Esses dispositivos foram essenciais para a compreensão da tipificação dos crimes cibernéticos e das medidas punitivas aplicáveis.

Outro aspecto central da metodologia foi a análise das teorias que sustentam a regulamentação do ambiente virtual. Foram discutidas a teoria libertária, a teoria da arquitetura de rede, a teoria internacional e a teoria tradicionalista, permitindo uma reflexão crítica sobre suas contribuições e limitações para a regulação dos crimes no ciberespaço. Essa abordagem teórica possibilitou uma visão ampla das diferentes correntes que orientam o Direito Digital no contexto global e nacional.

A pesquisa também contemplou o estudo da tipificação dos crimes cibernéticos, classificando-os como próprios e impróprios, e analisou os desafios enfrentados pelo Poder Judiciário na identificação da autoria e na coleta de provas digitais. Para isso, foram examinados casos emblemáticos e julgados que ilustram a aplicação prática das normas, bem como as dificuldades encontradas na persecução penal de crimes virtuais.

Por fim, as fontes foram selecionadas com base em sua relevância acadêmica e jurídica, abrangendo livros, artigos científicos e documentos legais atualizados. Apesar do enfoque qualitativo, a ausência de dados empíricos sobre a incidência dos crimes cibernéticos pode ser considerada uma limitação, restringindo a análise quantitativa do tema. Contudo, a abordagem adotada permitiu uma reflexão crítica e detalhada sobre a evolução legislativa e os desafios enfrentados no combate aos crimes cibernéticos no Brasil.

3. A história do direito eletrônico no brasil e no mundo

A história do Direito Eletrônico está intimamente ligada aos avanços cibernéticos da era digital. Nas últimas duas décadas, o mundo presenciou uma formidável revolução tecnológica, impulsionada principalmente pela difusão da informática em todos os setores da sociedade.

Nos dizeres de Pimentel (2000, p. 152), o Direito Eletrônico experimentou expressivas transformações sociais, econômicas, políticas e culturais, tanto no plano nacional quanto no internacional, especialmente em países mais desenvolvidos. Diante dessas prerrogativas, é fundamental estabelecer uma relação abrangente com o tema. Assim, o Direito Eletrônico pode ser definido como o ramo jurídico que estuda o conjunto de normas, aplicações, processos, relações jurídicas, doutrinas e jurisprudências decorrentes da utilização e desenvolvimento da informática, direcionado à consecução de objetivos específicos.

Segundo Paesani (2010, p. 2), a revolução na área da informática, ocorrida nos últimos 20 anos, geralmente é discutida como um fenômeno isolado. No entanto, ela está promovendo mudanças significativas na ordem econômica mundial, especialmente no estabelecimento de uma nova divisão internacional do trabalho.

No percurso histórico do Direito Eletrônico, destaca-se sua rápida difusão global e o surgimento de amplas perspectivas no mercado de trabalho. Entretanto, essa expansão também trouxe desafios, como o aumento dos chamados crimes virtuais ou cibernéticos. É importante pontuar que, no Brasil, a preocupação com o domínio da tecnologia e a promoção da indústria nacional de eletrônica digital começou no início da década de 1970, conforme afirma Paesani (2010, p. 3).

Com o advento da década de 1990, observou-se um substancial aumento dos investimentos em tecnologia nos países industrializados. No Brasil, contudo, algumas dificuldades impediram o acompanhamento desses avanços, entre elas *"as indefinições contidas nas inúmeras políticas tecnológicas e industriais, fixadas pelo governo, inibiram qualquer ação do setor privado, inclusive pela ausência de legislação adequada e internacionalmente aceita."* (Paesani, 2010, p. 3).

Assim, com base na autora mencionada, observa-se que as conquistas no âmbito virtual não ocorreram de forma imediata. Posteriormente, houve intervenções do governo brasileiro que impactaram principalmente o setor privado, impedindo o acesso imediato aos avanços tecnológicos.

A história do Direito Eletrônico passou por grandes transformações até que, finalmente, o ser humano conseguisse avançar significativamente no campo da informática. Entre as implicações que ajudam a compreender o contexto histórico do Direito Eletrônico, é pertinente destacar que:

> Depois do advento do ábaco (desde o século III a.C.) pouco ou quase nada de significativo foi desenvolvido na área de processamento de dados. Foi necessário dar um salto de quase 20 séculos para chegar em estudos e trabalhos que serviram de base para as mais recentes pesquisas em computação. (Paesani, 2010, p. 5).

Do que se depreende da citação anterior, observa-se que a autora é enfática ao afirmar que foi necessário o transcorrer de muitos séculos desde o advento do ábaco até que o ser humano finalmente se apropriou de conhecimentos eletrônicos, os quais, até então, não eram tão sofisticados quanto os atuais.

Dessa forma, conforme Paesani (2010, p. 4), historicamente, o jusfilósofo Mario G. Losano, em sua obra Lições de Informática Jurídica, ensinou que os

computadores eletrônicos foram inicialmente utilizados pelas indústrias norte-americanas, com a criação de normas conhecidas como legislação antitruste (destinada a punir práticas anticompetitivas que utilizam o poder de mercado para restringir a produção, aumentar os preços e impedir a atração de novos competidores ou eliminar a concorrência), também chamada de legislação antimonopólio.

No que se refere à cronologia do surgimento da era eletrônica, observa-se que:

> O moderno computador eletrônico é o resultado de inúmeras tentativas que o homem vem realizando através dos séculos para ajudá-lo no trabalho de processamento de dados. Entretanto, essa máquina, cada vez mais aprimorada pelo homem, apresenta-se como “uma faca de dois gumes”, pois à medida que crescem sua sofisticação e utilidade, cresce paralelamente a dependência com relação a esse instrumento. (Paesani, 2010, p. 4).

Em consonância com o que dispõe a autora citada, o computador eletrônico é uma ferramenta importante que auxilia o ser humano em seu trabalho e em outras atribuições. No entanto, ele oferece um "perigo" por revelar uma outra faceta, ou seja, a dependência que o uso excessivo pode causar. Esse fator, porém, não diminui seu mérito de ser um ótimo aliado no cotidiano, seja no âmbito de trabalho, em pesquisas, no entretenimento, ou em outras áreas.

