UNIVERSIDADE FEDERAL DE CAMPINA GRANDE – UFCG

CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS – CCJS

UNIDADE ACADÊMICA DE DIREITO

IGOR MÁRCIO TOLENTINO DE ARAÚJO

A ATUAÇÃO DO DIREITO DIGITAL NO ENFRENTAMENTO AOS CIBERCRIMES

SOUSA-PB

2023

IGOR MÁRCIO TOLENTINO DE ARAÚJO

A ATUAÇÃO DO DIREITO DIGITAL NO ENFRENTAMENTO AOS CIBERCRIMES

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande - UFCG, como exigência parcial para obtenção do título de Bacharela em Direito.

Orientadora: Prof. Dra. Vaninne Arnaud de Medeiros Moreira

SOUSA-PB
2023

A662a Araújo, Igor Márcio Tolentino de.
A atuação do Direito Digital no enfrentamento aos cibercrimes / Igor Márcio Tolentino de Araújo – Sousa, 2023.
44 f. : il. color.

Monografia (Bacharelado em Direito) - Universidade Federal de Campina Grande, Centro de Ciências Jurídicas e Sociais, 2023.
"Orientação: Profa. Dra. Vaninne Arnaud de Medeiros Moreira."
Referências.

1. Crimes Cibernéticos. 2. Direito Digital. 3. Legislação Específica. 4. Resolução de Conflitos no Direito Digital. I. Moreira, Vaninne Arnaud de Medeiros. II. Título.

CDU 34:007(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA ITAPUANA SOARES DIAS GONÇALVES CRB-15/093

IGOR MÁRCIO TOLENTINO DE ARAÚJO

A ATUAÇÃO DO DIREITO DIGITAL NO ENFRENTAMENTO AOS CIBERCRIMES

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande - UFCG, como exigência parcial para obtenção do título de Bacharela em Direito.

Orientador: Prof. Dra. Vaninne Arnaud de Medeiros Moreira

Data de aprovação: 09/11/2023

Banca Examinadora

Prof. Vaninne Arnaud de Medeiros Moreira

Orientador – CCJS/UFCG

Prof. Eduardo Jorge Pereira de Oliveira

Examinador – CCJS/UFCG

Prof. João de Deus Quirino Filho

Examinador – CCJS/UFCG

“Nada é orgânico, é tudo programado

E eu achando que tinha me libertado

Mas lá vem eles novamente

Eu sei o que vão fazer

Reinstalar o sistema”.

- Pitty

AGRADECIMENTOS

Primeiramente, gostaria de expressar minha profunda gratidão a Deus, cuja graça e orientação me sustentaram ao longo desta jornada. Sua luz iluminou o caminho e me deu força para superar os desafios que encontrei na realização deste curso e deste trabalho.

À minha família, um agradecimento especial. Vocês são minha base, meu apoio. Sem o amor, incentivo e compreensão de vocês, nada disso teria sido possível. Meu pai, meus irmãos, minhas avós, e demais familiares, cada um de vocês desempenhou um papel fundamental na minha vida.

Agradecimento especial à minha mãe, que durante todo meu percurso me apoiou e me incentivou. Reconheço todo esforço que faz por mim, todas as noites que passou em claro para que nunca me faltasse nada e que eu nunca precisasse me preocupar com algo além dos estudos. Minha gratidão vai muito além do que consigo colocar em palavras.

Aos meus amigos, que estiveram ao meu lado durante os altos e baixos desta jornada, quero expressar minha sincera gratidão. Aqueles de minha cidade natal, que mesmo distante se fizeram presente de alguma forma, é de conhecimento todo carinho que tenho por cada um. As cocotas, a panelinha depressão, o red kallangos e o beats, obrigado por todas as risadas, todo acolhimento e pela amizade significativa de cada um, vocês fizeram Sousa se tornar um lar para mim.

Aos que sempre foram meus companheiros desde o início, Duanny, Jade, Malu, Marina, Mel e Stefany, meu mais sincero agradecimento a cada um de vocês por tornar tudo mais fácil. A amizade de vocês é muito preciosa e espero encontrá-los novamente muito em breve. Minha amiga Mel, que sempre foi minha dupla pessoal e acadêmica, obrigado por todo companheirismo, por somar tanto, nossa sintonia não ocorreu por acaso, é tudo culpa das mentes conectadas. Os que me ajudaram tanto no meu primeiro ano, Anna Beatriz, Sabrina, Vitória, Joyce e Mateus. Em especial o meu colega de apartamento que enfrentou comigo todos os desafios de morar longe, obrigado por todo companheirismo.

A minha orientadora, que me guiou e compartilhou seu conhecimento ao longo da construção desta pesquisa, sou profundamente grato. Suas orientações e conselhos foram inestimáveis para o desenvolvimento deste trabalho.

Agradeço a todos da 2ª Vara Mista de Sousa, que me acolheram, guiaram e me ensinaram tanto. Obrigado, Sandra, Socorro, Augusto e Loreto por me ensinarem o direito na prática e o papel da justiça. E também estendo aos meus queridos colegas estagiários, onde dividimos os perrengues e também tantos bons momentos.

Por fim, agradeço a todos que, de uma forma ou de outra, contribuíram para a realização deste TCC. Seu apoio e encorajamento foram essenciais. Este trabalho é dedicado a todos vocês.

RESUMO

A sociedade está em constante transformação e evolução, enfrentando, assim, diversas mudanças sociais, que alteram a forma de viver dos indivíduos nela inseridos. Frente a esse cenário de mudanças tecnológicas e comportamentais, o avanço tecnológico apresentou novas formas de cometer crimes, através do meio digital. A título de introduzir o leitor ao assunto e aos conceitos básicos, é demonstrado o contexto em que a rede mundial é trazida à realidade, até o momento em que chega aos lares dos brasileiros. Após isso, devido a vulnerabilidade que apresenta e as ferramentas que dispõe, demonstrou ser capaz de tornar-se um meio de práticas criminosas. Diante disso, o Direito não poderia ser inerte. Assim, se dá o aparecimento de uma ciência jurídica que busca responsabilizar os atos criminosos que ocorrem no ciberespaço. A legislação específica ainda é escassa, então utiliza das leis já vigentes em outros ramos, através da dinâmica interpretativa e da autorregulamentação. Além da utilização dos meios de resolução alternativos, como arbitragem e mediação. Diante desse cenário, questiona-se: há leis suficientes para regulamentar essas condutas criminosas? Como o Direito Digital age frente a esses atos delitivos? Como a carência legislativa é superada pelo direito digital? A partir de tais indagações, surge o presente trabalho, o qual apresenta pesquisa descritiva. Quanto à finalidade, trata-se de pesquisa básica estratégica. Quanto ao método de pesquisa, utilizou-se o dedutivo, com aplicação dos procedimentos bibliográfico e documental. A título de conclusão, restou demonstrado o contexto histórico da internet e como é utilizada como ferramenta para práticas criminosas. Além disso, foi exposto como o Direito Digital age quanto a isso, as legislações vigentes específicas, ou de outros ramos, e a necessidade dessa abordagem.

Palavras-chave: Crimes cibernéticos. Direito digital. Legislação específica. Resolução de conflitos no direito digital.

ABSTRACT

Society is in constant transformation and evolution, thus facing various social changes, which alter the way of life of the individuals within it. Faced with this scenario of technological and behavioral changes, technological advances have presented new ways of committing crimes through digital means. In order to introduce the reader to the subject and basic concepts, the context in which the global network is brought into reality is demonstrated, until the moment it reaches the homes of Brazilians. After that, due to the vulnerability it presents and the tools it has at its disposal, it demonstrated that it was capable of becoming a means of criminal practices. Given this, the Law could not be inert. Thus, the emergence of a legal science that seeks to hold criminal acts that occur in cyberspace accountable. Specific legislation is still scarce, so it uses laws already in force in other areas, through interpretative dynamics and self-regulation. In addition to the use of alternative means of resolution, such as arbitration and mediation. Given this scenario, the question arises: are there sufficient laws to regulate these criminal conducts? How does Digital Law act in the face of these criminal acts? How is the legislative shortage overcome by digital law? From such questions, the present work arises, which presents descriptive research. As for the purpose, it is strategic basic research. As for the research method, the deductive method was used, with the application of bibliographic and documentary procedures. By way of conclusion, the historical context of the internet and how it is used as a tool for criminal practices was demonstrated. Furthermore, it was explained how Digital Law acts in this regard, the specific legislation in force, or other areas, and the need for this approach.

Keywords: Cyber crimes. Digital Law. Specific law. Conflict resolution on digital law.

SUMÁRIO

1 CONSIDERAÇÕES INICIAIS

O surgimento e a evolução das tecnologias representaram uma mudança comportamental na sociedade, apresentaram novas formas para praticar ações antes praticadas por outras vias, entre elas, as condutas criminosas, que quando realizadas em ambiente digital recebem o nome de cibercrimes.

Na prática veremos que há diferentes tipos de crimes cibernéticos, inclusive os crimes tradicionais que ganham uma forma “cyber”, fazendo até com que legislações sejam modificadas para atender ou tornar mais graves esses casos específicos, como será possível observar no decorrer da monografia.

Em detrimento dessas novas formas de práticas delitivas, também é necessário um ramo que tutele e busque a segurança nesse meio. O Direito Digital, dentre tantas outras coisas, busca punir e tipificar as condutas danosas que ocorrem no ciberespaço. Como será demonstrado, a legislação específica ainda é limitada então o Direito Digital utiliza do princípio e suas características para regular essas relações e preencher lacunas.

Desta forma, mostrará-se a evidente carência legislativa, porém que é recompensada, em certos aspectos, pelas formas no qual o Direito Digital responde a isso. É uma ciência que abarca todos os ramos do direito, e de forma necessária, para assim conseguir um arcabouço jurídico fundamentado e mais próximo do completo.

É uma problemática que necessita de atenção jurídica, visto a real imersão da sociedade no mundo digital, onde incontáveis coisas são possíveis de realização com um dispositivo ao alcance.

Desse modo, está suficientemente demonstrada a justificativa da realização da presente monografia, diante da relevância do assunto e dos impactos sociais causados pela evolução tecnológica, como forma de demonstrar como o direito digital age na deficiência legislativa cibernética.

Assim, tem-se como objetivo realizar uma análise do contexto histórico da internet até a sua inserção na sociedade, bem como expor a classe de crimes que ocorre através dela e sua classificação, e por fim, demonstrar como o direito digital enfrenta essas condutas passíveis de punição.

A presente monografia encontra-se dividida em três capítulos. O primeiro capítulo tem o intuito de apresentar o contexto histórico da rede mundial, desde sua

criação até o momento de chegada nos lares brasileiros. Além disso, traz o conceito chave de ciberespaço e apresenta as vulnerabilidades que esse ambiente traz consigo.

O segundo capítulo apresenta a ideia sobre do que se trata o cibercrime, além de apresentar uma classificação para melhor entendimento sobre e também demonstrar como algumas condutas criminosas passaram a utilizar o meio digital como ferramenta para cometer ações delituosas.

