CARLOS EDUARDO SOUZA CASTRO

CRIMES DIGITAIS TRANSNACIONAIS E A DIFICULDADE DE SE DETERMINAR A COMPETÊNCIA

Guarapari -ES

2024

CARLOS EDUARDO SOUZA CASTRO

CRIMES DIGITAIS TRANSNACIONAIS E A DIFICULDADE DE SE DETERMINAR A COMPETÊNCIA

Trabalho de Conclusão de Curso apresentado na Faculdade Doctum campos Guarapari, tem como requisito básico para a conclusão do Curso de Direito. Sob a orientação do Dr. Leonardo Fontes.

Guarapari – ES
2024

CARLOS EDUARDO SOUZA CASTRO

CRIMES DIGITAIS TRANSNACIONAIS E A DIFICULDADE DE SE DETERMINAR A COMPETÊNCIA

Trabalho de Conclusão de Curso apresentado na Faculdade Doctum campos Guarapari, tem como requisito básico para a conclusão do Curso de Direito. Sob a orientação do Dr. Leonardo Fontes.

Banca Examinadora

Prof. Dr. Rubens dos Santos filho
Coordenador DOCTUM

Dr. Lincoln Bruno Cavalcante Silva
Convidado

Guarapari – ES
2024

Agradecimentos

A realização deste trabalho de conclusão de curso é fruto de um longo percurso de aprendizado, esforço e dedicação, no qual muitas pessoas contribuíram de maneira significativa. Por isso, gostaria de expressar meus sinceros agradecimentos a todos que me apoiaram ao longo desta jornada.

Primeiramente, agradeço a Deus pela saúde e força que me permitiram chegar até aqui.

À minha família, pelo amor, compreensão e apoio incondicional em todos os momentos, especialmente aos meus pais, Carlos Augusto Castro e Cleisa de Souza Silva Castro que sempre acreditaram em meu potencial e me incentivaram a buscar meus sonhos, a minha avó maria do Carmo, Meu avô Sebastião (in memoriam), aos meus irmãos, Gabriel, Daniel e Leonardo e a minha Noiva Stephanie por todo o apoio.

A todos os professores e funcionários da DOCTUM Guarapari que contribuíram para minha formação acadêmica e pessoal, fornecendo o suporte necessário e criando um ambiente propício para o aprendizado.

Por fim, agradeço a todos que, direta ou indiretamente, colaboraram para que este trabalho se tornasse realidade.

Muito obrigado!

Guarapari – ES
2024

RESUMO

Os crimes digitais são uma forma de crime transnacional em expansão. Sua natureza complexa de crime que ocorre no ciberespaço, sem fronteiras, é agravada pelo crescente envolvimento de grupos do crime organizado.

Deste modo, é possível colocar em analise que, os transgressores de crimes cibernéticos e suas vítimas, podem estar localizados em diferentes regiões, e os efeitos desses crimes podem atingir sociedades de todo o mundo. Assim, os crimes digitais transnacionais vêm representando uma crescente ameaça e complexidade, pois tais crimes ocorrem no ciberespaço, ultrapassando fronteiras geográficas e envolvendo grupos do crime organizado.

PALAVRAS-CHAVE: Crimes digitais - cyberespaço - Cibernético

ABSTRACT

Digital crimes are an expanding form of transnational crime. Its complex nature of crime that occurs in cyberspace, without borders, is worsened by the growing involvement of organized crime groups.

In this way, it is possible to analyze that cybercrime offenders and their victims can be located in different regions, and the effects of these crimes can affect societies around the world. Thus, transnational digital crimes have represented a growing threat and complexity, as such crimes occur in cyberspace, crossing geographic borders and involving organized crime groups.

KEYWORDS: Digital crimes - cyberspace - Cyber

SUMÁRIO

1 INTRODUÇÃO

Os crimes digitais transnacionais são infrações cometidas no ciberespaço que ultrapassam fronteiras nacionais.

Esses crimes envolvem ações ilegais realizadas por meio de tecnologias de informação e comunicação, afetando vítimas em diferentes regiões do mundo. O crescente envolvimento de grupos organizados torna essa forma de crime ainda mais complexa e desafiadora de combater.

Essas transgressões podem incluir invasão de computadores, disseminação de vírus, roubo de senhas e outros delitos virtuais. A cooperação global e a adoção de convenções internacionais são essenciais para enfrentar esse cenário em constante evolução.

Esses crimes eles são classificados em Duas partes como afirma Gabriel Marcos Archanjo ORRIGO e Matheus Henrique Balego FILGUEIRA: Os crimes digitais próprios são aquelas em que, para se cometer o delito é necessário a utilização de um computador, ou seja, o computador é o meio de execução essencial.

Os bens jurídicos afetados pelo cibercrime próprio são os dados armazenados em outra máquina, rede ou algum meio de armazenamento de dados digitais. O delito é cometido por meio de computador e se consuma pelo meio informático.

Na nossa legislação um exemplo e é a invasão de Dispositivo informático para fins de roubo de dados. Já os crimes cibernéticos impróprios, também são cometidos por meio do computador, porém o bem jurídico ofendido aqui pode ser afetado de “n” maneiras, não necessariamente com a utilização do computador, ou seja, não é essencial a máquina, o delito atinge o mundo físico, diverso da informática.

São exemplos de crimes impróprios tipificados na nossa legislação: Calúnia; injúria; difamação; ameaça; furto; apropriação indébita; estelionato; dano; violação ao direito autoral; pedofilia; crime contra a propriedade intelectual; observe que todos eles podem ser cometidos sem o uso do computador, mas também é possível comete-los usando o computador como meio. (ORRIGO, Gabriel M. A. FILGUEIRA, 2015, p.3).

2 CONCEITO DE CRIMES DIGITAIS

A fenomenologia criminal relacionada às TIC – Tecnologias da Informação e Comunicação é cada vez mais intensa e variada, e sua presença muda constantemente, adaptando-se às novas potencialidades tecnológicas e sociais. (ROMEO CASABONA,2006. p. 1.)

Há quem diga que o uso de redes telemáticas, em especial a internet, se trata de fenômeno mais relacionado com a globalização que com outros fatores, dada sua característica de promover o envolvimento de culturas e sistemas jurídicos diferentes 75.

Concretamente, os crimes digitais importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.

Nota-se, assim, que o ciberespaço é campo para o cometimento de delitos que já são tipificados em ordenamentos jurídicos, mas, também, é área onde condutas ainda não necessariamente incriminadas no Brasil, mas altamente danosas, ocorrem. Isso graças à própria vulnerabilidade do ciberespaço, que pode ser verificada pelas seguintes características.

a) Capacidade de processar, guardar e circular, de forma automatizada e em tempo real, grandes quantidades de informações em formato digital dos mais variados (fotos, filmes, sons). Isso é facilitado pela própria estrutura descentralizada e não hierarquizada da internet que inviabiliza a existência de órgãos de controle da informação circulante e, como consectário lógico, torna praticamente impossível supervisionar a qualidade e o volume de informações;

b) O número enorme de usuários, a frequência com que acessam, a liberdade que têm para enviar, transferir, difundir e acessar informações, de modo que os internautas passam a ser potenciais vítimas, mas também potenciais sujeitos ativos de delitos;

c) As próprias características físicas, técnicas e lógicas das TIC, que podem ser acessadas de forma ilegítima, tendo seu conteúdo alterado. Consegue-se acesso a arquivos das mais distintas naturezas e aos mais variados programas de computador;

d) A enorme potencialidade de multiplicação das ações ilícitas. Isso decorre da própria estrutura das TIC, como mencionado acima. A criação de fóruns de debates, páginas na internet, comunidades de relacionamento etc., podem facilitar a prática de delitos, podendo, ainda, dar maior repercussão a eles, como nas ofensas contra a honra, por exemplo.

Assim, o Direito Penal enfrenta novas realidades quanto às práticas delitivas, de modo que não se pode ignorar a realidade de novos modus operandi e novas ponderações sobre condutas danosas. Todavia, veremos mais adiante que não se pode considerar apenas a forma com a qual os delitos são praticados para que se possa defini-los como informáticos. (ROMEO CASABONA, p3-4)

É o que se verá ao discorrermos sobre os bens jurídicos peculiares a informática.

2.1 Bens jurídicos peculiares a informática

As transformações tecnológicas pelas quais passa o mundo interferem inexoravelmente no Direito Penal. Desde a Revolução Industrial, passando pela Segunda Grande Guerra, novos riscos sociais foram tomando lugar e alterando as relações entre os homens. Esse período e tais transformações têm sido constantemente questionados por juristas, mas também por filósofos e sociólogos, especialmente porque ainda que se pregue a aplicação do Direito Penal como ultima ratio, nota-se incremento de tipos penais relativos aos novos riscos. (SILVEIRA, p. 17.)

Dessa forma, não há como deixar de questionar se há novos bens jurídicos referentes ao avanço tecnológico e, ainda, se é o caso de receberem bens tutelados por parte do Direito Penal. Assim, não se pode mais tratar dos crimes digitais relacionados apenas e tão somente aos bens jurídicos tradicionalmente protegido. (ÁLVAREZ-CIENFUEGOS SOTO p 191)

Ao considerarmos as condutas ilícitas por meio da informática, verificamos a possibilidade de lesão a outros bens jurídicos. Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já gozam de proteção jurídica, como a vida, a integridade física, o patrimônio, a fé pública, mas, também as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações.

Nesse sentido, a “informação” hoje tem contornos de mercadoria. Pode-se até tratá-la como nova matéria-prima do gênero “bens imateriais”. Ela pode ser valorada

e valorizada, além da possibilidade de submetê-la a tratamentos diferentes como o armazenamento, a guarda, a cessão e a manipulação. Fazendo-se um paralelo com outros valores, como é o caso do meio ambiente, que sofreu processo de espiritualização, o mesmo se deu com a informação, que antes era apenas expressão em papel (jornais, revistas) e que hoje é composta por dados.

Não há como negar que, além da informação, os dados, a confiabilidade e segurança dos sistemas e redes informáticas e de comunicação sejam novos paradigmas de bem jurídicos a serem tutelados pelo Direito Penal. Isso não significa dizer que a objetividade jurídica tradicionalmente protegida deva ser deixada de lado. É o que sustentam Romeo Casabona e Bueno Arús, que consideram possível haver violação conjunta de bens jurídicos tradicionais e outros, peculiares à informática. (ROMEO CASABONA p. 190, BUENO ARÚS p. 1829)

Sob essa ótica, pode-se dizer que os crimes digitais são pluriofensivos na exata medida em que há a proteção de bens jurídicos tradicionais, mas, ao mesmo tempo, proteção de novos interesses derivados da sociedade de risco e de informação. Sem essa concepção parece não existir categoria específica dessa criminalidade. Justamente por isso que foi dito não ser correto atrelar única e exclusivamente o meio pelo qual se pratica a conduta, devendo se constituir em torno da afetação da informação como bem jurídico protegido, primordial e basicamente, ainda que não de forma exclusiva. Resta pensar qual o principal bem jurídico afetado: a informação? Os dados? Os sistemas informáticos e de telecomunicações? Rovira del Canto discorre no sentido de se entender a informação como sendo o bem jurídico principal nos crimes digitais e, secundariamente, os dados ou os sistemas. Essa ideia parte do princípio de que os dados constituem nada mais que a representação eletrônica ou digital da informação, ainda que com valores variáveis, ao passo que os sistemas nada mais são que os mecanismos materiais de funções automáticas de armazenamento, tratamento e transferência. (ROVIRA DEL CANTO, p 72.)

2.2 Crime cibernético como um fenômeno jurídico

O sistema jurídico, especialmente a área do Direito Penal, enfrenta atualmente desafios significativos, considerando o progresso da tecnologia e a sua ligação cada vez mais forte com a vida diária das pessoas. Foi necessário adaptar-se a essa evolução e garantir a proteção de direitos que sequer existiam anteriormente, surgindo

assim a urgência de punir atos ilícitos de maneira inovadora. Um exemplo dessa modernidade traz consigo o crime cibernético, que se transformou em um fenômeno legal de grandes proporções. Sua natureza transcende fronteiras e seus impactos são abrangentes em escala global. (*UNODC)*

2.3 Contextualização dos Crimes Digitais

A contextualização dos crimes digitais precisa começar destacando os avanços tecnológicos que foram importantíssimos e proporcionaram mudanças substantivas na maneira como interagimos e operamos no mundo. Essa revolução tecnológica não ocorreu sem suas adversidades. Os avanços levaram à emergência de novas formas de criminalidade, explicitadas pelo fenômeno do crime digital. Tais crimes são caracterizados pela sua execução através de meios eletrônicos e por ocorrerem no ciberespaço, um ambiente digital intangível consistindo de redes de informações, incluindo a internet (Barbosa, 2009).

Os crimes digitais englobam uma ampla gama de atividades ilegais. Podem variar desde atividades criminosas comuns que foram facilitadas pelos meios digitais, como a fraude bancária, até crimes únicos ao ciberespaço, como a invasão de sistemas informáticos. Estes crimes podem ser perpetrados por indivíduos, grupos organizados ou até mesmo estados-nacionais, através de ações de espionagem e sabotagem. A escala desses crimes pode englobar atividades ilegais locais, bem como crimes que transcendem fronteiras nacionais, resultando em complexidades jurisdicionais (SCHRÖDER, 2022).

A transnacionalidade dos crimes digitais é inerente à sua natureza. A estrutura do ciberespaço proporciona um ambiente onde as informações podem ser facilmente enviadas e recebidas além das fronteiras nacionais. Isso facilitou a ocorrência de crimes nos quais suas componentes constitutivas ocorrem em diferentes jurisdições. O alcance transnacional desses crimes levanta questões específicas em relação à determinação da competência jurisdicional (RODRIGUES; AVELINE, 2022).

A determinação da competência em casos de crimes digitais transnacionais envolve encarar desafios formidáveis. O primeiro desafio relaciona-se à natureza fluida do ciberespaço que impede a ligação das atividades ilegais a uma localização física específica. Como resultado, questões de aplicação da lei e de competência tornam-se intrincadas de necessitar detalhamento. Diferentes jurisdições possuem

diferentes leis, regulamentos e práticas em relação aos crimes digitais, complicando ainda mais a situação (RODRIGUES; AVELINE, 2022).

