Revista Jurídica do Nordeste Mineiro, v.4, 2024
ISSN 2675-4312

TRATAMENTO JURÍDICO DOS CRIMES COMETIDOS EM AMBIENTE VIRTUAL

LEGAL TREATMENT OF CRIMES COMMITTED IN A VIRTUAL ENVIRONMENT

Ana Luiza Gouveia Domingos

Aluna do 9º Período do Curso de Direito da Faculdade AlfaUnipac - Teófilo Otoni/MG, Brasil. E-mail:analuizagouveiadomingos@gmail.com

Samuel Huhn Saldanha Santos

Aluno do 9º Período do Curso de Direito da Faculdade AlfaUnipac - Teófilo Otoni/MG, Brasil. E-mail:samuelsaldanha21@gmail.com

Yan Pablo Souza Huhn Santos

Aluno do 9º Período do Curso de Direito da Faculdade AlfaUnipac - Teófilo Otoni/MG, Brasil. E-mail: ypssantos@gmail.com

Cristiane Xavier figueiredo

Professora Orientadora da Faculdade Alfa Unipac de Teófilo Otoni/MG. Brasil, E-mail: cristianetotoni@yahoo.com.br

Resumo

O presente artigo busca fazer uma breve análise a respeito do tratamento jurídico dado aos crimes praticados no ambiente virtual. Tal estudo do tema é de relevante importância, tendo em vista que a internet é uma rede que, cada vez mais, conecta pessoas de todos os lugares do mundo. Esse fato contribui para que crimes cibernéticos ocorram cada vez com mais frequência, produzindo vítimas por todas as partes do planeta. Este trabalho tem como principal objetivo fazer uma breve análise sobre o tema, definindo o conceito de crimes virtuais, destacando os principais crimes cometidos atualmente na internet, e o tratamento jurídico dado aos criminosos cibernéticos, destacando a evolução da legislação penal brasileira no que tange a responsabilização desses criminosos, bem como a competência para os julgamentos dos crimes relacionados. Para isso, foram realizadas consultas em doutrinas, jurisprudências, em legislações penal e civil e processuais, bem como de artigos da internet e blogs jurídicos. Busca-se, ademais, através disso, o conhecimento sobre alguns crimes virtuais, alertando para a prevenção e a possibilidade de responsabilização de criminosos cibernéticos.

Palavras-chave: Cibercrime; Internet; Legislação.

Abstract

This article seeks to provide a brief analysis of the legal treatment given to crimes committed in the virtual environment. Such a study of the topic is of relevant importance, considering that the internet is a network that, increasingly, connects people from all over the world. This fact contributes to cybercrimes occurring more and more frequently, producing victims all over the planet. This work's main objective is to make a brief analysis of the topic, defining the concept of virtuais crimes, highlighting the main crimes currently committed on the internet, and the legal treatment given to cyber criminals, highlighting the evolution of Brazilian criminal legislation regarding the accountability of these criminals, as well as the competence to judge related crimes. To this end, consultations were carried out on doctrines, jurisprudence, criminal and civil and procedural legislation, as well as internet articles and legal blogs. Furthermore, through this, knowledge is sought about some virtual crimes, warning about prevention and the possibility of holding cybercriminals accountable.

Keywords: Cybercrime; Internet; Legislation

1. Introdução

O presente artigo tem como principal objetivo fazer uma breve análise sobre o que são os crimes virtuais, alguns exemplos de crimes praticados no ambiente virtual, o avanço das legislações no país que abordam sobre o tema de forma específica, bem como a responsabilidade de criminosos. Este artigo é importante para evidenciar o quanto a tecnologia tem avançado, e que apesar dos benefícios na vida das pessoas, criminosos têm feito dela uma arma poderosa para ofender a honra de outras pessoas, para se beneficiarem de maneiras ilícitas, seja roubando dados pessoais ou invadindo dispositivos eletrônicos para adulteração de dados.

Os crimes virtuais, também conhecidos como crimes cibernéticos, são atividades ilegais praticadas no ambiente virtual, envolvendo o uso de computadores, redes de computadores ou outros dispositivos conectados à internet. Esses crimes são frequentemente cometidos por indivíduos com conhecimentos tecnológicos, como hackers e cibercriminosos. O aumento da quantidade de usuários na internet tem contribuído para o crescimento desses delitos. Esses crimes são divididos em quatro categorias: crimes virtuais impróprios, próprios, mistos e crimes sexuais contra crianças e adolescentes.