Por fim, no terceiro capítulo conceitua-se o direito digital. Apresentando, além da conceituação, a exposição de características inerentes. Bem como, a legislação específica, as formas de resolução de conflitos e pontos que venham a ser pertinentes para maior compreensão.

Quanto à metodologia de pesquisa, trata-se de uma pesquisa descritiva. Realizando, desta forma, a exposição das características deste fenômeno. Analisando o cenário a ser exposto, considerar-se-á esta pesquisa como básica estratégica. A técnica de análise apresentada fora a qualitativa, tendo sido utilizado o método de pesquisa dedutivo. Além disso, a presente monografia emprega o procedimento bibliográfico e documental, tendo em vista que valeu-se de doutrinas, artigos científicos, legislações e jurisprudências para consolidação do referencial teórico.

2 A INTERNET E O CIBERESPAÇO

Este capítulo tem como objetivo situar o leitor quanto ao assunto desta monografia. Para melhor entendimento do que são e como se dão os crimes cibernéticos, é fundamental ter entendimento sobre alguns conceitos e temas.

2.1 ASPECTOS HISTÓRICOS E CHEGADA AO BRASIL

Essencialmente, para iniciar a discussão, é interessante que possa se pensar em como o tempo foi sendo construído socialmente, também por um aspecto comercial, as relações vão se adaptando para servir aos interesses das classes dominantes. Com isso, a partir da década de 70, Alvin Tofler traz a ideia de uma sociedade da informação e também a diferença entre o tempo analógico e o tempo virtual, a qual se traduz em que o tempo analógico corresponde ao cotidiano usual, já o tempo virtual, pode ser relativizado, usado simultaneamente no espaço-tempo criado naquele contexto (PINHEIRO, 2021).

Essas ações devem ser feitas em um tempo paralelo, tanto no mundo físico quanto digital, isto é, essas organizações serão fundamentadas principalmente na velocidade das informações que são estabelecidas naquele momento, isso traz consequências para o campo jurídico, que acabam ultrapassando o tempo exigido por essas instituições, cada vez mais essas informações circulam e evoluem progressivamente na sociedade.

Ao longo dos períodos, percebeu-se a transição a partir de veículos de comunicação, entre eles, pode-se citar a Era Agrícola, a Revolução Industrial e a Era da Informação, três marcos definidores sobre essa sociedade da informação (PINHEIRO, 2021). A internet surge como um ápice da Era da Informação, além da velocidade das informações, as origens dessas são descentralizadas, ou seja, há uma massificação dessa comunicação.

Mesmo com a previsão da ideia de “aldeia global”, isto é, o aumento do número de pessoas que cada vez mais estão conectadas em suas relações sociais, não se imaginava como ia também aumentar as possibilidades de escolhas dentro desses meios de comunicação, essa ideia afeta diretamente como será aplicado dentro da própria área do Direito.

> Os desafios jurídicos do Direito Digital incluem a quebra de paradigmas, a descentralização, a dificuldade em definir limites territoriais e físicos, a velocidade com que as decisões devem ser tomadas e a crescente capacidade de resposta dos Indivíduos. A Internet gera uma infinidade de nações virtuais — pessoas, empresas e instituições de várias partes do mundo unidas por interesses os mais variados (Pinheiro, 2021).

A comunicação através do uso de máquinas sempre foi considerada uma possibilidade. Desde que os primeiros computadores surgiram, com as experiências como as de Alan Turing durante a Segunda Guerra Mundial (Isaacson,p 55-61,2014), a troca de mensagens e informações transmitidas com rapidez entre máquinas virou realidade. Desse modo, a internet é criada com a finalidade de alcançar um poder mundial por parte dos Estados Unidos da América como uma reação contra a União Soviética (URSS) para proteger as linhas de comunicação e assegurar essa hegemonia.

E ainda nesse contexto de conflitos bélicos, a internet teve muito de sua criação na ARPANET (Advanced Research Projects Agency Network), que foi um projeto militar estadunidense que nasceu durante a Guerra Fria. Tinha o papel de desenhar uma rede de comunicações indestrutível, ou facilmente recuperável, que resistisse a qualquer tentativa ou controle por parte das outras potências. A ARPANET foi acionada em 1969 e apresentou o correio eletrônico, uma forma de comunicação direta e rápida (Muñoz e Turner, p. 23, 1999).

Posteriormente, no início da década de 1980, o emprego do TCP/IP (Transmission Control Protocol/Internet Protocol) como protocolo de comunicação na ARPANET possibilitou a interconexão entre redes distintas, expandindo significativamente a abrangência da rede. A ARPANET evoluiu para a NSFnet (National Science Foundation’s Network), estabelecendo conexões com outras redes, inclusive aquelas fora dos Estados Unidos, e promovendo a interligação de centros de pesquisa e universidades em todo o mundo (Muñoz e Turner, p.23, 1999).

Entretanto, “o grande marco dessa tecnologia se deu em 1987, quando foi convencionada a possibilidade de sua utilização para fins comerciais, passando-se a denominar, então, “Internet” (Pinheiro, p.40, 2021). Foi nesse ponto que a ARPANET passou a ser reconhecida como a 'internet', sendo predominantemente utilizada como uma plataforma para a troca de informações no ambiente acadêmico.

Cada vez mais, a internet desempenhava um papel importantíssimo na construção social, como afirma Turner e Muñoz (2002, p. 15 apud ABREU, 2009, p. 3), “os gestos definiram a estrutura social do Homem de Neanderthal. A escrita e a pintura definiram o Cromagnon, e o bit definirá o ser Infosocial”.

Ao longo dos anos, a internet e essa rede de computadores foram sendo consideradas instrumentos muito lucrativos, as pessoas começavam a entender como esse novo negócio poderia ser benéfico, principalmente, quando esse sistema de comunicações antes considerado um sistema da elite, naquele momento, tornava-se um sistema de comunicação para a massa, um sistema livre, aberto e sem proprietários (ABREU, 2009, p. 4).

Toda essa relação estava atrelada à ideia de poder social e da liberdade do povo, como se as pessoas que pudessem ter esse acesso a todas as informações disponíveis na internet, pudessem ter um poder e liberdade enorme dentro da sociedade, isto é, esses mecanismos foram sendo usados para lucrar cada vez mais nessas relações sociais.

Em 1995, a internet foi transferida para a administração de instituições não-governamentais, que se encarregam, entre outras coisas, de estabelecer padrões de infraestrutura e funcionamento geral.

> Devido ao grande aumento de usuários no início da década de 90 a internet foi transferida para a administração de instituições não-governamentais, que se encarregam, entre outras coisas, estabelecer padrões de infraestrutura, registrar domínios, etc. Exemplos dessas instituições são a Internet Society, situada nos Estados Unidos, mas atuando no mundo inteiro, e o Comitê Gestor da Internet que atua restritamente no Brasil (Monteiro, 2001).

Assim, a rede mundial de computadores, a internet, torna-se uma ferramenta acessível a toda a população mundial.

No Brasil, as primeiras iniciativas no sentido de disponibilizar a internet ao público em geral surgiram ainda em 1995, através da atuação do governo federal, utilizando o Ministério da Comunicação e do Ministério de Ciência e Tecnologia para implantar a infraestrutura necessária e definir parâmetros para a posterior operação de empresas privadas provedoras de internet no país.

Desde então, a internet no Brasil experimentou um crescimento espantoso. Logo nos anos seguintes a sua chegada, a era digital tornava-se cada vez mais real e próxima, demonstrando que ocorria ali as primeiras etapas na sua

imersão tecnológica. A tecnologia e a informática começavam a ser inseridas nas vidas e nos lares dos brasileiros.

2.1.2 A internet hoje no Brasil

É necessário apresentar e é de conhecimento popular que o computador foi o principal e primeiro veículo de propagação da internet, porém, atualmente é possível utilizá-la nos mais variados tipos de dispositivos. O avançar da tecnologia, principalmente dos Smartphones, proporcionou uma maior presença da internet através dos aparelhos celulares, na vida e no cotidiano da grande massa de pessoas. E devido a essa acessibilidade que o celular se tornou o principal meio de comunicação com internet, fazendo parte da vida de milhões de brasileiros.

Ao abordar a rede mundial, é impossível ignorar o fenômeno que as redes sociais se tornaram. Elas desempenharam um papel significativo no aumento exponencial do acesso à internet, tornando-se quase uma ferramenta essencial para a interação social e a comunicação contemporânea. A facilidade de se conectar, compartilhar e consumir conteúdo através das redes sociais atraiu milhões de pessoas para o mundo digital.

As redes sociais têm revolucionado a maneira como as pessoas se relacionam e interagem online. Proporcionaram um meio para se conectar com pessoas de todo o mundo. A possibilidade de compartilhar pensamentos, fotos, vídeos e experiências em tempo real transformou a comunicação, tornando-a visual e praticamente instantânea.

E também, as redes sociais se tornaram um meio essencial para a disseminação de informações e conteúdo. Partindo de notícias e entretenimento até conscientização sobre causas sociais, as redes sociais desempenham um papel fundamental na formação da opinião da grande massa da população. Portanto, as redes sociais moldam a relação com a internet e o mundo digital, e assim influenciando na forma de viver o cotidiano.

A Pnad (Pesquisa Nacional por Amostra de Domicílios) em parceria com o IBGE (Instituto Brasileiro de Geografia e Estatística), apontam através de pesquisa, que o acesso à Internet, à televisão e à posse de telefone móvel celular para uso pessoal, relativa ao ano de 2021, apresentou um aumento no número de domicílios com internet, chegando a 90,0% dos lares brasileiros. Desses lares, o

celular é o principal dispositivo de acesso, estando presente em 95,5% dos domicílios com disposição à internet (IBGE, 2021).

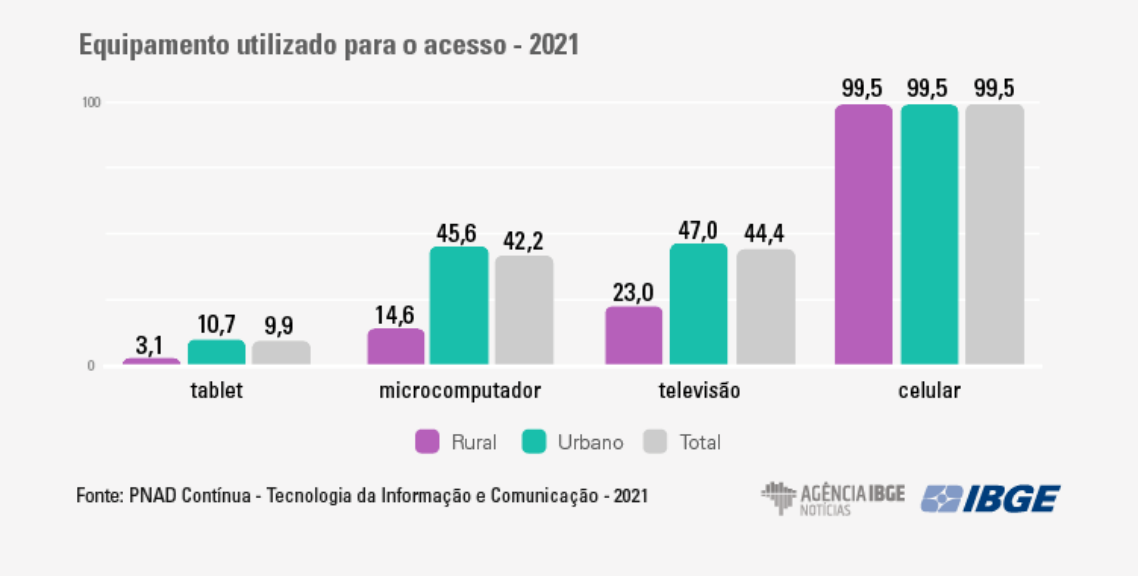

Figura 1: Ranking dos dispositivos mais utilizados nos domicílios para acessar a internet no Brasil.

