A responsabilidade do estado na dificuldade no processo de identificação da autoria e da falta de punibilidade nos crimes cibernéticos

João Augusto Moreira Semprebom, Direito, Centro Universitário Integrado, Brasil, joaosemprebom123@gmail.com

Caroline Bittencourt Silveira, Direito, Centro Universitário, Brasil, caroline.silveira@grupointegrado.br

Resumo: O presente artigo tem como objetivo destacar as questões relacionadas à evolução histórica da internet, bem como a evolução dos delitos virtuais e seu significativo avanço, com ênfase em suas consequências negativas. Serão abordadas a responsabilidade do Estado diante das dificuldades na identificação da autoria dos *cibercrimes* e a consequente impunidade dos criminosos, que em sua maioria se ocultam por meio de perfis e endereços IP falsos. O artigo busca apresentar melhorias nas técnicas de identificação dos possíveis autores desses crimes, além de propor soluções que acelerem os processos de identificação e punição, visando um desempenho mais eficiente e célere. Para tanto, foi adotado o método indutivo, utilizando-se de pesquisas bibliográficas, artigos de periódicos, dissertações de mestrado, matérias disponíveis na internet, Julgado de Tribunais, entre outros, relativos à matéria. Busca-se demonstrar através do presente estudo um levantamento amplo e organizado das principais causas das dificuldades na identificação da autoria desses crimes, bem como das soluções propostas para superar esse problema. Além disso, ressaltará a importância de promover o uso correto e seguro da internet e de meios afins como estratégia essencial no combate a tais crimes.

PALAVRAS-CHAVE: Crime Cibernético. Internet. Responsabilidade do Estado. Falta de Punibilidade.

ABSTRACT: This article aims to highlight issues related to the historical evolution of the internet, as well as the evolution of virtual crimes and their significant advancement, with an emphasis on their negative consequences. The State's responsibility will be addressed in the face of difficulties in identifying the authorship of cybercrimes and the consequent impunity of criminals, most of whom hide through false profiles and IP addresses. The article seeks to present improvements in the techniques for identifying possible perpetrators of these crimes, in addition to proposing solutions that speed up the identification and punishment processes, aiming for more efficient and faster performance. To this end, the inductive method was adopted, using bibliographical research, periodical articles, master's theses, materials available on the internet, Court Judges, among others, relating to the matter. It is concluded that the present study will provide a broad and organized survey of the main causes of difficulties in identifying the authorship of these crimes, as well as the solutions proposed to overcome this problem. Furthermore, it will highlight the importance of promoting the correct and safe use of the internet and similar means as an essential strategy in combating such crimes.

KEY-WORDS: Cybercrime. Internet. State responsibility. Lack of Punishment

INTRODUÇÃO:

A sociedade contemporânea enfrenta um novo tipo de delito: os Crimes Virtuais, ou, tecnicamente, os Crimes Cibernéticos. A ausência de identificação dos autores, aliada à falta de punibilidade, agrava a situação das vítimas desses delitos.

É evidente que as redes sociais se tornaram essenciais em diversas esferas, desde a aquisição de produtos, passando pela comunicação, até o lazer, consolidando-se como uma necessidade indispensável.

No contexto da era tecnológica, em que o acesso à informação é fácil e sua disseminação ocorre com notável rapidez, surgem, assim como na sociedade fora do ciberespaço, indivíduos que cometem delitos, conhecidos como "*cibercrimes*".

Assim, a identificação dos autores de crimes cibernéticos na atualidade enfrenta desafios consideráveis, resultando em uma significativa impunidade dos cibercriminosos. Esses indivíduos se ocultam por meio de perfis falsos e localizações fictícias, o que agrava ainda mais a situação. Ademais, a falta de conhecimento das vítimas sobre os potenciais crimes cibernéticos ou virtuais contribui para esse cenário desafiador.

Corroborando com o exposto, o Estado, em sua totalidade, carrega a responsabilidade pelos atos delitivos ocorridos na sociedade. No que tange aos cibercrimes, essa responsabilidade não deveria, nem poderia, ser distinta. Contudo, observa-se uma notável falta de celeridade na resolução desses delitos, acompanhada de uma carência significativa na punição dos criminosos.

Este artigo tem como objetivo propor melhorias no campo da identificação de possíveis cibercriminosos, além de apresentar informações sobre as investigações conduzidas para sua identificação e a aplicação das sanções correspondentes, conforme estabelecido pelo Ordenamento Jurídico Brasileiro.

Dessa forma, é essencial proporcionar à sociedade brasileira o conhecimento acerca desse novo tipo de delito, a fim de evitar que se torne tão recorrente quanto, lamentavelmente, são os crimes penais. Assim, torna-se imprescindível promover o uso correto e seguro da internet.

Portanto, é necessário esclarecer, por meio de prerrogativas, as propostas de melhorias para os problemas já identificados, que este artigo científico busca elucidar.

MÉTODO

Para o desenvolvimento do presente projeto, é necessário tratar da questão principal: A responsabilidade do estado na dificuldade no processo de identificação da autoria e da falta de punibilidade nos crimes cibernéticos, visando elucidar o tema proposto foi adotado o método indutivo, utilizando-se de pesquisas bibliográficas, artigos de periódicos, dissertações de mestrado, matérias disponíveis na internet, julgado de tribunais, entre outros, relativos à matéria.

RESULTADOS E DISCUSSÕES

1 ORIGEM DOS DELITOS VIRTUAIS

1.1 CONTEXTO HISTÓRICO DA INTERNET

A gênese da Internet está intrinsecamente vinculada à resposta do governo dos Estados Unidos ao lançamento do satélite Sputnik pela antiga União Soviética, sob a liderança da Rússia, durante o contexto da Guerra Fria em 1957. A concepção da Internet está profundamente associada ao trabalho de peritos

militares norte-americanos, que desenvolveram a ARPANET, uma rede criada pela Agência de Projetos de Pesquisa Avançada dos Estados Unidos, no cenário de disputa pela hegemonia global com a URSS (Almeida, 2005).

As Forças Armadas dos Estados Unidos, em 1962, segundo Turner e Muñoz (2002, p. 27), “encomendou um estudo para avaliar como suas linhas de comunicação poderiam ser estruturadas de forma que permanecessem intactas ou pudessem ser recuperadas em caso de um ataque nuclear”.

De acordo com Crespo (2011, p. 31, 32) o financiamento disponibilizado pelo governo dos Estados Unidos, por meio das pesquisas realizadas pelo Departamento de Defesa através da ARPA – Agência de Projetos de Pesquisa Avançada, a partir de 1968, foi de importância crucial para o desenvolvimento do sistema de informações em rede.

Concebido inicialmente com propósitos militares, o sistema visava assegurar a continuidade operacional dos componentes, dado que não estavam interligados de maneira hierárquica, uma característica marcante desse setor. A estrutura em rede garantia que o núcleo do programa permanecesse intacto em caso de ataque. Era imperativo que a arquitetura do sistema fosse distinta daquela empregada na rede de telefonia norte-americana (OLIVEIRA, 2014)

O funcionamento da comunicação em rede, conforme relatado por Briggs e Burke (2006, p. 301), permitia que "qualquer computador se conectasse à rede de qualquer lugar, com a informação sendo imediatamente trocada em 'fatias' dentro de 'pacotes'". A ideia de fragmentar mensagens em "pacotes de informação" remonta, segundo Briggs e Burke (2006), a conceitos mais antigos, presentes nas pesquisas de computação desde o final da década de 1960. Para viabilizar essas "trocas" de informações entre máquinas, era essencial a existência de interfaces que permitissem o processo de codificação, decodificação e recodificação entre microcomputadores que utilizavam diferentes formatos e linguagens.

Em 1975, com aproximadamente dois mil usuários, a *Net* oferecia acesso livre a professores e pesquisadores que utilizavam essa tecnologia. As universidades, com uma visão educacional, percebiam a rede como uma oportunidade para a disseminação e o compartilhamento de informações.

Em resumo, a origem da internet está profundamente enraizada no contexto da Guerra Fria, como uma resposta estratégica dos Estados Unidos ao lançamento do Sputnik pela União Soviética. Inicialmente concebida com propósitos militares, a ARPANET foi desenvolvida para garantir a continuidade das comunicações em caso de ataque nuclear, utilizando uma arquitetura de rede descentralizada. O financiamento governamental e as pesquisas conduzidas pelo Departamento de Defesa foram cruciais para o desenvolvimento da rede, que posteriormente se expandiu para além do âmbito militar, tornando-se uma ferramenta vital para universidades, pesquisadores e, eventualmente, para a sociedade global. A evolução tecnológica que permitiu a troca de informações em "pacotes" e a interoperabilidade entre diferentes sistemas foi o alicerce para a transformação da ARPANET na internet que se conhece atualmente.

1.2 O USO DIÁRIO DA INTERNET

A internet representa, sem dúvidas, a maior revolução tecnológica do último século. Com sua expansão, surgem novas tecnologias de informação que transformam o contexto social contemporâneo. A comunicação virtual entre as pessoas se intensifica de forma inédita, contribuindo positivamente para o fenômeno da globalização, ao criar novas oportunidades para práticas comerciais, novos relacionamentos, maior velocidade e acesso irrestrito à informação, entre outras vantagens. Contudo, paralelamente, cresce também o uso desse importante meio tecnológico para a prática de atos ilícitos (TRENTIN, TRENTIN, 2012).