Ao longo do tempo, a legislação brasileira tem evoluído para lidar com esses crimes, incluindo leis como a Lei Carolina Dieckmann, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e a Lei que alterou o Código Penal para abordar crimes

cibernéticos. As autoridades também podem responsabilizar pessoas jurídicas

envolvidas nesses crimes.

Em resumo, os crimes virtuais representam uma ameaça crescente no mundo digital, exigindo uma evolução constante na legislação e na aplicação da lei para combater essas atividades ilícitas e proteger os direitos das vítimas.

2. Crimes Virtuais

Os crimes virtuais, também conhecidos como crimes cibernéticos ou eletrônicos, têm como principal meio de uso os computadores, uma rede de computadores ou dispositivos conectados à internet. Grande parte desses crimes são praticados por pessoas com alto conhecimento tecnológico, como os hackers ou cibercriminosos. Destaca-se a importância de tratar acerca de tais crimes, diante do crescente número de usuários de internet, pois conforme aumenta o número de usuários, o número de crimes cibernéticos também aumenta. Ademais, é fundamental conhecer com mais detalhes a sua definição e as categorias desses tipos de crimes (KASPERSKY, 2023).

2.1 Conceito

Os crimes virtuais, também conhecidos como crimes cibernéticos, constituem uma ampla gama de atividades ilícitas perpetradas no ambiente digital, seja por meio de computadores ou de celulares. O termo “cibercrime” foi utilizado pela primeira vez na década de 90. Sua ocorrência se dá através da manipulação de dados e arquivos ou até mesmo no constrangimento de pessoas no meio digital. (FIA, 2021); (TELECOM, 2023).

Tais crimes decorrem, principalmente, da evolução social e tecnológica. Com a evolução digital, a internet tem se tornado o centro da vida de muitas pessoas, com isso, pessoas passam mais tempo conectadas na web, ficando suscetíveis a mais riscos, como violação de dados pessoais e/ou bancários, fotos íntimas etc. (TELECOM, 2013).

Nesse sentido, Rogério Greco (2017), complementa:

> Com a utilização da internet, delitos considerados como tradicionais, a exemplo do estelionato, podem ser praticados sem que a vítima conheça sequer o rosto do autor da infração penal. Nossa vida pessoal pode ser

> completamente devassada e colocada à disposição de milhões de pessoas. Nossa intimidade, enfim, estará disponível com apenas um toque no computador (GRECO, 2017, p.584).

O direito digital apresenta dois tipos de crimes virtuais distintos, mas que merecem atenção: delitos de informática e delitos comuns praticados no meio virtual. Aqueles, por sua vez, foram introduzidos pelo Código Penal através da Lei de Crimes Cibernéticos. Esses crimes são abordados como sendo condutas praticadas por meio de serviços tecnológicos, como invasão de computadores, indisponibilidade de serviços de internet e alteração de dados de empresas (JUSBRASIL, 2019).

Por outro lado, os delitos comuns praticados na internet correspondem a condutas que já existiam antes mesmo da criação dessa lei, como a ofensa a honra, o engano para obter vantagens, e atribuir a terceiro um crime sabidamente como sendo falso. Nesses casos, a internet apenas foi responsável por ampliar o alcance dos infratores (JUSBRASIL, 2019).

Nesse diapasão, Damásio e Milagre (2016) explicam que o crime cibernético se trata de um fenômeno diretamente ligado às transformações tecnológicas vivenciadas pela sociedade, de modo que, diretamente, influenciam no direito penal. Portanto, trata-se de um crime praticado por meios eletrônicos, em que há a extração de dados de terceiros sem o consentimento ou autorização das vítimas.

Portanto, pode-se definir os crimes virtuais como sendo os crimes cibernéticos ou eletrônicos, caracterizados pela atividade ilegal no meio digital, em que o uso de tecnologias de informação e comunicação são os principais meios utilizados pelos criminosos. Ademais, esses crimes podem abranger uma vasta variedade de atos, que não se limitam ao “hacking”, mas referindo-se, também, a invasão de sistemas de computadores, contas ou redes, em que se tem o objetivo de roubar dados ou corromper arquivos.