Paulatinamente, ao abordar o contexto do Direito Eletrônico e a história do surgimento da era digital, o objetivo é construir, a partir desses dispositivos, uma correlação entre o Direito Eletrônico e os crimes cibernéticos. Nesse sentido, é relevante discutir como surgiram termos como "internet", "documento digital", entre outros.

Assim, no que tange aos avanços observados desde a criação da era digital e sua expansão na sociedade, é pertinente abordar o seguinte:

> No mundo atual, mais e mais se utilizam a Internet e os computadores para transmissão e armazenamento de informações, desde os mais banais, até segredos de relevo e significado pessoal, profissional, fiscal ou empresarial, enquanto, por outro lado, a fragilidade da rede pode tornar vulneráveis todas essas informações, permitindo o acesso por intrusos, alguns mais mal-intencionados do que outros. (Marcacini, 2002, p. 180).

Nos dizeres do autor citado, observa-se que, na conjuntura da vida em sociedade pós-moderna, o uso de computadores e o acesso à internet tornaram-se cada vez mais necessários para as relações pessoais e interpessoais em diferentes partes do mundo. Esses recursos são essenciais, seja para tratar de informações de caráter restrito, seja por sua função como ferramentas indispensáveis para o convívio social contemporâneo. Contudo, no caso de acesso desenfreado, podem surgir os chamados crimes virtuais, que representam um ponto central para o tema abordado neste estudo.

3.1 Direito informático

Para que o Direito Eletrônico seja compreendido em suas acepções e teorias, é necessário, também, compreender alguns aspectos do que constitui o Direito Informático. Portanto, a expressão recai sobre o conceito de que *“é uma disciplina já reconhecida em nações mais desenvolvidas, possuindo todas as características de um direito especializado e ao mesmo tempo interdisciplinares e universal.”* (Pimentel, 2000, p.153).

No que tange à citação acima, Pimentel (2000) afirma que o Direito Informático assume características próprias, fundamentais para os avanços na era da informática. Assim, conforme o autor citado, o Direito Informático é mais reconhecido nas nações mais desenvolvidas.

Nos dizeres de Pimentel (2000, p. 154), o Direito Informático é especializado (seu objeto recai sobre a tecnologia informática, abrangendo o tratamento da informação e da comunicação), interdisciplinar (implicando uma grande complexidade) e universal (pois o Direito transfere informações, ultrapassando as fronteiras de um determinado Estado). Portanto, essas três características do Direito Informático explicam parte de sua evolução na era digital atual.

Outro fator relacionado ao Direito Informático é sua instrumentalidade, que pode auxiliar os demais ramos do Direito em sua aplicação, pois ela *"tem como objetivo efetivação da aplicação da justiça empregando-lhes a nota da celeridade associada à necessária segurança que a concretização do direito exige."* (PIMENTEL, 2000, p. 153).

Dessa forma, o Direito Informático desempenha um papel fundamental nos avanços tecnológicos dentro do campo jurídico, pois facilita a celeridade na aplicação de determinados direitos. O uso do Direito Informático, para fins de interesse judiciário, abrange a regulamentação das novas tecnologias da informação e comunicação, com ênfase na informática e na telemática, conforme descrito por Pimentel (2000), que observa que este campo é inequivocamente jurídico, delimitado pelo setor normativo dos sistemas jurídicos contemporâneos e orientado por um conjunto de regras voltadas para a regulamentação dessas tecnologias.

O Direito Informático se estende aos mais variados setores da sociedade, sendo especialmente relevante no contexto dos sistemas jurídicos, onde busca integrar a informação e comunicação, assegurando que as novas tecnologias estejam profundamente conectadas ao Direito Eletrônico e, posteriormente, ao próprio Direito Informático.

Um dos aspectos essenciais nesse contexto é o direito à informação e comunicação, mediado pelos meios tecnológicos. Dessa forma, surge a necessidade de compreender como a internet se originou, pois é somente a partir desse entendimento que as interconexões entre internet e informática podem ser interpretadas na medida exigida para a proposição de crimes virtuais.

3.2 Noções de internet

A internet é, atualmente, alvo de intensas pesquisas e acessos em todo o mundo, e seu percurso histórico é marcado por eventos iniciados em meados da década de 1960, quando o governo americano iniciou o projeto denominado "Arpanet" (Agência de Pesquisa Avançada e Rede), criado para internalizar as comunicações. Em decorrência das guerras da época, esse projeto se tornou um marco importante no avanço da informática e do Direito Digital, conforme afirma Carneiro (2012, p. 1).

Carneiro (2012, p. 10) também destaca que, em 1973, houve uma evolução significativa da internet, consolidando-se entre um número reduzido de usuários, com a criação do Protocolo de Controle de Transmissão *(TCP/IP – Transmission Control Protocol/Internet Protocol).* Este código possibilitou a interconexão de sistemas e programas incompatíveis, permitindo a comunicação virtual entre eles.

De acordo com Carneiro (2012, p. 1), foi em 1985, nos Estados Unidos, que o projeto *Arpanet* foi substituído pelo termo *NSFnet.* Um ano depois, esse projeto deu origem ao que hoje conhecemos como a internet. É importante frisar que o uso

comercial da internet foi liberado apenas em 1987, após a fusão dos termos *Arpanet e NSFnet.*

Conforme observado no contexto histórico do Direito Eletrônico, o grande impulso da internet ocorreu na década de 1990, o que evidenciou sua importância sob a seguinte ótica de que *"a internet se tornou uma ferramenta indispensável no cotidiano social, surgindo assim um novo ambiente que mereceu regulação como outros grandes meios de comunicação."* (Carneiro, 2012, p.1).

Conforme retratado por Carneiro (2012), a internet passou a ser considerada fundamental para o cotidiano social, uma vez que possibilitou avanços tecnológicos significativos, utilizados em diversas partes do mundo.

Em outras palavras, a internet surgiu a partir da necessidade humana de aprimorar constantemente os meios de comunicação. Assim, nos dias contemporâneos, a internet configura-se como uma das ferramentas indispensáveis para seus usuários, que, de maneira ampla, garantem seus direitos no que tange ao uso das novas tecnologias.

Por outro lado, a revolução tecnológica, que tem se desenvolvido nos últimos anos, tem sido um fator crucial na construção dessa nova era, e *"por meio da internet é possível navegar por uma imensidão de costumes e contextos culturais. Isso pode aproximar pessoas e/ou grupos que estejam em polos opostos do globo, como também pode acirrar diferenças. (...)"* (Guerra, 2012, p. 132).