Outra camada de complexidade é adicionada pela divergência de abordagens jurídicas adotadas em relação aos crimes digitais. Enquanto algumas jurisdições optam por abordagens baseadas no local da ocorrência do crime, outras podem adotar abordagens baseadas no dano causado. A falta de uma abordagem unificada aumenta o desafio de determinar competências e também aumenta o risco de crimes digitais permanecerem impunes (Primo, 1969).

Segundo Barbosa (2009, p. 134):

> A legislação existente relativa aos crimes digitais também apresenta dificuldades. Muitas leis foram formuladas sem considerar a complexidade e a natureza única dos crimes digitais transnacionais. Muitas vezes falta a habilidade para lidar eficazmente com os desafios apresentados por esses crimes, tanto em termos de investigação, quanto de punição. A inadequação da legislação existente contribui para a persistência do problema.

Entidades supranacionais como a União Europeia e a Interpol reconhecem a necessidade de uma abordagem cooperativa interjurisdicional para lidar com crimes digitais transnacionais. Contudo, apesar do desenvolvimento de frameworks legislativos para impulsionar a cooperação internacional, a implementação prática mostra-se desafiadora. Há obstáculos legais, culturais e de infraestrutura que dificultam a cooperação efetiva (Primo, 1969).

Pertinentemente, as iniciativas privadas apresentam um papel essencial na luta contra os crimes digitais. Empresas de tecnologia, em particular, têm a capacidade de monitorar, detectar e responder a atividades maliciosas em suas plataformas. Estes atores privados apresentam um papel importante para complementar os esforços das autoridades públicas na prevenção e combate aos crimes digitais (PAGLIOSA; RIBEIRO, 2022).

No que diz respeito a soluções futuras, salienta-se a necessidade de se buscar uma maior unificação das abordagens jurídicas a problemática dos crimes digitais. A harmonização das leis e a construção de instituições internacionais dedicadas a este tipo de crime podem se tornar imprescindíveis, dado o crescente aumento da atividade criminal no ciberespaço. A concretização dessas propostas, contudo, requereria

notável cooperação e coordenação entre os diferentes atores relevantes, um desafio que não deve ser ignorado (MEDEIROS et al., 2024).

Por conseguinte, a natureza transnacional dos crimes digitais oferece uma oportunidade para se repensar em parâmetros tradicionais de jurisdição e competência. A capacidade de adaptar abordagens jurídicas à realidade do ciberespaço será determinante no combate aos crimes digitais. A própria transformação que permitiu a existência de crimes digitais está prestes a ser a chave para a sua resolução, mas requer um esforço cooperativo entre os vários interessados para se atingir esse objetivo (PAGLIOSA; RIBEIRO, 2022).

2.4. História dos crimes digitais

A história dos crimes digitais subjaz ao desenvolvimento e ao avanço da própria tecnologia. Remonta aos anos 1960, com o início da exploração teórica dos computadores e a inflexão para uma digitalização das comunicações e dos ambientes de trabalho. Curiosamente, o termo 'hacker' foi inicialmente atribuído a pessoas com habilidades significativas em informática dos anos 1960, sem malignidade associada. À medida que a tecnologia avançava e se expandia para domínios cada vez mais integrais à vida humana, também aumentava o espaço para usos inescrupulosos, dando origem ao fenômeno dos crimes digitais (Primo, 1969).

No final dos anos 70, nos Estados Unidos, começaram a ser relatados os primeiros casos de pirataria de software comercial. Os criminosos digitais de então eram principalmente candidatos a programadores, ansiosos por explorar as novas tecnologias para seus próprios fins. Em um tempo onde a lei de direitos autorais ainda não existia no espaço cibernético, piratas virtuais operavam com relativa impunidade, criando a base do crime digital (GIAMUNDO NETO, 2020).

A década de 1980 assistiu a uma alarmante evolução dos crimes digitais, de simples pirataria de software para atividades mais destrutivas, tais como a criação de vírus informáticos. Um subconjunto dos hackers começou a explorar vulnerabilidades em sistemas informáticos para fins de destruição ou roubo de informações, desviando-se da tradição inicial de esforços exclusivamente exploratórios. Este período foi marcado pelo surgimento do primeiro worm, criado por Robert Tappan Morris, apontando assim para as crescentes ameaças do ciberespaço (SILVA; RAMOS, 2023).

A sofisticação dos crimes digitais continuou a aumentar durante a década de 1990, quando o advento da internet global acelerou exponencialmente seu potencial de alcance e destruição. Crimes engenhosos como esquemas de scam e phishing começaram a aparecer, explorando vulnerabilidades humanas tanto quanto falhas de segurança tecnológicas. Este período testemunhou o surgimento de novos tipos de crimes digitais, incluindo ciberterrorismo e ciberbullying, que ampliaram ainda mais o escopo e a gravidade da criminalidade online (MEDEIROS et al., 2024).

No início do século XXI, crimes digitais evoluíram para se tornar ferramentas de grandes organizações criminosas e até mesmo nações-estado, devido à premência da era da informação, escancarando um novo e infame capítulo na história dos crimes digitais. Espionagem cibernética, ciberataques orientados e crimes digitais altamente organizados são agora comuns e apresentam um desafio significativo para a segurança informática em todo o mundo (ROCHA; CHAVES, 2024).

Juntamente com a evolução dos crimes digitais, surgiu um conjunto correspondente de leis e regulamentos, numa tentativa de lidar com a nova e desconhecida arena da criminalidade. A partir da década de 1980, os países começaram a instituir legislação especificamente destinada a combater os crimes digitais, marcando um passo importante nas tentativas de impor limites legais à atividade criminosa online (FARIAS, 2021).

A eficácia dessas leis tem sido amplamente debatida. Muitos argumentam que a lei não conseguiu acompanhar a velocidade da evolução do crime digital, resultando em uma falta de capacidade de reagir adequadamente à crescente onda de crimes online. Questões relacionadas à jurisdição e à competência transnacional têm apresentado desafios significativos na aplicação efetiva da lei contra crimes digitais (SPERVER; ZILIOTI, 2021).

O quadro legislativo internacional é ainda mais complicado pelo fato de que os crimes digitais são basicamente sem fronteiras, cruzando facilmente os limites geográficos e jurisdicionais. Isso tem levado, por sua vez, a desafios no estabelecimento de jurisdição em casos de crime digital, e a questões sobre como se deve punir eficazmente os responsáveis (ROCHA; CHAVES, 2024).

Hoje em dia, além da implementação de leis e regulamentos, também se observa um crescimento na criação de estruturas institucionais para combater os crimes digitais. Organismos nacionais e transnacionais dedicados a este fim têm sido criados para fortalecer a luta contra a criminalidade digital. Estas instituições

funcionam no âmbito da cooperação internacional e se esforçam para harmonizar as abordagens na luta contra os crimes digitais (SOUZA; WESLEY, 2023).

O atual cenário de crimes digitais, influenciado pela era da informação e pelas complexidades da lei internacional, mostra a adaptabilidade e a persistência do crime digital. A complexidade da legislação e a transnacionalidade dos crimes digitais impõe desafios expressivos para os órgãos de direito, o que impulsiona a necessidade de soluções cada vez mais sofisticadas e globais para a prevenção e o combate. (FREITAS, 2018).

2.5. Evolução tecnológica e impactos legais

A evolução tecnológica indubitavelmente alterou o cenário jurídico internacional em várias vertentes. A junção entre progresso tecnológico e a globalização tem possibilitado a consumação de atos ilícitos em escala transnacional, trazendo à tona complexos problemas de competência jurisdicional. Desta forma, tem se tornado cada vez mais desafiador determinar a jurisdição competente para julgar e punir crimes digitais que ultrapassam fronteiras nacionais (MUNGUAMBE; PINTO; FREIRE, 2017).

Apesar dos avanços na legislação sobre crimes digitais, surge a questão de como isso se aplica aos crimes ocorridos em outra jurisdição. O direito penal tradicional baseia-se na noção de territorialidade, que muitas vezes não pode ser aplicada ao espaço virtual. Vários casos de delitos digitais não possuem um palco físico determinado, ocorrendo em rede e podendo afetar várias jurisdições simultaneamente, tornando a definição da competência um desafio válido (Pouzada et al., 2020).

A densidade tecnológica dos meios digitais e a capacidade de alcançar escala global têm levado à necessidade de se desenvolver uma estrutura legal internacional adaptada a essas novas condições. Temos visto iniciativas no âmbito global, como a Convenção de Budapeste sobre Ciber criminalidade, que buscam adequar o direito a essas novas realidades, embora encontrem resistência pela diversidade cultural e jurídica que caracteriza o panorama mundial (SILVA; RAMOS, 2023).

Não obstante, ainda prevalecem grandes obstáculos para a formação de um consenso jurídico internacional sobre crimes digitais. As diferenças entre os sistemas de justiça criminal, assim como as concepções divergentes sobre privacidade e liberdade de expressão, dificultam a harmonização das normas. Isto é relevante

especialmente quando os atos ilícitos digitais estão relacionados com questões controvertidas como discurso de ódio, difamação e invasão de privacidade (DOYLE; OLINTO, 2021).

A evolução tecnológica também gerou novas modalidades de crimes, em que a tipificação penal se torna problemática. A manobra dos ciberdelitos, sua constante mutação e a evasão das fronteiras nacionais significa que as leis e os sistemas jurídicos muitas vezes estão atrasados em relação ao desenvolvimento da cibercriminalidade. Essa defasagem entre a evolução dos crimes digitais e o arcabouço legal não só fomenta a impunidade, mas também pode desencadear um conflito de competências jurisdicionais (MITANI, 2012).

Há a preocupação com a aplicabilidade e efetividade do direito penal ao universo digital. A rastreabilidade dos responsáveis por crimes digitais transnacionais apresenta desafios significativos devido à possibilidade de anonimato, ao uso de criptografia e à falta de cooperação entre as entidades envolvidas. Isso demanda uma adaptação dos métodos convencionais de investigação, exigindo uma formação mais técnica dos operadores do direito (MUNGUAMBE; PINTO; FREIRE, 2017).

Do outro lado, surge a problemática dos direitos fundamentais dos indivíduos. As novas tecnologias permitem um nível de vigilância e coleta de dados sem precedentes, que coloca em risco o objeto do direito à privacidade. Este risco tem se tornado cada vez mais mensurável com o aumento da tecnologia de punição e vigilância digital, que muitas vezes opera sob uma jurisdição incerta. É necessário equilibrar as demandas de segurança e a necessidade de prevenir e punir crimes digitais com a proteção dos direitos fundamentais (ROCHA; CHAVES, 2024).

Ademais, a natureza descentralizada da internet propõe um desafio adicional à delimitação da competência jurisdicional. Em um ambiente onde os usuários têm cada vez mais possibilidade de compartilhar, criar e disseminar conteúdo, identificar a origem de atos ilícitos torna-se uma tarefa particularmente complexa. Os avanços na tecnologia da informação desafiam a validade do princípio da territorialidade, tornando cada vez mais difícil determinar a competência de uma jurisdição (MUNGUAMBE; PINTO; FREIRE, 2017).

Considerando que a tecnologia continua a evoluir rapidamente, mantendo-se à frente das normas legais existentes, o desafio é desenvolver regulamentações que sejam flexíveis o suficiente para adaptar-se a tecnologias emergentes, como a inteligência artificial e blockchain. O desafio para o Direito é prever e adaptar-se às

mudanças tecnológicas, mas isto nem sempre é possível devido à velocidade deste progresso. Enquanto os legislativos nacionais e internacionais estão gradualmente se adaptando à nova realidade, muitas questões críticas permanecem sem resposta, demandando estudo e debates constantes (SPERVER; ZILIOTI, 2021).

3. Tipologias de Crimes Digitais

Os crimes digitais transnacionais, em contínua evolução à medida que a tecnologia avança, adotam diversas formas, representando a diversidade de práticas ilegais que podem ser conduzidas através da Internet ou utilizando dispositivos eletrônicos. A tipologia destas atividades ilícitas é grandemente abrangente e complexa, tornando ainda mais acentuada a dificuldade de se determinar a competência para a sua persecução penal (RODRIGUES; AVELINE, 2022).

Entre a gama de crimes digitais, destacam-se os crimes contra a privacidade, abrangendo a violação de dados e a espionagem digital. Impossibilitando a garantia de uma segurança infalível das informações pessoais ou corporativas, estes crimes consistem em acessar, interceptar ou disseminar informações confidenciais armazenadas em meios digitais e enfrentam entraves na sua investigação e coibição, especialmente quando praticados de forma transnacional (MEDEIROS et al., 2024).

Uma segunda tipologia frequentemente associada aos crimes digitais corresponde aos delitos econômicos. A fraude através da Internet e as operações financeiras clandestinas, como a lavagem de dinheiro digital e o pagamento a atividades criminosas, são algumas nuances desta categoria. A natureza transnacional destas práticas, frequentemente articuladas por redes criminosas complexas, encerra desafios significativos ao estabelecimento de competências jurisdicionais adequadas (FREITAS, 2018).

Os ciberataques também compõem o rol dos crimes digitais, o que inclui ações de sabotagem digital, crimes de denegação de serviço (DoS) e ataques de ransomware. Estes delitos, geralmente perpetrados por hackers, podem ter como alvo sistemas de informática de indivíduos, empresas ou até mesmo de órgãos governamentais, atingindo proporções transnacionais e acarretando consequências graves, tais como paralisação de serviços essenciais e perdas financeiras (Primo, 1969).

Outra tipologia diz respeito ao cibercrime contra a propriedade intelectual, que envolve atividades como pirataria de software, violação de direitos autorais e distribuição de conteúdo protegido sem autorização. Com a Internet facilitando a disseminação de material protegido em escala global, a definição de competências para lidar com este tipo de crime apresenta entreves processuais e legislativos (FARIAS, 2021).

Os crimes digitais de natureza sexual apresentam dinâmicas altamente preocupantes, que se manifestam na forma de exploração sexual infantil, pornografia online, assédio e sextortion. A sua prática a nível transnacional reflete a complexidade e a amplitude da Internet, constituindo uma teia de atividades ilícitas que, frequentemente, ocorrem ocultas na deep web e exigem estratégias de investigação e intervenção diligentes e eficazes (MEDEIROS et al., 2024).