2.2 Classificação

Os crimes virtuais podem ser divididos em categorias, quais sejam: crimes virtuais impróprios, próprios e mistos. Os crimes impróprios são aqueles praticados mediante o uso de computadores, no entanto, não há ofensa a inviolabilidade de dados. Pode-se citar, nesses casos, os crimes de ameaça, estelionato, injúria, difamação. É importante observar que, nesse tipo de crime, os crimes praticados pelos

infratores já se encontravam previstos na legislação, valendo-se, no entanto, da internet para a sua prática, não havendo, portanto, que se falar na prática de novos tipos penais (MACHADO, 2013).

Conforme Justiano (2016), os crimes próprios são aqueles praticados exclusivamente através de computadores. Diferentemente dos impróprios, os crimes próprios necessitam de legislação especial, diante de que passam a configurar novos tipos penais, como ocorre com

os crimes de invasão de dispositivo informático, previsto no artigo 154-A e 154-B do Código Penal (CP), bem como a inserção de dados falsos em sistemas de informação (art.313-A do CP) e modificação não autorizada de dados em sistema de informação (art. 313-B do CP).

Já nos crimes mistos, o alvo dos criminosos deixa de ser o computador em si e passa a ser os bens das vítimas, assim, a internet passa a ser utilizada como o principal meio para a realização do crime. Um exemplo desse crime são as transferências de bens ou valores realizadas de forma ilícita. Sendo assim, os dispositivos telefônicos, computadores etc., passam a ser meios necessários para a realização dos crimes (PINHEIRO, 2022).

3. Tipos mais comuns de crimes virtuais

Os crimes virtuais, também conhecidos como crimes cibernéticos, são delitos praticados mediante o uso de redes de computadores ou outros dispositivos conectados a uma rede de internet. Podem ser praticados tanto de forma individual, quanto por meio de grupos especializados em ataques virtuais, em que uma das principais intenções dos criminosos se baseia na coleta de informações para se beneficiarem com vantagens ilícitas. Esses criminosos infectam computadores ou outros dispositivos com vírus ou malware, danificando serviços ou gerando instabilidades, disseminando informações falsas, ou simplesmente roubando ou excluindo dados (MENDES, 2021).

3.1 Crimes contra a honra

Com o uso de internet, principalmente, com o alcance das redes sociais, crimes contra a honra, como a injúria, calúnia e difamação, tornaram-se uns dos principais

crimes praticados no meio virtual. Com o avanço da internet, pessoas de todos os lugares passam a ter cada vez mais a possibilidade de acesso à internet e, consequentemente, a fazerem uso das redes sociais. Tal fato abre margem para a diversidade de ideias e opiniões. No entanto, algumas pessoas falam o que querem sem medo de retaliação (DEBS, 2022).

Muitas pessoas usam da internet para ferir a honra de outros, talvez, até na falsa ideia de que a internet é uma “terra sem lei”, que seus atos não ensejarão punições. Entretanto, não é bem assim, já que esses crimes, ainda que cometidos em meio virtual, podem ensejar sanções civis e/ou penais. Um exemplo disso, é que uma única mensagem no Facebook ou outras redes sociais, dependendo do seu conteúdo, pode ser suficiente para configurar crimes, como injúria, difamação ou calúnia (FREDERIGHI, 2021).

Contudo, é importante compreender como certas condutas passam a ser enquadradas como crimes virtuais. Para isso, utilizam-se os crimes contra a honra, definidos no Código Penal Brasileiro, para servir como parâmetro para a responsabilização de criminosos no meio virtual. Nesse diapasão, é importante citar o artigo 138 do CP:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.

O crime de calúnia configura-se quando alguém atribui, falsamente, a outrem, o cometimento de um fato considerado como crime. Por outro lado, definido no art. 139 do CP encontra-se a difamação, crime com prática muito comum nas redes sociais, pois ocorre quando alguém publica, ou até mesmo encaminha no privado, mensagens, textos, vídeos em que atribui a outrem um fato ofensivo a sua reputação que, no entanto, não representa crime. Já a injúria, crime disposto no art. 140 do CP, ocorre quando há ofensa a dignidade ou o decoro (FREDERIGHI, 2021).

3.2 Roubo de dados

São inúmeros os tipos de ataques virtuais e práticas de roubos de dados na internet. Frisa-se que ataques voltados para esse tipo podem ocorrer tanto contra pessoas quanto empresas, sendo que, neste último caso, os efeitos de um ataque

cibernético podem ser devastadores. Diante disso, é necessário compreender os diversos tipos de ataques voltados para o roubo de dados na internet, sendo o *backdoor, phishing, ransomware e spoofing* os mais comuns (FRAGA, 2022).