O significativo desenvolvimento tecnológico das últimas décadas, aliado à redução dos custos de dispositivos como smartphones, smart TVs, laptops, tablets, consoles de videogames e computadores pessoais (PCs), possibilitou um crescimento exponencial de usuários na rede mundial de computadores, a Internet. De acordo com dados das Nações Unidas, o Brasil ocupa o 4º lugar em número de internautas, com mais de 120 milhões de pessoas conectadas à rede, conforme dados de 2018 (ANATEL, 2018).

Um relatório da Norton Cyber Security, do início de 2018, colocou o Brasil como o segundo país com maior número de casos de crimes cibernéticos, ficando atrás apenas da China. Por volta de 62 milhões de brasileiros foram afetados por algum crime cibernético em 2017. De acordo com uma pesquisa realizada pela Agência Nacional de Telecomunicações (Anatel), o uso da internet no Brasil cresceu durante a pandemia entre 40% e 50%, número esses que fizeram crescer a pratica dos delitos virtuais.

Em conclusão, embora a internet tenha impulsionado transformações positivas na sociedade, facilitando a globalização, a comunicação e o acesso à informação, seu crescimento exponencial também deu origem a novas formas de criminalidade. O aumento do número de usuários, impulsionado pela acessibilidade de dispositivos tecnológicos, resultou em uma ampliação da vulnerabilidade das pessoas aos crimes cibernéticos. O Brasil, sendo um dos países com maior número de internautas, figura entre os principais alvos desses delitos, conforme demonstrado pelos dados alarmantes sobre o impacto do crime digital. Esse cenário evidencia a necessidade de maior atenção e medidas efetivas para proteger os usuários e mitigar os riscos decorrentes do uso indevido dessa tecnologia.

1.3 OS DELITOS VIRTUAIS (CRIMES CIBERNÉTICOS)

Com o progresso tecnológico, os crimes também se transformaram, seguindo a evolução da internet, esses delitos transitaram para o ambiente virtual, espelhando aspectos da realidade física. A rápida expansão deste novo contexto tem suscitado preocupações substanciais entre os juristas, que frequentemente não conseguem acompanhar tal avanço, resultando em uma legislação defasada em relação às mudanças sociais, dessa forma, os crimes cibernéticos tornaram-se uma presença constante no cotidiano, manifestando-se de formas cada vez mais sofisticadas.

Segundo estudos de Rocha, este define os crimes virtuais como: “Aqueles que têm por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos” (ROCHA, 2000).

Nos crimes cibernéticos, costumam emergir três papéis distintos: o agressor, a vítima e o espectador.

O agressor é aquele que humilha, menospreza ou prejudica os demais para alcançar uma sensação de poder, atrair atenção ou ganhar popularidade no ambiente digital em que atua. Assim, ao exercer sua malícia, o agressor procura satisfazer seus instintos de controle e a sensação de impunidade.

Na internet, o anonimato confere uma vantagem ao agressor, uma vez que sua identidade não está sujeita ao escrutínio público. Isso permite que ele mantenha sua conduta agressiva por vários anos sem atrair atenção. (SANTOMAURO, 2010, apud LUCCHESI, 2018).

Resultando assim em uma dificuldade para imputar a penalização do comportamento desse indivíduo devido à falta de identificação, conferindo-lhe a falsa sensação de impunidade.

A vítima, ou mártir, pode ser qualquer pessoa; no entanto, indivíduos que demonstram insegurança ou desconhecimento acerca do delito tendem a serem alvos mais suscetíveis devido à sua vulnerabilidade, tornando-se, portanto, presas mais fáceis para os agressores.

As agressões implicam em adversidade conforme Ana Beatriz Barbosa Silva (apud SANTOMAURO, 2010, apud LUCCHESI) explica que, agressões como essas, podem desencadear doenças psicológicas na pessoa, como depressão, crises de ansiedade, transtorno de pânico, podendo levar a vítima a tirar sua própria vida.

No âmbito dos crimes cibernéticos, surge a figura do espectador. Embora não participe diretamente da agressão, o espectador exerce um papel fundamental na continuidade da disseminação do ataque. Exemplos dessa dinâmica incluem os milhares de 'likes' ou 'dislikes', que refletem a quantidade de pessoas que visualizam ou interagem com tais publicações.

É como uma testemunha ocular dos fatos ocorridos, porém não possui posição de apoio ou defesa. Muitos incentivam a continuação dos crimes ou simplesmente são omissos aos atos (RODRIGUES, LUCCHESI).

Em síntese, o avanço tecnológico trouxe consigo uma transformação significativa no panorama criminal, especialmente no que tange aos crimes cibernéticos, que espelham e ampliam a realidade física para o ambiente virtual. As implicações desses delitos, somadas à dificuldade de identificação e punição dos agressores devido ao anonimato proporcionado pela internet, tornam esse tipo de crime um desafio para o sistema jurídico contemporâneo.

O impacto psicológico sobre as vítimas, conforme indicado pelos estudos de especialistas, pode ser devastador, culminando em sérios transtornos mentais e, em casos extremos, no suicídio. Além disso, a figura do espectador, embora não atue diretamente, contribui para a perpetuação dessas agressões ao interagir passivamente com o conteúdo. Dessa forma, o fenômeno dos crimes cibernéticos

exige não apenas um arcabouço legal atualizado, mas também uma conscientização mais ampla da sociedade para enfrentar a complexidade e as consequências desse tipo de violência digital.

1.4. MARCO CIVIL DA INTERNET NO BRASIL

A Lei nº 12.965, promulgada em 23 de abril de 2014, constitui o marco regulatório do uso da internet no Brasil, ao dispor sobre os princípios, garantias, direitos e deveres dos usuários, bem como ao estabelecer diretrizes para a atuação do Estado no ambiente digital.

Antes de sua vigência, inexistia uma regulamentação específica para as questões atinentes ao uso da internet, especialmente no que se refere à proteção da privacidade. Tais matérias eram analisadas à luz do artigo 5º da Constituição Federal, que prevê a inviolabilidade do sigilo das correspondências, das comunicações de dados e das comunicações telefônicas, ressalvadas as hipóteses de quebra de sigilo por ordem judicial, conforme disposto em lei para fins de investigação criminal ou instrução processual penal (VIANNA,2023).

A lei tem por objetivo a promoção “do direito de acesso à Internet a todos”, conforme o artigo 4°. Em seguida, no capítulo II, artigo 7º, estabelece que o acesso à Internet seja “essencial ao exercício da cidadania”.

A "neutralidade da rede" constitui um relevante avanço estabelecido pelo Marco Civil da Internet, sendo fruto das demandas de distintos setores da sociedade civil. De acordo com a definição da Coalizão Global pela Neutralidade da Rede, organização que congrega especialistas e ativistas de diversos países, este princípio preconiza que o tráfego na internet deve ser tratado de forma equânime, sem qualquer discriminação, restrição ou interferência, independentemente do emissor, destinatário, tipo de conteúdo ou natureza das informações. Assim, assegura-se que a liberdade dos usuários não seja cerceada por práticas de favorecimento ou restrição de transmissões ligadas a conteúdos, serviços, aplicações ou dispositivos específicos (VIANNA, 2023).

No ordenamento jurídico pátrio, de acordo com o disposto no artigo 9º, da Lei Federal 12.965/2014 (Marco Civil da Internet):

> Art. 9° O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação”, ou seja, corolário do princípio da isonomia na transmissão de pacotes de dados sem qualquer tipo de distinção (BRASIL,204).

Além disso, a Lei versa sobre a liberdade da expressão de seus usuários, em seu artigo 19 o qual foi elaborado a partir de intenso debate multissetorial, que contou com espaços de ampla participação da sociedade civil organizada, do governo e do setor privado.

A legislação define as condições em que um provedor de aplicações de internet, como plataformas de redes sociais, pode ser civilmente responsabilizado por danos decorrentes de conteúdos publicados por terceiros. Conforme o disposto, os provedores somente poderão ser responsabilizados se, após o

recebimento de uma ordem judicial específica, não removerem, dentro do prazo adequado, o conteúdo considerado ilícito (VIANNA, 2023).

O artigo 19 dispõe que a determinação sobre a licitude dos conteúdos publicados nas plataformas cabe, em última instância, ao Poder Judiciário, de modo que tais empresas não podem ser responsabilizadas por material de terceiros, exceto nos casos de descumprimento de ordem judicial de remoção. Embora as plataformas detenham a liberdade para estabelecer suas próprias diretrizes e proceder à moderação de conteúdos, elas não têm a obrigação de indenizar por não atenderem a demandas extrajudiciais formuladas por usuários.

Por último, merece destaque a disposição que garante a proteção de dados e a privacidade dos usuários no contexto digital. O artigo 3º estabelece, entre outros princípios, a proteção da privacidade e dos dados pessoais, que são assegurados aos usuários da internet pelo artigo 7º. Este artigo garante a inviolabilidade e o sigilo do fluxo de suas comunicações, bem como a inviolabilidade e o sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

O artigo 10, §1º, trata especificamente da proteção de registros, dados pessoais e comunicações privadas, esclarecendo que o fornecimento de dados pessoais deve ocorrer unicamente mediante requisição judicial. Dessa forma, o responsável pela guarda dos dados é obrigado a disponibilizá-los sempre que houver solicitação formal por parte de um juiz.