Dentro da esfera de crimes digitais ainda encontramos os delitos relacionados à censura e à liberdade de expressão, que englobam práticas de discurso de ódio online, cyberbullying e intimidação. Estes crimes, além de apresentarem sérios impactos psicológicos para as vítimas, destacam a tensão subjacente entre a proteção da liberdade de expressão e a prevenção de danos e violência no ambiente digital (Barbosa, 2009).

Os cibercrimes associados ao terrorismo também fazem parte desta tipologia, seja no recrutamento de militantes, na disseminação de propaganda extremista ou na coordenação de ataques. As plataformas digitais têm sido utilizadas como ferramenta poderosa por grupos terroristas, com o agravante de sua natureza transnacional, tornando a avaliação de competência um grande desafio para a justiça e a segurança internacional (FRANK; BACKES, 2015).

As práticas de desinformação online, embora menos perceptíveis como crimes, podem ser classificadas como tais quando utilizadas para prejudicar indivíduos, empresas ou instituições. A disseminação de notícias falsas ('fake news') e campanhas de difamação digital, tornaram-se mais frequentes com o aumento da polarização política e social exacerbada pelas redes sociais (Primo, 1969).

Por último, mas não menos importante, vale ressaltar os crimes digitais que envolvem práticas discriminatórias, que incluem o racismo, o sexismo e a homofobia online. A perseguição aos grupos vulneráveis através das mídias digitais vem se intensificando e ganhando proporções transnacionais, o que acarreta a necessidade de discursos específicos e políticas públicas confrontando estas práticas ilícitas. A

compreensão do impacto e das implicações desses crimes é essencial para a implementação de medidas preventivas e reativas efetivas (SPERVER; ZILIOTI, 2021).

3.1. Crimes contra a segurança de sistemas

Os crimes contra a segurança dos sistemas representam uma grande parcela da criminalidade digital transnacional. A penetrabilidade desses sistemas, que pode ser forçada através de múltiplos mecanismos, põe em risco não apenas informações privadas de indivíduos, mas também dados cruciais para a manutenção e funcionamento de empresas, organizações e instituições governamentais. Isso desemboca em uma série de consequências negativas, muitas das quais são transfronteiriças, dada a natureza global do ciberespaço (SCHRÖDER, 2022).

A primeira tipologia desses crimes refere-se ao hacking, que se concretiza quando o perpetrador ultrapassa as barreiras de segurança do sistema para obter acesso não autorizado. O hacking pode ser motivado por várias razões: desde a busca por informações sensíveis até o mero exercício de habilidades tecnológicas excepcionais. Independentemente da motivação, este ato criminoso tem potencial para causar danos catastróficos, pois abre caminho para outras modalidades de crimes, tais como o roubo de identidade e a fraude (SCHRÖDER, 2022).

Outra modalidade se refere à disseminação de software malicioso, conhecido como malware. Tais programas são implantados clandestinamente nos sistemas e, muitas vezes, são projetados para operar sem o conhecimento do usuário. As funções de um malware podem variar, desde a coleta de dados, como é o caso dos keyloggers, até a destruição de arquivos e programas, como os cavalos de Tróia. Essas operações dependem da vulnerabilidade dos sistemas, e os danos causados podem ser irreversíveis (SCHRÖDER, 2022).

Os ataques de negação de serviço, também conhecidos como DDoS (Distributed Denial of Service), constituem uma outra forma de crime virtual. Nessa modalidade, os criminosos sobrecarregam o sistema com tráfego inútil de rede, ocasionando a paralisação dos serviços disponíveis. Isso causa enormes transtornos a empresas e usuários, além de poder configurar uma forma de ataque cibernético, pois pode ser utilizada para mascarar atividades ilegais mais graves (FREITAS, 2018).

Os crimes de Insider também têm tido grande relevância na criminalidade digital em questão. Eles ocorrem quando indivíduos com autorização legítima para acessar um sistema o utilizam de maneira imprópria. Estes são passíveis de causar danos significativos, uma vez que esses indivíduos têm acesso a ambientes altamente sensíveis e, muitas vezes, são altamente qualificados na manipulação de sistemas (Barbosa, 2009).

As invasões para a instalação de rançongiciels, ou ransomwares, também merecem menção. O rançongiciel é um tipo de malware que restringe o acesso ao sistema até que um resgate seja pago. A incapacidade de acessar informações é capaz de causar imenso aborrecimento e potencial perda financeira, tornando este um crime particularmente prejudicial (MITANI, 2012).

A manipulação de códigos de computador para a criação de armadilhas também faz parte dos crimes contra a segurança de sistemas. Isso pode ocorrer através do spoofing de IP, onde os criminosos se disfarçam com um IP diferente para enganar o sistema ou os usuários. Outra forma é criar sites fraudulentos, idênticos aos sites legítimos, com o objetivo de enganar os usuários e coletar suas informações pessoais (Primo, 1969).

A injeção de SQL é outra técnica utilizada para infringir a segurança dos sistemas. Esta técnica envolve a introdução maliciosa de código SQL em um sistema para alterar, destruir ou recuperar informações da base de dados. Uma implementação de segurança inadequada e falhas na estrutura do sistema, muitas vezes, propiciam esses ataques, aumentando os riscos dessa prática criminosa (FREITAS, 2018).

As técnicas de phishing também são uma ameaça significativa à segurança dos sistemas. Através de mensagens eletrônicas fraudulentas que simulam ser de organizações respeitáveis, os criminosos persuadem as vítimas a revelar informações sensíveis. Este método está se tornando cada vez mais sofisticado, o que abre espaço para uma eficácia maior do ataque e, consequentemente, maiores prejuízos para as vítimas (FREITAS, 2018).

Os crimes direcionados à rede de Internet das Coisas (IoT) são uma categoria concernente que está ganhando relevância. Com a popularização dos dispositivos inteligentes, aumenta a preocupação com a segurança desses sistemas, pois muitos deles não estão adequadamente protegidos contra ataques. A invasão desses dispositivos pode resultar na coleta indevida de informações pessoais, bem como na

tomada de controle de dispositivos de uma residência ou empresa (RODRIGUES; AVELINE, 2022).

3.2. Fraudes digitais

No vasto universo de atividades criminosas que permeiam o digital, a fraude reina supremamente como um dos crimes mais comuns e destrutivos. A fraude digital abrange uma ampla gama de atividades ilegais que enganam os indivíduos para obter ganho financeiro ou de outro tipo. Estas podem variar de esquemas de phishing, onde os criminosos enganam os indivíduos para que compartilhem suas informações pessoais e financeiras, até fraudes de cartão de crédito, onde as informações do cartão são roubadas e usadas de forma ilegal (DOYLE; OLINTO, 2021).

Um elemento que amplifica a magnitude da fraude digital é a velocidade em que esses crimes podem ser cometidos. Um criminoso pode obter informações de milhares de pessoas com um único ataque de phishing, ou drenar as contas bancárias de várias vítimas em questão de minutos através de um ataque de skimming de cartão automatizado. Esta rapidez e eficácia transformam a fraude digital em uma arma de escolha para muitos criminosos da era digital (SPERVER; ZILIOTI, 2021).

Segundo Primo (1969, p. 88):

> A natureza transfronteiriça desses crimes adiciona uma camada extra de complexidade ao problema. Muitas vezes, o criminoso e a vítima estão situados em diferentes jurisdições, com leis e regulamentos diferentes, tornando difícil e complicada a persecução e o julgamento dos criminosos. A identificação da jurisdição competente é frequentemente um desafio e a falta de cooperação entre os países pode prejudicar a investigação e a persecução desses crimes.

A virtualidade dos crimes de fraude digital e a falta de uma localização física específica colocam mais desafios às forças de segurança. Localizar a origem de um ataque de phishing ou rastrear o autor de uma fraude de identity theft pode ser grandemente difícil, devido à habilidade dos criminosos em esconder seus rastros e à evolução constante das tecnologias e táticas utilizadas para executar esses crimes (SILVA; RAMOS, 2023).

A sofisticação das técnicas utilizadas pelos criminosos também apoia a persistência da fraude digital. Com o uso de tecnologias avançadas como botnets,

malware e dark web, os criminosos digitais podem não só cometer seus atos ilegais com uma eficácia sem precedentes, mas também permanecer no anonimato e evitar a detecção. Esta constante adaptação e evolução das táticas criminais tornam a luta contra a fraude digital uma batalha contínua das agências de segurança e nossas sociedades (FRANK; BACKES, 2015).

Por outro lado, a falta de consciência e educação da sociedade em cibersegurança amplifica a prevalência da fraude digital. Isso é visto quando os indivíduos revelam inadvertidamente suas informações pessoais para atacantes ou quando as instituições falham em adotar as normas de segurança necessárias, tornando-se um alvo fácil para os criminosos (FREITAS, 2018).

As vítimas de fraudes digitais sofrem uma série de consequências, que vão desde perdas financeiras até danos à reputação e ao bem-estar emocional. Os efeitos psicológicos da fraude, incluindo estresse, ansiedade e depressão, são frequentemente subestimados, mas podem ser tão prejudiciais quanto os danos financeiros, se não mais (MITANI, 2012).

Além da dificuldade de rastrear e julgar os criminosos, um obstáculo significativo a enfrentar é a sensação de impunidade que muitas vezes envolve a fraude digital. Dada a natureza oculta desses crimes e a latência das regras e leis existentes para combatê-los, os criminosos digitais frequentemente operam com uma sensação de invulnerabilidade que os encoraja a persistir nesses atos ilegais (FREITAS, 2018).

A complexidade do cenário de fraude digital é múltipla, composta por elementos tecnicamente sofisticados, legais e sociais. Essa complexidade respalda a urgência de abordagens novas e eficazes para mitigar a fraude digital. Necessitamos de esforços sustentados para aprimorar a capacidade técnica das organizações para detetar e prevenir fraudes, melhorar a compreensão e consciência da sociedade sobre as táticas de fraude e desenvolver mecanismos legais robustos e eficazes para punir os criminosos (SPERVER; ZILIOTI, 2021).

3.3. Roubo de identidade e dados

O roubo de identidade e dados é um crime digital que transcende fronteiras, caracterizado pela apropriação ilícita de informações pessoais com a finalidade de cometer fraudes em nome da vítima. A atuação nesse tipo de crime pode ser notada

na aplicação de diversas técnicas, como o phishing, onde o criminoso utiliza mensagens falsas para induzir o indivíduo a revelar seus dados pessoais ao acreditar que está em uma interface segura (Primo, 1969).

Este crime, muitas vezes, é transitado em âmbito transnacional, uma vez que para a sua efetiva ocorrência a presença física do agente na jurisdição da vítima não se faz necessária. O criminoso pode estar em qualquer lugar do mundo, utilizando a internet como ferramenta principal, o que dificulta, e muito, a determinação da competência jurisdicional para apurar e julgar tais crimes (Pouzada et al., 2020).

Ademais, a complexidade desse tipo de delito é elevada, tendo em vista que muitas vezes as informações coletadas são utilizadas não imediatamente, mas guardadas para uso em um posterior momento, dificultando assim a detecção do roubo. Criminosos costumam utilizar redes de computadores zumbis e técnicas sofisticadas de ocultação de identidade, o que torna a rastreabilidade ainda mais complexa (SOUZA; DANTAS, 2023).

O rastreamento dos dados roubados também é um entrave na investigação do roubo de identidade. Muitas vezes, a informação é vendida em mercados negros na dark web para outros criminosos, multiplicando assim a ameaça e dificultando ainda mais o rastreamento e recuperação dos dados. Por vezes a informação sai do domínio da jurisdição de origem e é armazenada em servidores localizados em outra jurisdição, o que traz desafios adicionais (ROCHA; CHAVES, 2024).

Outro fator importante é a falta de normativas específicas para tratar desta questão em muitos países, o que deixa o cenário ainda mais incerto. Leis de privacidade e proteção de dados variam amplamente de país para país, o que complica a determinação de competência e extradição de criminosos. Há um esforço crescente pela harmonização de leis aplicáveis a crimes digitais, como evidenciado pela Convenção de Budapeste, por exemplo (SPERVER; ZILIOTI, 2021).

A Convenção de Budapeste, também conhecida como Convenção do Cibercrime, foi o primeiro tratado internacional sobre crimes cometidos em meio virtual e posiciona a troca de informações e a cooperação internacional como elementos cruciais para combater o cibercrime. Nem todos os países são signatários da Convenção, o que pode dificultar a cooperação mútua no caso de crimes de roubo de identidade e dados (MEDEIROS et al., 2024).

A impunidade é outra característica desse complexo cenário. A incapacidade de responsabilizar o infrator faz com que o cibercrime seja percebido como de baixo

risco, incentivando ainda mais a prática do roubo de identidade. A estrutura do ambiente virtual alimenta essa impunidade, com o anonimato na internet facilitando as operações criminosas (MITANI, 2012).

A nível de prevenção, a conscientização dos usuários de internet e a adoção de tecnologias anti-fraude são vistas como ferramentas essenciais. Tais medidas sozinhas não são suficientes para proteger completamente indivíduos e instituições contra o roubo de identidade e dados. É necessária uma colaboração ativa entre agências governamentais, especialistas em segurança da informação e provedores de serviços de internet (SOUZA; WESLEY, 2023).

As campanhas de conscientização podem auxiliar na redução da incidência de crimes de roubo de identidade, à medida que os usuários se tornam mais capazes de identificar tentativas de phishing e outras técnicas comumente utilizadas pelos criminosos. Já as soluções tecnológicas, como a biometria e a autenticação em dois fatores, podem oferecer níveis avançados de proteção para os dados do usuário (MITANI, 2012).

O desafio principal reside na cooperação internacional e na adoção de uma abordagem unificada para rastrear e punir os autores do roubo de identidade e dados. A instituição de um marco legal claro que estabelece competências definidas e mecanismos de cooperação pode ser um passo importante nessa direção (DOYLE; OLINTO, 2021).

3.4. Exploração e abuso online

Exploração e abuso online são fenômenos globais que ocorrem em um universo digital sem fronteiras nacionais, o que complexifica a aplicação da justiça e a responsabilidade penal. O espectro dos crimes digitais transnacionais inclui uma variedade de delitos, como fraude online, cibercrimes financeiros, cyberstalking e exploração sexual online. Vítimas de diferentes nacionalidades e jurisdições tornam a determinação da competência um desafio para as autoridades competentes. Nuvens jurídicas tornam-se ainda mais densas quando os perpetradores cometem crimes a partir de localizações geograficamente isoladas, utilizando servidores em diferentes países para evitar a detecção e a acusação (RODRIGUES; AVELINE, 2022).