Em síntese, o *backdoor* refere-se a uma espécie de ataque remoto, em que um *maware* é introduzido no computador, explorando falhas no aparelho ou vulnerabilidades em navegadores, além de facilitar o retorno do invasor no computador afetado, com o principal objetivo de roubar informações privilegiadas. Já o *Ransomware* se trata de um ataque virtual que gera a indisponibilidade do aparelho afetado, sendo a sua principal característica o pedido de resgate para que o funcionamento do computador volte a ficar disponível (MULLER, 2018).

Já com relação ao p*hishing*, este se refere a uma forma que os criminosos usam para enganar alguém, e com isso roubar informações pessoais, como dados de contas bancárias, senhas, endereços etc. Geralmente, esse tipo de golpe ocorre através do envio de mensagens

ou e-mail que, aparentemente, são legítimos, porém, os links anexados nas mensagens direcionam para sites fraudulentos, capazes de roubarem dados pessoais, como, por exemplo, mensagens de banco pedindo para recadastrar senha de modo on-line, ou confirmar dados bancários. Já o *spoofing* são falsos domínios de correio eletrônico utilizados pelos criminosos, porém, aparentemente, são legítimos. A grande parte desses ataques são direcionados para falsificações, em que o principal objetivo é o acesso de informações sensíveis (RUDRA, 2022).

Conforme a Cartilha de Segurança para a Internet (2021), em todas as situações expostas, os principais riscos desses ataques são voltados para o vazamento de dados que podem expor pessoas e empresas, ocasionando o furto de identidade e invasão de contas online, tentativas de golpes, furto de identidade capazes de provocarem prejuízos financeiros, violação de privacidade e outros. A cartilha alerta, ainda, para a necessidade de sempre estar alerta a esses tipos de riscos, evitando abrir ou acessar sites, links, ou documentos suspeitos. Em caso de vazamento de dados, é importante trocar imediatamente as senhas expostas, ativar a verificação em duas etapas e, em caso de roubo de dados bancários, comunicar as instituições responsáveis pelo cartão, e contestar possíveis lançamentos irregulares identificados.

3.3 Crimes sexuais contra crianças e adolescentes

Outro crime que merece forte destaque é quanto a pedofilia na internet. Conforme dados do Ministério dos Direitos Humanos, todos os dias são denunciados, no Brasil, mais de 360 casos de crimes cibernéticos, sendo a maioria de suas vítimas crianças e adolescentes. Com base nisso, apenas no primeiro semestre de 2022, quase 80 mil casos de crimes sexuais contra menores foram denunciados na Ouvidoria Nacional de Direitos Humanos. Uma situação que chama a atenção é quanto aos avanços da Inteligência Artificial, em que facilita a ação de criminosos para que se passem por outras pessoas, a fim de conquistarem a confiança desses menores e cometerem os crimes, como os *deepfake* (NAZAR, 2023).

O d*eepfake* se refere a um recurso que usa a inteligência artificial para alterar as características físicas do criminoso, como o rosto, corpo e até mesmo a voz em um vídeo. Os resultados dessas alterações podem ser extremamente convincentes. Entretanto, é necessário alertar que no que pese o avanço desse tipo de tecnologia, crianças e adolescentes continuam sendo alvos fáceis para pedófilos na internet, seja através das redes sociais ou de jogos online, por exemplo. Algo em comum em quase todos os tipos de crimes dessa espécie é o anonimato

do criminoso, pois na maioria das vezes eles se apresentam através de perfis falsos, utilizando de interesses comuns que chamam a atenção desses menores (ARAÚJO, 2023).

4. Tratamento Jurídico dos crimes virtuais

Com o avanço da internet em praticamente todos os lugares do mundo, pessoas de diversas regiões e de classes diferentes passaram a ter acesso a internet, consequentemente, houve um aumento de ataques cibernéticos em escala global. Com base nisso, houve a necessidade de que as autoridades de diversos países do mundo, inclusive do Brasil, voltassem a atenção para esses ataques virtuais e, com isso, implementassem medidas capazes de criminalizarem e criarem responsabilidades civis e penais (MOREIRA, 2023).