Além disso, ainda segundo a PNAD, a proporção de pessoas conectadas aumentou em todas as faixas etárias no ano de 2021. Com o destaque para o grupo 60 anos ou mais, que representou o maior crescimento proporcional no levantamento de dados feito, passando de 44,8% para 57,5% (IBGE, 2021).

Uma das possíveis explicações é a pandemia de Covid-19, que teria levado as pessoas a dependerem e acessarem ainda mais a internet, em função das medidas de isolamento social. Seja para realizar atividades de trabalho remoto, ensino à distância, ou até mesmo por entretenimento. Ao todo, 84,7% dos brasileiros utilizaram a internet no período de 2021 (IBGE, 2021). Esse percentual representa cerca de 155,7 milhões de brasileiros presentes no ciberespaço.

2.2 O CIBERESPAÇO

O escritor américo-canadense William Gibson antecipou uma breve ideia da palavra “Ciberespaço” no ano de 1982, na publicação do seu livro “burning chrome”, e posteriormente popularizou o conceito com a publicação do seu romance de ficção científica “neuromancer”, em 1984. Ao utilizar o termo, Gibson escreve:

> Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade se afastando... (Gibson, p. 80).

O termo surge antes mesmo da criação da internet propriamente dita. Designa uma noção de espaço não físico, fruto da civilização ascendente da era pós-industrial.

Para Pierre Lévy, ciberespaço não é apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informação que ela abriga, assim como os seres humanos que navegam e alimentam esse universo (Lévy, p.17, 1999).

Esse espectro que é o Ciberespaço torna possível a ligação entre várias pessoas e várias culturas, contribuindo para a construção de um novo modo de viver e agir. É uma era de inclusão e também de exclusão, a imersão tecnológica nos aproxima do distante e nos distancia do próximo.

Para Singer e Friedman (2014), o ciberespaço, antes de tudo, é um ambiente de informação composto por dados digitalizados que são criados, armazenados e compartilhados, não se tratando de um lugar físico e, portanto, desafiando a medição física. No entanto, não se trata de um ambiente puramente virtual, compreendendo os computadores, os sistemas e toda infraestrutura que permite seu fluxo, incluindo a Internet, redes de computadores, intranets, celulares, cabos de fibra óptica e comunicações baseadas em satélites, como também abrangendo as pessoas por trás desses equipamentos e toda a rede de comunicação que circunda essa estrutura virtual (Singer e Friedman, 2014).

É um universo virtual, porém real, que predispõe inúmeras possibilidades e acontecimentos, e que impacta diretamente no que entendemos como “vida real”. Essa interação, que vai além das telas e dispositivos, tem ditado a forma como as pessoas agem, como se vestem, o que compram, o que ouvem, ou vêem. Dita e influencia o estilo de vida de milhões de pessoas.

A grande presença da internet fez superar obstáculos e apresentou uma facilidade de comunicação, informação, superação de distâncias, oportunidade de trocas, compras e vendas, dentre outros. Os pontos negativos também surgem por

consequência. Os recursos que mantém o ciberespaço apresentam vulnerabilidades que possibilitam que crimes sejam cometidos.

Esse ciberespaço trouxe consequências sociais enormes para o campo do Direito, principalmente, pela constante relação entre Direito e tecnologia, segundo Pinheiro (2009 apud FRANCESCHETTO, 2013), “toda mudança tecnológica é uma mudança social, comportamental, portanto jurídica.”, com isso, a internet continua nessa ideia de existir em um território livre e com uma enorme variedade de interações sociais.

> O ciberespaço constituiu-se como um novo espaço de sociabilidade – apesar de não-presencial – com impactos na esfera cultural e social. O ciberespaço, sendo um espaço sócio virtual – baseado em técnicas informacionais em rede – como espaço social que é, permite a interacção [sic] social.
> [...]
> É no ciberespaço que assistimos a uma união perfeita entre informação, comunicação e tecnologia a que poderemos chamar de cibercultura. Temos de entender a cibercultura como uma manifestação da vitalidade social contemporânea. Não é uma subcultura particular ou a cultura de uma ou algumas “tribos”. Pelo contrário, é uma nova forma de cultura. Não é nem a negação da oralidade nem da escrita, mas sim o prolongamento destas (SILVA, 2002 apud FRANCESCHETTO, 2013).

Nesse sentido, a constituição desse ciberespaço e dessa cibercultura interferem diretamente na construção dos sujeitos em sociedade, principalmente, quando se percebe essa relação tríade de informação, comunicação e tecnologia. Isso faz com que os grupos sociais dos mais variados possam estar em constante comunicação dentro desse espaço e dessa realidade.

Apesar da frequência dos assuntos ligados ao ciberespaço, a internet e os efeitos causados nos cidadãos, grande parte dos juristas e legisladores procuram entender melhor como essas questões estão sendo fundamentadas, associando mecanismos tradicionais que acabam não seguindo a velocidade da internet e criam projetos de leis cada vez mais sem reflexões sobre esse assunto tão presente e importante dentro da sociedade (FRANCESCHETTO, 2013).

Por isso, surge um ramo do Direito que será discutido nos próximos capítulos sobre o “Direito do Ciberespaço”, regulamentações, leis, todo um aparato jurídico que fundamenta e centra suas discussões no envolvimento dessas redes de comunicação com os cidadãos. Assim, urge a necessidade de compreender melhor sobre as discussões tratadas acerca do ciberespaço, esse mundo virtual com uma

infinidade de possibilidades e escolhas com as legislações que permitam a segurança desses usuários e os assegurem de seus direitos.

2.3 AMEAÇAS E VULNERABILIDADES DA TECNOLOGIA

Diariamente, uma variedade exuberante de informações, abrangendo tanto dados públicos quanto privados, é inserida no ciberespaço, onde é arquivada para fins diversos, como divulgação, pesquisa, consulta e preservação. Contudo, por armazenar uma riqueza inestimável de informações e dados, torna-se vulnerável a possíveis invasões e manipulações. E também contando com a malícia dos criminosos, que recorrem a métodos enganosos, com o objetivo principal de persuadir os usuários a tomar ações ou fornecer dados.

Atualmente, é bastante comum a prática de crimes de natureza cibernética, nos mais variados meios e com os mais distintos fins. O ambiente virtual ressignificou, dentre tantas outras coisas, as formas e circunstâncias para a prática de delitos. A empresa de cibersegurança Norton Cyber Security, em parceria com o The Harris Poll, publicou uma pesquisa que mostrou que no ano de 2021 cerca de 71 milhões de brasileiros sofreram algum tipo de ataque cibernético. (EXAME, 2022). Dentre esses, pode-se incluir crimes como roubos de identidade, cyberstalking, pornografia de vingança e cyberbullying.

E falando em vulnerabilidades, há de se falar naquelas especialmente tecnológicas, dentre tantas outras, algumas como a invasão de servidores, pirataria de softwares, malware, e phishing.

Qualquer usuário da rede mundial está suscetível de ser vítima em práticas de invasão ou hackers, um simples link clicado pode dar acesso a todos os seus arquivos ou dados privados. “Os usuários domésticos sofrem um risco menor quando comparados com empresas, pois, mesmo que seus computadores possam ser mais vulneráveis a todo tipo de ataque de hackers ou crackers, geralmente, preferem atacar empresas” (Teixeira, p.70, 2022). Interessante mencionar que muitas vezes os grandes hackers são contratados por empresas ou até mesmo por departamentos governamentais, para prestarem serviços, e essa prestação de serviços é legal. A configuração como crime só ocorre quando não há autorização ou quando há intenção de obter informações.

Quanto a pirataria de software, é “a forma como é conhecida a violação dos direitos de programas de computador” (Teixeira, p.455, 2022). Software é um programa de computador, ou seja, é uma sequência de algoritmos escritos em linguagem de programação, programadas para serem executadas em uma sequência, e quando executados chegam a uma finalidade. No caso do software, é responsável por fazer com que o dispositivo funcione, dando a funcionalidade através de operações. Nesse contexto, a Lei. 9.609/98, conhecida como Lei do software, legisla sobre

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

De forma que cada sequência é uma criação, tal qual uma obra literária, tanto que é conferido ao autor do programa o direito autoral da sua programação. Também da Lei do software

> Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

Assim, a pirataria de softwares consiste na violação do direito autoral, reprodução ou cópia ilegal do programa. Além dos direitos do autor, esses programas pirateados estão suscetíveis a controles ou alterações clandestinas na intenção de prejudicar aquele que o reproduz ou utiliza. Por isso, não obstante do respeito ao direito do criador do software, é uma questão de segurança. Esses softwares ganham o nome de malware, tem a mesma conceituação, só que a diferença está no objetivo calculado através do código de programação.

Para a McAfee, uma das maiores empresas de cibersegurança do mundo, malware “é um termo genérico para qualquer tipo de software malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável” (McAfee, 2023). Os criminosos cibernéticos costumam usá-lo para extrair dados ou informações daqueles que foram afetados, na maioria dos casos com finalidade de obter ganhos financeiros. Os vírus são um tipo de malware, que possuem diversas ações para infectar o dispositivo.

Já a técnica do phishing consiste em golpes disfarçados de fontes confiáveis, que utilizam disso para facilitar o acesso a todos os tipos de dados confidenciais (Microsoft, 2023). Utilizam da interface ou de informações fazendo parecer que são parte de alguma coorporação ou órgão governamental, e através disso furtam informações pessoais, dados ou dados de cartão de crédito, por exemplo.

São inúmeras as formas de violações cibernéticas, e o combate é superiormente difícil, tanto em investigação como em estrutura e preparação adequadas. Legislar sobre é um desafio, visto que a legislação não consegue acompanhar o compasso evolutivo da era digital, então para chegar a um passo de segurança e de aparato adequado, é necessário a utilização das mais diversas áreas do direito, abarcando assim a maior quantidade de condutas tipificadas. Alguns autores defendem que o Direito Digital é o futuro próximo do direito, e que não trata de um ramo, mas sim, abarca vários ramos do Direito para legislar com propriedade sobre o que acontece no digital.