A natureza transnacional da Internet possibilita que criminosos evitem detecção e acusação, explorando lacunas nas regulamentações e leis de vários países. O

anonimato oferecido pela Internet proporciona uma sensação de invulnerabilidade e impunidade aos perpetradores desses crimes. O modus operandi de muitos desses criminosos envolve a obtenção de informações pessoais de suas vítimas, que muitas vezes são coletadas através de técnicas de engenharia social ou invasão de sistemas (MUNGUAMBE; PINTO; FREIRE, 2017).

A exploração sexual online, em particular, tem se mostrado um desafio formidável para as autoridades, devido a suas múltiplas camadas de complexidade. A pornografia infantil e a exploração sexual de menores são crimes digitais transnacionais que ocorrem em uma escala alarmante. Infelizmente, as vítimas muitas vezes permanecem sem identidade, enquanto os perpetradores escapam à detecção, abrigados pela invisibilidade que a Internet proporciona (FRANK; BACKES, 2015).

Embora seja uma questão criminosa de caráter transnacional, muitas vezes os regulamentos locais são insuficientes para combater esses crimes. Uma das principais dificuldades reside na diferença entre os quadros legais de diferentes países, o que impede a realização de esforços concentrados para prender e processar os culpados. Frequentemente, os perpetradores operam de países com legislação menos rigorosa, onde o alcance dos mecanismos de aplicação da lei de outras nações muitas vezes é limitado (MITANI, 2012).

Os crimes de abuso online também alcançam um nível perturbador de invasões de privacidade, tais como a disseminação não consentida de imagens íntimas, conhecida como 'pornô de vingança', que tem um impacto psicológico e emocional duradouro sobre as vítimas. A capacidade de manipulação e extorsão dos perpetradores sobre suas vítimas aumenta exponencialmente em um ambiente digital onde a proximidade física não é necessária para cometer tais abusos (MEDEIROS et al., 2024).

As dificuldades em determinar a competência são intensificadas pelo contínuo desenvolvimento tecnológico. A ascensão da Internet das Coisas (IoT) e do uso crescente de dispositivos conectados à Internet em todas as áreas da vida quotidiana oferecem novas fronteiras para os cibercriminosos explorarem. Máquinas infectadas e redes de botnets podem ser commandadas a partir de um local remoto, adicionando uma camada adicional de dificuldades para rastrear a origem dos crimes (Pouzada et al., 2020).

A falta de cooperação internacional eficaz adiciona outra camada de complexidade ao problema. Embora existam várias iniciativas promissoras, tais como

o Cybercrime Convention Committee do Conselho da Europa, a implementação prática da cooperação transnacional ainda é problemática. Diferenças de jurisdição, questões de privacidade e direitos humanos criam barreiras significativas a serem superadas (SOUZA; DANTAS, 2023).

Por outro lado, a fragilização da privacidade dos dados e a vigilância massiva apresentam um paradoxo difícil de resolver. Embora possa ser necessário invadir a privacidade dos cibercriminosos para efetuar sua captura, tais medidas levantam questões significativas sobre a invasão da privacidade do cidadão comum. O delicado equilíbrio entre a garantia da segurança cibernética e o respeito pelos direitos à privacidade apresenta um desafio contínuo aos legisladores e aplicadores da lei (SOUZA; DANTAS, 2023).

O anonimato proporcionado pelas moedas virtuais e criptomoedas complica ainda mais a tarefa de rastrear e prender os culpados. Esses recursos financeiros digitais são frequentemente explorados para o financiamento de atividades criminosa online, desde a compra de bens e serviços ilegais até a lavagem de dinheiro e o financiamento do terrorismo. A falta de regulamentação global consistente e a natureza descentralizada dessas moedas formam obstáculos consideráveis para tornar eficientes as investigações financeiras (SOUZA; WESLEY, 2023).

É necessário um amplo espectro de soluções para abordar eficazmente a questão dos crimes digitais transnacionais. Estes incluem a harmonização da legislação penal internacional, a melhoria da cooperação transnacional, o desenvolvimento de capacidades técnicas avançadas para rastrear e identificar criminosos, e a educação do público sobre práticas seguras online. Entretanto, qualquer resposta deve também considerar os impactos sobre a liberdade individual, os direitos humanos, e a privacidade dos dados (SILVA; RAMOS, 2023).

4. Aspectos Jurídicos e Legais

O ambiente legal para lidar com crimes digitais transnacionais é vasto e complexo. A própria natureza descentralizada da Internet e a diferença entre as fronteiras jurisdicionais tornam os esforços para construir um marco legal harmonizado uma tarefa complicada. Mas essa complexidade não diminui a urgência de uma abordagem legal robusta que torne possível responsabilizar os criminosos transfronteiriços e proteger efetivamente as vítimas. Também é altamente desafiador

estabelecer competências, considerando que instituições responsáveis pela aplicação da lei muitas vezes enfrentam limitações do próprio âmbito geográfico, enquanto os crimes digitais ultrapassam essas fronteiras (GOMES, 2016).

As dificuldades inerentes à determinação da competência courts levaram vários países a tomarem medidas para definir um âmbito jurídico frente a esses crimes. As abordagens diferem significativamente. Alguns países baseiam a jurisdição na localização do criminoso, na do servidor do crime ou na localização da vítima. Outros adotam uma abordagem universalista, alegando jurisdição sobre qualquer crime que afete seus cidadãos, independentemente de onde o crime tenha ocorrido (FREITAS, 2018).

O embasamento legal da Competência Universal é um conceito resultante do Direito Penal Internacional e, embora ainda controverso, é possível que seja uma solução para lidar com crimes de natureza transnacional. Entretanto, há desafios em usar tal abordagem devido às complicações em estabelecer uma jurisdição universal para os crimes cibernéticos. A cooperação internacional em conjunto à capacidade de extradição precisaria ser significativamente aprimorada (PAGLIOSA; RIBEIRO, 2022).

A Convenção de Budapeste, que é um tratado internacional que trata dos crimes cibernéticos, busca orientar a cooperação global para combater essas ofensas. Nem todos os países assinaram essa convenção e essa falta de consenso global dificulta um combate efetivo. Outro ponto de consideração são os aspectos de privacidade e proteção de dados pessoais que são desafiados ao lidar com crimes transnacionais de natureza digital (GOMES, 2016).

Um recurso emergente no quadro jurídico internacional que pode auxiliar na determinação de competência para crimes digitais transnacionais é o auxílio jurídico mútuo (MLA). Encorajado pelo Conselho da Europa, o MLA é um acordo formal entre os países para fornecer assistência em investigações ou processos criminais. Contudo, a eficácia dos acordos de auxílio mútuo é ainda uma incógnita, pois são frequentemente dificultados por aspectos processuais (SOUZA; DANTAS, 2023).

Por outro lado, a nível regional, a União Europeia introduziu a Diretiva sobre Ataques a Sistemas de Informação e adotou o conceito de competência, permitindo aos Estados membros assumir uma competência extraterritorial em certos casos de crimes cibernéticos. Esta abordagem pode fornecer uma base para outros países considerarem ao moldar suas legislações nacionais (PAGLIOSA; RIBEIRO, 2022).

Apesar das tentativas de resposta legal em nível local e global, os esforços permanecem fragmentados. As normas jurídicas variam geograficamente, criando não apenas diferenças substanciais na aplicação da lei, mas também "paraísos seguros" para os criminosos. A hipótese desses redutos de impunidade demonstra a urgente necessidade de harmonização legal a nível global nessa área (Pouzada et al., 2020).

Em meio à pressa de adotar leis para combater o crime digital transnacional, é vital garantir que os direitos humanos não sejam negligenciados. A equação entre segurança cibernética e privacidade é delicada. A proteção eficaz contra crimes digitais não pode ser adquirida às custas de violações generalizadas da privacidade. Este é um desdobramento necessário e intrincado para qualquer legislação a ser considerada no cenário de crimes digitais transnacionais (ROCHA; CHAVES, 2024).

As novas tecnologias também trazem desafios adicionais para a questão legal. A aplicação da lei frequentemente se depara com pontas soltas legais ao tentar lidar com fenômenos emergentes, como criptomoedas e cadeia de blocos (Blockchain). Esses elementos adicionam uma nova camada de complexidade à maneira como ajudamos a aplicação da lei a navegar em territórios desconhecidos na paisagem transnacional de crimes digitais (Barbosa, 2009).

Ademais, a sofisticação crescente dos crimes digitais requer uma atualização contínua das leis. Os agentes do cibercrime estão sempre à frente, aproveitando novas tecnologias e lacunas legais existentes. Há uma necessidade constante, mas desafiadora, de adaptar e modernizar constantemente as disposições legais para manter o ritmo. As leis devem ser capazes de prever práticas criminosas potenciais que ainda não se materializaram, provando ser um grande desafio à capacidade de prevenção e garantia legal de crimes digitais transnacionais (FARIAS, 2021).

4.1. Legislação internacional aplicável

Com um olhar voltado ao problema dos crimes digitais transfronteiriços, é essencial abordar os esforços da comunidade internacional em criar legislações adequadas para regulamentar a jurisdicionalidade. A luta por um direito penal internacional vem acelerando com o advento dos crimes digitais e a complexidade da cibercriminalidade. Contudo, existe uma necessidade urgente de mecanismos jurídicos e institucionais eficazes para enfrentar a extensão e a profundidade dessa problemática (RODRIGUES; AVELINE, 2022).

A Convenção sobre o Cibercrime do Conselho da Europa, conhecida como Convenção de Budapeste, foi o primeiro tratado internacional a abordar amplamente os crimes cibernéticos. Seu principal objetivo é conciliar diferenças entre as legislações nacionais e estabelecer um conjunto comum de delitos e procedimentos processuais no contexto da criminalidade digital. Apesar do alcance e da relevância, esta convenção apresenta certas limitações, principalmente devido à sua adoção não universal (FRANK; BACKES, 2015).

O papel da Organização das Nações Unidas (ONU) também é significativo na busca por leis que possam ser aceitas universalmente. A ONU tem promovido várias iniciativas para combater a cibercriminalidade, o que inclui elaborar uma nova convenção abrangente. A intenção é unificar a legislação internacional em matéria de cibercriminalidade, providenciando uma orientação mais clara para os países e para cooperação internacional no combate aos crimes digitais transnacionais (SOUZA; WESLEY, 2023).

As diretrizes das Nações Unidas sobre a prevenção e o controle da criminalidade também incluem recomendações expressas para países que desenvolvem estratégias eficazes para enfrentar cibercrimes. Essas diretrizes preveem a necessidade de que todas as nações adotem abordagens equilibradas envolvendo prevenção, sanção e recuperação, visando possibilitar a aplicação adequada da lei aos crimes cibernéticos (SCHRÖDER, 2022).

Ademais, o G8 e a Interpol desenvolveram programas de cooperação internacional visando o combate aos crimes cibernéticos, incluindo o roubo de identidade, a fraude eletrônica e a pornografia infantil. Estes programas servem para preencher as lacunas deixadas pelos esforços individuais dos governos, que frequentemente se deparam com barreiras legais e técnicas difíceis de superar sozinhos (RODRIGUES; AVELINE, 2022).

Outros instrumentos internacionais relevantes incluem as Diretrizes de crime cibernético e segurança da informação do G20, bem como as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) que já foram aceites por muitos de seus países-membros. A OCDE atua definição de uma agenda global para abordar a cibercriminalidade, com diretrizes que ajudam os governos a implementar estratégias de cibersegurança e legislações de crimes cibernéticos (SPERVER; ZILIOTI, 2021).

No que se refere ao espaço da União Europeia, o Diretivo da UE 2013/40/EU representa o mais recente esforço de padronização de normativas sobre cibercrimes. O Diretivo introduziu uma série de medidas para harmonizar as leis penais contra a cibercriminalidade entre os Estados-Membros, facilitando assim a cooperação transfronteiriça na detecção e no processamento de tais crimes (PAGLIOSA; RIBEIRO, 2022).

A mera existência de tratados e convenções internacionais não garante que sejam efetivamente implementados e respeitados pelos estados-membros. Fatores como a ausência de capacidades técnicas, a insuficiência de conhecimento jurídico e a falta de vontade política podem impedir ou atrasar a aplicação efetiva da legislação internacional sobre crimes cibernéticos em um contexto doméstico (ROCHA; CHAVES, 2024).

Além do desenvolvimento de legislação internacional, é importante considerar auxílios para os países menos desenvolvidos em termos de capacidade técnica e orçamentária. A cooperação internacional no compartilhamento de melhores práticas, auxílio técnico e formação de capacidades é essencial para combater a complexidade dos crimes digitais transnacionais (FREITAS, 2018).

4.2. Cooperação jurídica entre países

A cooperação jurídica entre países é essencial para combater os crimes digitais de caráter transnacional. Essa colaboração se torna cada vez mais relevante devido à natureza pervasiva da internet e ao aumento constante das atividades digitais. A digitalização da sociedade elevou o espaço cibernético, um ambiente sem fronteiras geográficas, a um campo fértil para a prática de delitos que transcendem as barreiras nacionais. No campo da cibersegurança jurídica internacional, dentre os quais se destacam a obtenção de provas, as operações encobertas, as suspensões telefônicas e a extradição, refletem a necessidade urgente de cooperação entre nações (GOMES, 2016).

Contrapõem-se as dificuldades inerentes a essa cooperação no conceito de soberania nacional. No sistema internacional, cada Estado possui o direito de exercer seu poder livremente dentro de seu território, o que inclui a implementação de seus próprios regimes jurídicos e penais. Este princípio é posto à prova quando um delinquente virtual comete um delito num Estado, porém reside ou se encontra num

território distinto. A colaboração jurídica internacional nesse cenário apresenta desafios significativos, entre eles circunscrições políticas distintas, variações nas regulamentações judiciais e na lei penal, entre outros (FRANK; BACKES, 2015).