Conforme mencionado, a internet não é terra sem lei, sendo que a prática de condutas criminosas no meio virtual é passível de responsabilidade, sejam elas penal ou cível. Nesse diapasão, a responsabilidade penal ocorre com base na tipicidade do

crime, como ocorre com os crimes de estelionato, roubo de dados, pornografia infantil, crimes contra a honra e outros. Além desses crimes, existem aqueles inseridos na legislação penal especial, que regulamentam especialmente os crimes praticados no meio virtual, como a lei do marco civil, a lei Geral de Proteção de dados, a Lei Carolina Dieckmann e outras (VARGAS, 2023).

Destaca-se, que a prática de crimes no ambiente virtual também poderá ensejar responsabilidades penais às pessoas jurídicas. Tal inovação foi dada através da Convenção de Budapeste, em que previu que os países signatários da convenção deveriam instrumentalizar punições criminais às pessoas jurídicas que venham a ser favorecidas pelos crimes cibernéticos. A criminalização dessas pessoas jurídicas torna-se essencial, já que é uma forma de evitar que empresas sirvam para ocultar criminosos ou produtos de crimes (CAMPOS, 2023).

Constata-se que a prática de crimes em ambientes virtuais representa uma grande afronta a princípios fundamentais, como o princípio da dignidade da pessoa humana, bem como o princípio da personalidade. A dignidade da pessoa humana implica na proteção da integridade física, psicológica e moral dos indivíduos. Nos crimes virtuais, como cyberbullying ou divulgação não autorizada de informações pessoais, a dignidade da vítima pode ser violada. Nesses casos, as leis devem ser aplicadas para proteger a integridade e a autonomia dos indivíduos (SILVA, 2019).

Já os direitos da personalidade garantem e protegem os direitos fundamentais da pessoa natural, prevenindo violações desses direitos e, caso ocorra transgressão, assegurando

uma reparação por danos morais, materiais ou até mesmo penais. Esse princípio garante a proteção de direitos à intimidade e à imagem, bem como reconhece que cada indivíduo possui direitos inalienáveis sobre sua própria pessoa, incluindo sua privacidade, intimidade e imagem (BARROS, 2019).

Portanto, é importante destacar que tanto o princípio da dignidade da pessoa humana quanto o princípio da personalidade a aplicabilidade devem ser aplicados e respeitados nas condutas praticadas em ambiente virtual, já que os crimes cometidos em ambiente virtual enfatizam a importância de proteger esses direitos. As leis e políticas devem ser desenvolvidas e implementadas de forma a garantir que o ambiente virtual seja seguro, respeitoso e inclusivo para todos os indivíduos.

4.1 Evolução da legislação penal brasileira aplicada aos crimes virtuais

Por muito tempo os crimes praticados no ambiente virtual não ensejavam qualquer tipo de responsabilidade, diante da carência de normas voltadas exclusivamente para esses crimes. No entanto, diante da ausência de leis específicas, passou-se, com o tempo, a aplicar o Código Penal e o Código Civil para condutas que coincidiam com aquelas já criminalizadas, com a diferença que seriam adaptadas para o ambiente virtual. Além de ambos os códigos, a Lei 9.296, que tipificava os crimes de interceptação telefônica, e a lei 9.609, que tratava da propriedade intelectual, também passaram a serem aplicadas (SILVA, 2021).

Até meados de 2012 não havia, no Brasil, legislações que tratassem especificamente dos crimes virtuais. A principal legislação que deu início a todo esse processo contra os crimes cibernéticos foi a legislação de n 12.737/2012, também conhecida como a Lei Carolina Dieckmann. Determinada lei foi a primeira a regular acerca dos crimes digitais, no que tange invasão de dispositivos e violação de dados. Tal norma foi criada a partir da grande repercussão de um caso envolvendo a atriz, em que teve suas fotos compartilhadas na internet após invasão (POSESA, 2019).

Outra grande evolução ocorreu em 2014, com a criação do Marco Civil da Internet, através da lei de nº 12.965 de 2014. Determinada norma tem como objetivo regular garantias, direitos e deveres na internet. Ademais, são estabelecidos princípios que visam gerar mais segurança e democracia nos meios virtuais. Assim, essa lei veio como uma forma de minimizar a insegurança vivida no ambiente virtual, garantindo a liberdade de expressão, proteção dos dados pessoais, deveres dos provedores da internet e outras garantias (AURUM, 2023).