3 OS CIBERCRIMES

Para Greco, o crime remete a “um fato típico, ilícito e culpável” (Greco, 2016, p. 199), o crime pode ser entendido a partir das suas características e delimitado de acordo com a conduta praticada. Com isso, antes de falar de cibercrimes, é necessário conceituar o fenômeno “crime” em si, a partir de duas concepções: a de caráter formal e a de caráter substancial

> A primeira atém-se ao crime *sub especie iuris*, no sentido de considerar o crime 'todo o fato humano, proibido pela lei penal'. A segunda, por sua vez, supera este formalismo considerando o crime 'todo o fato humano lesivo de um interesse capaz de comprometer as condições de existência, de conservação e de desenvolvimento da sociedade (Bettiol, p. 209, 2000 apud Greco, p.196, 2016).

Outra concepção que atua em conjunto com o entendimento de crime pode ser definida como “todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social” (Capez, 2011, p. 134). É uma atitude delitiva que esbarra no direito alheio ao ser, gerando uma conduta ilegal.

No que refere a essas condutas, mais especificamente ocorridas no meio digital, denomina-se cibercrime. Para Helena Carrapiço, “é a denominação dada a um conjunto específico de crimes relacionados com a utilização de computadores e de redes informáticas”. Que indo além, a autora define ainda que esta expressão pode igualmente ser empregue no que se refere “à facilitação de atividades ilegais tradicionais através do recurso a meios informáticos” (Carrapiço, 2005, p.181).

Nesse sentido, o cibercrime é a nomenclatura dada tanto àquele crime de atividade tecnológica, onde o bem jurídico protegido é unicamente ligado à tecnologia, quanto àquele onde a utilização da rede mundial é apenas um fator facilitador. Na primeira hipótese, poderia se exemplificar com a invasão a um banco de dados virtual, onde a prática envolve a exclusividade do tipo. Enquanto na segunda hipótese, seriam exemplos os crimes contra a honra, visto que esses crimes já ocorreriam fora do ambiente virtual, porém, quando praticado na internet, torna-se também em um crime virtual.

Em conformidade com esta conceituação, Júlio César Alexandre Júnior (2019. p. 343), diz que “o cibercrime está associado ao fenômeno da criminalidade

informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para a prática do crime ou como elemento de tipo legal de crime". Partilhando de ambos os vieses, esse será o conceito utilizado ao longo desta monografia quando referindo aos cibercrimes. Crimes cibernéticos, cibercrimes, crimes virtuais ou crimes digitais, serão tratados como sinônimos ao decorrer desta monografia.

No Brasil, são datadas notícias sobre crimes cibernéticos desde o século passado, em 1999 foi noticiado um crime cibernético que tratava uma ocorrência de phishing scam bancário, uma espécie de "pescaria de senhas" (Jesus, p.21, 2016). Para a reportagem, suspeitava que o autor havia cometido ao menos seis transferências de contas correntes, de cinco bancos privados, de maneira irregular e através da internet (Folha, 1999).

Esses crimes cibernéticos estão ganhando força no contexto social, resultando em um aumento significativo no número de vítimas desses golpes, onde vários fatores contribuem para esse cenário preocupante. Em primeiro lugar, o aumento constante do tráfego na internet e o crescente número de pessoas, o que amplia o rol de potenciais alvos para os criminosos cibernéticos. Quanto mais pessoas estiverem conectadas, mais oportunidades os infratores têm de explorar vulnerabilidades.

E ainda, a multiplicação de sites maliciosos com intuito de roubar informações pessoais e financeiras dos usuários contribui para o aumento desses crimes. Muitos desses sites são projetados para se parecerem com as plataformas legítimas, o que torna ainda mais difícil para os usuários identificar entre o que é seguro e o que é perigoso online.

Porém, à medida que os crimes cibernéticos se tornam mais comuns, também estão surgindo medidas de segurança mais sofisticadas para proteger os usuários contra possíveis golpes. Isso inclui a implementação de firewalls avançados, software antivírus, autenticação de dois fatores e programas de conscientização digital. Empresas e órgãos governamentais estão visando a importância e investindo em tecnologias e recursos para fortalecer a cibersegurança e educar o público sobre os riscos associados ao uso da internet.

Ainda que os desafios relacionados à segurança cibernética continuem a evoluir, também é esperançoso observar a crescente conscientização sobre esses problemas e os esforços para proteger os usuários no ciberespaço. O equilíbrio

entre o aproveitamento das oportunidades oferecidas pela internet e a proteção contra as negativas é um desafio contínuo, onde é necessário sempre conhecimento e evolução.

Em 1998, através do julgado do HC 76.689-0/PB, relatado pelo Ministro Sepúlveda Pertence, o Supremo Tribunal Federal enfrentava um caso envolvendo pornografia infantil num antigo sistema de interface, parecido com a internet. (Jesus, p. 22, 2016). O Ministro, em relatório, entendeu que nem todos os delitos cibernéticos precisavam de uma nova tipificação, que bastava a realização do núcleo da ação punível.

> Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. (STF, 1998.)

Seguindo nesse mesmo compasso, 25 anos depois , ainda há de se mencionar a pequena legislação específica para crimes virtuais, apesar de apresentar avanços com a criação de algumas leis, que veremos no decorrer da monografia.

3.1 QUANTO A CLASSIFICAÇÃO

A título de classificação, Wendt e Nogueira apontam essas condutas indevidas praticadas por computadores ou dispositivos móveis em “crimes cibernéticos” e “ações prejudiciais atípicas”. Classificando ainda, os crimes cibernéticos em abertos ou exclusivamente cibernéticos (Wendt e Nogueira, 2020).

3.1.1 Ações prejudiciais atípicas

As ações prejudiciais atípicas são aquelas onde a conduta praticada, por intermédio dos dispositivos informáticos, causa algum tipo de prejuízo para a vítima, porém, não existe uma previsão penal para puni-la (Wendt e Nogueira, 2020).

Desse modo, devido à inexistência de normas que assegurem esses direitos, as pessoas ficam à mercê desses crimes, sem que haja uma legislação adequada para lidar com esses problemas na sociedade brasileira.

A título de exemplificação, o Código Penal brasileiro torna ilegal algumas condutas envolvendo dispositivo informático de uso alheio, conectado ou não à internet.

> art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Brasil, 1940).

No entanto, apesar da possibilidade de responsabilização pelo Direito Civil, o indivíduo que invade o computador de um conhecido sem objetivo de cometer nenhuma das ações nucleares do art. 154-A do Código Penal, não seria criminalmente punido, visto que não se adequaria a nenhum dos elementos. Então, entende-se que “ações prejudiciais atípicas” são aquelas que apesar de causar prejuízo à vítima, não resultam em sanção na esfera penal, por não existirem leis tipificando tais condutas.

3.1.2 Crimes cibernéticos abertos

Para a classificação dos crimes cibernéticos abertos, "são aqueles que podem ser praticados da forma tradicional ou por intermédio de dispositivos informáticos, ou seja, o dispositivo é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele" (Wendt e Nogueira, 2020).São aqueles que poderiam ocorrer ocasionalmente sem o uso de quaisquer tipos de tecnologia, mas que na oportunidade são praticados através do advento informático.

A título de exemplificação, o crime de ameaça, o Código Penal tipifica o ato de “Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave” (Brasil, 1940). É um delito existente antes mesmo do advento da internet, mas que independente do meio no qual ocorre, é abrangido pela legislação do Código Penal. Sendo assim, a ameaça feita através da internet ou das redes sociais continua incumbido no delito do art. 147 do CP.

3.1.3 Crimes cibernéticos exclusivos

Diferentemente dos abertos, “estes são os que somente podem ser praticados com a utilização de dispositivos informáticos” (Wendt e Nogueira, 2020). Nessa classificação de cibercrimes a utilização do meio digital faz parte da ação nuclear do crime.

Utilizando para exemplificar a classificação, os autores acima mencionados apontam o crime de aliciamento de crianças praticado por intermédio de salas de bate-papo na internet:

> art. 244-B. Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la:
>
> § 1 º Incorre nas penas previstas no **caput** deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet. (Brasil, 1990)

O artigo do Estatuto da Criança e do Adolescente tipifica a conduta específica do aliciamento através do uso de salas de bate-papo online, tornando essencial a utilização do meio virtual para a tipificação no §1° do art 244-B, desta forma, é exclusivamente cibernético.

3.2 A ADAPTAÇÃO DOS CRIMES AO CYBER

Muitos dos crimes já existentes podem ser praticados pela internet, isso porque as características do tipo penal se referem à conduta, e não necessariamente à maneira em que se deu o fato. Com o avanço digital alguns delitos que eram praticados de maneira “tradicional” passaram a utilizar o meio virtual como ferramenta base para a nova prática em novos espaços, causando alterações nas leis e até categorizando algumas condutas com sua versão “cyber”.

A título de exemplificação, um crime que apresenta uma vertente cibernética é o crime de Cyberstalking. Diferente do crime de Stalking, ou “Perseguição” como no Código Penal, as condutas do cyberstalking são realizadas exclusivamente pela internet

> Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade (Brasil, 1940).

O Stalking, que anteriormente era considerado apenas contravenção penal, foi acrescido ao Código Penal, passando a fazer parte do rol de crimes da Lei 2848/40, a alteração foi feita pela Lei 14.132/21 e aumentou também a pena nos casos de condenação. O cyberstalking tem as mesmas características do stalking, mas esse é previsto e ocorre exclusivamente através da internet ou de instrumentos informáticos, seja através de emails, redes sociais, invasão de webcam ou outros tipos… Por se tratar de uma vertente, o Cyberstalking incorre no delito de Perseguição, previsto no art. 147- A do Código Penal.

Outra classe de crimes tradicionais ao Código Penal que se expandiu no ambiente virtual foi a dos crimes contra a honra, tipificados nos arts.138, 139 e 140 do CP. Pinheiro diz que “o anonimato associado à impunidade faz aumentar a agressividade e a violência entre as pessoas dentro da Internet, especialmente no que diz respeito aos crimes contra a honra” (Pinheiro, 2021, p.63). Motivo pelo qual,através da Lei 13.964/2019, o §2° do art 141 foi alterado para punição com o triplo da pena nos casos em que o crime é cometido ou divulgado em qualquer modalidade de rede social da internet (Brasil, 1940).

Um caso clássico de ocorrer na internet é no tocante a violação de direitos autorais

> A violação de direitos autorais na internet se dá em especial quanto às pulverizações de obras literárias, científicas e artísticas (principalmente músicas e livros), por meio da disseminação dos respectivos arquivos com o áudio, vídeo, texto, fotos (especificamente sobre a ilicitude da pirataria de software, discorreremos adiante) (Texeira, 2022, p.451)

O que fica evidente é que os direitos autorais são particularmente vulneráveis à violação por meio eletrônico, especialmente na internet. No entanto, é inquestionável que a legislação deve se aplicar quando ocorre violação de direitos autorais em ambiente virtual, inclusive que sejam aplicadas as disposições penais previstas.