Um importante marco na cooperação jurídica internacional para a perseguição de crimes digitais transnacionais é a Convenção de Budapeste. Este tratado, elaborado pelo Conselho da Europa e em vigor desde 2004, fornece um quadro para a cooperação internacional em investigações de natureza digital e também estabelece guidelines para a legislação nacional relevante. Ainda agora, esta convenção é o único instrumento jurídico vinculativo a nível global que aborda o fenômeno do crime digital em um contexto transfronteiriço, enfatizando a importância da colaboração jurídica entre países para julgar atos delituosos cometidos online (GIAMUNDO NETO, 2020).

Considerando a multiplicidade de jurisdições, uma das soluções sugeridas para otimizar a cooperação jurídica é a implementação de uma jurisdição universal para crimes digitais. Essa solução levanta várias preocupações, principalmente em termos de violação de direitos humanos e liberdades individuais, uma vez que uma jurisdição global pode levar, em sua acusação culminante, a uma justiça penal sem fronteiras, com sérias ramificações para a soberania dos Estados (SCHRÖDER, 2022).

Complicações jurisdicionais abrangem não só a distinção entre territórios físicos, mas também a questão da privacidade dos dados. Com efeito, muitas vezes os investigadores se deparam com a necessidade de aceder a provas armazenadas fora da sua jurisdição, o que levanta questões legais complexas no que diz respeito à extraterritorialidade da apreensão de dados. Assim, a colaboração entre as autoridades judiciárias e os prestadores de serviços online é imprescindível para superar tais desafios (MITANI, 2012).

Um aspecto importante que ocupa um lugar central na cooperação jurídica internacional é a formação de equipes conjuntas de investigação. Estas forças-tarefa permitiriam a troca de informações em tempo real, acelerando significativamente as investigações e simplificando os processos judiciais. Contudo, a criação desses grupos requer acordos intergovernamentais claros, bem como comprometimento em compartilhar informações sensíveis, o que pode ressaltar potenciais conflitos de interesse entre os países (MUNGUAMBE; PINTO; FREIRE, 2017).

Frequentes são as discrepâncias substanciais entre os diferentes sistemas jurídicos em termos de legislação penal relacionada ao cibercrime. Enquanto alguns países possuem legislação robusta e detalhada, outros ainda estão desenvolvendo

suas estruturas legais correspondentes. Isso contribui para um cenário fragmentado, onde a eficácia da colaboração é muitas vezes prejudicada pelas diferenças na taxa de penalização e classificação dos cibercrimes (ROCHA; CHAVES, 2024).

A necessidade de cooperação jurídica internacional nos cibercrimes é ainda enfatizada pela tendência de os criminosos organizarem suas operações em países com infraestrutura tecnológica avançada, mas com rigorosas proteções de privacidade. Essa estratégia permite que os cibercriminosos se escondam eficientemente, enquanto realizam ataques em qualquer região do globo. Desta forma, a harmonização legal e a troca de informações são essenciais para combater efetivamente os flagelos do cibercrime (SILVA; RAMOS, 2023).

Respeitados os princípios de soberania e dos direitos humanos, a cooperação jurídica deve privilegiar a abertura, a reciprocidade e a eficácia. A criação de mecanismos de cooperação e harmonização das leis nacionais, destaca-se como uma necessidade primária para uma resposta eficaz. A regulamentação internacional do espaço cibernético representa um desafio contemporâneo singular e um elemento cada vez mais essencial da justiça penal transnacional, no qual o papel da cooperação jurídica se revela do pontal central (FRANK; BACKES, 2015).

A colaboração entre as entidades privadas, especificamente os gigantes da tecnologia, e as autoridades públicas tem um papel significativo no avanço da cooperação jurídica internacional. A responsabilidade compartilhada dos governos e dos atores do setor privado no combate aos crimes digitais pode dar lugar a uma vulnerabilidade reduzida ao cibercrime e uma maior segurança digital global. Sem dúvida, a criação de parcerias eficazes entre os setores público e privado é uma oportunidade estratégica para potencializar a cooperação internacional no campo do direito penal cibernético (SOUZA; DANTAS, 2023).

4.3. Tratados e convenções internacionais

O surgimento e a expansão das tecnologias digitais se revelaram como um divisor de águas nas relações internacionais, trazendo tanto vantagens significativas como desafios profundos para a governança mundial. Nesse contexto, os tratados e convenções internacionais se tornam ferramentas cruciais para lidar com a intricada teia de crimes digitais transnacionais que muitas vezes ultrapassam as fronteiras dos Estados-nação. A implementação e o respeito a essas normas, apesar de complexos,

são componentes fundamentais para se assegurar a cooperação entre as nações no enfrentamento a esses delitos (SILVA; RAMOS, 2023).

O ciberespaço, onde os crimes digitais são cometidos, não possui um território físico, tornando difícil rastrear e punir os criminosos. E é em resposta a essa complexidade que surgem os tratados internacionais, que buscam estabelecer regras comuns e procedimentos de cooperação mútua. A Convenção de Budapeste, por exemplo, é um instrumento legal mundial dedicado a esse tema, abordando a harmonização das leis nacionais, a melhora na capacidade investigativa e a cooperação internacional, para tentar enfrentar a impunidade que muitas vezes protege os criminosos cibernéticos (MEDEIROS et al., 2024).

O marco normativo internacional relacionado aos crimes digitais também é ilustrado pelo direito penal internacional e pelos diversos tratados que regulam a cooperação judicial e policial em matéria penal. Além da já citada Convenção de Budapeste, há outras normativas e acordos internacionais que buscam solucionar essa problemática, como a Convenção de Mérida da ONU sobre a corrupção, que faz uma abordagem holística do problema, inclusive considerando a prevenção, a incriminação e a cooperação internacional (RODRIGUES; AVELINE, 2022).

Uma abordagem alternativa é demonstrada pela Diretiva da União Europeia em matéria de Ataques contra Sistemas de Informação, que estabelece um quadro comum de respostas jurídicas para enfrentar os crimes digitais dentro do território da União. Outros tratados regionais também têm como objetivo aumentar a eficácia da cooperação entre seus membros na luta contra o crime cibernético, como a Convenção Interamericana sobre Cibercrime (MUNGUAMBE; PINTO; FREIRE, 2017).

Além da criação de normativas internacionais, a dificuldade em determinar eficazmente a competência nos crimes digitais transnacionais também impulsionou a busca por tratados de colaboração mútua para auxiliar na coleta e no compartilhamento de provas digitais. Leis que definem os procedimentos para o compartilhamento de provas são altamente relevantes neste contexto, como o Marco Legal para a Coleta, o Tratamento e a Transferência Internacional de Evidências Eletrônicas da União Europeia (SOUZA; DANTAS, 2023).

No campo estratégico, os principais países desenvolvidos já reconhecem a necessidade de estabelecer medidas para prevenir e responder aos ataques cibernéticos, refletindo isso em diversos documentos estratégicos de defesa. Por

exemplo, a estratégia de cibersegurança nacional dos Estados Unidos de 2018 identificou a necessidade de "manter um ciberespaço aberto, interoperável, seguro e confiável", o que pressupõe também o respeito aos principais tratados e convenções internacionais (MUNGUAMBE; PINTO; FREIRE, 2017).

Segundo Sperver e Zilioti (2021, p. 45):

> A efetividade dessas convenções e tratados internacionais depende, porém, de vários fatores, como sua rápida ratificação por parte dos estados e a adequação das leis nacionais. Muito embora esses documentos definam algumas obrigações claras para os estados, a eficiência da implementação dessas obrigações muitas vezes enfrenta obstáculos. As discrepâncias nas capacidades técnicas e legais entre países também podem dificultar a aplicação efetiva dessas normativas.

Enfrentar os crimes digitais transnacionais não envolve apenas questões técnicas e jurídicas, mas também questões éticas e políticas significativas. Como os criminosos cibernéticos podem operar de qualquer local do mundo, os estados precisam trabalhar em conjunto para evitar que países se tornem refúgios seguros para esses indivíduos. Isso obriga a comunidade internacional a revisar os princípios de soberania e não interferência, tanto em termos de jurisdição quanto no que se refere ao direito de perseguir indivíduos que cometem crimes cibernéticos (DOYLE; OLINTO, 2021).

Por outro lado, mesmo que essas convenções e tratados internacionais já representem um avanço em direção a uma maior cooperação internacional na luta contra os crimes digitais, a rápida evolução da tecnologia pode continuar a desafiar sua eficácia. As novas formas de delitos digitais e o uso cada vez mais sofisticado da criptografia, por exemplo, requerem constante atualização das normativas, dos processos e dos mecanismos de cooperação, o que exige um compromisso contínuo por parte dos estados com o desenvolvimento do direito penal internacional no espaço cibernético (Barbosa, 2009).

5. Desafios na Determinação da Competência

A determinação da competência em crimes digitais transnacionais é uma tarefa incrivelmente complexa, devido ao próprio caráter intrínseco da Internet. Como uma rede sem fronteiras físicas, a Internet permite que indivíduos cometam atos criminosos

em uma jurisdição enquanto estão fisicamente presentes em outra, tornando a atribuição de competência jurídica um desafio. A natureza sem fronteiras do ciberespaço faz com que a aplicação de leis e regulamentos seja uma tarefa delicada, pois uma ação que pode ser legal em um estado pode ser ilegal em outro (GOMES, 2016).

Esse é o conceito de "normas em conflito", a controvérsia gerada pela impossibilidade de aplicar adequadamente a lei de um determinado Estado em face de uma ação ilegal cometida no mundo digital. A possibilidade de cometer crimes a partir de qualquer localidade no globo lança desafios para a jurisprudência e a aplicabilidade das leis, pois implica diretamente na competência dos tribunais na persecução penal e na aplicação de sentenças (SCHRÖDER, 2022).

A soberania é outro desafio ao se determinar a competência em crimes digitais, pois a Internet desafia as tradicionais estruturas de poder do Estado. Em âmbito global, os estados têm limitações sobre a extensão de sua competência legislativa, o que afeta diretamente a eficácia das leis nacionais e internacionais. Nestes termos, a ausência de acordos globais abrangentes e coerentes compromete a capacidade dos Estados nacionais de perseguir e processar crimes cometidos no ciberespaço (Primo, 1969).

A falta de padrões de identificação e autenticação de usuários na Internet obstaculiza a investigação e a prova de crimes digitais. Um infrator pode esconder facilmente a sua identidade através de tecnologias como anonimato e criptografia, complicando a localização e identificação dos perpetradores. Esta realidade adiciona novas camadas de complexidade ao processo de determinação da competência judicial em crimes digitais (FARIAS, 2021).

A perícia digital é um terreno em constante mutação em resposta à crescente sofisticação das técnicas de cibercrime. As ferramentas atuais de análise de crimes digitais podem ser rapidamente obsoletas à medida que novas tecnologias e táticas de cibercriminosos surgem. Assim, a falta de recursos e experiência técnica também dificulta a determinação efetiva da competência jurídica em casos de cibercrime (Primo, 1969).

A morosidade do processo de cooperação internacional também é um desafio significativo. As divergências entre os meios de obtenção de provas, conflitos de leis e a falta de uma estrutura internacional sistematizada de cooperação são obstáculos à determinação da competência. Tais barreiras podem resultar em perda de tempo

valioso durante o qual as evidências podem ser perdidas ou destruídas (SOUZA; WESLEY, 2023).

A disparidade no estado de desenvolvimento e implementação de leis de cibercrime em países diferentes também adiciona uma camada de complexidade. Alguns países podem ter leis avançadas e eficazes, enquanto outros podem ter regulamentos fragmentados ou inexistentes, que não são adequados para enfrentar o problema em seu todo e impedem a ação coordenada entre as jurisdições (MITANI, 2012).

Outra questão é a distinção entre crimes digitais e crimes tradicionais cometidos através do ciberespaço. Esta distinção é importante para determinar qual corpus jurídico é aplicável, pois muitas legislações não contemplam especificamente os crimes digitais, aplicando as leis de crimes convencionais a casos que envolvem aspectos tecnológicos (ROCHA; CHAVES, 2024).

Por último, os desafios também residem no domínio ético, pois a determinação da competência em crimes digitais pode abrir precedentes para a violação de direitos fundamentais, como a privacidade. As tentativas de rastrear e identificar os perpetradores de crimes digitais podem levar à vigilância e monitoramento excessivo, tornando-se um paradoxo de proteção e de potencial transgressão dos direitos individuais (MEDEIROS et al., 2024).

Os desafios no estabelecimento da competência em crimes digitais transnacionais são múltiplos e complexos. Um olhar mais atento para as questões envolvidas é essencial para uma discussão progressiva e efetiva neste campo da lei (MUNGUAMBE; PINTO; FREIRE, 2017).

5.1. Natureza transnacional dos crimes digitais

A natureza transnacional dos crimes digitais apresenta um desafio assustador em relação à governança e jurisdição em um mundo cada vez mais interconectado. Esses crimes desafiam os sistemas legais existentes e as correspondentes jurisdições territoriais, pois o crime ocorre frequentemente em um ambiente virtual que cruza fronteiras geográficas e sistemas legais. Neste contexto, os criminosos podem estar localizados em uma jurisdição, as vítimas em outra e os servidores e dados que facilitam o crime ainda em outra. Esta deslocalização e fluidez dos crimes digitais

dificultam não apenas a identificação e persecução dos criminosos, mas também a implementação de mecanismos de prevenção eficazes (FARIAS, 2021).

Ademais, a infraestrutura tecnológica disponível permite que os criminosos escondam sua localização física efetiva e, assim, dificultem a localização e a atuação das autoridades. Esse anonimato fortalece os criminosos, pois permite que eles atuem de maneira quase ilimitada, sem temer retaliação ou punição. A utilização de redes privadas virtuais (VPN), proxies e Tor para mascarar o endereço IP e a localização dos criminosos dificultam ainda mais a investigação e a responsabilização desses indivíduos (Barbosa, 2009).

A complexa natureza desses crimes frequentemente requer uma competência altamente especializada e ferramentas técnicas avançadas para sua investigação e atribuição. A sofisticação do malware utilizado em crimes digitais está em constante evolução, e a exploração de vulnerabilidades e a infiltração em sistemas são muitas vezes muito sutis e difíceis de detectar. Essas potencialidades não apenas exigem uma sofisticação técnica considerável por parte dos órgãos de investigação, mas também apresentam desafios significativos para a coleta e a apresentação de provas em processos judiciais (Primo, 1969).