Em consonância com o que pontua o autor acima referido, a internet atende a uma vasta gama de usuários ao redor do mundo e se expande à medida que possibilita uma aproximação virtual entre as pessoas. No entanto, assim como pode ser utilizada para fins positivos, também incide sobre ela o mau uso, ou seja, quando a internet é empregada para a prática de crimes.

Dessa forma, é relevante que sejam examinadas as noções de crimes eletrônicos, a fim de estabelecer uma relação entre tais crimes e os avanços observados nas esferas legislativa, judiciária e jurisdicional.

3.3 Noções de crimes eletrônicos

Ao delimitar os crimes eletrônicos, é necessário compreender o significado da palavra "crime" em seu sentido amplo. Assim, o termo "crime" refere-se a qualquer violação grave da lei, seja ela moral, civil ou religiosa, incluindo atos ilícitos, contravenções, entre outras designações.

No que diz respeito às especificidades dos crimes, estes podem ser de natureza dolosa, culposa, comum, entre outras. Para o estudo em questão, é relevante entender as noções de crimes eletrônicos, e, para tanto, convém citar que:

> O crime eletrônico, é, em princípio, um crime de meio, utiliza-se de um meio virtual. Não é um crime de meio de fim, por natureza, ou seja, o crime cuja modalidade só ocorre em ambiente virtual, à exceção dos crimes cometidos por hackers (pessoas que conseguem invadir sistemas de empresas e outros sistemas conectados à rede), que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. (Pinheiro, 2013, p. 307).

Com base nas disposições da autora mencionada, observa-se que os crimes eletrônicos são caracterizados como crimes do meio, ou seja, aqueles que estão diretamente relacionados ao ambiente virtual. Nesse sentido, o acesso indevido à rede poderá resultar na tipificação do crime, que será enquadrado conforme o que estabelece a lei.

Nos dizeres de Pinheiro (2013, p. 310), os crimes eletrônicos ou cibernéticos apresentam modalidades distintas, dependendo do bem jurídico tutelado. Assim, o crime de intercepção telefônica e de dados se enquadram nessa categoria, uma vez que ambos protegem como bem jurídico os dados.

Por outro lado, os crimes eletrônicos enfrentam um problema ainda mais complexo: a escassez de denúncias e, pior, o despreparo da polícia investigativa e da perícia para apurá-las. Nesse contexto, o combate a esse tipo de crime torna-se extremamente difícil por dois motivos principais, que são:

> a) falta de conhecimento do usuário, que, dessa forma, não passa as autoridades informações relevantes e precisas e
> b) a falta de recursos em geral das autoridades policiais. (Pinheiro, 2013, p. 311).

Paralelamente ao que é abordado na citação acima, Pinheiro (2013) afirma que o que torna os crimes eletrônicos um problema é a falta de denúncias desse tipo de crime, além da escassez de recursos necessários para solucioná-los.

3.4 Da origem dos crimes cibernéticos e sua efetiva proteção pela justiça

Os crimes cibernéticos não são fenômenos recentes e já causam prejuízos a seus usuários por meio de diversas práticas ilícitas, como clonagem de cartões, desbloqueio de documentos oficiais, entre outras. Ou seja, o acesso à internet, nesse contexto, é utilizado como ferramenta para a prática de crimes. Por isso, é importante ressaltar que *"o crime cibernético se configura na invasão não autorizada, no furto de informações confidenciais, no acesso não permitido, independentemente do uso de senha autorizada."* (Pinheiro, 2013, p. 313).

Paralelamente ao que afirma Pinheiro (2013), observa-se que a prática de crimes cibernéticos tem se tornado cada vez mais frequente em todo o mundo. Sob essa ótica, também se percebe uma tendência crescente de que o acesso não autorizado às informações seja o alvo de pessoas que utilizam a internet para cometer crimes dessa natureza.

Nos dizeres de Pinheiro (2013), um fator importante que pode ajudar a explicar o surgimento dos crimes cibernéticos está relacionado às organizações mafiosas, que, para otimizar decisões e dar logística não apenas às empresas legais, mas também às empresas ilegais, foram as primeiras a perceber o imenso potencial das transações eletrônicas para a lavagem de dinheiro. Assim, essas organizações passaram a usar as facilidades da rede para fechar negócios bilionários, o que deu origem ao fenômeno que hoje é denominado "Ciberterrorismo".

No Brasil, os crimes cibernéticos ganharam grande repercussão em meados de 2011, quando ocorreram ataques a sites do governo brasileiro, que ficaram instáveis até saírem do ar. Diante disso, houve uma crescente preocupação em criar soluções para o problema, o que levou à criação e sanção dos projetos de Lei nº 2.793/2011 e nº 84/99, sancionados em 30 de novembro de 2011.

Quanto à efetiva proteção da justiça quando são detectados crimes cibernéticos, devem ser observados os três estágios a seguir:

> 1º estágio – ter lei que trate os novos delitos e condutas ilícitas que ocorrem no ambiente da web – alcançado pelo Brasil em 2012 mesmo que de modo inicial;
> 2º Estágio – garantir a capacidade de guarda de prova de autoria para a penalização do infrator – o Brasil ainda está discutindo no âmbito do Marco Civil da Internet.

> 3º Estágio – criar um modelo próprio de cárcere digital para colocar o criminoso versão 2.0, evitando que haja apenas cárcere físico e ele continue, mesmo que preso, a agir por meio da web, em como investir em sua reintegração na sociedade no combate ao próprio crime digital – isso o Brasil nem iniciou, pois exigiria a revisão de todo o modelo de execuções penais e penitenciário, como outros países já estão fazendo, em especial EUA e Comunidade Europeia. (PINHEIRO, 2013, p. 314)

Conforme elencado por Pinheiro (2013), observa-se que a proteção da justiça no que se refere aos estágios mencionados no Brasil ainda ocorre de forma gradativa. No primeiro estágio, destaca-se a tipificação da Lei nº 12.737/12, que constitui um dos marcos legais nesse contexto.

Além disso, no que tange ao primeiro estágio de efetiva proteção da justiça contra os crimes cibernéticos, um exemplo recente é o Projeto de Lei Carolina Dieckmann, que altera o Código Penal para tipificar como infrações diversas condutas no ambiente digital, especialmente no que se refere à invasão de computadores. O projeto também estabelece punições específicas, algo inédito até então. É importante destacar que essa lei foi sancionada sem vetos.