Em suma, a promulgação da Lei nº 12.965/2014, o Marco Civil da Internet, representa um marco significativo na regulamentação do uso da internet no Brasil, estabelecendo um conjunto abrangente de princípios, direitos e deveres que visam garantir a proteção da privacidade, a neutralidade da rede e a liberdade de expressão dos usuários.

Ao definir claramente as responsabilidades dos provedores de serviços e assegurar que o Judiciário detenha a autoridade final sobre a licitude dos conteúdos, a legislação promove um ambiente digital mais seguro e democrático. A ênfase na proteção de dados pessoais e na inviolabilidade das comunicações reforça o compromisso do Estado em resguardar os direitos dos cidadãos no espaço virtual.

Dessa forma, o Marco Civil da Internet não apenas estabelece diretrizes fundamentais para o uso responsável da internet, mas também busca garantir que todos os usuários tenham acesso equitativo a este importante recurso, essencial ao exercício da cidadania no mundo contemporâneo.

2 CONCEITO E CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

2.1 CONCEITOS (DEFINIÇÃO) DO QUE É UM CYBERCRIME

O conceito de cybercrime refere-se a delitos cometidos por meio de sistemas informáticos e redes de computadores, abrangendo diversas atividades ilícitas que utilizam a internet como meio ou alvo. Segundo Luiz Flávio Gomes, "o cybercrime pode ser definido como toda conduta criminosa praticada através do uso de tecnologias da informação e comunicação" (GOMES, 2010).

Já Marco Aurélio Greco destaca que o cybercrime "é caracterizado pela utilização de dispositivos eletrônicos e redes para a prática de atos ilícitos, explorando a vulnerabilidade digital" (GRECO, 2011).

De forma geral, os cybercrimes englobam uma ampla gama de infrações, desde fraudes eletrônicas até ataques cibernéticos mais sofisticados, como roubo de dados, invasão de sistemas e disseminação de malwares. Fernando Capez ressalta que:

> o fenômeno do cybercrime tem características próprias, que dificultam a sua prevenção e a responsabilização dos infratores, especialmente pela velocidade com que as informações transitam no ambiente virtual (CAPEZ, 2012).

Em sentido amplo, a criminalidade informática engloba toda atividade criminosa realizada por computadores ou meios de tecnologia da informação. Em sentido stricto, a criminalidade informação engloba crimes, de acordo com Simas (2014, p. 12), “quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital”. Esses crimes, pela sua natureza transnacional e a dificuldade de identificação dos criminosos, representam um grande desafio para os sistemas de justiça ao redor do mundo.

Com isso a informática pode servir como meio para a prática de crimes tradicionais, ou seja, aqueles que não exigem necessariamente um suporte informacional para serem consumados, nem integram, de forma direta, a tipificação legal. Nesse contexto, é possível mencionar crimes contra a honra e a dignidade da pessoa humana, os quais podem ser perpetrados mediante o uso de recursos tecnológicos para a sua divulgação, como e-mails ou redes sociais (JÚNIOR, 2019).

Além disso, há situações em que a informática atua como elemento integrador, sem que o bem jurídico protegido seja, exclusivamente, a própria tecnologia. Um exemplo são os crimes contra softwares, onde o bem jurídico tutelado não é a informática em si, mas os direitos autorais associados ao software (JÚNIOR, 2019).

A doutrina jurídica brasileira, através da Lei n.º 12.737, de 30 de novembro de 2012, que trata da criminalização de delitos informáticos, modifica o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – o Código Penal – e estabelece outras medidas correlatas. No Art. 154-A, essa legislação define de maneira clara os crimes praticados por meio de recursos tecnológicos.

> Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012, s.p.)

A legislação penal brasileira prevê a imposição de pena de detenção de 3 (três) meses a 1 (um) ano, cumulada com multa. Além disso, a referida norma estipula que estará sujeito a essa sanção aquele que produzir, oferecer, distribuir, comercializar ou disseminar dispositivos ou programas de computador com o objetivo de facilitar a prática de condutas ilícitas, especialmente quando houver dano econômico ou quando a invasão resultar na obtenção de conteúdo

confidencial. Nos casos de maior gravidade, a pena de reclusão pode ser aplicada, variando de 6 (seis) meses a 2 (dois) anos, também acompanhada de multa. Ademais, a penalidade será aumentada se o delito for praticado em detrimento da Administração Pública municipal, estadual ou federal.

Em conclusão, o *cybercrime* representa um fenômeno em constante evolução, que abrange tanto crimes tradicionais adaptados ao ambiente digital quanto delitos que têm a tecnologia como elemento central. A crescente sofisticação das atividades criminosas no ciberespaço impõe desafios significativos aos sistemas de justiça, especialmente em razão de sua natureza transnacional e da dificuldade de identificação dos autores. A legislação brasileira, por meio da Lei n.º 12.737/2012, procurou avançar na tipificação desses crimes, estabelecendo penalidades proporcionais às condutas ilícitas cometidas no âmbito digital. No entanto, a celeridade com que as tecnologias se desenvolvem demanda constante atualização normativa e aprimoramento dos mecanismos de combate ao cibercrime, visando à proteção eficaz dos direitos individuais e coletivos, bem como à segurança da informação em um mundo cada vez mais interconectado.

2.2. A CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Os delitos ocorridos no ambiente digital são frequentemente denominados como crimes cibernéticos, digitais, eletrônicos, informáticos, crimes na internet, *cybercrimes*, fraudes eletrônicas, delitos computacionais, entre outros. Independentemente da nomenclatura, todos se referem à prática de atos ilícitos no meio digital.

Dessa forma, torna-se imperativa a necessidade de classificar os diversos tipos de crimes praticados no ambiente digital. A esse respeito, existem inúmeras classificações doutrinárias, amplamente debatidas e apontadas por diversos autores no campo jurídico.

Segundo o conceito doutrinário, os delitos no ambiente digital podem ser classificados em ações prejudiciais atípicas e crimes cibernéticos. As ações prejudiciais atípicas são condutas que, embora causem danos ou transtornos às vítimas por meio da rede mundial de computadores, não possuem tipificação específica na legislação vigente, escapando, portanto, de uma punição direta no campo jurídico. Essas ações, apesar de não configurarem crimes no sentido estrito, podem gerar graves consequências, como a violação de direitos pessoais e patrimoniais, o que evidencia a necessidade de atualizações legislativas para abarcar novas modalidades de condutas nocivas (JORGE; WENDT, 2012).

Por outro lado, os crimes cibernéticos dividem-se em duas categorias principais: crimes cibernéticos abertos e crimes exclusivamente cibernéticos. Os crimes exclusivamente cibernéticos são aqueles que só podem ser cometidos por meio do uso de tecnologia da informação. Um exemplo clássico é o crime de invasão de dispositivo informático, previsto nos artigos 154-A e 154-B do Código Penal, introduzido pela Lei 12.735/2012, conhecida como a Lei Carolina Dieckmann, que surgiu em resposta à crescente necessidade de regulamentar condutas ilícitas relacionadas à privacidade e segurança digital. Nesses casos, a ação criminosa depende diretamente do ambiente informático para sua

realização, não podendo ocorrer sem o uso de dispositivos digitais ou redes de comunicação (JORGE, 2012).

Os crimes cibernéticos abertos são aqueles que podem ser praticados por meio digital como também fora dele. Um exemplo é o crime de violação de direitos autorais, que pode ocorrer tanto no ambiente virtual, com a distribuição ilegal de conteúdo protegido por direitos autorais através da internet, quanto no mundo físico, por meio da reprodução não autorizada de obras. Essa dualidade demonstra a flexibilidade de certas infrações, que se adaptam ao contexto digital e também ao analógico, o que impõe desafios para a tipificação legal e para a atuação dos órgãos de repressão (WENDT, 2012).

Esse panorama evidencia a complexidade dos crimes cibernéticos e a necessidade de uma constante atualização das normas jurídicas, a fim de abarcar as especificidades dos delitos praticados no ambiente digital, que se expandem e evoluem com o avanço da tecnologia e o aumento da conectividade global.

Outra parte da doutrina entende que os crimes cibernéticos podem ser estudados, levando-se em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito:

> (...) 1) quando o computador é o alvo – p. Ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação de conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo por fora da empresa; 2) quando computador é o instrumento para o crime – ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraude de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime – ex.: crimes contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado; 4) quando o crime está associado com computador – p. Ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas de comércio ilegal de equipamentos e programas (Ferreira 2021, pg.135).

Outra corrente doutrinária classifica os crimes relacionados à informática em três categorias: crimes puros, crimes mistos e crimes comuns.

Os crimes puros são aqueles em que o sistema informático constitui o principal alvo do agente. Nesses casos, as condutas incluem, por exemplo, atos de vandalismo direcionados à integridade dos sistemas ou acessos não autorizados a dispositivos informáticos. Os crimes mistos, por sua vez, ocorrem quando o agente visa a um bem jurídico distinto do informático, mas utiliza o sistema informático como ferramenta indispensável para a realização do delito. Por fim, os crimes comuns são aqueles em que o sistema informático é empregado como um recurso adicional, mas não essencial para a consumação do crime. Neste contexto, a informática atua apenas como uma ferramenta auxiliar, não sendo imprescindível para a prática delituosa (TEIXEIRA, 2014).