Também se deve enfatizar a rapidez com que os crimes digitais podem ser cometidos e o vasto alcance que eles podem ter. Um único ataque pode afetar milhares ou mesmo milhões de usuários e, ainda, pode ser lançado e concluído em questão de segundos. Ao comparar-se com o mundo não virtual, tal cenário de crimes dificilmente seria possível de se observar. A agilidade e a disseminação massiva dos crimes digitais exacerbam as dificuldades já discutidas e ampliam as consequências para as vítimas (FRANK; BACKES, 2015).

Por outro lado, essa natureza veloz e disseminada dos crimes digitais amplifica a necessidade de uma resposta ágil e eficaz. A lentidão resultante do processo de solicitação de assistência jurídica internacional, somada à eventual falta de cooperação entre as jurisdições, pode contribuir para a impunidade dos criminosos e para a persistência do problema. Este quadro, por sua vez, intensifica a sensação de insegurança das vítimas e sociedade em geral, alimentando a desconfiança nas capacidades das autoridades locais e internacionais para combater os crimes digitais (SOUZA; WESLEY, 2023).

Destaca-se ainda o fato de que os crimes digitais não reconhecem fronteiras culturais ou sociais. Vários grupos de indivíduos podem ser afetados, desde empresas

e governos até usuários individuais em suas casas. Isso resulta em uma enormidade de impactos que variam desde a violação de direitos individuais como a privacidade e a liberdade de expressão até implicações macroeconômicas e geopolíticas (MITANI, 2012).

Outro elemento digno de nota é a mais recente tendência no desenvolvimento de tecnologias que dão suporte a atividades criminosas virtuais, que são na sua essência transnacionais. A blockchain e as criptomoedas são relevantes exemplos dessa tendência. Elas reforçam a natureza transnacional dos crimes, pois permitem transações e transferências de recursos ilegais sem a necessidade de um intermediário financeiro tradicional, o que dificulta o rastreamento da atividade criminosa (PAGLIOSA; RIBEIRO, 2022).

O advento da Internet das Coisas (IoT) amplia o escopo dos crimes digitais transnacionais. O crescente número de dispositivos conectados à internet aumenta a quantidade de pontos de entrada potenciais para ataques cibernéticos. Assim, a IoT introduz uma nova dimensão ao problema, tornando ainda mais complexa a tarefa de responsabilização pelos atos ilícitos (FRANK; BACKES, 2015).

A natureza transnacional dos crimes digitais cria desequilíbrios na capacidade de resposta entre as nações. Aquelas com menos recursos para investir em segurança cibernética e infraestrutura tecnológica sofrem mais com os ataques e têm mais dificuldades em rastrear e processar os criminosos. Os desafios inerentes à natureza transnacional dos crimes digitais requerem uma coordenação e uma cooperação internacionais sem precedentes para desenvolver soluções eficazes para enfrentá-los (MEDEIROS et al., 2024).

5.2. Jurisdição territorial versus jurisdição digital

A jurisdição territorial, em geral, é determinada pela localização física da origem da atividade ilícita. A natureza das operações digitais e a velocidade com que ocorrem no ciberespaço dificultam a aplicação tradicional deste princípio, deixando em evidência os limites da jurisdição territorial. As atividades digitais, frequentemente transnacionais, ocorrem em um meio que transcende as fronteiras físicas, entretanto, os sistemas de jurisdição permanecem ancorados em estruturas territorialistas, criando um abismo entre jurisdição e realidade digital (SOUZA; WESLEY, 2023).

O princípio da jurisdição digital é, sem dúvida, uma área emergente e a sua formação é decorrente da tecnologia que desafia continuamente os paradigmas das leis de base territorial. O conceito de jurisdição digital é ainda mais complexo do que a jurisdição territorial devido à natureza deslocalizada do ciberespaço, onde a noção de fronteiras é ofuscada. Um indivíduo pode acessar redes e servidores localizados em várias jurisdições diferentes, sem nunca sair fisicamente de sua jurisdição de origem, e causar danos que transcendem as fronteiras geográficas (Barbosa, 2009).

A internacionalização e virtualização inerente aos crimes digitais tornam insuficiente a abordagem tradicional de determinação de competência jurisdicional, baseada em limites geográficos ou territorialidade. Este fenômeno enfatiza a necessidade de uma abordagem flexível e adaptada à dimensão sem fronteiras do ciberespaço, que denomino jurisdição digital. A eficácia das investigações e processos legais reside na capacidade da jurisdição de se adaptar à natureza transnacional do delito (Pouzada et al., 2020).

Os crimes digitais transnacionais levantam questões de competência jurisdicional e aplicação da lei que são agravadas devido à ausência de um regime global de governança da internet. O atual direito internacional, com suas regras de base territorial, proporciona uma grave dificuldade na responsabilização dos culpados por crimes digitais que transcendem as fronteiras nacionais. É comum que as atividades criminosas ocorram em um lugar, o servidor usado para cometer o crime esteja localizado em outro, e a vítima esteja em um terceiro país, criando um verdadeiro desafio para determinar a competência (FARIAS, 2021).

Os desafios que as questões de jurisdição e competência de crimes digitais transnacionais apresentam para o ordenamento jurídico global salientam o fato de que a natureza desses delitos requer um novo modelo jurídico. É importante que este modelo não apenas reconheça a realidade virtual e física como potencialmente congruentes em termos de delitos, mas também os responda de maneira eficaz. As estratégias de combate aos crimes digitais devem incluir novas formas de cooperação internacional e mecanismos de compartilhamento de informações (FREITAS, 2018).

Outra questão relevante está relacionada ao problema da dupla incriminação. Devido às disparidades entre as definições dos crimes, especialmente em um ambiente digital, um comportamento pode ser considerado uma infração penal em um país e perfeitamente legal em outro. Isso dificulta ainda mais o processo de localização

da jurisdição competente e amplia a discussão sobre a necessidade de um consenso internacional em relação aos delitos digitais (FARIAS, 2021).

O anonimato que a rede proporciona e a capacidade de apagar quaisquer vestígios digitais são outros elementos que complicam o estabelecimento da jurisdição digital. A eficiência da investigação desses crimes passa necessariamente pela cooperação internacional, pelo compartilhamento de informações e pela elaboração de legislação harmonizada que acompanhe a evolução rápida da internet e a transnacionalidade inerente aos delitos digitais (GOMES, 2016).

A compreensão e o tratamento dos crimes digitais apenas através dos mecanismos de jurisdição territorial não oferecem respostas suficientes ao fenômeno transnacional da criminalidade digital. Não há dúvida de que estamos diante de um quadro jurídico internacional que não foi concebido para combater a complexidade dos crimes digitais e que está se mostrando cada vez mais impotente frente a esses desafios (GOMES, 2016).

A lacuna entre jurisdição territorial e jurisdição digital realça a necessidade de adequação do ordenamento jurídico para lidar com os crimes digitais. O debate acadêmico e político sobre os meios mais eficazes de combater esses crimes deve continuar e intensificar-se. A própria concepção de jurisdição territorial deve ser repensada, considerando a emergência e expansão das tecnologias digitais que tornam o ciberespaço um palco para atividades criminosas (Primo, 1969).

5.3. Casos emblemáticos e jurisprudência

Entre os casos emblemáticos que ilustram a dificuldade de se determinar a competência em crimes digitais transnacionais, o incidente do hacker romeno Adrian Ghighina oferece um dos exemplos mais esclarecedores. No início dos anos 2000, Ghighina embarcou em uma série de fraude nas redes digitais, especialmente via eBay e PayPal, desencadeando uma investigação que se expandiu pelo globo. A dificuldade de determinar a jurisdição veio à tona quando os investigadores americanos tentaram processar Ghighina, que estava baseado na Romênia na época (SPERVER; ZILIOTI, 2021).

Adicionando complexidade ao caso, as vítimas de Ghighina estavam localizadas em várias jurisdições, tanto dentro quanto fora dos Estados Unidos, tornando a busca pela justiça um verdadeiro labirinto jurídico. O esforço conjunto das

agências de investigação em múltiplos países permitiu o indiciamento de Ghighina em Illinois, e depois sua extradição para os Estados Unidos para ser julgado, essa ação deixou muitos a se perguntar se as jurisdições locais onde as vítimas estavam localizadas foram devidamente consideradas (FRANK; BACKES, 2015).

Um cenário semelhante se desenrolou no caso dos hackers russos, Bogachev e Belan, criminosos digitais que estavam na lista dos mais procurados pelo FBI. A dificuldade de determinar a competência aqui foi ainda mais pronunciada, já que ambos os hackers estavam supostamente sob a proteção do governo russo. Essa situação levantou questões sobre a interação entre a aplicação da lei em nível local, nacional e internacional, abrindo uma discussão sobre a necessidade de cooperação transnacional no enfrentamento de crimes digitais (GIAMUNDO NETO, 2020).

Segundo Primo (1969, p. 72):

> Também digno de menção é o caso Megaupload, que elevou a notoriedade e a severidade dos crimes digitais para o grande público. O site de compartilhamento de arquivos da Nova Zelândia foi acusado de violações maciças de direitos autorais e lavagem de dinheiro, apanhado em uma intricada rede de leis de diferentes jurisdições. O caso representou um divisor de águas na discussão sobre competência em crimes digitais transnacionais e destacou a necessidade urgente de uma abordagem mais harmonizada entre diferentes jurisdições.

O caso de Julian Assange e o Wikileaks forneceu mais lenha à fogueira do debate sobre jurisdição e crimes digitais. A publicação de documentos classificados e protegidos por direitos autorais levantou questões complexas não apenas sobre onde e como Assange deveria ser processado, mas também sobre a fronteira entre o ativismo digital e o crime. A jurisdição nesse caso tem sido um campo de batalha jurídico, politizado e contencioso (DOYLE; OLINTO, 2021).

No contexto europeu, o caso de Maxim Senakh, um hacker russo acusado de fraudes cibernéticas de grande escala, é notável. A cooperação entre os Estados Unidos e a Finlândia permitiu a captura, extradição e processamento de Senakh nos Estados Unidos. A questão persistente na mente dos pesquisadores é se a competência poderia ou deveria ter sido determinada de outra forma, dada a natureza transfronteiriça do crime (FRANK; BACKES, 2015).

Avançando para a jurisprudência, a decisão de 2014 no caso do Tribunal de Justiça da União Europeia relacionada à responsabilidade dos provedores de internet

em crimes digitais é um exemplo de precedente jurídico. Esta decisão determinou que os provedores de internet não podem ser considerados automaticamente responsáveis por informação ilícita divulgada, mas eles poderiam ser considerados culpados se não agissem rapidamente para remover ou bloquear o acesso a tais informações assim que fossem avisados (Primo, 1969).

Nos Estados Unidos, a decisão de 1996 do Supremo Tribunal Federal no caso "United States v. Thomas" estabeleceu o precedente de que os crimes cometidos online podem de fato ser perseguidos. Esta foi uma das primeiras vezes que se aplicou a jurisdição baseada em "efeitos adversos", um componente importante para a aplicação da lei de crimes digitais em anos posteriores (MITANI, 2012).

Ainda neste contexto, o caso "Microsoft v. United States", também conhecido como 'caso do email da Irlanda', é um marco. Neste caso, foi debatida a possibilidade de as agências de aplicação da lei dos Estados Unidos acessarem dados armazenados em servidores no exterior. A decisão resultante trouxe nuances significativas à questão da jurisdição em crimes digitais transnacionais (MUNGUAMBE; PINTO; FREIRE, 2017).

Na Ásia, um precedente significativo foi estabelecido com o caso da Suprema Corte de Cingapura, "Public Prosecutor v. Wan Poh San". Aqui, pela primeira vez, a Suprema Corte determinou que a competência poderia ser estendida a crimes digitais cometidos no exterior por cidadãos de Cingapura. Este caso representa uma orientação significativa para a compreensão atual da jurisdição em crimes digitais na Ásia (SILVA; RAMOS, 2023).

6. Mecanismos de Cooperação Internacional

A cooperação internacional é uma ferramenta essencial na luta contra os crimes digitais transnacionais, considerando a natureza muitas vezes indistinta e física da internet, a qual não respeita fronteiras nacionais. Essa cooperação é apoiada por uma série de instrumentos formais e informais que vão desde acordos multilaterais e tratados, até cooperação pautada em proximidade geográfica ou semelhança legislativa. Entenda-se que tais mecanismos não se restringem apenas a questões relacionadas ao direito penal, mas abrangem outros campos do direito e, sobretudo, a diplomacia, a política e a tecnologia (FARIAS, 2021).

Primeiro, há acordos multilaterais que constituem uma rede complexa de conexões legais entre Estados. Um exemplo proeminente é a Convenção de Budapeste, formalmente conhecida como Convenção sobre o Crime Cibernético do Conselho da Europa, que é o primeiro tratado vinculante internacional a abordar tanto a repressão de crimes cometidos através da Internet e de outros sistemas de redes, quanto a recolha de provas eletrônicas de crimes. Essa Convenção é um catalisador significativo para um amplo espectro de cooperação, desde a assistência jurídica mútua à harmonização legislativa (ROCHA; CHAVES, 2024).

Tratados bilaterais, que estipulam a cooperação entre dois Estados, também podem ser tão extensos quanto acordos de livre comércio com disposições sobre delitos cibernéticos, ou tão específicos quanto tratados de extradição ou assistência jurídica mútua focados em delitos cibernéticos. Esses acordos são especialmente eficazes quando há uma harmonização significativa nas leis de ambos os países e uma disposição para cooperar estreitamente (SOUZA; DANTAS, 2023).

Os regimes de cooperação regional, tais como a União Européia, a Associação das Nações do Sudeste Asiático e a Organização dos Estados Americanos, também proporcionam bases sustentáveis para a cooperação em crimes digitais transnacionais. Estes organismos, por sua vez, criam ambiente para que ocorra a troca de informações em tempo real, capacitação técnica entre os Estados membros e a implementação coesa de normas de conduta (RODRIGUES; AVELINE, 2022).

Da mesma forma, a cooperação intergovernamental entre agências de aplicação da lei oferece uma plataforma para a troca rápida e eficaz de informações. Este mecanismo é especialmente relevante em casos em que a condução de uma investigação sobre um crime digital transnacional requer cooperação imediata. Agências como a Interpol e Europol possuem estruturas dedicadas ao combate ao cibercrime que auxiliam os Estados membros na resolução de crimes digitais (Barbosa, 2009).