Dessa forma, esse projeto representa um avanço no combate aos crimes cibernéticos. Com base nele, é possível afirmar que a regulamentação do ambiente virtual é imprescindível para o combate eficaz aos crimes cibernéticos, conforme preconiza a legislação.

Diante do exposto sobre os crimes eletrônicos, surgem as chamadas teorias da arquitetura, teoria tradicionalista, teoria libertária e teoria internacional. Essas teorias são fundamentais para uma compreensão mais aprofundada da regulamentação do ambiente virtual.

4. O mundo virtual e sua regulamentação

A regulamentação do mundo virtual é crucial, pois pode prevenir a ocorrência de diversos crimes cibernéticos. Dessa forma, tal regulamentação é sustentada por algumas teorias que, de maneira direta ou indireta, explicam a evolução do direito digital.

Assim, para compreender a proposta de regulamentação do mundo virtual, é fundamental distinguir as diferentes teorias do direito digital. Nesse contexto, as seguintes teorias são essenciais para esse entendimento: Teoria Libertária, Teoria da Arquitetura de Redes, Teoria Internacional e Teoria Tradicionalista, conforme discutido no texto que se segue.

4.1 Teoria Libertária

De acordo com Lima (2012, p. 45), a teoria libertária, também chamada de teoria liberatória, foi proposta por Daniel David Johnson, com base nas ideias de John Barlow. Essa teoria defende uma clara fronteira entre o direito real e o direito virtual, propondo que os princípios do direito aplicados no mundo físico não devem ser diretamente transferidos para o ambiente digital. A corrente libertária advoga por um modelo de direito mais descentralizado, em que a internet seria governada por um conjunto de normas próprias, dissociadas da estrutura tradicional e estatal, permitindo uma maior autonomia dos usuários e uma liberdade maior para a criação de novas formas de interação online.

Nesse contexto, Lima (2012) ainda destaca que a teoria libertária assume um conceito fundamental: *"o direito a ser aplicado à internet e aos ambientes eletrônicos deveria ser pautado pela chamada reconstrução da área de estudos a partir de novos princípios"* (Kunh, 1997, p. 20). Esse pensamento abre caminho para uma

reinterpretação do direito, no qual a internet é vista não apenas como uma ferramenta tecnológica, mas como um novo espaço de criação de normas e regulamentações, fundamentado por princípios que atendam à dinâmica digital.

Em relação ao que pontua Kunh (1997), é possível observar que a internet e os ambientes virtuais se expandem de maneira tão rápida e abrangente que oferecem inúmeras possibilidades para a reconstrução da área de estudos do Direito, desafiando as normas jurídicas tradicionais e forçando a adaptação dos sistemas legais. A convergência de novas tecnologias, como inteligência artificial, blockchain e criptomoedas, apenas intensifica essa necessidade de uma reformulação do direito digital. Com isso, surge uma tendência crescente para que novos princípios jurídicos sejam formulados, visando não só regulamentar os crimes cibernéticos, mas também assegurar direitos fundamentais na era digital.

Assim, ao lado da teoria libertária, destaca-se a teoria da Arquitetura de Rede, que também se faz crucial para compreender a relação entre o direito e o ambiente digital. Essa teoria, defendida por Lawrence Lessig, enfatiza que a estrutura tecnológica da rede de computadores, com seus mecanismos de controle e regulação, tem um impacto direto sobre os comportamentos dos usuários e as normas que podem ser aplicadas no ciberespaço. Em outras palavras, a própria arquitetura da internet — suas configurações de software e hardware — pode ser vista como um mecanismo regulador que influencia a maneira como as pessoas interagem online. Essa teoria oferece uma perspectiva de como a internet pode ser moldada para garantir tanto liberdade quanto segurança, equilibrando o controle e a autonomia dentro do ambiente digital.

4.2 Teoria da Arquitetura da Rede

Defendida por Lawrence Lessig, a teoria da Arquitetura de Rede aborda o uso de mecanismos tecnológicos que influenciam diretamente o comportamento dos usuários da internet. Esses mecanismos, muitas vezes sobrepostos às características originais da Rede, têm o poder de restringir ações, forçar comportamentos específicos e, em alguns casos, coibir práticas ilícitas. Segundo Vidal (2010, p. 4), esses controles tecnológicos não são neutros, mas são planejados para moldar as interações no ambiente virtual de acordo com normas estabelecidas.

Além disso, Vidal (2010, p. 5) aponta que, atualmente, uma proposta amplamente discutida é a reestruturação arquitetônica da rede. Nesse contexto, o papel do direito seria fundamental para a criação de mecanismos tecnológicos eficazes, capazes de controlar o fluxo de informações nos canais da rede de maneira mais eficiente. O direito, nesse sentido, deixaria de ser apenas uma ferramenta normativa e passaria a atuar diretamente no controle da estrutura tecnológica que rege a internet.

Uma das principais características da teoria da Arquitetura de Rede, conforme observado por Vidal (2010, p. 7), é que ela se configura como uma modalidade de regulação. A própria arquitetura da rede, com seus sistemas e protocolos, exerce um papel regulatório, ao passo que molda a interação dos indivíduos e as normas do ciberespaço. Em outras palavras, a arquitetura de rede não apenas facilita o acesso à informação, mas também determina como essa informação é acessada e distribuída, funcionando como um mecanismo regulador intrínseco ao próprio funcionamento da internet.

Portanto, a Arquitetura de Rede vai além da simples infraestrutura tecnológica; ela representa o "cerne da regulação" (Vidal, 2010, p. 7), impactando diretamente o comportamento social, econômico e legal dos usuários da internet.

Diante disso, a teoria da Arquitetura de Rede merece uma análise aprofundada, pois oferece uma compreensão mais ampla sobre como a regulação da internet pode ser realizada por meio de suas próprias estruturas tecnológicas.

4.3 Teoria Internacional

A teoria Internacional, conforme apontada por Vidal (2010, p. 7), surge como uma tentativa de preencher a lacuna deixada pela teoria libertária, especialmente no que diz respeito à questão da territorialidade no ciberespaço. Enquanto a corrente libertária propõe um modelo sem fronteiras, a teoria Internacional sugere que a regulamentação das atividades online deve ser construída por meio de acordos internacionais, permitindo a harmonização das regras que regem a internet em uma esfera global.