De acordo com Tulio Viana e Felipe Machado (2013), os crimes digitais podem ser classificados em quatro categorias, tendo como principal bem jurídico

protegido pela legislação penal a inviolabilidade da informação automatizada (dados).

Os crimes informáticos impróprios referem-se àqueles em que o computador é utilizado como meio para a prática do delito, mas que não envolvem a infração da inviolabilidade da informação automatizada. Exemplos dessa categoria incluem ameaças e incitação ao crime. Em contrapartida, os crimes informáticos próprios são aqueles que visam especificamente proteger a inviolabilidade de dados. Um exemplo significativo é o crime de invasão de dispositivo informático, previsto nos artigos 154-A e 154-B do Código Penal, assim como a inserção de dados falsos em sistemas de informações, conforme estipulado no artigo 313-A, e a modificação ou alteração não autorizada de sistemas de informações, conforme o artigo 313-B do mesmo código (MACHADO; VIANA, 2013).

Os crimes mistos são caracterizados pela proteção da inviolabilidade de dados, ao mesmo tempo em que visam resguardar um bem jurídico de natureza distinta, como exemplificada pelo crime eleitoral previsto no artigo 72 da Lei nº 9.504/1997. Finalmente, os crimes informáticos mediatos ou diretos são aqueles considerados delitos de natureza não informática, mas que utilizam o meio digital como um elemento essencial para a consumação do crime.

Dessa forma, podem ser considerados crimes digitais aqueles que se realizam no ambiente digital, incluindo, mas não se limitando a: crimes contra a honra, ameaças, induzimento ou instigação e auxílio ao suicídio, furto, falsificação de documentos, estelionato, espionagem industrial, violação de segredo, apologia a crimes, racismo, atentados contra serviços de utilidade pública, pornografia infantil, corrupção de menores em salas de bate-papo na internet, violação de direitos autorais, inserção de dados falsos em sistemas de informações, crimes contra equipamentos de votação e invasão de dispositivos informáticos.

3 A RESPONSABILIDADE DO ESTADO NOS CRIMES CÍBERNETICOS

3.1. A CO-CULPABILIDADE E A RESPONSABILIZAÇÃO DO ESTADO NO CRIME EM UM CONTEXTO GERAL.

É amplamente reconhecido que indivíduos em condições socioeconômicas desfavoráveis frequentemente recorrem ao crime como meio de assegurar sua subsistência no contexto social em que estão inseridos. Todavia, o Estado dispõe de instrumentos para conter essas condutas, que comprometem a “ordem social”, utilizando-se, para tanto, de medidas coercitivas (BAYER, 2014).

O Direito Penal exerce uma função crucial, configurando-se como o principal mecanismo de controle social na contemporaneidade e se destacando pela eficácia na repressão de determinadas práticas e na proteção dos bens mais valiosos para a sociedade. Dessa forma, é considerado a *última ratio*, sendo acionado quando os demais ramos do direito revelam-se inadequados.

Dentre os mecanismos de controle exercidos pelo Estado, pode-se citar a prisão, um dos recursos empregados pelo Direito Penal com o objetivo de reabilitar o autor do delito, também reflete as mazelas sociais, já descritas por Beccaria em sua obra Dos Delitos e das Penas:

> As vantagens de uma sociedade devem ser distribuídas equitativamente entre todos os seus membros. Entretanto, numa reunião de homens, percebe-se a tendência contínua de concentrar no menor número os privilégios, o poder e a felicidade, e só deixar à maioria miséria e debilidade (BECCARIA, 2006, p. 15).

O conceito de co-culpabilidade surgiu em resposta à omissão do Estado em prover recursos essenciais para uma existência digna, o que contribui para o aumento da criminalidade.

Esse princípio visa considerar os fatores sociais que impactam a prática de atos ilícitos, investigando se tais atos decorrem da falha estatal em garantir condições básicas de vida. Assim, busca-se atribuir ao Estado uma parcela de responsabilidade e, consequentemente, reduzir a reprovação social sobre o indivíduo. Como destaca Silva (2011, p. 2):

> O princípio da co-culpabilidade reconhece, com certo compromisso, as desigualdades sociais inerentes ao modo capitalista de produzir como importantes condicionantes de certos crimes, defendendo meios de se compensar a seletividade do direito penal que incide em maior frequência nos setores sociais marginalizados da sociedade.

Em outra direção, pergunta-se qual a legitimidade do Estado para cobrar respeito a deveres, se ele próprio não cumpre os deveres de estado mais básicos que compromete a fornecer a sociedade, deveres estes que são assegurados a todos na Constituição Federal.

Quando o indivíduo se encontra em situação de vulnerabilidade e não dispõe de meios para se manter dentro da ordem social e assegurar uma vida digna, a probabilidade de que ele adote uma atividade criminosa aumenta (BAYER,2014).

Assim, se o Estado, por negligência, deixa de oferecer ao indivíduo direitos fundamentais, como saúde, educação e inclusão socioeconômica, deve compartilhar a responsabilidade pelo ato delituoso, ao lado do infrator, e atenuar a reprovação sobre ele, considerando que certos crimes resultam das desigualdades que o próprio Estado, por omissão, contribuiu para criar.

Portanto, ao violar constantemente os deveres que assumiu, o Estado também se torna responsável pelas desigualdades sociais, cabendo-lhe reconhecer sua parcela de responsabilidade na criminalidade.

É importante ressaltar, entretanto, que o princípio da co-culpabilidade não busca transferir ao Estado a infração penal em si, mas sim reconhecer sua parcela de responsabilidade no contexto do crime, sem desvirtuar sua função punitiva. Conforme destaca Silva (2011, p. 14):

> [...] não se quer culpar o Estado por um crime cometido por um individuo, mas responsabilizá-lo em virtude de sua ausência prévia quando não forneceu condições para que aquele indivíduo tomasse outro rumo que não o estreito caminho da conduta ilícita.

Em uma pesquisa exploratória, constatou-se que os dados referentes ao Brasil revelam índices alarmantemente elevados de criminalidade.

João Farias Júnior (2008, p. 75) explica que a população cresce, em média, 2% ao ano, enquanto a criminalidade aumenta a uma taxa de 20% ao ano. O índice de reincidência no Brasil atinge 80%. Em 1990, havia 90 mil presos; em 1996, esse número subiu para 150 mil; em 2007, alcançou 476 mil, e em 2008, o total era de 550 mil detentos, em 2022 total de presos era de 839, 7 mil pessoas, conforme dados Senappen em fevereiro de 2024. Tal crescimento descontrolado é preocupante e contraria qualquer norma que vise à obtenção da paz. Esses índices evidenciam a ineficácia do Sistema Penal.

Em suma, a co-culpabilidade e a responsabilização do Estado no contexto da criminalidade revelam uma interconexão entre as desigualdades sociais e a prática de atos delituosos. A ineficácia do Sistema Penal, evidenciada pelos alarmantes índices de criminalidade e reincidência, destaca a necessidade urgente de uma abordagem que não apenas reconheça a responsabilidade do indivíduo, mas também a do Estado, que deve garantir condições mínimas para uma vida digna. O fortalecimento das políticas públicas e a promoção da inclusão socioeconômica são imperativos para mitigar esses problemas e restaurar a confiança na ordem social.

3.2 A COMPETÊNCIA TERRITORIAL DE JULGAMENTO DOS CRIMES CIBÉRNETICOS CORRELACIONADA COM A RESPONSABILIDADE DO ESTADO EM SUA CONSUMAÇÃO

É importante, compreender que os crimes cibernéticos não têm impacto apenas no território brasileiro. Devido à velocidade de propagação proporcionada pelo meio digital, esses crimes podem alcançar também outros países, afetando, portanto, diversas nações além do Brasil, Consoante Ferreira (2001, p. 212-213), diz que:

> “A mobilidade dos dados nos sistemas de informática, que facilita largamente que os delitos sejam cometidos à distância, usando-se um computador num determinado país e ocorrendo os resultados em outro, bem como os atentado às redes de telecomunicações internacionais, que atravessam vários países, o uso indevido de programas importados, a necessidade de proteção dos exportados, tudo isso provocou a internalização da questão, que deve ser discutida pelos diversos países para a harmonização das normas penais aplicáveis e de outras medidas de caráter extra-penal”.

Dessa forma, torna-se imprescindível que o Brasil busque cooperação internacional para a investigação e o julgamento de crimes cibernéticos, visto que, pela própria natureza e pelos meios de execução desses delitos, suas consequências podem extrapolar as fronteiras nacionais e alcançar diversas jurisdições ao redor do mundo.

Destaca-se que o Brasil integra tratados e convenções que permitem a aplicação de normas processuais penais a crimes originados em território nacional, ainda que seus efeitos se façam presentes em outras nações. Exemplos desses instrumentos incluem a Convenção sobre o Crime de Racismo e a Pornografia Infantil (VALIN apud ARAS, 2001).

No que concerne à pornografia infantil, o Decreto Legislativo nº 28, de 24 de setembro de 1990, e o Decreto Presidencial nº 99.710, de 21 de novembro de 1990, incorporaram ao ordenamento jurídico brasileiro a Convenção da ONU sobre os Direitos da Criança. Já o crime de racismo, tipificado pela Lei nº 7.716/89, é uma prática vedada pela Convenção sobre a Eliminação de Todas as Formas de Discriminação Racial, ratificada pelo Brasil em 1968 e vigente no país desde a promulgação do Decreto Presidencial nº 65.810, de 8 de dezembro de 1969 (MPF/SP, 2006).