As Organizações Não Governamentais também atuam neste cenário cooperativo. O esforço realizado por estes grupos, que vai desde a defesa de políticas de segurança cibernética até a coleta de dados sobre crimes digitais transnacionais, contribui não só para a detecção, mas também para a prevenção desse tipo de crimes. Esta atuação preenche lacunas que podem existir na ação dos Estados, tanto criando novos conhecimentos como articulando discussões em torno de questões contemporâneas (SPERVER; ZILIOTI, 2021).

Um mecanismo de cooperação em ascensão é o fortalecimento de acordos entre setor público e privado. Devido à natureza digital do cibercrime, muitas vezes as infraestruturas, informações ou mesmo soluções necessárias para combatê-lo estão na posse de empresas privadas. Por seu lado, a colaboração entre as empresas de tecnologia e os órgãos de aplicação da lei é necessária não apenas para a detecção e rastreamento de atividades criminosas, mas também para a prevenção eficaz do cibercrime (RODRIGUES; AVELINE, 2022).

A capacitação cruzada entre países é outro aspecto vital da cooperação internacional no combate aos crimes digitais. Este aspecto engloba todo o tipo de formação e transferência de conhecimentos, desde estratégias de investigação e técnicas forenses, até formas de promover a sustentabilidade e resiliência das infraestruturas digitais. Esta cooperação tem como objetivo garantir uma resposta abrangente e atualizada ao fenômeno transnacional dos crimes digitais (MITANI, 2012).

As organizações internacionais emergem como atores fundamentais na promoção da cooperação contra os crimes digitais transnacionais. Instituições, como a Organização das Nações Unidas, através de suas diversas subentidades, exercem um papel essencial na definição de padrões internacionais e na facilitação da cooperação multilateral nestas questões (GOMES, 2016).

Por último, mas não menos importante, estão os acordos de troca de experiências e tecnologia. Estes são instrumentos valiosos para melhorar a eficácia dos esforços nacionais na luta contra o crime digital transnacional, permitindo que cada país beneficie dos avanços tecnológicos, abordagens e melhores práticas de outros. Tal sinergia evidencia o alto grau de interdependência entre os países na luta contra os crimes digitais e reforça a ideia de que a cooperação internacional é uma necessidade nesta área (RODRIGUES; AVELINE, 2022).

6.1. Interpol e outras organizações

A Interpol, ou Organização Internacional de Polícia Criminal, tem como principal objetivo a cooperação entre polícias de diversos países para combater e prevenir o crime a nível internacional. No âmbito dos crimes digitais transnacionais, a Interpol exerce um papel essencial como interface de cooperação, troca de informações e coordenação de operações internacionais. A Interpol possui uma unidade

especializada no combate ao cibercrime, que oferece apoio em casos de crimes informáticos transfronteiriços, produzindo avaliações de ameaças e coordenando operações em vários países simultaneamente (SCHRÖDER, 2022).

A burocracia é um elemento de destaque na atuação da Interpol, que precisa intermediar as diferenças legislativas, processuais e culturais dos países membros. A organização opera dentro de parâmetros estritos para garantir a equidade e o respeito à soberania dos países envolvidos, por isso, algumas operações podem ser lentas e complexas, fator que favorece a continuidade dos crimes transnacionais e a dificuldade de sua competência (SILVA; RAMOS, 2023).

O Grupo de Ação Financeira Internacional (GAFI) é outra organização que atua no panorama dos crimes digitais transnacionais, em particular aqueles relacionados à lavagem de dinheiro e financiamento do terrorismo. O GAFI estabeleceu uma série de recomendações que se tornaram o padrão internacional para combater a lavagem de dinheiro e o financiamento do terrorismo, incluindo crimes que envolvem componentes digitais, como a exploração de criptomoedas para fins ilícitos (MEDEIROS et al., 2024).

A Organização de Cooperação e Desenvolvimento Econômico (OCDE), tem foco nas questões que vão além da mera investigação e repressão de crimes, voltando-se para o estudo de como esses crimes afetam a economia global e como podem ser combatidos de maneira integrada e consistente em diferentes jurisdições. A OCDE também contribui para a formulação de políticas públicas e elaboração de estratégias para enfrentar os crimes digitais, incluindo a harmonização das legislações e cooperação em investigações transnacionais (RODRIGUES; AVELINE, 2022).

O papel dos tribunais internacionais também é relevante no combate aos crimes digitais transnacionais, sobretudo na determinação da competência em casos complexos. O Tribunal Penal Internacional, por exemplo, possui uma esfera mais restrita, focando em crimes de maior gravidade como genocídio, crimes contra a humanidade e crimes de guerra. Esse tribunal tem um papel simbólico importante, mostrando que o direito penal internacional tem capacidade para responsabilizar os perpetradores de crimes graves (SOUZA; DANTAS, 2023).

A Rede 24/7 de Pontos de Contato do Conselho da Europa, por exemplo, é uma das colaborações mais promissoras na luta contra os crimes digitais, uma vez que proporciona um canal de comunicação rápida entre as autoridades de diferentes jurisdições para solicitar e fornecer assistência legal mutua em matéria de cibercrime.

O objetivo é garantir que as autoridades competentes possam cooperar e entregar respostas eficientes em tempo real, mesmo quando o crime digital ocorra em múltiplos territórios (ROCHA; CHAVES, 2024).

Outra tentativa de abordar os problemas de competência relacionados aos crimes digitais é a Convenção de Budapeste sobre Cibercrime do Conselho da Europa. A Convenção procura harmonizar as leis nacionais, melhorar as capacidades de investigação e promover uma cooperação internacional efetiva. Fica patente a diversidade dos trabalhos de combate ao cibercrime e sua complexidade, sendo essa uma prova da dificuldade de se determinar a competência dessas atividades (Barbosa, 2009).

Todavia, a Enfopol, grupo de trabalho do Conselho da União Europeia para a cooperação policial, tem promovido debates e discussões sobre os desafios da implementação de medidas preventivas e medidas de combate ao cibercrime mais eficazes, tais como o desenvolvimento de um quadro comum de cooperação para ações contra o cibercrime no território europeu. Essencialmente, a Enfopol tem o objetivo de promover um diálogo frutífero entre as forças policiais dos Estados membros da União Europeia, além de orientar a investigação e o procedimento legal no âmbito do cibercrime (PAGLIOSA; RIBEIRO, 2022).

O icônico FBI (Federal Bureau of Investigation) também possui sua parcela no enfrentamento ao cibercrime, através do seu Centro de Combate ao Crime Cibernético. A agência se coordena com várias instituições a nível nacional e internacional, trabalhando com elas para notificar, investigar e deter as operações de cibercriminosos. Estas organizações traçam de maneira permanente um cenário em constante modificação no qual a necessidade de regular e impor a procedência de crimes virtuais se mostra cada vez mais emergente (MEDEIROS et al., 2024).

Ressalta-se, ainda, a Europol, entidade significativa para o combate ao cibercrime na Europa. Com sua unidade de cibercrime, a EC3, busca coordenar e reforçar as respostas da União Europeia a este tipo de delito. Sua atuação vai desde a preparação de avaliações de ameaças até o apoio direto a investigações em campo em casos de alto perfil (SPERVER; ZILIOTI, 2021).

6.2. Parcerias público-privadas

Em vista da necessidade de enfrentar os desafios dos crimes digitais transnacionais, a criação de parcerias público-privadas (PPPs) tem se mostrado um recurso pertinente. Tais parcerias, compondo uma estratégia coletiva de atuação, podem se manifestar de diferentes formas, desde a colaboração em projetos de pesquisa e inovação até a troca de informações e recursos entre diversas agências e organizações. Dessa forma, estabelece-se uma frente unificada contra a crescente sofisticação dos cibercriminosos (Primo, 1969).

O estabelecimento de PPPs fomenta a cooperação transnacional para a investigação de crimes digitais. A interconexão das redes informáticas aboliu barreiras físicas, viabilizando ações premeditadas para violar a segurança de sistemas e bases de dados de países distantes. Tais ataques, perpetrados por indivíduos ou organizações de várias origens, exonera-os, na maioria das vezes, da ação jurisdicional direta das entidades lesadas. Logo, a cooperação internacional através de parcerias público-privadas emerge como uma abordagem eficaz para ultrapassar a dificuldade de se determinar a competência em crimes digitais transnacionais (GOMES, 2016).

É importante inserir o privado na esfera de enfrentamento aos crimes digitais transnacionais, em virtude do alcance e da dimensão técnica que as empresas de tecnologia proporcionam. Elas detêm a infraestrutura das redes de comunicação e informação que sustentam a economia digital e o cotidiano das sociedades contemporâneas, além de possuírem conhecimentos especializados que podem ser essenciais para a prevenção, identificação e resolução dos crimes digitais. Porém, essa inclusão deve ser cautelosamente regulamentada para evitar conflitos de interesse e abusos de poder (Pouzada et al., 2020).

Ademais, as PPPs atuam como um aparato eficaz para a prevenção de crimes digitais transnacionais. Aspectos preventivos poderiam ser contemplados numa combinação de esforços para promover a educação digital, a consciência sobre a segurança cibernética e a criação de sistemas de segurança mais robustos e resistentes. Tal colaboração promoveria um ambiente digital mais seguro, dificultando ações cibercriminosas (Barbosa, 2009).

Mencionando especificamente a identificação desses crimes, as PPPs são cruciais para rastrear os autores. Atualmente, empresas privadas do setor de

tecnologia detêm amplo acesso a dados e informações que podem auxiliar na identificação e localização precisa desses criminosos. É através de uma cooperação contínua que essas informações podem ser compartilhadas agilmente com as autoridades competentes (MITANI, 2012).

No que tange a resolução desses crimes, as parcerias público-privadas podem facilitar a aplicação da legislação penal e subsidiar a criação de normativas transnacionais acerca da matéria. Movimento este que demanda um acordo institucional substancial e contínuo entre os Estados e a esfera privada, comprovando mais uma vez a necessidade de parcerias sólidas e duradouras (FARIAS, 2021).

Ademais, é preciso lembrar que a configuração das modernas infraestruturas de tecnologia e a natureza intangível do espaço cibernético inevitavelmente lançam desafios jurídicos, éticos e técnicos sem precedentes. Estes desafios podem ser melhor encarados através do engajamento participativo em parcerias público-privadas, que técnicos, juristas, estados e corporações conciliem as complexidades inerentes ao enfrentamento dos crimes digitais transnacionais (GIAMUNDO NETO, 2020).

A definição da competência jurisdicional, em casos de crimes digitais transnacionais, é uma questão complexa em virtude do princípio de soberania dos Estados e da localização física frequentemente incerta dos perpetradores desses crimes. O envolvimento de empresas privadas de tecnologia que operam além das fronteiras nacionais através de redes interconectadas poderia, através das PPPs, facilitar a cooperação transnacional necessária para a adjudicação eficaz desses crimes (MUNGUAMBE; PINTO; FREIRE, 2017).

Isso tudo sem mencionar os benefícios potenciais que as PPPs trazem no âmbito do fortalecimento institucional e da capacitação. Os órgãos públicos podem se beneficiar da experiência e do conhecimento técnico dos atores privados, enquanto as empresas privadas podem se beneficiar de um ambiente digital mais seguro e regulado. Um diálogo constante e a troca de informações entre estas entidades podem resultar em uma eficiência operacional superior e em uma maior resilência frente aos crimes digitais transnacionais (DOYLE; OLINTO, 2021).

Porém, mesmo com todos esses benefícios e potenciais, a operacionalização das PPPs no combate a esses crimes ainda enfrenta diversos desafios. Estes incluem a necessidade de um alinhamento de interesses entre órgãos públicos e empresas privadas, a proteção dos direitos humanos e da privacidade dos indivíduos, e questões

de responsabilidade legal. Nota-se que, em meio a esse cenário complexo, há uma demanda por uma compreensão mais profunda e um quadro regulatório robusto que ampare estas parcerias (Primo, 1969).

6.3. Casos de sucesso na cooperação internacional

A cooperação internacional efetiva entre nações tem sido um elemento determinante para o sucesso da resolução de crimes digitais transnacionais. Um exemplo proeminente deste tipo de colaboração bem-sucedida foi evidente no caso da rede de distribuição on-line de pornografia infantil "Playpen", que operava na darknet. Este incidente foi marcado por uma parceria multifacetada entre a lei americana e as autoridades europeias, resultando em mais de 870 prisões em todo o mundo e a identificação e proteção de centenas de crianças (ROCHA; CHAVES, 2024).

A Operação Astra, um esforço conjunto entre a Agência Europeia de Cooperação Judiciária (Eurojust) e a Agência Europeia de Polícia (Europol), bem como várias autoridades nacionais de aplicação da lei, fornece outro exemplo de uma resposta internacional bem-sucedida. Nesta operação, um grupo de criminosos cibernéticos baseado na Ucrânia foi desmantelado, que havia realizado uma série de ataques cibernéticos sofisticados contra instituições financeiras e individuais, causando danos estimados em várias dezenas de milhões de euros (FARIAS, 2021).

O caso do botnet "Avalanche", uma infraestrutura utilizada para a distribuição de mais de vinte campanhas de malware e operações de phishing em todo o mundo, é mais um marco na história do combate ao cibercrime. A operação para desmantelar o Avalanche envolveu a cooperação entre autoridades de vários países e resultou na apreensão de 39 servidores e na detenção de cinco indivíduos. Mais importantemente, a operação levou ao bloqueio de mais de 800.000 domínios da web utilizados pelo botnet (PAGLIOSA; RIBEIRO, 2022).

No campo da cooperação jurídica, o takedown do Notorious Silk Road, um dos mercados mais dominantes na Darknet para o comércio ilegal, destaca-se como um caso de estudo. A operação, conduzida pelo FBI em parceria com várias outras agências internacionais, resultou na prisão do fundador e na apreensão de Bitcoins no valor de milhões de dólares. Este caso demonstrou a eficácia da cooperação entre

diversas jurisdições na identificação e no julgamento de crimes digitais transnacionais (ROCHA; CHAVES, 2024).