Essa teoria do Direito Internacional implica que, no contexto digital, as diversas sociedades e nações podem e devem se unir para criar um conjunto de regras comuns. Esses acordos internacionais visam estabelecer um padrão de normas que seja reconhecido por todos, com o objetivo de regulamentar o uso da internet e resolver disputas que envolvam múltiplos territórios. Em outras palavras, a teoria Internacional busca integrar o direito digital a um sistema de regras que transcende as fronteiras nacionais, promovendo a cooperação entre países para lidar com os desafios globais impostos pela internet.

Nesse contexto, a teoria pode ser vista como uma abordagem "imaterial", ou seja, ela não é limitada pelas fronteiras físicas dos Estados. Como afirma Lima (2012, p. 44), essa teoria permite que, enquanto uma pessoa se encontra em um país, ela possa simultaneamente estar em outro, dado o caráter transnacional da internet. Assim, a teoria Internacional propõe uma abordagem que reconhece a fluidez e a conectividade do ciberespaço, permitindo que as regras e soluções para os conflitos digitais sejam moldadas por uma cooperação global.

Portanto, a teoria Internacional oferece uma perspectiva importante para a regulação da internet, buscando integrar as normas nacionais e internacionais, garantindo que os direitos e deveres no ciberespaço sejam respeitados globalmente. Ela também sugere a implementação de soluções para conflitos transterritoriais, como questões envolvendo a privacidade, a propriedade intelectual e a responsabilidade por crimes digitais, que exigem uma abordagem colaborativa entre diferentes jurisdições.

4.4 Teoria Tradicionalista

A teoria tradicionalista aborda aspectos relevantes, entre os quais se destaca a Convenção de Budapeste, de 2001, que tratou sobre o cybercrime, ou seja, a prática de fraudar a segurança de computadores ou redes empresariais.

Com base na corrente tradicionalista, a Convenção de Budapeste foi um marco significativo, pois, em março de 2007, o Brasil manifestou seu interesse em integrar a rede de computação internacional. No entanto, de acordo com algumas cláusulas dessa convenção, as expectativas quanto ao seu alcance foram prejudicadas pela lentidão do sistema judiciário brasileiro, o que dificultou sua implementação efetiva.

Além disso, com relação à teoria tradicionalista, é importante destacar que o surgimento do Projeto de Lei nº 89/2003, no Brasil, gerou protestos significativos por parte do mercado de internet. Muitos alegaram que diversas atividades que movimentavam a Web foram descritas na referida lei como ilegais, o que gerou

preocupações quanto à liberdade de uso da internet e ao impacto de tais regulamentações sobre o setor.

Por essa razão, a teoria tradicionalista foi vista com poucas perspectivas de sucesso, especialmente devido à estagnação de novos modelos regulatórios que poderiam fazer a diferença nas futuras descobertas no meio digital. A teoria foi, portanto, considerada insuficiente para lidar com os desafios e as inovações do ambiente digital em constante evolução.

5. Da tipicidade do crime eletrônico

A teoria tradicionalista aborda aspectos relevantes, entre os quais se destaca a Convenção de Budapeste, de 2001, que tratou sobre o cybercrime, ou seja, a prática de fraudar a segurança de computadores ou redes empresariais.

Com base na corrente tradicionalista, a Convenção de Budapeste foi um marco significativo, pois, em março de 2007, o Brasil manifestou seu interesse em integrar a rede de computação internacional. No entanto, de acordo com algumas cláusulas dessa convenção, as expectativas quanto ao seu alcance foram prejudicadas pela lentidão do sistema judiciário brasileiro, o que dificultou sua implementação efetiva.

Além disso, com relação à teoria tradicionalista, é importante destacar que o surgimento do Projeto de Lei nº 89/2003, no Brasil, gerou protestos significativos por parte do mercado de internet. Muitos alegaram que diversas atividades que movimentavam a Web foram descritas na referida lei como ilegais, o que gerou preocupações quanto à liberdade de uso da internet e ao impacto de tais regulamentações sobre o setor.

Por essa razão, a teoria tradicionalista foi vista com poucas perspectivas de sucesso, especialmente devido à estagnação de novos modelos regulatórios que poderiam fazer a diferença nas futuras descobertas no meio digital. A teoria foi, portanto, considerada insuficiente para lidar com os desafios e as inovações do ambiente digital em constante evolução.

5.1 Classificação dos crimes virtuais e suas atribuições

De maneira geral, os crimes virtuais são classificados em próprios e impróprios. No que diz respeito aos crimes próprios, o sujeito utiliza o computador de forma ilícita para se apropriar de informações não autorizadas. Nesse contexto, entende-se que qualquer pessoa física ou jurídica que tenha seus bens desviados, seu patrimônio deteriorado ou que tenha suas informações violadas configura o sujeito passivo do crime virtual.

5.1.1 Crimes informáticos próprios

Os crimes próprios ou específicos compõem uma das classificações dos crimes virtuais. Esses crimes têm uma característica essencial: são crimes que, para sua ocorrência, demandam a utilização do ambiente digital como meio para a prática do ato ilícito. Neste contexto, vale destacar que "*os crimes próprios só podem ser cometidos no ciberespaço, ou seja, devem ser realizados no ambiente virtual, para que a conduta seja concretizada, possuindo um tipo penal distinto do tradicional.*" (Lima, 2012, p. 175).

Dessa forma, como enfatiza Lima (2012), a concretização dos crimes próprios está intrinsicamente ligada ao ambiente virtual. Ou seja, o meio digital não é apenas um facilitador ou instrumento para a realização do crime, mas um requisito essencial para que o crime exista, definindo sua natureza e tornando-o distinto de outros tipos

penais. A característica essencial desses crimes é que eles só podem ocorrer no espaço cibernético, onde as regras do mundo físico não se aplicam da mesma maneira. Isso inclui, por exemplo, crimes como invasão de sistemas, roubo de dados e a distribuição não autorizada de informações.

A teoria dos crimes próprios é crucial para entender as infrações que afetam o espaço digital, pois ela delimita claramente as ações que são exclusivas do ambiente cibernético. Segundo Vianna (2003), citado por Gimenes (2013), os crimes informáticos próprios são definidos como aqueles que envolvem a violação da privacidade e da integridade das informações, ou seja, as infrações que afetam diretamente a inviolabilidade dos dados. Para que se configure um crime próprio, é imperativo que a violação seja realizada por meio de tecnologia informática. Por exemplo, um indivíduo pode não estar fisicamente em posse de uma informação, mas pode ainda assim cometer um crime ao violar as proteções digitais que garantem a integridade e a privacidade dessa informação.