Outra norma aplicável aos crimes cibernéticos é a Lei Geral de Proteção de Dados, Lei de nº 13.709 de 2018. Conforme o Ministério do Esporte, determinada lei foi criada com o principal objetivo de proteger os direitos fundamentais de liberdade e privacidade. Trata diretamente acerca da proteção de dados pessoais inseridos no ambiente digital, seja pessoa física ou jurídica. Os dados pessoais são tratados por dois agentes, o controlador e o operador. Ademais, existe o Encarregado, indicado pelo controlador para atuar no setor de comunicação. Nesse diapasão, o Ministério da Educação explica:

> Tema fundamental trabalhado pela Lei, o tratamento de dados diz respeito a qualquer atividade que utiliza um dado pessoal na execução da sua operação, como, por exemplo, coleta, produção, recepção, classificação,

> utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2023).

É importante destacar, ainda, nesse tópico, acerca da Lei de nº 14.155 de 27 de maio de 2021, que altera o Código Penal no que tange os crimes de violação de dispositivo informático, furto e estelionato praticados na internet. Essa lei passa agravar os crimes citados anteriormente como, por exemplo, o crime de invasão de dispositivo informático alheio, quando praticado com o fim de obter, alterar ou destruir dados ou informações sem consentimento. A pena para este crime é de reclusão de 1 a 4 anos e multa, além da possibilidade de aumento de 1/3 a 2/3 em caso da invasão resultar prejuízo econômico (BRASIL, 2021).

4.2 Competência para processar e julgar

Conforme visto, são diversos os crimes cometidos na internet, como os crimes contra a honra, compreendendo a injúria, difamação e calúnia; os crimes de fraude eletrônica, estelionato virtual e outros. Ressalta-se que esses crimes podem ser cometidos a quilômetros de distância de onde se encontra a vítima, transcendendo até mesmo fronteiras. Com base nisso, questiona-se qual o lugar competente para julgar os crimes cometidos no ambiente virtual.

Antes de adentrar na questão, é necessário compreender o que significa a competência. A competência refere-se à delimitação da jurisdição, ou seja, é delimitado um espaço em que o juiz ficará responsável pelo julgamento dos litígios ali ocorridos. Ela será estabelecida quando ocorre a distribuição do processo, e em regra, não sofre modificação. Um dos pontos a

ser destacados quanto a competência é o critério que a determina. Assim, a competência pode se dar quanto ao território, também definida como competência de “foro”; quanto ao valor da causa; quanto a matéria e quanto a função ou hierarquia (NOVACKI, 2018).

É válido mencionar, ainda, o artigo 69 do código de processo penal (1941), onde classifica a competência:

> Art. 69. Determinará a competência jurisdicional: I - o lugar da infração:
> II - o domicílio ou residência do réu; III - a natureza da infração; IV - a

> distribuição; V - a conexão ou continência; VI - a prevenção; VII - a prerrogativa de função

Neste ponto, cabe destacar que o Código de Processo Penal adotou a teoria da ubiquidade quanto ao local do crime. Assim, o lugar do crime é determinado a partir do local onde o crime foi consumado, ou praticado o último ato de ação ou omissão. Desse modo, para que se possa definir qual o juízo é competente para o julgamento de determinado fato, é necessário compreender qual foi o local do crime, bem como a natureza do delito e se o réu é benificiário de prerrogativa de função (CARDOSO, 2017).

Conforme visto, os crimes virtuais podem ser cometidos por qualquer pessoa, em qualquer lugar do planeta, tendo em vista que a internet é uma rede de grande extensão a nível mundial. Ressalta-se, que a teoria aplicada quanto ao local do crime é a teoria da ubiquidade, levando em consideração o local em que o crime foi consumado, onde ocorreu a última ação ou a omissão. No brasil, a competência quanto a esses crimes fica limitados à interpretação dos tribunais superiores. Diante disso, esses tribunais têm firmado entendimento no sentido de que a competência a ser observada para esses crimes é o local onde esteja o provedor, isso quando o crime ocorra dentro do próprio Estado, e desde que nenhum bem da união seja atingido (SOUZA, 2016).

Destaca-se quanto aos crimes internacionais, nos quais tenham se dado início no país e prosperado no exterior. Um exemplo disso é a pornografia infantil, em que tenha se iniciado no Brasil, mas visualizada em outro país. Nesse ponto, a competência será da Justiça Federal, conforme art. 88 do CPP, tendo em vista a transposição da barreira nacional (SOUZA, 2016).

> Art. 88. No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República (BRASIL, 1941).