Entretanto, o Brasil não figura como signatário da Convenção de Budapeste, um dos mais relevantes tratados internacionais no enfrentamento aos crimes cibernéticos. Esta convenção, estabelecida na Hungria, serve como referência para os países aderentes na aplicação de normas penais e processuais relativas a crimes cometidos pela internet e ataques a sistemas informáticos (crimes cibernéticos propriamente ditos).

A competência para o julgamento de crimes no campo da informática deve observar o território e a jurisdição em que o delito ocorreu. Segundo o entendimento de Celso Valin, o principal obstáculo decorre do caráter transnacional da rede: na internet, não há fronteiras, de modo que qualquer conteúdo publicado se encontra disponível em escala global. Surge, assim, a questão de como determinar o foro competente para julgar um crime cibernético específico (VALIN apud ARAS, 2001).

O artigo 70 do Código de Processo Penal dispõe que a competência territorial é definida pelo local onde a conduta criminosa se consumou ou, em caso de tentativa, pelo local do último ato de execução. Távora e Alencar (2013, p. 262) complementam, ao salientar que essa norma deve ser lida em conjunto com o artigo 14, inciso I, do Código Penal, que considera consumado o crime quando todos os elementos de sua definição legal estão presentes.

Considerando que o crime cibernético ocorre em um meio cujos efeitos podem extrapolar limites locais e, por vezes, alcançar a esfera internacional, torna-se essencial analisar tais delitos com base na extensão de seus impactos. Caso os efeitos da conduta se restrinjam ao território nacional, ainda que em várias localidades (crimes plurilocalizados), aplica-se a jurisdição interna. Entretanto, se a conduta ultrapassar as fronteiras do país, impactando outras nações, trata-se de um crime transnacional ou de alcance à distância (OLIVEIRA, 2011).

É relevante destacar que, em crimes plurilocais nos quais a conduta tenha sido praticada em mais de um local, será considerado, para a definição de competência sob a perspectiva de crime em sua forma tentada, o local onde ocorreram os últimos atos executórios (OLIVEIRA, 2011, p. 267).

Nesse sentido Tourinho Filho (2012, p. 147) explica que:

> Nem se pode, nem se deve invocar a regra do artigo 6º do CO, segundo a qual “considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”, porquanto essa norma diz respeito, apenas e tão somente, às hipóteses em que se deve aplicar a lei brasileira, tendo em vista o ordenamento jurídico de outros Estados soberanos. Assim, para que seja

> determinada a competência em razão do lugar em consonância com o previsto pela lei processual penal brasileira no tocante aos crimes cibernéticos, é necessário saber antes de qualquer coisa saber se o lugar onde se deu o resultado ou teve o último ato de execução do crime (tentativa) faz parte da composição do território nacional brasileiro (n.p).

Assim, quando é possível localizar o dispositivo utilizado pelo agente para cometer o crime, a questão da competência se resolve. Por exemplo, se Cabral criou uma página na internet no laboratório de informática da Universidade Veiga de Almeida, no Rio de Janeiro, contendo mensagens discriminatórias contra um grupo religioso específico, a competência para o processo e julgamento será da comarca do Rio de Janeiro (CASTRO, 2003, p. 107).

A teoria do resultado é particularmente relevante em crimes plurilocais, em que os atos executórios ocorrem em um local distinto do lugar onde o resultado se consuma, desde que ambos se situem dentro do território nacional. Como exemplo, pode-se citar o caso de uma carta injuriosa redigida em Teresina e enviada a João Pessoa, onde a vítima reside. Nesse cenário, a competência territorial será de João Pessoa, local onde a infração foi consumada (TÁVORA; ALENCAR, 2013, p. 262).

Nos crimes à distância, Capez (2012, p. 277) explica que, se um crime é praticado no Brasil e o resultado ocorre em outro país, aplica-se a teoria da ubiquidade, conforme o artigo 6º do Código Penal Brasileiro. Nesse caso, a competência pode ser tanto do local onde ocorreu a ação ou omissão quanto do lugar onde se produziu o resultado. Assim, o foro competente será o do local onde se praticou o último ato de execução no Brasil (art. 70, § 1º) ou o lugar no exterior onde o resultado se materializou, como exemplo o autor dispões a seguinte situação: o agente escreve uma carta injuriosa em São Paulo, e a vítima lê o conteúdo ofensivo em Buenos Aires. A competência, então, será de São Paulo ou Buenos Aires.

Oliveira (2011, p. 266-267) observa, de forma relevante, que a jurisprudência vem abrandando, em casos excepcionais, o rigor da teoria do resultado, permitindo a competência do foro onde ocorreu a ação criminosa, mesmo que a consumação tenha ocorrido em outro local, em função da preservação do conjunto probatório disponível.

A pesquisa jurisprudencial demonstra que, para os crimes cometidos via internet ou dispositivos informáticos, a teoria da ubiquidade é aplicada no Brasil. Contudo, essa aplicação não visa estritamente à determinação do local do crime para fins de aplicação da lei penal, conforme o artigo 6º do Código Penal, mas busca garantir a preservação das provas geradas por tais crimes. Em determinados casos, a competência é definida pelo local do provedor de acesso, pelo local de consumação do crime ou com base no critério de prevenção.

Em síntese, a complexidade dos crimes cibernéticos, especialmente aqueles de natureza transnacional, exige uma abordagem cuidadosa na determinação da competência territorial e jurisdicional. A teoria da ubiquidade, aliada ao entendimento de que o impacto de tais crimes pode transcender fronteiras, proporciona um arcabouço jurídico essencial para a aplicação da lei penal tanto em âmbito nacional quanto internacional. A preservação das provas e

a definição clara do foro competente são aspectos cruciais para garantir a eficácia da investigação e do julgamento desses delitos, reforçando a importância da cooperação entre os países e a harmonização das normas processuais no combate ao crime cibernético.

3.3 A LEGISLAÇÃO VIGENTE

No Brasil, como já foi anteriormente abordado, a legislação não avança na mesma medida da evolução tecnológica; contudo, existem certos dispositivos legais que merecem ser destacados.

É imprescindível salientar que, conforme o artigo 5º, inciso XXXIX, da Constituição Federal Brasileira, o qual dispõe: “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal (BRASIL, 1988)” Este princípio expressa a reserva legal e a legalidade, significando que, para a imposição de sanções relativas a práticas criminosas no ambiente digital, deve haver uma previsão legal anterior que qualifique tais ações como crimes. Assim, a conduta deve estar previamente tipificada como crime e se ajustar aos tipos penais estabelecidos; do contrário, será considerada uma conduta atípica.

Em relação aos crimes virtuais, por um longo período, persistiu uma significativa lacuna jurídica. No entanto, a partir de 2012, foram aprovadas as primeiras legislações específicas sobre o assunto, as quais introduziram inovações significativas no âmbito do Direito Digital.

A primeira dessas legislações foi a Lei 12.735/12, que estabeleceu a criação de delegacias especializadas no combate a crimes praticados em redes de computadores, dispositivos de comunicação e sistemas informatizados (BRASIL, 2012).

De acordo com ALMEIDA (2015), essa legislação também promoveu alterações no inciso II do § 3º do art. 20 da Lei 7.716/89, que aborda os crimes de preconceito de raça ou cor, conferindo ao juiz a prerrogativa de determinar a suspensão de transmissões eletrônicas.

Ainda no ano de 2012, a Lei 12.737/12 tipificou atos como invasão de computadores, roubo de senhas, violação de dados de usuários e divulgação de informações pessoais (tais como fotos e mensagens). Essa legislação é frequentemente referida como Lei Carolina Dieckmann, em alusão ao caso da divulgação não autorizada de fotos íntimas da atriz na internet.

Em 2014, foi sancionada a Lei 12.965, comumente conhecida como Marco Civil da Internet, que regulamentou os direitos e deveres dos internautas, estabelecendo a proteção de dados pessoais e a privacidade dos usuários. Dessa forma, a quebra de dados e informações pessoais em sites ou redes sociais somente pode ocorrer mediante ordem judicial, o que impõe desafios à investigação por parte das autoridades competentes (BRASIL, 2014)

Além disso, em 2020, entrou em vigor a Lei 13.709/18, também chamada de Lei Geral de Proteção de Dados, que regulamenta a política de proteção de dados pessoais e privacidade, alterando alguns artigos do Marco Civil da Internet e influenciando a forma como empresas e órgãos públicos lidam com a segurança e a privacidade das informações de usuários e clientes.

É importante ressaltar o projeto de lei 1.258/2020, que visa criminalizar a disseminação de notícias falsas (fake news) durante períodos de calamidade pública, estado de defesa, ou de sítio e intervenção no meio digital.

Além da Lei nº 14.155/2021 (Lei do Estelionato Digital) introduziu a criminalização do crime de furto qualificado mediante fraude eletrônica, popularmente conhecido como "golpe do Pix" (BRASIL, 2021).