Esses crimes virtuais estão, portanto, cada vez mais interligados com o desenvolvimento de novas tecnologias e suas aplicações. A proteção dos dados pessoais, a segurança dos sistemas de informação e a regulamentação da comunicação digital são áreas que ganham cada vez mais relevância no cenário jurídico contemporâneo.

Nas palavras de Vianna (2003, p. 6), um exemplo clássico de crime informático próprio é a interceptação telemática ilegal, conforme previsto no artigo 10 da Lei nº 9.296/96 (Lei Federal Brasileira). Este artigo define que: *"Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei."* O crime descrito neste artigo envolve a captura de informações confidenciais, sem o consentimento da pessoa ou da parte envolvida, e é um claro exemplo de como a legislação brasileira já reconhece a existência de crimes próprios no âmbito digital. Nesse caso, o bem jurídico protegido é a privacidade e a confidencialidade das comunicações, sendo essencial a utilização de mecanismos legais para a devida autorização da interceptação de dados, seja no âmbito telefônico, seja em outros meios digitais.

A Lei nº 9.296/96 é um marco importante na regulamentação dos crimes próprios relacionados à informática, pois ao criminalizar a interceptação sem autorização, ela busca proteger direitos fundamentais como a privacidade e a segurança da comunicação. Esses crimes, ao serem cometidos no ciberespaço, estão sujeitos a uma estrutura normativa que visa garantir que a rede de computadores e sistemas de comunicação sejam usados de forma ética, segura e de acordo com as leis de proteção à privacidade.

Portanto, a classificação dos crimes próprios é fundamental para entender o direito penal digital, uma vez que ela estabelece que o uso do ambiente virtual para a prática de crimes, como o roubo de dados, a invasão de sistemas e a interceptação ilegal de comunicações, deve ser tratado de maneira específica. A natureza do crime cibernético, no caso dos crimes próprios, não pode ser dissociada do ambiente digital em que ocorre, e sua tipificação penal deve levar em consideração as particularidades e os desafios do ciberespaço.

5.1.2 Crimes informáticos impróprios

Uma outra classificação de crimes virtuais refere-se aos denominados *crimes impróprios ou comuns*, os quais, segundo Lima (2012, p. 173), são crimes que podem ser cometidos tanto no mundo físico ou material quanto no ciberespaço.

Diferentemente dos crimes próprios, que exigem o uso exclusivo do ambiente digital, os crimes impróprios podem ocorrer em qualquer contexto, mas ganham novas dimensões e características quando cometidos no ciberespaço.

De acordo com Carneiro (2012), os crimes impróprios estão intimamente vinculados ao computador, que serve como meio para a realização de atos ilícitos. Esses crimes, ao contrário dos próprios, não dependem exclusivamente da tecnologia para sua configuração, mas o ambiente digital proporciona novas oportunidades e formas de cometê-los. O uso de ferramentas digitais, como e-mails, redes sociais e plataformas de comunicação online, tem sido um dos principais meios pelos quais essas infrações são cometidas. Como resultado, esses crimes impactam diretamente a privacidade dos usuários da internet, violando bens jurídicos previamente protegidos por legislações tradicionais, como o direito à honra, à imagem e à intimidade.

Carneiro (2012, p. 3) exemplifica alguns crimes impróprios virtuais, citando a *calúnia* (art. 138 do Código Penal Brasileiro), a *difamação* (art. 139 do Código Penal Brasileiro) e *a injúria* (art. 140 do Código Penal Brasileiro). Esses crimes, que envolvem ofensas à honra e à dignidade de uma pessoa, podem ser praticados, por exemplo, através do envio de um e-mail ou de postagens em redes sociais. Outro exemplo de crime impróprio é o previsto no artigo 241 do *Estatuto da Criança e do Adolescente (ECA),* da Lei nº 8.069/90, que trata da produção, reprodução, distribuição e posse de imagens pornográficas envolvendo crianças ou adolescentes, o que também pode ocorrer através de plataformas digitais.

Além desses exemplos, a classificação de crimes virtuais ajuda a entender como as infrações ganham novas contextualizações com o avanço e a dinâmica da rede de computadores e da internet, conforme destacado por Carneiro (2012). À medida que novas tecnologias são desenvolvidas, os crimes virtuais se adaptam, oferecendo novos desafios para a regulamentação e a aplicação da lei. A internet, com sua natureza global e interconectada, permite que práticas ilícitas que antes eram limitadas ao ambiente físico se expandam e se tornem mais difíceis de serem controladas e punidas.

Portanto, a classificação dos crimes virtuais não apenas define os diferentes tipos de infrações, mas também fornece uma base para compreender como o ambiente digital altera a forma como esses crimes são cometidos e tratados. Outro aspecto a ser considerado, especialmente quando se discute os crimes virtuais, é a autoria desses crimes, um tema que tem se difundido no mundo todo. A autoria, que envolve questões como a identificação do criminoso e a responsabilidade jurídica no contexto digital, será abordada no tópico seguinte.

5.2 Identificação da autoria

A autoria de crimes virtuais é, sem dúvida, um dos assuntos que suscita diversas questões, devido à complexidade envolvida. Isso ocorre porque, na maioria dos casos em que se comprovam crimes virtuais, a autoria quase sempre não é descoberta.

Assim, um dos principais desafios na identificação da autoria de crimes virtuais decorre do fato de que, embora seja possível identificar a máquina ou o computador que praticou o crime, os provedores geralmente não armazenam essas informações por muito tempo e dependem de autorização judicial para liberar esses dados, o que, nesse caso, é considerado oneroso, conforme afirma Carneiro (2012).

Na busca de soluções para o problema da identificação da autoria de crimes virtuais, foi idealizado e aprovado o projeto de lei do senador Eduardo Azeredo (PSDB-MG), que trata do seguinte:

> Prevê que será necessário armazenar, por três anos, apenas os dados sobre a origem, hora e data da conexão. O repasse para as autoridades policiais será feito somente com decisão judicial. Os provedores não são obrigados a fiscalizar, mas têm que repassar denúncias que receberem sobre conteúdos publicados. (Carneiro, 2012, p. 05).