Quantos aos crimes contra a honra praticados na internet, é válido mencionar um entendimento da Terceira Seção do Superior Tribunal de Justiça (STJ), em que firmou entendimento de que em caso de injúria praticada em mensagem privada, o crime se consuma no local em que a vítima toma conhecimento da ofensa. Ressalta-se, que nesse caso, trata-se de mensagens privadas, em que não houve o conhecimento por parte de terceiros (BRASIL, 2022).

5. Considerações finais

O tratamento jurídico dos crimes cometidos no ambiente virtual ainda representa um grande desafio a ser superado no sistema legal. Nesse sentido, um ponto que merece ser destacado é quanto a complexidade que envolve os crimes cibernéticos, já que no ambiente virtual há a possibilidade da ocorrência de diversos crimes, desde ataques cibernéticos, fraudes online, disseminação de conteúdo ilegal etc. A natureza complexa que envolve esses tipos de crimes dificultam em muitas das vezes as investigações pelas autoridades e, respectivamente, a responsabilidade desses criminosos.

Outro ponto destacado ao longo do trabalho é quanto a competência e a jurisdição para o julgamento dos crimes cometidos em ambiente virtual. A internet possibilita que alguém ultrapasse fronteiras sem sequer sair de casa, possibilita, por outro lado, a prática de crimes em outro país, com consequências devastadoras para a vítima. Tal fato, resulta em mais um desafio para as autoridades, tornando a delimitação da jurisdição e a firmação de competência um desafio.

Portanto, o tratamento jurídico dos crimes virtuais continua sendo um desafio e uma necessidade para os usuários da internet, tendo em vista a importância da garantia de segurança no ambiente virtual, com a responsabilização eficaz de criminosos cibernéticos. Para isso, é fundamental que leis penais e civis evoluam cada vez mais a fim de acompanharem as profundas e velozes mudanças que ocorrem no cenário tecnológico. Destaca-se, ainda, que essas normas zelem pela cooperação global com vista ao respeito pelos direitos individuais.

Referências

BARROS, Suely Araújo de. Crimes virtuais: Efeitos civil e penal. Repositório.aee. Anápolis, 2019. Disponível em < http://repositorio.aee.edu.br/bitstream/aee/8599/1/TCC%20COMPLETO%20-%20SUELY%20CORRE%C3%87%C3%83O%20VERS%C3%83O%20FINAL.pdf> Acesso em 01 de março de 2024.

BRASIL. Decreto Lei º 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm > . Acesso em 01 de mar. de 2024.

BRASIL. Superior Tribunal de Justiça. Portal STJ, 2022. Disponível em: < https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/03032022-Injuria-em- mensagens-privadas-na-internet-se-consuma-onde-a-vitima-toma-conhecimento-da-ofensa-.aspx >. Acesso em 25 de outubro de 2023.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Ministério do Esporte, 2023. Disponível em: <https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd >. Acesso em 15 de outubro de 2023.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Diário oficial da República do Brasil, Poder executivo, Brasília, 27. Mai. 2021. Disponível em:< https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm >. Acesso em 24 de outubro de 2023.

CAMPOS, Wilson Knoner. Cybercrimes e responsabilização criminal da pessoa jurídica no Brasil. Revista Migalhas, 2023. Disponível em: <https://www.migalhas.com.br/depeso/384959/cybercrimes-e-responsabilizacao-criminal-da- pessoa-juridica >. Acesso em 19 de outubro de 2023.

CARDOZO, Alexandro Gianes. Competência nos crimes cibernéticos. Revista Jusbrasil, 2017. Disponível em: <https://www.jusbrasil.com.br/artigos/competencia-nos-crimes- ciberneticos/514359859 >. Acesso em 15 de outubro de 2023.

CARTILHA DE SEGURANÇA PARA INTERNET. Fascículo: vazamento de dados. Revista cert, 2021. Disponível em: <https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo- vazamento-de-dados.pdf >. Acesso em 15 de outubro de 2023.

EL DEBS, Aline Iacovelo. Dos crimes contra a honra na seara digital. Revista Consultor Jurídico, 2022. Disponível em:<https://www.conjur.com.br/2022-set-03/aline-iacovelo- crimes-honra-seara-digital >. Acesso em 10 de outubro de 2023.

FARIA, Isaque Murilo Benedito. Lei 12.965/14: tire as suas dúvidas sobre o Marco Civil da internet. Aurum, 2023. Disponível em: <https://www.aurum.com.br/blog/marco-civil-da- internet/ >.Acesso em 25 de setembro de 2023.