Tratando ainda dos casos que podem ocorrer no ambiente digital, há casos de inclusão na lei, como a fraude eletrônica e o furto mediante fraude por meio de dispositivo eletrônico, presentes nos artigos 171, § 2°- A e 155, §4º- B do Código Penal, respectivamente. Essas alterações, promovidas pela Lei 14.155/2021, ocorreram com o intuito de tornar mais graves as penas dos crimes contra o patrimônio quando cometidos de forma eletrônica.

E tratando de crimes contra o patrimônio, representa um bom exemplo de como a internet pode se tornar um meio facilitador para esse tipo de infração, pois, segundo informações publicadas pelo Anuário Brasileiro de Segurança Pública, em 2022 a quantidade de casos de estelionato digital passou de 200,3 mil golpes no Brasil, uma variação de 65% em comparação com o ano de 2021 (União, 2023).

Em decorrência desses e de outros delitos ocasionados de maneira digital, o ordenamento jurídico necessitou de apresentar algumas respostas para maior segurança virtual, assim criando leis específicas para alguns crimes específicos que precisavam de maior aparato judicial. Isso resultou na criação de leis específicas projetadas para lidar com crimes que apresentam características exclusivas quando cometidos online, que desempenham papel fundamental na adaptação do sistema legal às complexidades do mundo digital, buscando responsabilizar os infratores.

4 DIREITO DIGITAL

Na concepção de Marcelo Barreto de Araújo, o Direito se desenvolveu, em grande parte, pelo conflito de liberdades, ou seja, cada indivíduo tem sua esfera de liberdade limitada à esfera de outrem (Araújo, p.19, 2017). E é essa ligação que resultou no que conhecemos hoje como Estado Democrático de Direito, onde “cada pessoa exerce legitimamente seus direitos, com as garantias jurídicas a eles inerentes, respeitados os direitos das demais pessoas e o funcionamento das instituições públicas e privadas” (Araújo, p.19, 2017).

Numa sociedade de normas jurídicas e direitos irrenunciáveis, a liberdade começa e termina pelas mesmas fontes. O ordenamento que dá como direito a liberdade é o mesmo que a limita, e que é necessária essa limitação, diga-se de passagem.

> “Taken in its broadest sense this means people should obey the law and be ruled by it. But in political and legal theory it has come to be read in a narrower sense, that the government shall be ruled by the law and subject to it” (Raz, p. 212, 1979).

Em tradução livre, Joseph Raz diz que: “em sentido mais amplo, as pessoas devem obedecer a lei e serem reguladas por elas. Mas em uma teoria política e legal isso deve ser lido em um sentido mais restrito, que o governo deve ser regulado pelas leis e submetido a elas”. Em um Estado que concede ao cidadão o status de sujeito de direito, proporcionando-lhe uma esfera de proteção e de limites impostos a ele, a autocontenção implica um respeito pelo direito de terceiros, e cabe também a contenção àqueles que a regulam.

Na presença de normas jurídicas, a conduta humana adquire, em certos aspectos, um caráter obrigatório, deixando de ser uma escolha. Patrícia Peck quando se referiu ao Estado de Direito disse: “tem como princípio fundamental a liberdade do homem, sendo seus estatutos concebidos para adequar, dentro do ordenamento jurídico-social, os conceitos basilares que limitam essa liberdade, conferindo ao cidadão um direito subjetivo e irrenunciável” (Pinheiro, p.36, 2021).

> Compete ao Sistema Legislativo fazer o filtro de todas as valorações e expectativas de comportamento da sociedade, mediante processos decisórios, para que elas possam adquirir validade jurídica. A capacidade da norma de refletir a realidade social determina o grau de eficácia jurídica de um ordenamento. Eficaz é aquilo que é capaz

> de efetivamente produzir efeitos, ou seja, o conceito de eficácia envolve aceitação e obediência (Pinheiro, p. 36, 2021).

A Constituição Federal brasileira definiu no art 1°, caput, que “a República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito” (Brasil, 1988). Dessa forma, há o Brasil que apresentar um direito legítimo, constitucional e que respeite a democracia do povo brasileiro.

> Significa, portanto, não apenas aquele que impõe a submissão de todos ao império da mesma lei, mas onde as leis possuam conteúdo e adequação social, descrevendo como infrações penais somente os fatos que realmente colocam em perigo bens jurídicos fundamentais para a sociedade (Capez, p.78, 2020)

Significa, portanto, que o Brasil adota um sistema com conteúdo social, onde se procura uma igualdade entre todos, não apenas uma submissão de todos sob a mesma lei, mas que esta lei possua um valor social, onde o princípio da dignidade humana caminha com o Direito Penal. E, ainda, como democracia, regulando o poder dos que estão representando o povo, para que não se crie um autoritarismo.

Para uma norma ser eficaz ela precisa gerar efeitos positivos, ser obedecida e cumprida pela sociedade. Nesse contexto, entra o dever do Direito Digital (e do Direito como um todo) de se adaptar à realidade social e de criar normas que deem segurança, de uma maneira eficaz, a todos inseridos naquele espaço (ou do ciberespaço).

Na explicação de Patrícia Peck Pinheiro sobre o Direito Digital

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.) (Pinheiro, 2021, p.49).

Ou seja, não se trata de uma área, mas sim da evolução do Direito onde as mais diversas áreas jurídicas são aplicadas sob o bem que está sendo tutelado digitalmente. Chegando assim, a conclusão que trata-se da aplicação de todas as áreas já existentes, porém fazendo parte do meio tecnológico moderno.

Araújo conceitua o Direito Digital como “uma nova disciplina jurídica que consiste na incidência de normas jurídicas aplicáveis ao chamado ciberespaço, num

reconhecimento de que a legislação e a doutrina jurídica tradicionais são insuficientes para regular as relações no mundo virtual" (Araújo, 2017, p.21). Essa disciplina, mais que as outras, têm de apresentar uma dinâmica diferente, e tem como referência preencher as lacunas que ainda não foram preenchidas.

Para José Eduardo Pimentel, o Direito Digital nasce a partir da necessidade de se regular questões surgidas com a evolução da tecnologia e da internet, elementos esses que são responsáveis por profundas mudanças comportamentais e sociais, bem como para fazer frente aos novos dilemas da nova sociedade, que o autor denomina como "sociedade da informação" (Pimentel, 2018, p.3).

> Seja aplicando as leis atuais, seja recorrendo ao mecanismo da analogia, dos costumes e dos princípios gerais de direito, o Direito Digital tem o dever de regulamentar essas relações e intermediar os conflitos gerados por elas (Pinheiro, p.52, 2021)

A lacuna existente no Direito convencional em relação ao mundo digital resulta do fato que a norma está constantemente perseguindo os acontecimentos, quando o progresso tecnológico está a todo momento acontecendo. Apesar de aparentar ser uma nova disciplina jurídica, utiliza-se dos princípios e da legislação que vigora no Direito costumeiro, as leis em vigor são aplicáveis a maioria das matérias que existem, o que pode preencher eventuais lacunas é a forma de interpretá-las.

O Direito Digital não é apenas o Direito da Internet, é a evolução do Direito em si, onde a Internet é um novo recurso tecnológico que está presente massivamente na população, e apresenta demandas jurídicas a serem legisladas. Nesse sentido, a natureza dinâmica do Direito Digital, para resolver os conflitos trazidos, recorre a interpretações análogas e aplicação do Direito convencional, levando em consideração as práticas e costumes observados atualmente.

Em termos de legislação propriamente pensada ao digital, ainda existem poucas aprovadas nos últimos anos, mas que podemos citar as que serão explicitadas posteriormente nesta monografia: a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. Dito isso, a era digital já é uma realidade, e embora o Direito Digital ainda tenha que caminhar a passos largos, vem se mostrando como um ramo fundamental para a continuação dessa era.

Para Patrícia Peck, as características do Direito Digital são “a celeridade, dinamismo, autorregulamentação, poucas leis, base legal na prática costumeira, o uso da analogia e solução por arbitragem” (Pinheiro, p.52, 2021). Auto explicativas e familiares são as expressões usadas pela autora, o Direito Digital não se distancia tanto do costumeiro, porque trata-se de uma renovação na forma de compreendê-lo, uma releitura do Direito frente ao impacto que a internet causou na sociedade, de modo que deve refletir as grandes mudanças culturais e comportamentais causadas.

Seu principal desafio é se adaptar de maneira perfeita às diversas culturas, o que requer a criação de flexibilidade no pensamento, em vez de estar vinculado a uma legislação codificada e engessada que pode se tornar obsoleta rapidamente. Para não cair nessa obsolescência, o Direito Digital compartilha dos vieses legislativo e interpretativo, o primeiro sobre a criação de leis que regulamentem as consultas ocorridas no ciberespaço que ainda não estão tipificadas, o segundo para a aplicação das leis que já tipificam as situações que podem ocorrer online.

4.1 DA LEGISLAÇÃO ESPECÍFICA

A maioria dos crimes cometidos na internet também ocorre no mundo físico, a internet funciona principalmente como um fator facilitador. As principais inovações legais no contexto legal digital dizem respeito à questão da territorialidade, à investigação de provas e à necessidade de criar tipificações específicas para certas modalidades de crime que, devido às suas características particulares, requerem a definição de tipos penais próprios.

O aumento dos crimes na internet, que muitas vezes espelham crimes no mundo físico, é facilmente atribuível à relativa impunidade que a web pode oferecer. A sensação de anonimato proporcionado pela internet pode encorajar alguns indivíduos a cometerem atos ilícitos que talvez não realizariam no mundo real.

No contexto do Direito Penal Digital, as inovações legais concentram-se na necessidade de lidar com questões de territorialidade, já que a internet ultrapassa qualquer tipo de fronteira, tornando complexa a determinação de qual jurisdição deve tratar um caso específico. Além disso, a investigação de provas no ambiente

digital requer métodos e técnicas especiais, dadas as peculiaridades das evidências eletrônicas.

Outro aspecto importante é a tipificação de crimes específicos no âmbito digital. Muitas vezes, as práticas criminosas na internet têm características únicas que justificam a criação de tipos penais específicos para abordar adequadamente essas atividades, proporcionando uma base legal sólida para processar os infratores. Por isso, à medida que a tecnologia e a sociedade evoluem, o Direito Penal Digital continua a tentar essa adaptação para enfrentar os desafios emergentes e garantir a justiça no ciberespaço.

Além disso, o Direito Digital apresenta um princípio normativo, a autorregulamentação, que consiste no deslocamento do eixo legislativo para os participantes e interessados diretos na proteção de determinado direito e na solução de determinada controvérsia. Ou seja, o Direito Digital possibilita uma via alternativa, que não a via legislativa, para criar regras de conduta para a sociedade digital, sendo elas ditadas e determinadas pela própria sociedade (Pinheiro, 2021, p.80).