O projeto de lei mencionado anteriormente estabelece que a criação de um ambiente seguro na internet seria uma alternativa para evitar a ocorrência de crimes virtuais. Ou seja, o projeto não propõe novidades substanciais, mas destaca a necessidade de penalidades para aqueles que cometem infrações no ambiente digital.

Para auxiliar na identificação da autoria dos crimes virtuais, foram criados alguns sites com o objetivo de denunciar esses delitos. Um dos principais referenciais para denúncias de crimes virtuais é o Safernet Brasil, uma associação civil de direito privado, reconhecida nacionalmente no combate a crimes e violações aos Direitos Humanos na Internet. Nesse contexto, outro importante aliado no enfrentamento dos crimes virtuais é o Universo Online (UOL), que oferece suporte semelhante ao do Safernet Brasil.

Segundo Carneiro (2012), as denúncias contra a autoria de crimes virtuais podem ser anônimas ou identificadas. Após o recebimento das denúncias, elas são encaminhadas às delegacias especializadas em crimes virtuais. No entanto, devido à grande quantidade de casos ocorrendo no Brasil e no mundo, as delegacias especializadas são poucas para atender a toda demanda.

Dessa forma, para abordar com maior precisão a questão da tipificação dos crimes virtuais, o próximo tópico apresentará algumas considerações sobre a Lei nº 12.737/12, que é de fundamental importância para esclarecer os pontos relacionados às sanções e penalidades aplicáveis aos crimes virtuais.

5.3 A Lei n° 12.737/12 sobre a tipificação criminal de delitos informático

A tipificação criminal de delitos informáticos, no que tange à *Lei nº 12.737/12*, altera o *Decreto-Lei nº 2.848*, de 7 de dezembro de 1940, que institui o *Código Penal*, e dá outras providências, conforme estabelece o *artigo 1º* da referida lei.

Dessa forma, de acordo com o *artigo 2º* da *Lei nº 12.737/12*, o *Decreto-Lei nº 2.848*, de 7 de dezembro de 1940 (*Código Penal*), é acrescido dos seguintes artigos: *154-A* e *154-B*. No que se refere ao *artigo 154-A*, considera-se *invasão de dispositivo informático* o seguinte:

> 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, 2012).

No que se pode entender das disposições do *artigo 154-A*, o crime informático ocorre quando há a invasão de informações restritas de um usuário da rede de computadores e da internet. Essa invasão é considerada uma violação de dados e informações, podendo ser penalizada por meio de detenção do acusado ou, ainda, com a aplicação de multa.

De acordo com o *artigo 154-B*, cabe ação penal caso haja representação pelos crimes cometidos contra a administração pública direta ou indireta de qualquer

um dos três Poderes da União, estados, Distrito Federal, Municípios ou contra empresas concessionárias de serviços públicos.

Assim, conforme estabelece a *Lei 12.737/12*, os *artigos 266* e *298* do *Decreto-Lei nº 2.848/40* ganharam nova redação, e, sob a ótica do *artigo 3º*, explicita-se que, no ato de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, o *artigo 266* estabelece o seguinte:

> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2o "Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (Brasil, 2012).

Portanto, conforme esclarece a citação acima, percebe-se que, se o crime informático ou de outra natureza for cometido contra a administração pública, os responsáveis pela ação ilícita estarão sujeitos a uma ação penal, cuja penalidade pode ser duas vezes mais severa do que a aplicada em crimes virtuais cometidos contra pessoas físicas.

No que diz respeito ao *artigo 298* do *Decreto-Lei nº 2.848/40*, em caso de falsificação de documento particular, serão aplicadas as penalidades cabíveis àquele que, de maneira indevida, fizer uso de cartão de terceiros para usufruir de bens de consumo ou outros serviços.

Paulatinamente, as disposições da *Lei 12.737/12* explicam que a tipificação de delitos informáticos é um assunto novo e, portanto, ainda pode ser alterado conforme a necessidade. Assim, além da lei mencionada, é importante destacar que existem outros dispositivos legais que tratam da tipificação de crimes virtuais, um assunto que será tratado no próximo tópico.

5.3 Dos demais dispositivos e diplomas legais pertinentes aos crimes virtuais

No Brasil, além da *Lei nº 12.737/12*, podem ser mencionados outros dispositivos legais que tratam de crimes virtuais, entre eles, a *Lei nº 9.609/98*, que dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no país. Na referida lei, o programa de computador é definido, em seu *art. 1º*, como:

> 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, Lei de nº. 9.609/98).

Conforme as disposições da lei mencionada anteriormente, os programas de computador deveriam ser utilizados para dar suporte ao usuário no que diz respeito à necessidade de organizar, codificar informações, entre outras atribuições que pudessem auxiliar os usuários em seus anseios e necessidades cotidianas com o uso do computador.

Em relação à *Lei nº 9.983/00*, esta alterou o Código Penal, em seus *artigos 153, 313-A, 313-B* e *325*. No caso da tipificação de crimes virtuais, a lei em questão estabelece, em seu *art. 12*, o seguinte:

> Tipifica-se a conduta de *"Violar direitos de autor de programa de computador",* prevendo-se uma pena de detenção de seis meses a dois anos

> ou multa. Nesta mesma sanção incorre *"quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral".* (Moreira, 2012, p.7).

Em consonância com o que dispõe Moreira (2012), um dos exemplos que explicam bem a questão pode ser conferido no que trata o *art. 12* da *Lei nº 9.983/00*, que alterou o texto redacional do *Código Penal*.

Paralelamente ao que se observa nos dispositivos ou diplomas que tratam de crimes virtuais, ou ainda das situações que configuram tais crimes, é relevante destacar os avanços obtidos no âmbito da justiça em relação aos crimes virtuais. Dessa forma, no tópico que se segue, são apresentadas algumas explicações pertinentes ao tema abordado.

6. Dos avanços legislativos, doutrinários e jurisprudenciais

Os avanços legislativos, doutrinários e jurisprudenciais no âmbito do direito digital são considerados um enfoque novo, pois ainda existem muitos desafios na obtenção de habilidades para a adequação de sistemas voltados a esse fim.

Nos dizeres de Pinheiro (2013, p. 294), a eliminação do papel no decorrer do processo ou até mesmo na etapa de finalização reduz a parte burocrática, até certo ponto. O que deve ser levado em conta, no entanto, é se existem profissionais amplamente preparados para fazer uso dos avanços tecnológicos que tendem a se tornar cada vez mais presentes no meio legislativo, judiciário e administrativo.