Esse contexto evidencia um avanço gradual na legislação brasileira em resposta à crescente complexidade dos crimes virtuais, embora os desafios ainda sejam significativos. A partir de 2012, com a promulgação de legislações específicas, o Brasil começou a preencher lacunas jurídicas que por muito tempo comprometeram a eficácia das ações de prevenção e combate aos delitos cibernéticos. As leis mencionadas, incluindo o Marco Civil da Internet e a Lei Geral de Proteção de Dados, marcam importantes etapas na proteção dos direitos dos usuários e na regulamentação das práticas digitais.

No entanto, a continuidade da evolução tecnológica demanda um acompanhamento constante por parte dos legisladores, a fim de garantir que a legislação se mantenha atualizada e eficaz diante das novas ameaças e desafios que surgem no ambiente digital. Assim, o fortalecimento e a atualização das normas jurídicas são essenciais para assegurar a proteção dos cidadãos e a integridade do ambiente virtual no Brasil.

4 A FALTA PUNIBILIDADE DOS CRIMINOSOS VIRTUAIS

4.1 COMO A DIFICULDADE DA IDENTIFICAÇÃO IMPACTAM NA PUNIBILIDADE DOS DELITOS VIRTUAIS

Com o progresso tecnológico e a utilização intensiva de dispositivos eletrônicos, os crimes virtuais têm aumentado de forma proporcional, uma vez que os infratores estão em constante aprimoramento de suas técnicas. Contudo, as autoridades encarregadas da investigação e punição desses delitos frequentemente não conseguem acompanhar o ritmo de evolução.

A investigação e a sanção dessas infrações são dificultadas pelo fato de que muitos criminosos atuam de maneira a deixar o mínimo de vestígios, utilizando o ambiente digital para agir de forma anônima e discreta. Tal circunstância torna a identificação desses indivíduos mais complexa, visto que os infratores costumam empregar dispositivos tecnológicos em locais públicos, valendo-se de recursos que lhes permitem operar sem revelar sua identidade (MEIRELES, 2020).

O anonimato é especialmente associado à Deep Web, uma porção da internet que não é indexada pelos mecanismos de busca convencionais e que é utilizada para comunicações e trocas de arquivos de maneira sigilosa. O acesso à Deep Web é predominantemente realizado por meio de aplicativos como o TOR (The Onion Router), que oculta os rastros dos usuários. Apesar das medidas de segurança oferecidas, alguns sites exigem que os usuários façam login utilizando navegadores comuns, o que pode comprometer parcialmente a privacidade (TOCANTINS, 2023).

É imperativo mencionar a Dark Web, uma subparte da Deep Web, onde os sites e redes também não são indexados por mecanismos de busca. No entanto, a Dark Web se distingue por ser predominantemente utilizada para práticas criminosas, sustentando-se na dificuldade de rastreamento das atividades realizadas em suas redes. A principal diferença entre essas duas camadas é que a Dark Web é focada em atividades ilícitas, enquanto a Deep Web abriga domínios essenciais para o funcionamento da internet.

Conforme afirma o advogado criminalista e especialista em cibercrimes D'URSO (2019), em entrevista ao Jornal Estadão, uma das maiores dificuldades no combate a esses delitos reside na complexidade de se estabelecer provas e investigar a origem dos crimes, incluindo a materialidade e a autoria. Além disso, a falta de conhecimento técnico por parte dos usuários, que muitas vezes são as supostas vítimas, os torna alvos vulneráveis para os cibercriminosos, e a variedade de delitos é praticamente ilimitada.

Um dos principais obstáculos é a falta de preparo dos profissionais encarregados de lidar com essa problemática, que afeta diretamente a eficiência de suas ações, especialmente no que diz respeito ao domínio da tecnologia. Além disso, há uma carência de ferramentas adequadas para investigação, sendo crucial que as instituições forneçam os meios necessários para aprimorar o desempenho de seus colaboradores.

Outro empecilho significativo está relacionado à obtenção de provas criminais por meio de perícias. Para que o perito possa realizar um exame, é imprescindível que ele tenha acesso ao dispositivo eletrônico do infrator; no entanto, a análise é frequentemente realizada de forma indireta, utilizando outro aparelho similar, o que requer autorização da autoridade competente.

Assim leciona FROTA e PAIVA (2017):

> Como no flagrante, onde se consegue o IP (internet protocol) do computador, porém é necessária a autorização judicial para a obtenção das informações disposta pelo IP, que são localização da máquina e os acessos feitos na mesma, contudo os provedores não armazenam tais informações por um longo tempo. O que compromete a eficácia do trabalho do agente combatente (n.p).

Outro elemento que dificulta a obtenção de provas e a punição dos delitos virtuais é a insuficiência na capacitação dos profissionais especializados no combate a esses crimes. É imperativo que os responsáveis por esta área busquem atualização contínua para exercer suas funções de maneira eficaz.

Ademais, o Brasil enfrenta um desafio considerável decorrente do atraso na criação de legislações específicas sobre o tema, as quais devem ser elaboradas em consonância com a evolução da sociedade. Tais questões configuram alguns dos obstáculos que permeiam a abordagem dessa problemática. Então, FROTA e PAIVA (2017) mencionam:

> Portanto, fica claro que os avanços que até aqui ocorreram em virtude dos crimes virtuais são, contudo, poucos em meio ao grande mundo cibernético e a ilimitada conduta ilícita dos que, travestido de usuários de boa-fé, agem em busca de suas vítimas. Sendo assim, faz-se necessário que seja repensada a maneira,

> pela qual os operadores do direito estão colaborando para a repressão dessas condutas (n.p).

Outro desafio encontrado diz respeito aos aplicativos de comunicação, como WhatsApp, Facebook, Instagram e Telegram, nos quais o suporte à proteção dos usuários é insatisfatório. Um dos mecanismos de controle utilizados por esses sistemas para garantir a segurança é a notificação por meio de alertas quando novos dispositivos se conectam à conta do usuário. Contudo, conforme já mencionado, essa proteção não se revela completamente segura. Assim, é imperativo implementar melhorias na comunicação entre os usuários e os desenvolvedores ou criadores do sistema, além de garantir acessibilidade para aqueles que não têm familiaridade com o uso do aplicativo. Adicionalmente, recomenda-se a disponibilização de cartilhas informativas que orientem os usuários sobre como se proteger contra roubos, fraudes de conta e acessos indevidos a informações privadas (TOCANTINS, 2023).

Na ausência de uma lei específica, a Justiça tem recorrido principalmente ao Código Penal (Decreto-Lei 2.848/40) para punir os chamados crimes digitais ou cibernéticos. O relator do projeto que tipifica essas condutas (PL 84/99), deputado Regis de Oliveira (PSC-SP), estima que cerca de 95% dos crimes praticados na rede mundial podem ser julgados com base na legislação vigente. No entanto, para os 5% restantes pode imperar a impunidade.

Especialista em Direito Digital, o advogado Alexandre Atheniense sustenta que, sem lei específica, os crimes típicos de internet dificilmente são punidos, porque a legislação penal não admite analogia.

> Se o fato não está definido como crime não há punição; acesso não autorizado a sistema, como aconteceu recentemente na Receita Federal, não é crime, mas passará a ser se o projeto for aprovado.

Regis de Oliveira argumenta que "os hackers e os pedófilos estão se aproveitando disso". Segundo ele, "os juízes têm de dar um jeito de espremer uma interpretação para condenar esses crimes, de pedofilia, de invasão da intimidade das pessoas". De acordo com Oliveira, "a omissão é do Congresso, que tem de dar uma resposta" (2003, pg. 268).

Um levantamento realizado pela empresa Symantec, fabricante de softwares de segurança, mostrou que cerca de 80% dos usuários de internet no Brasil não acreditam que os autores de crimes cibernéticos serão levados à Justiça. Os estudos também apontaram que 76% dos brasileiros adultos usuários da internet já foram vítimas de algum crime digital. O índice é 11 pontos percentuais maior que o vigente para a população global adulta alvo desse tipo de contravenção.

Segundo Alexandre Atheniense, os crimes praticados por meio eletrônico no mundo em 2010 já superaram, em termos de prejuízo de valor, os crimes presenciais, como roubo de ativos físicos ou de estoques.

Em síntese, a evolução tecnológica, embora traga inúmeras facilidades, também propicia um ambiente favorável para o aumento dos crimes virtuais, que, por sua natureza, desafiam as capacidades das autoridades responsáveis pela investigação e punição. A atuação discreta e anônima dos infratores,

frequentemente respaldada por recursos da Deep e da Dark Web, complica ainda mais o cenário, tornando a identificação e a responsabilização uma tarefa árdua. As dificuldades são ampliadas pela falta de preparo e capacitação dos profissionais encarregados do combate a esses delitos, bem como pela carência de legislação específica que se adeque à realidade dinâmica do cibercrime.

Adicionalmente, a inadequação das ferramentas disponíveis para investigação e a insuficiência de suporte nos aplicativos de comunicação contribuem para a vulnerabilidade dos usuários. A percepção de impunidade, evidenciada por pesquisas que revelam a desconfiança da população em relação à justiça, agrava o quadro e ressalta a urgência de uma resposta legislativa e institucional robusta. Assim, é imperativo que haja uma reavaliação das estratégias de combate ao cibercrime, incorporando inovação e colaboração entre todos os envolvidos, a fim de garantir a segurança e a proteção dos usuários na era digital (ALMEIDA, 2015).