O princípio orientador da autorregulamentação reside em legislar com a menor quantidade possível de burocracia, respeitando estritamente a Constituição e as leis em vigor. Tornando possível uma maior adaptação do direito à realidade social, bem como almejando uma maior agilidade e flexibilidade para garantir sua eficácia ao longo do tempo. A tendência à autorregulamentação representa uma das abordagens mais adequadas para atender à crescente demanda do Direito Digital, não apenas no sentido de aplicar as normas, mas também no sentido de demonstrar a dinâmica para acompanhar o ritmo das mudanças na sociedade digital

4.1.1 Marco Civil da Internet e a LGPD

Para a tecnologia, o que será descoberto amanhã já está obsoleto, por isso que uma das áreas que mais passa por transformação no Direito é a que regulamente sobre ela. Nesse sentido, a Lei n.12.965 de abril de 2014, conhecida como “Marco Civil da Internet”, estabelece uma proteção jurídica regulando as relações de uso da Internet

> art. 1º. Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para

> atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (Brasil, 2014).

Dessa forma, Teixeira define o “Marco Civil da Internet” como a demarcação dos direitos do cidadão quanto ao uso da rede mundial de computadores, especialmente no âmbito brasileiro. O autor aduz da lei de 2014 os três princípios basilares: a garantia à liberdade de expressão, a inviolabilidade da privacidade e a neutralidade do uso da internet (Teixeira, 2022, p. 91).

O primeiro dos pilares, sendo um direito assegurado pela Constituição, assegura “a livre expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença” (Brasil, 1988). No mesmo compasso, o segundo pilar também representa um direito constitucional, garantindo que sejam 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). Por sua vez, para a Lei do Marco Civil, a neutralidade implica em dizer que o “responsável pela transmissão ou roteamento deverá tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação” (Brasil, 2014).

A Lei Geral da Proteção de Dados, com a alteração feita pela Lei 13.853/2019, passa a ter papel no ordenamento para dispor

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

É de cunho da LGPD defender uma série de princípios essenciais para a proteção da privacidade e dos dados pessoais. Teixeira diz que “o objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, por meio da premissa da boa-fé para todo o tipo de tratamento de dados pessoais” (Teixeira, 2022, p.284). Tem de ser clara a finalidade, a necessidade e a proporcionalidade, com que são exigidos os dados, e que sejam coletados para fins legítimos, explícitos, havendo uma relação direta entre a finalidade e a quantidade de dados coletados.

Dessa forma, cabe a difícil tarefa do legislador equilibrar a relação entre a liberdade de expressão e o direito à privacidade com a responsabilização dos atos e dos danos que o indivíduo venha a causar, de forma que se extinga a sensação de internet como sendo uma terra sem lei, discernindo que "há limites naturais ao direito à privacidade quando atinge interesses coletivos" (Pinheiro, 2021, p.61).

4.1.2 Lei Carolina Dieckmann

A Lei n° 12.737, de novembro de 2012, conhecida como Lei Carolina Dieckmann, incluiu a tipificação de crimes virtuais e delitos informáticos no Código Penal (Brasil, 2012). Em vigor há mais de 10 anos, a Lei Carolina Dieckmann foi a primeira lei brasileira a punir crimes cibernéticos.

Popularmente conhecida por esse nome, a Lei leva o nome da atriz brasileira Carolina Dieckmann, conhecida nacionalmente por interpretar papéis novelescos. Em 2011 ela teve sua intimidade violada, quando invadiram o seu computador pessoal e divulgaram 36 fotos íntimas depois da atriz não ceder à extorsão dos criminosos (Rádio Senado, 2023). Carolina, que leva uma vida pública, teve sua intimidade invadida, e foi extorquida para que suas fotos não fossem divulgadas na internet, ao não ceder à extorsão, teve suas fotos publicadas.

Com grande discussão e repercussão do caso, no mesmo ano, seis deputados federais apresentaram uma proposta para tratar sobre invasões de dispositivos eletrônicos e o uso de alguma informação obtida através desta. (Rádio Senado, 2023) Dessa maneira, ressaltando a necessidade de medidas de combate relativas à privacidade e aos dados pessoais na internet.

As penas para os crimes previstos na Lei Carolina Dieckmann tiveram um aumento em 2021, através da Lei 14.155/21 que alterou o Código Penal para "tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet" (Brasil, 2021).

Dessa forma, é possível observar que existem algumas ações de enfrentamento ao cibercrime no ordenamento jurídico brasileiro, principalmente no tocante à privacidade e proteção de dados. Porém, o ciberespaço é de tamanho e possibilidades incontáveis, onde são praticados das mais diversas formas os crimes das mais diversas áreas. Como forma de contenção, e no intuito de oferecer maior

segurança jurídica para a sociedade, é necessária a atuação e consolidação do Direito Digital.

4.2 CONVENÇÃO DE BUDAPESTE

Atualmente, estamos diante de novos comportamentos e de práticas antigas que demandam uma nova abordagem punitiva. Por isso, é imprescindível uma atualização sólida no que tange aos delitos eletrônicos. Nesse sentido, foi promulgado pelo Governo Federal em 2023, através do Decreto n° 11.491, a Convenção sobre o crime cibernético, firmada em Budapeste.

Através dessa aderência à Convenção de Budapeste as autoridades brasileiras passam a ter à disposição um novo instrumento para auxiliar nas investigações de crimes cibernéticos, bem como de outras infrações penais que exijam a obtenção de provas eletrônicas ou digitais armazenadas em territórios estrangeiros. Além disso, a convenção também incentiva o Governo Federal a expandir e desenvolver sua política diante a criminalidade no ciberespaço.

Para Teixeira, a Convenção de Budapeste representa “ uma espécie de força internacional de combate ao crime cibernético ”. A Convenção dos Cybercrimes conta com a participação de grande parte do continente europeu, além de países como Estados Unidos, Coreia do Sul e Canadá. Dentre esta rede, ainda há a presença de empresas como a Microsoft, e investigadores e juristas de mais de 40 países (Teixeira, 2022, p.472). Assim sendo, envolve os esforços e a cooperação de grandes potências mundiais e especialistas da área cibernética, unidos no intuito de facilitar a investigação e obtenção de provas digitais armazenadas nos territórios estrangeiros aliados.

A convenção de Budapeste foi promulgada pelo Conselho Europeu em 2001, o Brasil foi convidado a juntar-se em 2019, tendo sido aprovada a sua adesão em 2021 e publicado o decreto de promulgação em 2023. É do preâmbulo:

> Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às

> referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável (Convenção de Budapeste, 2001).

Em suma, a Convenção de Budapeste trata-se de do primeiro tratado internacional sobre os cibercrimes, elaborado pelo Comitê Europeu. O documento visa o combate e o apoio para enfrentar os principais crimes cometidos através da internet. Em torno de 66 países já assinaram o tratado e cerca de 158 usam como meio de orientação para suas legislações nacionais (Agência Senado, 2021).

Muito se discutiu acerca da necessidade do ingresso ou do Brasil a essa Convenção, visto que há uma importante legislação sobre o assunto que está em vigor no Brasil, que é o Marco Civil. O governo federal considerou necessária a entrada, visto que apesar do grande aparato legislativo e da estrutura que o MCI criou, os meios digitais não apresentam fronteiras territoriais, e que essa seria uma importante ferramenta de cooperação entre países estrangeiros (Agência Senado, 2021).

4.3 DA RESPONSABILIDADE CIVIL E DANO MORAL

Gonçalves (2017, p.557) diz que ““responsabilidade” origina-se do latim *re-spondere*, que encerra a ideia de segurança ou garantia da restituição ou compensação do bem sacrificado. Teria, assim, o significado de recomposição, de obrigação de restituir ou ressarcir”. É a prerrogativa de responsabilizar alguém por algum ato danoso praticado, moral ou patrimonialmente.

Na era da sociedade digital que segue em constante evolução, a responsabilidade civil enfrenta mudanças substanciais. O ciberespaço, um espaço global e sem limitações de tempo ou lugar, redefine os valores a serem preservados, independentemente da localização das partes envolvidas. No campo do Direito Digital, a responsabilidade civil está passando por uma revisão e adaptação, introduzindo alterações nos conceitos tradicionais de culpa e risco (Pinheiro, 2021, p.305).

A teoria do risco assume uma maior relevância no Direito Digital, uma vez que, na era da Internet, o potencial para causar danos indiretos é significativamente maior do que os danos diretos. Portanto, a responsabilidade é estabelecida mesmo

na ausência de culpa, baseada no princípio de equilíbrio de interesses e equidade. Além disso, o Direito Digital considera o nível de conhecimento necessário para os prestadores de serviços e os usuários, impedindo que qualquer uma das partes alegue sua própria negligência

Quanto à aplicação aos cibercrimes, a dificuldade está no tocante à responsabilização do agente causador de danos, tendo em vista a árdua tarefa investigativa, de localizar, processar e processar devidamente aquele que causou (Teixeira, 2022, p.311).

Um ponto crítico é a responsabilidade pelo conteúdo na Internet, uma vez que a Internet é uma plataforma fundamental para a liberdade de expressão e a disseminação de informações. Questões sobre a responsabilidade dos provedores de conexão e aplicação e os limites dessa responsabilidade estão em constante debate. O Marco Civil da Internet, por exemplo, influenciou significativamente essa discussão, priorizando a liberdade de expressão e impondo restrições à remoção de conteúdo sem ordem judicial. Além disso, a discussão sobre danos morais na Internet é complexa, pois o ambiente digital amplia a capacidade de causar danos, e a lei ainda está em processo de adaptação para lidar com essa realidade (Pinheiro, 2021, p.306)

Todavia, a introdução de limitações técnicas para a remoção de conteúdo, como previsto pelo Marco Civil da Internet, levanta preocupações sobre a capacidade de garantir a proteção das vítimas de conteúdo ofensivo e ilícito. Há um desafio em buscar o justo entre a proteção da liberdade de expressão e a responsabilização por conteúdo prejudicial.

4.4 DAS FORMAS DE RESOLUÇÃO DE CONFLITOS

O Estado não é detentor absoluto da resolução de conflitos, é possível que seja feita de formas extrajudiciais, sendo estas admitidas pelo Direito – inclusive incentivadas pelo ordenamento jurídico. Tais formas de resolução, de acordo com Neves (2018, p. 61) são chamadas de “equivalentes jurisdicionais” ou “formas alternativas de resolução de conflitos”.

A solução alternativa dos conflitos não é realmente uma questão alternativa no mundo digital, é uma das únicas vias sustentáveis dentro da velocidade de mudança imposta pela tecnologia. Isso devido apresentarem soluções

mais céleres e eficientes para resolução de questões, por isso, é necessária aplicação da mediação e arbitragem no Direito Digital (Pinheiro, 2021, p.78).

Na ótica de Patrícia Peck

> Para o Direito Digital não existe melhor forma de resolução de conflitos que o uso dos mecanismos legais de arbitragem e mediação. As vantagens do juízo arbitral vêm ao encontro das necessidades geradas pelas novas formas de relacionamento na sociedade digital, principalmente no tocante à celeridade dos processos e ao conhecimento específico envolvido em cada caso (Pinheiro, 2021, p.330).