6.1 Da Justiça digital em tempos de contemporaneidade

Quanto à questão dos avanços que estão se tornando cada vez mais eminentes na sociedade contemporânea, é relevante atentar para o seguinte:

> Nos últimos anos, as decisões judiciais forma aprimorando-se no tocante aos temas de direito digital, especialmente no uso de provas eletrônicas na Justiça. A tal ponto que estamos vivendo um marco histórico que é a migração para o processo eletrônico. (Pinheiro, 2013, p.293).

Com base nas palavras de Pinheiro (2013), as decisões judiciais não estão isentas da influência da era digital, ou seja, da rede e de outros atributos ligados a essa era. É de suma importância que esses elementos sejam reconhecidos para promover melhorias no atendimento do Judiciário.

Pinheiro (2013, p. 293) ressalta que não há como obter uma decisão eficaz do Judiciário, mesmo com o devido preparo por parte da empresa, que combine medidas jurídicas, técnicas e de recursos humanos, visto que o uso de ferramentas como e-mail corporativo, redes, internet, smartphones e notebooks exige a criação de uma nova cultura interna e de bom senso geral, que ainda está sendo estabelecido no cotidiano.

No contexto dos avanços da era digital no âmbito da Justiça, pode-se citar a *Lei nº 11.419/2006* como um marco regulatório da informatização judicial, pois abrange todas as fases e atividades necessárias para a implantação do Poder Judiciário no Brasil. Nesse sentido, o *artigo 11* da referida lei trata do seguinte:

> Art. 11: Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais. (Brasil, Lei nº 11. 419/2006).

Portanto, com base no que preceitua o artigo acima citado, o uso de documentos eletrônicos tende a garantir os direitos de seus usuários da mesma forma que os documentos escritos. O que é positivo nesse procedimento é que se percebem avanços significativos com o uso da era informatizada.

Com efeito, o Poder Judiciário brasileiro, em matéria de Direito Processual Civil, já se preparou para as mudanças com o advento do novo Código de Processo Civil, que tramita atualmente no Congresso Nacional pelo PL nº 166/2010, e adotou o processo eletrônico (para a comunicação de seus atos, realização de audiências, recebimento de documentos, provas eletrônicas, etc.), conforme afirma Pinheiro (2013, p. 297).

Por conseguinte, o que se pode aferir de tal afirmação é que, aos poucos, o uso da era informática vai se consolidando no âmbito do Poder Judiciário, e, com isso, a Justiça só tem a ganhar com o uso de novas tecnologias.

7. Conclusão

O estudo dos crimes cibernéticos e sua regulamentação evidencia um cenário jurídico em constante transformação, impulsionado pelo avanço tecnológico. A pesquisa demonstrou que, embora a legislação brasileira tenha evoluído com marcos importantes, como a Lei nº 12.737/12 e o Marco Civil da Internet, ainda existem lacunas a serem preenchidas. A aplicação da justiça no ambiente digital enfrenta desafios relacionados à identificação de autores, à preservação de provas e à capacitação das autoridades competentes. Além disso, as teorias jurídicas, como a libertária e a tradicionalista, oferecem diferentes perspectivas sobre a regulação do ciberespaço. Conclui-se que o Direito deve continuar a se adaptar às novas realidades digitais, buscando soluções que conciliem segurança, liberdade e inovação tecnológica. O sucesso no combate aos crimes virtuais dependerá não apenas da criação de novas leis, mas também da cooperação internacional e do desenvolvimento de mecanismos eficazes de proteção e investigação no ambiente digital.

Referências

BARONE, Victor. O que é a Convenção de Budapeste. Disponível em: http://www.escrivinhas.blogs.com.br. Acesso em: 27 ago. 2024.

BRASIL. **Estatuto da Criança e do Adolescente (ECA)**. Lei n. 8.069, de 13 de julho de 1990. Disponível em: http://www.planalto.com.br. Acesso em: 15 set. 2024.

BRASIL. **Lei n. 9.609, de 19 de fevereiro de 1998**. Disponível em: http://www.planalto.com.br. Acesso em: 3 set. 2024.

BRASIL. **Lei n. 9.983, de 14 de julho de 2000**. Disponível em: http://www.planalto.com.br. Acesso em: 10 set. 2024.

BRASIL. **Lei n. 11.419, de 19 de dezembro de 2006**. Disponível em: http://www.planalto.com.br. Acesso em: 22 out. 2024.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012**. Disponível em: http://www.planalto.com.br. Acesso em: 5 nov. 2024.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, v. XV, n. 99, p. xx-xx, abr., 2012. Disponível em: http://www.ambitojuridico. Acesso em: 11 set. 2024.

FERREIRA, Ivette Senise. **Direito & Internet: aspectos jurídicos relevantes**. 2. ed. São Paulo: Quartier Latin, 2005.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina TRF4**, [s.l.], p. xx-xx. Disponível em: http://www.revistadoutrina.trf4.jus.br. Acesso em: 14 ago. 2024.

GUERRA, Sidney. **Direitos humanos & cidadania**. São Paulo: Atlas, 2012.

KUHN, Thomas S. **A estrutura das revoluções científicas**. 5. ed. São Paulo: Perspectiva, 1997.

LOSANO, Mario G. **Lições de informática jurídica**. São Paulo: Resenha Tributária Ltda., 1974.

MARCACINI, Augusto Tavares Rosa. **Direito e informática: uma abordagem jurídica sobre a criptografia**. Rio de Janeiro: Forense, 2002.

MOREIRA, Rômulo de Andrade. A nova lei sobre a tipificação de delitos informáticos: até que enfim um diploma legal necessário. Disponível em: http://jus.com.br. Acesso em: 25 set. 2024.

PIMENTEL, Alexandre Freire. **O direito cibernético: um enfoque teórico e lógico-aplicativo**. Rio de Janeiro: Renovar, 2000.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed. ver., atual. e ampl. São Paulo: Saraiva, 2013.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informática**. Rio de Janeiro: Forense, 2003.

VIDAL, Gabriel Rigoldi. **Regulação do direito à privacidade na internet: o papel da arquitetura.** Disponível em: http://www.jus.com.art. Acesso em: 18 out. 2024.