Diante desse contexto, é patente que a crescente complexidade dos crimes virtuais demanda uma abordagem multifacetada e coordenada para enfrentar os desafios impostos por essa nova realidade. A ineficácia das investigações, a carência de capacitação adequada dos profissionais envolvidos e a ausência de legislações específicas ressaltam a urgência de ações concertadas para robustecer a resposta do Estado contra as práticas ilícitas no ambiente digital. A implementação de programas de capacitação contínua para os agentes de segurança, em conjunto com o desenvolvimento de legislações mais rigorosas e abrangentes, é imprescindível para que as autoridades consigam combater de forma efetiva a criminalidade cibernética.

Além disso, torna-se fundamental estabelecer um ambiente de conscientização e educação voltado aos usuários, capacitando-os a reconhecer e se resguardar de ameaças digitais. Somente por meio de uma ação integrada, que contemple tanto a necessidade de inovação tecnológica quanto a proteção dos direitos individuais, será possível mitigar os riscos associados aos crimes virtuais e promover um ambiente digital mais seguro para toda a sociedade.

5 A LEGISLAÇÃO NO AMBITO MUNDIAL EM COMPARAÇÃO A BRASILEIRA

Os crimes cibernéticos estão se tornando cada vez mais frequentes e representam uma crescente preocupação na sociedade atual. Esses ataques, que ocorrem globalmente, geram grandes prejuízos para indivíduos, empresas e governos. A questão da responsabilidade penal por tais delitos é complexa e depende das particularidades legais de cada nação.

Nos Estados Unidos, a legislação federal constitui a principal base normativa relacionada aos crimes cibernéticos. A Lei de Fraude e Abuso de Computadores (Computer Fraud and Abuse Act - CFAA) destaca-se como uma das legislações mais significativas nesse âmbito. Sancionada pelo Congresso em 1986, a CFAA tem sido objeto de diversas atualizações ao longo do tempo. Essa legislação impõe sanções a indivíduos que realizam acessos ilegais a computadores, bem como àqueles que provocam danos a sistemas ou dispositivos eletrônicos. Ademais, a CFAA estabelece punições para o

compartilhamento não autorizado de informações confidenciais ou sigilosas. (UNITED STATES DEPARTMENT OF JUSTICE, 2021).

No Reino Unido, a Lei de Uso Indevido de Computadores (Computer Misuse Act) representa a norma predominante no tratamento dos crimes cibernéticos. Essa legislação prevê sanções para indivíduos que realizam o acesso a sistemas de computador sem a devida autorização, assim como para aqueles que causam danos a tais sistemas. É importante ressaltar que a legislação britânica classifica a disseminação de vírus ou malware como um crime. Adicionalmente, a referida lei estabelece penalidades para delitos cibernéticos associados à "espionagem industrial" e ao furto de segredos comerciais.

Na Alemanha, a responsabilização penal pelos crimes cibernéticos encontra-se regulada no Código Penal. As condutas delituosas relacionadas aos sistemas de computador são sancionadas em conformidade com o § 202-A do Código Penal Alemão. Esta legislação estabelece penalidades para aqueles que obtêm ou tentam obter acesso não autorizado a dados eletrônicos, bem como para aqueles que causam danos ou comprometem a operação de sistemas de computador. A pena estipulada pode alcançar um máximo de dois anos de reclusão (SACHS,2018).

No que tange à responsabilidade penal, a legislação brasileira também contempla sanções para os crimes cibernéticos. Como já citado o Código Penal Brasileiro determina penalidades para indivíduos que realizam invasões em dispositivos eletrônicos (art. 154-A) ou que cometem crimes contra a honra de terceiros por meio da internet (art. 139, parágrafo 2º). Ademais, a Lei Carolina Dieckmann (Lei 12.737/12) estabelece punições para crimes cibernéticos relacionados à violação de dispositivos eletrônicos privados.

Diante do aumento contínuo dos crimes cibernéticos e de suas consequências prejudiciais para indivíduos, empresas e governos, torna-se imperativo que as legislações em diferentes países permaneçam atualizadas e eficazes na proteção dos direitos dos cidadãos no ambiente digital. As abordagens adotadas nos Estados Unidos, Reino Unido, Alemanha e Brasil evidenciam a diversidade de respostas legais a esse fenômeno, refletindo a complexidade da responsabilidade penal em um contexto global. Para que as normas estabelecidas cumpram seu papel de prevenção e combate aos crimes cibernéticos, é essencial não apenas a rigorosa aplicação dessas legislações, mas também o fortalecimento da conscientização pública acerca dos riscos e das responsabilidades associadas ao uso da tecnologia. Somente por meio de um esforço conjunto entre governos, autoridades legais e a sociedade civil será possível enfrentar os desafios impostos por esse novo cenário digital.

6 FORTALECIMENTO DA SEGURANÇA CIBERNÉTICA NO BRASIL: ANÁLISE DO DECRETO Nº 9.637/2018 E PROPOSTAS DE APRIMORAMENTO

Neste tópico, será abordado um novo e significativo decreto que possui grande relevância e serve como uma proposta de aprimoramento, além de possíveis soluções relacionadas ao processo de identificação das autorias.

O Decreto nº 9.637, de 26 de dezembro de 2018, denominado Política Nacional de Segurança da Informação, estabelece diretrizes sobre a governança da segurança da informação e modifica o Decreto nº 2.295, de 4 de agosto de 1997. Este último regulamenta o que está disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e trata da dispensa de licitação em situações que possam comprometer a segurança nacional.

O decreto acima referenciado visa à melhoria da segurança cibernética, assim como está expresso no artigo 2º:

> Art. 2º para os fins do disposto neste Decreto, a segurança da informação abrange: I - A segurança cibernética; II - A defesa cibernética; III - A segurança física e a proteção de dados organizacionais; e IV - As ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (BRASIL, 2018).

Assim, a implementação necessária deste decreto e sua ampliação configuram uma solução relevante para os crimes cibernéticos.

No Brasil, existem dois órgãos que desempenham funções no combate a esses delitos; contudo, ainda carecem da capacidade plena para atender a todas as ocorrências associadas a crimes cibernéticos. No âmbito federal, destacam-se o Ministério Público Federal (MPF), a Polícia Federal (PF) e a organização não governamental “Safernet”. É importante salientar que a Polícia Federal mantém um foco específico na investigação de crimes cibernéticos, conforme observado pelo Dr. Emerson, Delegado de Polícia.

> A atuação da PolíciFederal frente à problemática dos cibercrimes envolveu, em princípio, duas ações básicas essenciais: central de recebimento de denúncias de pornografia infantil (pedofilia) e análise, processamento e investigação de fraudes eletrônicas (WERNET, 2011, pág. 70).

O Brasil conta com o apoio da polícia judiciária; no entanto, é ainda iniciante no enfrentamento dos crimes cibernéticos. Em diversas regiões e cidades do país, não existem delegacias especializadas para lidar com essas ocorrências. Quando existem, geralmente se trata de uma única unidade responsável por atender todo o estado. Por exemplo, na capital do estado do Paraná, existe o Núcleo de Combate aos Cibercrimes – NUCIBER, que Conforme artigo 39 do Decreto nº 4.884/78 prevê que às Delegacias Especializadas compete a investigação dos crimes de sua atribuição no Município de Curitiba e considerando que o artigo 2º, III, da Resolução nº 293/05-SESP-PR que instituiu o Nuciber prevê que é sua atribuição “auxiliar os demais órgãos da Polícia Civil nas investigações e inquéritos policiais ou administrativos, quando haja necessidade de pesquisa na rede mundial de computadores”, evidencia-se que as situações ocorridas fora dos limites de Curitiba devem ser registradas e investigadas pela respectiva Delegacia da Comarca onde ocorreram, ficando este núcleo como suporte de auxílio no que tange às investigações envolvendo crimes cibernéticos (CUNHA,2021).

Dessa forma, conclui-se que, embora essa evolução tecnológica seja revolucionária e facilite diversos processos, ainda há muito a ser aprimorado. Nesse sentido, por meio de uma breve pesquisa, foram identificadas possíveis

propostas, a saber: A criação de uma Identidade eletrônica pessoal; A restrição de dados no ambiente virtual; promoção de palestras e campanhas periódicas sobre o cibercrime e afins; a criação de um sistema eficaz e eficiente na identificação da autoria de crimes cibernéticos; investimento considerável nos setores de solução ante os crimes cibernéticos, seja por meio de equipamentos, metodologias, dentre outros.

Diante do exposto, é evidente que a implementação e ampliação do Decreto nº 9.637/2018 são passos fundamentais para fortalecer a segurança cibernética no Brasil. Apesar dos esforços já existentes, como a atuação do Ministério Público Federal, da Polícia Federal e do Núcleo de Combate aos Cibercrimes, ainda há lacunas a serem preenchidas para garantir uma resposta eficaz aos crimes cibernéticos.

As propostas identificadas, incluindo a criação de uma identidade eletrônica pessoal, a restrição de dados no ambiente virtual e a promoção de campanhas educativas, destacam-se como medidas essenciais para aprimorar a governança da segurança da informação. Portanto, é imprescindível que haja um comprometimento contínuo em investimentos e ações que visem a prevenção e o combate a delitos cibernéticos, assegurando, assim, um ambiente digital mais seguro para toda a sociedade.

CONSIDERAÇÕES FINAIS

Conclui-se que este trabalho aborda a complexidade e os desafios inerentes aos crimes cibernéticos, com ênfase na responsabilidade do Estado tanto na identificação dos autores quanto na eficácia das punições.