De acordo com Neves (2018, p. 66) a arbitragem é “antiga forma de solução de conflitos fundada, no passado, na vontade das partes de submetem a decisão a um determinado sujeito que, de algum modo, exercia forte influência sobre elas”. E atualmente, a arbitragem segue figurando como uma das principais formas de resolução alternativas do Direito, sendo disciplinada pela Lei 9.307/1996.

A arbitragem refere-se ao método em que a decisão é feita por árbitro que ocupa posição neutra entre as partes e que não está munido de poder Estatal ou faz parte de quaisquer quadros públicos do Poder Judiciário. É praticada de forma que as partes envolvidas deverão escolher um terceiro de confiança de ambas as partes, terceiro este que ficará responsável pela resolução efetiva do conflito em questão. A decisão desse terceiro será impositiva, ou seja, tal resolução não dependerá da vontade das partes envolvidas.

Mais uma vez referenciando à um dos principais nomes do Direito Digital

> A arbitragem permite que as partes não só definam a jurisdição, uma vez que a arbitragem pode ser também internacional, mas também a legislação aplicável ao caso, a inclusão de uma cláusula arbitral nos contratos eletrônicos seria a melhor maneira de resolver eventuais litígios (Pinheiro, 2021, p.331).

A arbitragem oferece às partes a oportunidade de selecionar as normas e os fundamentos legais a serem utilizados para resolver um conflito, permitindo que elas determinem a legislação apropriada para a resolução de uma disputa específica, com base em convenções comerciais, práticas aceitas ou mesmo o discernimento imparcial do árbitro sobre o que é justo para a decisão.

No mundo digital os litígios podem ser longos, então esse é um instituto perfeitamente adequado, destacadas a eficiência e a celeridade que são características da arbitragem.

Quanto à figura da mediação, trata-se de “um procedimento extrajudicial que tem por fim a solução de conflitos por intermédio de um terceiro imparcial e não interessado no desfecho” (Teixeira, 2022, p.546). O principal papel do mediador consiste em restabelecer e simplificar a comunicação entre as partes envolvidas, que foi prejudicada devido ao conflito, com o propósito de ajudá-las a encontrar um ponto de acordo.

Tanto a arbitragem como a mediação podem ser utilizadas para a resolução de litígios decorrentes de conflitos ocorridos no digital, e ainda podem utilizar das ferramentas tecnológicas para tal. Como por exemplo, a realização de videoconferência, o aplicativo do PROCON, a plataforma Sistema de Mediação Digital, dentre tantos outros meios.

4.5 TEMPO, TERRITORIALIDADE E JURISDIÇÃO

Do tempo como fator

> A sociedade de direito institucionalizou o poder e deu ao ordenamento jurídico a tarefa de fazer a intermediação entre as atividades políticas e os valores morais, mediante uma fórmula tridimensional que consiste em Fato, Valor e Norma. O Direito Digital atua dentro destes conceitos, mas introduz um quarto elemento na equação: o Tempo. Torna-se, desse modo, um conjunto de estratégias que atendem a nossa sociedade digital e não mais apenas normas regulamentadoras (Pinheiro, 2021, p.53)

A princípio, é importante observar que toda norma possui um componente de tempo definido, conhecido como vigência, que determina por quanto tempo essa norma terá efeito no ordenamento jurídico. Contudo, no contexto do Direito Digital, o elemento tempo transcende a mera vigência e abrange a capacidade de resposta jurídica a eventos específicos. Em outras palavras, a aplicação eficaz do conjunto composto por "fato, valor e norma" exige uma resposta ágil para manter sua validade na sociedade digital. Esse elemento temporal pode assumir diferentes características, onde Pinheiro classifica como “ativo, passivo ou reflexivo”.

O tempo ativo refere-se à necessidade de uma resposta jurídica rápida para evitar a obsolescência de direitos subjetivos, onde a demora na decisão pode implicar danos irreversíveis. O tempo passivo é aquele explorado por agentes delituosos que contam com a morosidade jurídica para desencorajar a parte lesada a buscar seus direitos. O tempo reflexivo opera de forma ativa e passiva, causando

efeitos em cadeia e afetando outros conectados no espaço virtual, como nos casos de crimes na Internet e atuação de hackers (Pinheiro, 2021, p.54).

Quanto à territorialidade e jurisdição

> No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspectos: os recursos físicos que esse território contém e o raio de abrangência de determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói um novo território, dificilmente demarcável, no qual a própria riqueza assume um caráter diferente, baseada na informação, que, como vimos, é inesgotável e pode ser duplicada infinitamente (Pinheiro, 2021, p.54).

Para o Direito Penal, a lei brasileira será aplicada sempre que um crime for cometido dentro do território brasileiro. Mas como demarcar a territorialidade no ambiente virtual? Quando é possível, através de um simples dispositivo conectado à internet, se conectar com pessoas de todos os lugares do mundo. Patrícia Peck explica que hoje se aplicam diversos princípios para determinar qual a lei aplicável ao caso, alguns tendem pelo endereço eletrônico, outros pelo local onde foi realizada a conduta, ou ainda o domicílio do consumidor ou a localidade do réu. Para a lei do Marco Civil da Internet

> art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (Brasil, 2014).

Assim, foi ampliado o escopo da jurisdição brasileira para abranger questões que se relacionem de alguma forma com a interação dos dados de usuários ou internautas brasileiros. Parte da premissa que a lei nacional deverá ser aplicada caso a atividade tenha início ou origem, ou que seja parcialmente realizada algum ato de coleta de armazenamento ou tratamento de dados pessoais. Assim, o MCI é específico quanto à parte em que se cabe a jurisdição brasileira, podendo ainda sim serem aplicados mais de um ordenamento ou a lei específica de um país (Pinheiro, 2021, p.56).

Sobre controvérsias de jurisprudência, o STJ no tocante a essa classe de conflitos

> “CONFLITO NEGATIVO DE COMPETÊNCIA. JUÍZES ESTADUAIS DE COMARCAS DE ESTADOS DIFERENTES. INQUÉRITO POLICIAL. ASSOCIAÇÃO CRIMINOSA. CRIAÇÃO DE SITE NA INTERNET PARA COMERCIALIZAR MERCADORIAS QUE JAMAIS

> SERIAM ENTREGUES: CONDUTA QUE SE AMOLDA MAIS AO CRIME CONTRA A ECONOMIA POPULAR DO QUE AO ESTELIONATO. CONEXÃO TELEOLÓGICA E INSTRUMENTAL ENTRE OS DELITOS. COMPETÊNCIA DEFINIDA PELO LOCAL DA INFRAÇÃO QUE TEM A PENA MAIS GRAVE (ART. 78, II, A, CPP). 1. A criação de site na internet por quadrilha, sob o falso pretexto de vender mercadorias, mas sem a intenção de entregá-las, amolda-se mais ao crime contra a economia popular, previsto no art. 2º, IX, da Lei n. 1.521/51, do que ao estelionato (art. 171, caput, CP), dado que a conduta não tem por objetivo enganar vítima(s) determinada(s), mas, sim, um número indeterminado de pessoas, vendendo para qualquer um que acesse o site. 2. Nos termos do art. 2º, IX, da Lei n. 1.521/51, constitui crime contra a economia popular 'obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ('bola de neve', 'cadeias', 'pichardismo' e quaisquer outros equivalentes)'. 3. Verificada estreita conexão teleológica (art. 76, II, CPP) e probatória (art. 76, III, CPP) entre a associação criminosa e o crime contra a economia popular, no caso concreto, a definição da competência segue a regra posta no art. 78, II, a, do CPP (local da infração à qual foi cominada a pena mais grave). 4. Dado que o crime de associação criminosa possui pena mais grave (reclusão de 1 a 3 anos) do que a atribuída ao crime contra a economia popular (detenção de 6 meses a 2 anos e multa) e a associação criminosa consumou-se em Goiânia, pois seis dos sete investigados residiam naquela cidade, é forçoso reconhecer a competência do Juízo estadual de Goiânia para conduzir o inquérito policial. 5. Conflito conhecido, para declarar a competência do Juízo de Direito da 8ª Vara Criminal de Goiânia/GO, o suscitado" (STJ — CC: 133.534 SP 2014/0094026-9, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 28-10-2015, S3 — TERCEIRA SEÇÃO, Data de Publicação: DJe 6-11-2015).

Teixeira entende que os conceitos e princípios clássicos do Direito Penal, em certos pontos, já não estão alinhados com a nova realidade global resultante da expansão da internet. Em particular, cita o princípio da territorialidade, que requer adaptação para se adequar ao ambiente virtual. Todavia, em território nacional, o local do crime é considerado aquele onde estiver sediado o provedor hospedeiro da ofensa (Teixeira, 2022, p.468).

4.6 O DIREITO DIGITAL NO ENFRENTAMENTO DOS CIBERCRIMES

O Direito Digital não se limita à internet, a rede mundial representa uma espécie tecnológica que deve ser atendida por ele, assim como outras inovações que venham a aparecer. Porém, para o Direito Digital, toda relação realizada por ação humana-máquina gera direitos e responsabilidades que necessitam da aplicação de leis, seja por qualquer das formas de resolução escolhidas. Em suma,

a internet é uma parcela de tudo aquilo que abrange, porém é inegável que esta seja uma das mais importantes de se tutelar.

O campo do direito digital não é novo, isso porque ele tem sua guarda na maioria dos princípios do Direito atual, além de utilizar também da legislação em vigor (Pinheiro, 2021, p.53). Está em constante evolução devido às rápidas mudanças tecnológicas e à crescente inserção da tecnologia na sociedade. Para que o direito digital se consolide, algumas áreas de desenvolvimento e aprimoramento são essenciais.

> Historicamente, todos os veículos de comunicação que compõem a sociedade convergente passaram a ter relevância jurídica a partir do momento em que se tornaram instrumentos de comunicação de massa, pois a massificação do comportamento exige que a conduta passe a ser abordada pelo Direito, sob pena de criar insegurança no ordenamento jurídico e na sociedade. Foi assim com a imprensa, o telefone, o rádio, a televisão e o fax (Pinheiros, 2021, p.50)

.

Tomando por base o que já foi exposto, o Direito Digital traz a oportunidade de aplicar dentro de uma lógica jurídica uniforme uma série de princípios e soluções que já vinham sendo aplicados de modo difuso, no chamado Direito Costumeiro. Essa coesão de pensamento possibilita efetivamente alcançar resultados e preencher lacunas nunca antes preenchidas, tanto no âmbito real quanto no virtual, uma vez que é a manifestação da vontade humana em seus diversos formatos que une esses dois mundos no contexto jurídico.

Por consequência, o Direito Digital estabelece um relacionamento com o Direito Costumeiro, aplicando os elementos que tem de melhor para a solução das questões da Sociedade Digital. Esse vínculo entre a tradição jurídica e as novas demandas do mundo digital permite um enfoque mais completo e adaptável para resolver os desafios legais que surgem em um cenário tecnológico que está em constante evolução.