FIA BUSINESS SCHOOL. Crimes cibernéticos: o que são, tipo, como detectar e se proteger. Revista Fia, 2021. Disponível em: <https://fia.com.br/blog/crimes-ciberneticos/

FRAGA, Carol. O roubo de dados na internet está cada vez pior. Saiba evitar! Mutuus, 2022. Disponível em: <https://www.mutuus.net/blog/roubo-de-dados-na-internet/ >. Acesso em 10 de outubro de 2023.

FREDERIGHI, Daniel. Crime virtual de ameaça, calúnia e difamação, como proceder? Revista: Jusbrasil, 2021. Disponível em: <https://www.jusbrasil.com.br/artigos/crime-virtual- de-ameaca-calunia-e-difamacao-como-proceder/1313296011 >. Acesso em 12 de outubro de 2023.

GRECO, Rogério. Curso de Direito Penal: parte especial, volume II: Introdução à teoria geral da parte especial: crimes contra a pessoas. – 14. ed. Niterói, Rj: Impetus, 2017.
https://blog.algartelecom.com.br/ti/crimes-ciberneticos-2/ >. Acesso em 07 de outubro de 2023.

KASPERSKY. O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos. Revista Kaspersky, 2023. Disponível em?<https://www.kaspersky.com.br/resource- center/threats/what-is-cybercrime>. Acesso em 10 de outubro de 2023.

MOREIRA, Paulo Roberto Silvério. A responsabilidade penal dos crimes cibernéticos: análise comparativa de diferentes sistemas jurídicos. Revista migalhas, 2023. Disponível em: <https://www.migalhas.com.br/depeso/387502/a-responsabilidade-penal-dos-crimes- ciberneticos >. Acesso em 18 de outubro de 2023.

MULLER, Nicolas. Diferença entre ransomware, RAT, backdoo, worn e bot. Oficina da net, 2018. Disponível em: <https://www.oficinadanet.com.br/post/18266-diferenca-entre- ransomware-rat-

backdoor-worm-e-bot >. Acesso em 11 de outubro de 2023.

NAZAR, Susanna. Casos de pedofilia virtual se multiplicam no Brasil com os avanços da inteligência artificial. Revista Jornal da USP; Ribeirão Preto, 2023. Disponível em: <https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os- avancos-da-inteligencia-artificial/ >. Acesso em 20 de outubro de 2023.

PINHEIRO, Bruno Victor de Arruda. As novas disposições sobre os crimes cibernéticos: uma análise acerca das leis 14.132 e 14.155/2021. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 27, n.6899, 2022. Disponível em: https://jus.com.br/artigos/98006/as-novas- disposicoes-sobre-os-crimes-ciberneticos Acesso em 15 de outubro de 2023.

POSESA, Pós-graduação. Crimes cibernéticos: o que são, leis aplicáveis e mais! Posesa pós-graduação, 2023. Disponível em:<https://posesa.com.br/crimes-digitais-leis-aplicaveis/ > Acesso em 29 de setembro de 2023.

RUDRA, Ahona. Phishing vc spoofing. Power Marc, 2022. Disponível em: <https://powerdmarc.com/pt/phishing-vs-spoofing/ >. Acesso em 18 de outubro de 2023.

SILVA, Sandra Rita da. A dignidade da pessoa humana nos crimes contra a honra na internet. Jusbrasil, 2019. Disponível em < https://www.jusbrasil.com.br/artigos/a-dignidade-da-pessoa-humana-nos-crimes-contra-a-honra-na-internet/646726565#:~:text=A%20dignidade%20da%20pessoa%20humana%20tem%20um%20valor%20pessoal%20que,com%20a%20dignidade%20da%20pessoa>. Acesso em 01 de março de 2024.

SOUZA, Lucas. Competência para processar e julgar crimes virtuais. Revista Jusbrasil, 2016. Disponível em: <https://www.jusbrasil.com.br/artigos/competencia-para-processar-e-julgar- crimes-virtuais/417311418 >. Acesso em 10 de outubro de 2023.

VARGAS, Laryssa Alves. Os efeitos civis em crimes na internet. Revista Conteúdo Jurídico, 2023. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/61438/os-efeitos- civis-em-crimes-na-internet >. Acesso em 20 de outubro de 2023.

VIANNA, Túlio; MACHADO, Felipe. Crimes informáticos conforme a lei n 12.737 de 2012. Editora Fórum; 1.ed. São Paulo, 2017.