Observa-se que, apesar dos avanços tecnológicos e legais, o sistema jurídico ainda enfrenta grandes dificuldades na responsabilização dos infratores virtuais, devido à natureza anônima e global da internet.

A falta de capacitação e de ferramentas adequadas por parte das autoridades investigativas, somada à insuficiência de legislação específica e atualizada, contribui para um cenário de impunidade que reforça a sensação de insegurança no ambiente digital.

Nesse contexto, o trabalho destaca que o fortalecimento das políticas públicas e a ampliação de estratégias de cooperação internacional são cruciais para que o Estado possa responder com maior eficiência a esses desafios.

Reitera-se, ainda, a necessidade de uma abordagem multidisciplinar que inclua o aprimoramento contínuo das leis, a capacitação de profissionais e o desenvolvimento de tecnologias avançadas para monitoramento e investigação. Adicionalmente, salienta-se a importância de campanhas de conscientização sobre segurança digital, visando educar os usuários sobre os riscos e promover práticas seguras online.

Assim, o estudo conclui que, para garantir um ambiente digital mais seguro, é essencial o compromisso contínuo de todos os agentes envolvidos — governo, instituições, empresas e sociedade — na prevenção e combate aos delitos cibernéticos, assegurando a proteção dos direitos individuais e a segurança coletiva no ambiente virtual.

REFERÊNCIAS

AGENCIA SENADO; **Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia>. Acesso em 01 de out de 2024.

ALEXANDRE, Junior. **Cibercrime: um estudo acerca do conceito de crimes informáticos** – Junior Alexandre – revista eletronica da faculdade de direito de franca. 2018. Disponível em: <https://tede.ufrrj.br/jspui/handle/jspui/6664?mode=full>. Acesso em: 02 de set de 2024.

ALMEIDA, Maria Paula Castro de. **A evolução no combate aos crimes virtuais**. Rio de Janeiro, 2015. Escola de Magistratura do Estado do Rio de Janeiro. Disponível em: <https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2015/pdf/MariaPaulaCastrodeAlmeid>. Acesso em: 15 de out de 2024.

ARAS, Vladimir. **Crime de Informática. Uma Nova Criminalidade**. Teresina, ano 6, n. 51, Outubro de 2001. Disponível em: <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em 08 de out de 2024.

BAYER, Diego Augusto. **Co-culpabilidade e responsabilização do estado**. 2014. Disponível em: <https://www.jusbrasil.com.br/artigos/co-culpabilidade-e-responsabilizacao-do-estado/121943231>. Acesso em: 08 de out de 2024.

BECCARIA, Cesare. **Dos delitos e das penas.**São Paulo: Martin Claret, 2004. Disponível em: <https://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/17502/material/BECCARIA%2C%20C.%20Dos%20delitos%20e%20das%20penas.pdf>. Acesso em: 08 de out de 2024.

BRASIL, **Lei n. 2.848, de 07 de dezembro 1940**. Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em 09 de Setembro de 2024.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 09 de set de 2024.

BRASIL, **Lei nº 12.965, de 23 de abril de 2014.** Disponivel em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm- >. Acesso em 01 de out de 2024.

BRIGGS, Asa; BURKE, Peter. **Uma história social da mídia: de Gutenberg à Internet**. Tradução: DIAS, Maria Carmelita Pádua. Revisão técnica: VAZ, Paulo. 2°. Edição. Rio de Janeiro: Jorge Zahar Editor, 2006. Disponível em: <https://seminariostecmidi.wordpress.com/wp-content/uploads/2012/02/peter-burke-historia-social-da-mc3addia.pdf>. Acesso em: 26 de ago de 2024

BUDAPESTE, CONVENÇÃO. **Convenção sobre o Cribercrime**. Budapeste, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: ed. Saraiva, 2011. Disponível em: <http://biblioteca2.senado.gov.br:8991/F/?func=item-global&doc_library=SEN01&doc_number=000915942>. Acesso em: 02 de set de 2024.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2º Ed. Ver, ampl e atual. Rio de Janeiro, 2003.

D'URSO, Luiz Augusto Filizzola. **Tudo sobre cibercrimes**. 2019. Disponível. <https://www.estadao.com.br/politica/blog-do-fausto-macedo/tudo-sobre-os-cibercrimes/>. Acesso em: 15 de out de 2024.

FERREIRA, Ivete Senise**. A criminalidade informática**. In: LUCCA, Newton.; SIMÃO FILHO, Adalberto (Coord.). Direito e internet. Bauru: Edipro, 2001. Disponível em: <https://repositorio.usp.br/item/001225415>. Acessado em: Acesso em 09 de set de 2024.

FROTA, Jessica Olívia Dias; PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los**. 2017. Disponível em: <https://flucianofeijao.com.br/novoo/wpcontent/uploads/2018/11/ARTIGOS_CRIMES_VIRTUAIS\nDIFICULDADE>. Acesso em 15 de out de 2024.

GUSMÃO, Pompeia**. A responsabilidade do Estado na prevenção do crime.** 2014. Disponível em: https://www.jusbrasil.com.br/artigos/a-responsabilidade-do-estado-na-prevencao-do-crime/143479633. Acesso em 08 de out de 2024.

LUCCHESI, Ângela Tereza; HERNANDEZ, Erika Fernanda Tangerino. **Crimes Virtuais:ciberbullying, reveng porn, sextortion, estupro virtual.** 2018. Revista Officium: estudos de direito. Disponível em: <https://facdombosco.edu.br/wp-content/uploads/2018/12/%C3%82ngela-Tereza-Lucchesi-Erika-Fernanda-Tangerino-Hernandez-crimes-virtuais-Copia.pdf>. Acesso em: 02 de set de 2024.

MACHADO, Ralph. **CCJ aprova projetos que agrava pena para crimes cibernéticos**. 2019. Disponível em: <hppts://www.câmara.leg.br/noticias/594044-ccj-aprova-projeto-que-agrava-pena-para-crimes-ciberneticos>; Acesso em:15 de out de 2024.

MOREIRA, Paulo Roberto**. O que são Crimes Cibernéticos?** 2022. Disponível em: <https://www.jusbrasil.com.br/artigos/o-que-sao-crimes-ciberneticos/1583984125>. Acesso em: 02 de set de 2024.

NEVES, Maria, Regina Céli Assumpção. **Falta de lei sobre crimes digitais leva à impunidade**. 2010. Disponível em: <https://www.camara.leg.br/noticias/208500-falta-de-lei-sobre-crimes-digitais-leva-a-impunidade-diz-especialista/>. Acesso em 15 de out de 2024

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal. 15ª Ed**. Ver e atual. Rio de Janeiro: Lume Juris, 2011.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. Ed. São Paulo: Saraiva, 2013; Disponível em:< https://www.editoradodireito.com.br/livro-direito-digital-e-processo-eletronico-tarcisio-teixeira-saraiva-jur-9788553622351>. Acesso em 23 de set de 2024.

Sachs, M., & Hilker, B. **Cibersegurança e Direito Penal: uma análise do contexto brasileiro e alemão**. Rev. Fac. Direito Univ. São Paulo, v. 113, p. 533-565, 2018.

SILVA. Wender Charles. **Ensaio sobre o princípio da coculpabilidade**. Patos de Minas. 2011. Disponível em: <https://revistas.unipam.edu.br/index.php/ensaiojuridico/article/view/4224>. Acesso em: 08 de out de 2024.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática**. São Paulo: Saraiva, 2014; Disponível em: <https://bdjur.stj.jus.br/jspui/handle/2011/82913>. Acesso em 23 de set de 2024.

TOCANTINS, Hortencia de Matos. Crimes Cibernéticos na Atualidade: Desafios e Impactos na Sociedade Moderna. 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-na-atualidade-desafios-e-impactos-na-sociedade-moderna/2104354886>. Acesso em 15 de out de 2024.

TOURINHO FILHO, Fernando da Costa. **Processo Penal. 34ª Ed**. Ver. São Paulo: Saraiva, 2012. Vol. I.

TURNER, David; MUÑOZ, Jesus**. Para os filhos dos filhos de nossos filhos: uma visão da sociedade internet**. São Paulo: Summus, 2002. Disponível em: <https://www.martinsfontespaulista.com.br/para-os-filhos-dos-filhos-dos-nossos-filhos 188424/p?srsltid=AfmBOooXCdimFteOsJkU9WtcVF7NWNhbl5TztwBlw8h1GG-1YuRG4e3z>. Acesso em: 26 de ago de 2024.

United States Department of Justice. (2021). **Computer Crime & Intellectual Property Section**. Disponível em : <https://www.justice.gov/criminal-ccips>. Acesso em 22 de out de 2024.

VIANA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013; Disponível em: <https://pt.scribd.com/document/616493099/Crimes-Informaticos-PDF-1>. Acesso em: 23 de set de 2024.

WENDT, Emerson. **Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil** [recurso eletrônico] / Emerson Wendt. – Livro digital. – São Paulo: Editora Delfos, 2011. Disponível em: <https://rbi.abin.gov.br/RBI/article/view/80/63>. Acesso em: 29 de ago de 2024.

WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012. Disponível em: <https://www.editorabrasport.com.br/ebook-crimes-ciberneticos-ameacas-e-procedimentos-de-investigacao>. Acesso em: 23 de set. de 2024.