Além disso, por se tratar de um ramo transdimensional, trata de questões dos mais variados ramos do direito tradicional que ocorrem no meio digital. Seja uma decisão da seara civil ou da seara penal. Para isso,as leis do Direito Digital são as já vigentes e aplicáveis, como os Códigos Civil e Penal ou a Constituição Federal. Há as leis específicas, como explicitado anteriormente - como o Marco Civil da Internet e a Lei Carolina Dieckmann - e ainda os projetos de lei que visam atender questões

especiais do mundo tecnológico. Não obstante, há de se criticar a pouca legislação específica no ordenamento brasileiro, porém que tende ao crescimento.

Em suma, os cibercrimes representam uma categoria de crimes das mais diversas fontes e naturezas jurídicas. O Direito Digital é uma disciplina jurídica relativamente nova, quando comparada com as demais, porém, que apresenta aparatos e tem um potencial evolutivo de grande importância para julgar os crimes digitais. Suas características e formas de resolução dos conflitos demonstram potencial para oferecer uma cibersegurança aos usuários e somente tende ao crescimento e a consolidação, visto o aumento e a expressividade do meio tecnológico que só cresce a cada dia.

5 CONSIDERAÇÕES FINAIS

É evidente que a interseção entre o mundo virtual e a legislação é um campo de crescente importância e evolução na sociedade moderna. O cibercrime representa uma ameaça constante à segurança digital, em muitas maneiras, à privacidade, a o bem patrimonial, à honra, e dentre tantos outros, à integridade dos sistemas de informação em todo o mundo. Dessa maneira, torna-se imperiosa a existência de medidas legais que amparem os usuários da internet.

Frente a essa questão, o direito digital busca desempenhar um papel vital na criação de um ambiente legislativo propício para lidar com o cibercrime. Ele oferece ferramentas para definir, investigar e punir infrações cibernéticas, o que não é fácil, visto que ao mesmo tempo deve respeitar os direitos e liberdades individuais dos cidadãos, tuteladas por leis como a LGPD e o MCI. A evolução constante das tecnologias e das táticas dos criminosos cibernéticos desafia os legisladores a manterem-se atualizados, adaptando as leis às mudanças no cenário digital.

Considerando os resultados desta pesquisa, conclui-se que há a ausência de legislações específicas que regulamentem algumas situações que estão sob possibilidade de ocorrerem no ciberespaço. Entretanto, não confunde-se o pensamento apontando como solução a criação de uma infinidade de leis específicas, essa ciência necessita sim de maior aparato legal, porém, através de leis mais genéricas que permitam a dinâmica, característica do direito digital, para lidar com as questões aparentes.

Desse modo, diante da complexidade e da constância evolutiva do cenário cibernético, a abordagem para a regulamentação no mundo digital deve ser equilibrada. A criação excessiva de leis específicas pode ser contraproducente, pois o campo do direito digital é notavelmente dinâmico e fluido, a legislação seria limitada a um tempo e espaço. Em vez disso, é fundamental estabelecer um arcabouço legal mais amplo, flexível e adaptável, que forneça diretrizes gerais para enfrentar os desafios emergentes no ciberespaço que ainda não foram enfrentados.

O ordenamento jurídico brasileiro tem demonstrado a tendência ao enfrentamento dos crimes cibernéticos, agindo através de leis como o Marco Civil da internet e a LGPD para a proteção da privacidade e dos dados, a lei Carolina Dieckmann e a lei 14.155/2021 para tipificar e tornar mais graves os delitos informáticos, e ferramentas de cooperação internacional como a promulgação da

Convenção de Budapeste. Este último desempenhando um papel crucial na persecução dos infratores em níveis estrangeiros, disponibilizando colaboração entre governos, empresas e especialistas em segurança cibernética.

Em última análise, o direito digital desempenha um papel central na defesa da segurança digital em um mundo cada vez mais conectado. No entanto, o desafio de equilibrar a segurança cibernética, com a rápida mudança de nuances do ciberespaço, e com a preservação dos direitos individuais, permanece sendo uma tarefa contínua. A evolução tecnológica e a adaptação das leis são essenciais para enfrentar as ameaças em constante mudança apresentadas pelo cibercrime.

REFERENCIAL TEÓRICO

ABREU, Karen Cristina Kraemer. **História e usos da Internet.** BOCC–Biblioteca Online de Ciências da Comunicação, p. 1-9, 2009. E-book.

AGÊNCIA SENADO. **Aprovada a adesão do Brasil à convenção sobre o crime cibernético.** Brasília, 2023. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico Acesso em: 06 out. 2023.

ARAÚJO, Marcelo Barreto de. **Comércio eletrônico- Marco civil da internet- Direito digital.** Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 ago. 2023.

BRASIL. **Decreto nº 11.491 de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 27 ago. 2023.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 ago. 2023.

BRASIL. **Lei nº 12.737 de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 25 ago. 2023.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 ago. 2023.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 ago.2023.

BRASIL. **Lei nº 14.155 de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo

Penal), para definir a competência em modalidades de estelionato. Brasília, DF, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 02 set. 2023.

BRASIL. **Lei nº 8.069 de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 05 set. 2023.

BRASIL**. Lei nº9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília, DF, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em:12 set. 2023

BRASIL. Supremo Tribunal de Justiça. Conflito de competência nº 133.534-SP. 06 nov. 2015. **CONFLITO NEGATIVO DE COMPETÊNCIA. JUÍZES ESTADUAIS DE COMARCAS DE ESTADOS DIFERENTES. INQUÉRITO POLICIAL. ASSOCIAÇÃO CRIMINOSA. CRIAÇÃO DE SITE NA INTERNET PARA COMERCIALIZAR MERCADORIAS QUE JAMAIS SERIAM ENTREGUES: CONDUTA QUE SE AMOLDA MAIS AO CRIME CONTRA A ECONOMIA POPULAR DO QUE AO ESTELIONATO. CONEXÃO TELEOLÓGICA E INSTRUMENTAL ENTRE OS DELITOS. COMPETÊNCIA DEFINIDA PELO LOCAL DA INFRAÇÃO QUE TEM A PENA MAIS GRAVE (ART. 78, II, "A", CPP).** Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1459186&num_registro=201400940269&data=20151106&formato=PDF . Acesso em: 12 out 2023.

BRASIL. Supremo Tribunal Federal (1ª Turma). **Habeas Corpus N. 76.689-0/ PB. "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: Prova pericial necessária à demonstração da autoria: HC deferido em parte.** Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=76856. Acesso em: 26 set. 2023

CAPEZ, Fernando. **Curso de Direito Penal- parte geral.** 24ª ed. São Paulo: Saraiva Educação, 2020.

CARRAPIÇO, Helena. **O crime organizado e as novas tecnologias: uma faca de dois gumes**. Nação e Defesa, 2005. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/1156/1/NeD111_HelenaCarrapico.pdf. Acesso em: 05 set. 2023.

CASSOLI, Carol. **Casos de estelionato digital crescem 503,3% na Paraíba.** Anuário brasileiro de segurança pública. União, 2023. Disponível em: https://auniao.pb.gov.br/noticias/geral/casos-de-estelionato-digital-crescem-503-3-na-paraiba. Acesso em: 26 set. 2023.

FRANCESCHETTO, Henrique. **Importância Social e Jurídica do Ciberespaço**. Produção Científica Cejurps , v. 1, p. 357-364, 2013.

GIBSON, William. **Neuromancer.** Tradução: Fábio Fernandes. 5ª edição. São Paulo: Editora Aleph, 2016.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro 4.** 16ª ed. São Paulo: SaraivaJur, 2020.

GRECO, Rogério. **Direito Penal Estruturado.** 1ª ed. São Paulo: Editora Forense Ltda., 2019.

IBGE - Instituto Brasileiro de Geografia Estatística. **Internet já é acessível em 90,0% dos domicílios do país em 2021.** Rio de Janeiro: IBGE, 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 21 jul. 2023.

ISAACSON, Walter. **Os Inovadores.** Tradução de Berilo Vargas, Luciano Vieira e Pedro Maia. 1ª edição. São Paulo: Editora Schwarcz S.A., 2014.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informático.** 1ª ed. São Paulo: Saraiva, 2016.

JÚNIOR, Júlio César Alexandre. **CIBERCRIME: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS.** Revista Eletrônica da Faculdade de Direito de Franca, *[S. l.]*, v. 14, n. 1, p. 341–351, 2019. DOI: 10.21207/1983.4225.602. Disponível em: http://revista.direitofranca.br/index.php/refdf/article/view/602. Acesso em: 12 set. 2023.

LÉVY, Pierre. **Cibercultura**. Tradução: Carlos Irineu da Costa. Edição brasileira. São Paulo: Editora 34 Ltda., 1999.

MCAFEE. **O que é malware?** McAfee, 2023. Disponível em: <https://www.mcafee.com/pt-br/antivirus/malware.html>. Acesso em: 30 ago. 2023.

MICROSOFT. **O que é phishing?** Microsoft, 2023. Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-phishing>. Acesso em: 01 set. 2023.

MONTEIRO, Luís. **A INTERNET COMO MEIO DE COMUNICAÇÃO: POSSIBILIDADES E LIMITAÇÕES**. Campo Grande/MS: INTERCOM, XXIV Congresso Brasileiro da Comunicação, set. – 2001. Disponível em:http://www.portcom.intercom.org.br/pdfs/62100555399949223325534481085941280573.pdf. Acesso: em 20 jul. 2023.

MUÑOZ, Jesus; TURNER, David. Para os filhos dos filhos de nossos filhos: Uma visão da sociedade internet. 1ª edição. São Paulo: Plexus Editora Ltda., 1999.

NEVES, Daniel Amorim Assumpção. **Manual de Direito Processual Civil**. 10ª ed. Salvador: Editora jusPodivm, 2018.

PANCINI, Laura. **58% dos brasileiros sofreram crimes cibernéticos, aponta estudo da Norton**. Exame. 11 mar. 2022. Disponível em: <https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/>. Acesso em: 25 ago. 2023.

PEREIRA, Fabiana. **Quadrilha rouba correntistas via internet**. Folha de São Paulo, 1999. Disponível em: https://www1.folha.uol.com.br/fsp/cotidian/ff05089912.htm. Acesso em 14 set. 2023.

PIMENTEL, José Eduardo de Souza. Introdução ao direito digital. **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, v. 13, n. 1, p. 16-39, 2018. Disponível em: https://es.mpsp.mp.br/revista_esmp/index.php/RJESMPSP/article/view/352. Acesso em 02 out. 2023.

PINHEIRO, Patrícia Peck. **Direito Digital.** 7ª ed. São Paulo: Saraiva Educação, 2021. e-book.

RÁDIO SENADO. **Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos.** Rádio Senado. 2023. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em: 06 out. 2023.

RAZ, Joseph. **The authority of law**. 2ªed. Oxford: Oxford University Press, 2009. E-book.

SINGER, Peter; FRIEDMAN, Allan. **Cybersecurity and cyberwar: what everyone needs to know**. Oxford: Oxford University Press, 2014. E-book.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 6ª ed. São Paulo: SaraivaJur, 2022. E-book.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**. 3. ed. Rio de Janeiro: Brasport, 2021. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 26 set. 2023.