Devido a essas intervenções bem-sucedidas, as nações estão reconhecendo a necessidade da cooperação internacional na luta contra o cibercrime. Por exemplo, a recente formação da rede judiciária mundial para a cibercriminalidade pela Eurojust é um avanço significativo neste sentido. Esta rede visa facilitar a resolução rápida de questões jurídicas transfronteiriças e a melhorar a coordenação entre os Estados-Membros na luta contra o cibercrime (Primo, 1969).

O caso do ransomware "WannaCry" foi um dos mais concretos exemplos de sucesso da colaboração internacional em crimes digitais. A reação global rápida e unida contra o ataque do WannaCry demonstrou a força da colaboração internacional para responder a incidentes cibernéticos em grande escala. Os esforços de mitigação do ataque, que afetou mais de 300.000 computadores em 150 países, envolveram uma colaboração sem precedentes entre empresas do setor privado e agências de aplicação da lei em todo o mundo (SPERVER; ZILIOTI, 2021).

O aprimoramento da colaboração internacional no combate à cibercriminalidade pode ser vista na estrutura e na operação da Agência Europeia de Segurança da Informação e das Redes (ENISA). A ENISA tem desempenhado um papel vital na melhoria das capacidades de prevenção de cibercrimes dos Estados-Membros da UE, bem como na coordenação de respostas a incidentes de cibersegurança em uma base transnacional (GIAMUNDO NETO, 2020).

Também é notável o caso do vírus "Conficker", que gerou uma resposta internacional massiva logo após o seu surgimento em 2008. A resposta, que incluiu a cooperação entre muitos países e entidades privadas, resultou na criação do Conficker Working Group, uma entidade dedicada a erradicar o vírus. Este grupo colaborativo foi bem-sucedido na imposição de medidas de controle sobre o vírus, bem como na identificação e desativação de muitos dos sistemas que ele havia infectado (SILVA; RAMOS, 2023).

Contudo, não se deve esquecer o papel dos arranjos multilaterais na promoção da cooperação internacional contra o cibercrime. A Convenção do Conselho da Europa sobre o Cibercrime, também conhecida como Convenção de Budapeste, fornece um exemplo disto. Trata-se do primeiro tratado internacional sobre crimes cometidos através da Internet e de outras redes de computadores, oferecendo uma

abordagem amplamente adotada para crimes transnacionais na esfera digital (GIAMUNDO NETO, 2020).

A Agência Brasileira de Cooperação Internacional em Defesa Cibernética (AbraCID), por sua vez, tem colaborado ativamente com as autoridades internacionais. A ABRAcid tem demonstrado notável empenho na prevenção e na resposta a cibercrimes, mantendo forte colaboração com agências associadas em outros países. Através de sua dedicação à cooperação internacional, esta organização tem desempenhado um papel essencial na luta contra a cibercriminalidade no Brasil e além (RODRIGUES; AVELINE, 2022).

7. Propostas de Melhoria

Uma proposta de melhoria essencial para lidar com os crimes digitais transnacionais e a dificuldade de determinar a competência é a instituição de regulamentos internacionais mais rígidos e atualizados que correspondam à evolução global dos crimes cibernéticos. As legislações nacionais, por si só, dificilmente conseguem englobar todas as nuances e complexidades desses crimes, em virtude da própria natureza destes que não respeitam fronteiras geográficas. Exige-se um esforço conjunto por parte da comunidade internacional para estabelecer regras claras sobre a competência desses delitos (SCHRÖDER, 2022).

Outra medida que se mostra imperativa é o fortalecimento da cooperação e harmonização internacional no âmbito da justiça criminal. Trata-se de um recurso necessário, visto que muitos crimes digitais transnacionais envolvem atividades distribuídas por vários países. Neste contexto, os acordos de colaboração e assistência jurídica mútua podem ser considerados ferramentas de valor inestimável para a realização de investigações eficazes e para a imposição de sanções. Tais medidas garantiriam a extradição dos criminosos ou a possibilidade de os julgar nos países onde os efeitos dos crimes foram sentidos (FARIAS, 2021).

A inclusão de protocolos de compartilhamento de informações entre agências nacionais e internacionais é outra proposta viável. Isso permitiria que os órgãos envolvidos na prevenção e repressão de crimes digitais transnacionais compartilhassem informações e dados pertinentes de maneira segura e eficiente. Tal medida seria importante para identificar tendências emergentes em crimes cibernéticos e desenvolver estratégias de combate mais eficazes (Primo, 1969).

A necessidade de uma capacitação mais abrangente no campo da justiça é urgentemente necessária. Dito isso, não só os profissionais do penitenciário precisam ser treinados, mas também os oficiais de justiça que têm a responsabilidade de determinar a competência dos crimes. A formação deve se concentrar na compreensão das nuances da tecnologia, os aspectos jurídicos dos crimes digitais, condições sociais e legais na era digital e as habilidades necessárias para lidar com as dificuldades inerentes a crimes digitais transnacionais (Barbosa, 2009).

O fortalecimento das leis existentes é também uma proposta importante a ser considerada. O objetivo disto é proporcionar um ambiente jurídico mais eficaz que esteja equipado para lidar com os desafios únicos apresentados pelos crimes cibernéticos. Tal melhoria nas leis existentes implicaria um combate mais eficaz contra os crimes digitais transnacionais, garantindo que as vítimas tenham acesso à justiça de maneira oportuna e eficiente (Pouzada et al., 2020).

Outra proposta importante seria a conscientização e educação dos usuários digitais em relação à segurança online e aos perigos dos crimes cibernéticos. Isto pode ser feito através de campanhas de conscientização e programas educacionais voltados para a segurança cibernética, ajudando assim a prevenir que mais pessoas se tornem vítimas desses crimes (GOMES, 2016).

A implementação de avançadas técnicas de investigação, além de novas tecnologias e metodologias para lidar com as complexidades do cibercrime também se apresenta como necessária. Isso incluiria a adoção de ferramentas tecnológicas avançadas, como a inteligência artificial e aprendizado de máquina, para melhorar a capacidade de detectar e combater crimes cibernéticos (SCHRÖDER, 2022).

Segundo Silva e Ramos (2023, p. 45):

> Promover a criação de forças-tarefas de crimes cibernéticos em âmbito internacional poderia ser uma estratégia benéfica. Estes grupos multidisciplinares e multinacionais ajudariam a facilitar a colaboração global e a coordenação entre órgãos policiais, agências reguladoras, instituições financeiras e provedores de serviços de Internet na luta contra o cibercrime.

Provavelmente, também seria útil melhorar a infraestrutura de segurança cibernética em si. A segurança da informação tem sido uma questão de importância crescente e infraestruturas resilientes e robustas podem prevenir muitos crimes cibernéticos antes que ocorram. A implementação de melhores práticas de segurança

cibernética em organizações e a manutenção de sistemas à prova de invasões contribuiriam significativamente para a prevenção do cibercrime (FRANK; BACKES, 2015).

É necessária ainda uma abordagem sistêmica para combater os crimes digitais transnacionais, onde se considera não apenas os aspectos legais e tecnológicos, mas também os sociais e comportamentais. Esta abordagem integrada permite uma visão mais completa e eficaz da situação do cibercrime, e assim as chances de mitigação dos crimes e proteção das vítimas seriam amplamente melhoradas (DOYLE; OLINTO, 2021).

3 CONCLUSÃO

Para concluir, os delitos digitais transnacionais se configuram como uma modalidade de atividade criminosa intricada e desafiadora que ultrapassa fronteiras entre países, impactando indivíduos em diversas localidades ao redor do globo. A cooperação internacional e a adesão a tratados globais desempenham um papel fundamental na luta contra essa realidade em constante mutação. Ademais, o avanço tecnológico tem um impacto inevitável no campo do Direito Penal, gerando a necessidade de proteger um novo conjunto de interesses jurídicos específicos no âmbito da informática. O cibercrime, como um fenômeno legal de grandes proporções, transcende fronteiras e requer abordagens inovadoras para ser combatido efetivamente.

4 REFERÊNCIAS

A. G. *Competência nos Crimes*. JusBrasil, 05 mar. 2024. Disponível em: https://www.jusbrasil.com.br.

ÁLVAREZ-CIENFUEGOS SOTO, José Maria. *Informática i dret penal: els delictes relatius a la informática*. Stvdia Juridica, Barcelona, v. 13, p. 191-209, 1997.

BARBOSA, Fabio Marques. *Crimes de pesca no pantanal: de quem é a competência para legislar?* Revista do Direito, Santa Cruz do Sul: APESC - Associação Pró-Ensino em Santa Cruz do Sul, 2009. Disponível em: https://doi.org/10.17058/rdunisc.v0i0.1157.

BUENO ARÚS, F. *Els delictes relatius a la informática*. Barcelona, Stvdia Juridica, v. 13, p. 173-190, 1997.

DOYLE, Andréa; OLINTO, Gilda. *Práticas de ensino críticas de competência em informação, mídias e tecnologias digitais e a desconstrução de estereótipos de gênero*. Informação & Informação, Londrina, v. 26, n. 4, p. 575, 2021. DOI: 10.5433/1981-8920.2021v26n4p575

Encontro de iniciação científica.

FARIAS, Pedro Victor Viana Coutinho de Oliveira. *Host - e a dificuldade de se fazer cinema*. Revista Crises, Universidade Federal de Pernambuco, 2021. Disponível em: https://doi.org/10.51359/2763-7425.2021.250252.

FRANK, C. O.; BACKES, L. *O desenvolvimento da autonomia através de tecnologias digitais virtuais*. Revista Competência, v. 8, p. 2, 2015. Disponível em: https://doi.org/10.24936/2177-4986.v8n2.2015.291.

FREITAS, Francisco Igor Cavalcante. *A justiça eleitoral e os conflitos na fixação de competência nas hipóteses de conexão e contingência com os crimes eleitorais*. Suffragium - Revista do Tribunal Regional Eleitoral do Ceará, v. 9, n. 15/16, 2018. DOI: 10.53616/suffragium.v9i15/16.31.

GABRIEL, Marcos Archanjo; ORRIGO, M. H. *Crimes cibernéticos: uma abordagem jurídica sobre os crimes realizados no âmbito virtual*. 2015.

GIAMUNDO NETO, Giuseppe. *O tribunal de contas e a ausência de competência para determinar retenção de pagamentos em contratos administrativos*. Revista de Direito Administrativo e Infraestrutura - RDAI, 2020. DOI: 10.48143/rdai.14.ggn.

GOMES, Caio de Souza. *Pobre del cantor que no se imponga con su canción: conexões transnacionais no álbum trópicos, de Daniel Viglietti (1973)*. Outros Tempos: Pesquisa em Foco - História, Universidade Estadual do Maranhão, 2016. DOI: 10.18817/ot.v13i21.525.

MEDEIROS, Rosecleide de; PEIXOTO, Jefferson Freire; TEIXEIRA, Wagner Barros; MEDEIROS-COSTA, Mateus Estevam. *Competência docente frente às tecnologias digitais de informação e comunicação*. Cuadernos de Educación y Desarrollo, South Florida Publishing LLC, 2024. Disponível em: http://dx.doi.org/10.55905/cuadv16n10-025.

MITANI, Amanda Wendt. *A imprecisão da linguagem da lei e a dificuldade de comunicação entre delegados e peritos nos crimes de pornografia infantil pela internet*. Revista Brasileira de Segurança Pública, [S.l.], v. 6, n. 1, 2012. DOI: 10.31060/rbsp.2012.v6.n1.113.

MORAIS, K. *A criminalidade na era digital e os desafios para o direito penal*. 2023.

MUNGUAMBE, Rosa Manuela Teixeira Pinto; FREIRE, Gustavo Henrique Araújo. *A competência informacional dos técnicos da biblioteca central da universidade Eduardo Mondlane em Moçambique no uso das tecnologias digitais de informação e comunicação*. Pesquisa Brasileira em Ciência da Informação e Biblioteconomia, Portal de Periódicos UFPB, 2017. DOI: 10.22478/ufpb.1981-0695.2017v12n2.36645.

NETTO, A. E. *Limites da competência da Justiça Federal para julgamento de delitos praticados pela internet – crime à distância*. Jus.com.br, 01 abr. 2020. Disponível em: https://www.jus.com.br.

PAGLIOSA, B. M.; RIBEIRO, K. P. *A responsabilidade dos peacekeepers ao incorrer em crimes de competência do tribunal penal internacional*. Revista Ibero-Americana de Humanidades, Ciências e Educação, 2022. Disponível em: https://doi.org/10.51891/rease.v8i5.5589.

POUZADA, Thiago Avila; NOVELLO, Tanise Paula; AYRES, Luana Maria Santos da Silva; PEREIRA, Fabrine Diniz. *Potencialidades, desafios e dificuldade de ensinar geometria através das tecnologias digitais*. Revista Sergipana de Matemática e Educação Matemática - ReviSeM, 2020. Disponível em: https://doi.org/10.34179/revisem.v5i2.12221.

PRIMO, Carlos Frederico Carneiro. *Questões jurídicas do emprego das forças armadas no controle dos crimes transnacionais e ambientais*. Revista da Escola Superior de Guerra, 1969. Disponível em: http://dx.doi.org/10.47240/revistadaesg.v24i49.291.

ROCHA, Beatriz Vitória Silva; CHAVES, Solange Barreto. *As novas relações de trabalho: a uberização e a competência da justiça do trabalho dos assalariados digitais*. Revista Foco, South Florida Publishing LLC, 2024. DOI: 10.54751/revistafoco.v17n5-099.

RODRIGUES, Júlia de Almeida; AVELINE, Ricardo Strauch. *O tribunal penal internacional e os crimes previstos no estatuto de Roma de 1998: os casos Bolsonaro e Putin e a (in) competência do TPI para julgá-los*. Justiça & Sociedade, Instituto Porto Alegre da Igreja Metodista, 2022. Disponível em: http://dx.doi.org/10.15602/2525-3883/rjs.v7n2p161-221.

ROMEO CASABONA, Carlos Maria. *De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal*. In: _____ (Coord.). El cibercrimen:

nuevos retos jurídico-penales, nuevas respuestas político-criminales. Granada: Comares, 2006. p. 1.

ROMEO CASABONA, Carlos Maria. *La protección penal del software en el derecho español*. Actualidad Penal, n. 35, p. 1829, sept./oct. 1988.

ROVIRA DEL CANTO, Enrique. *op. cit.*, p. 72.

SCHRÖDER, Peter. *(Re)aproximando-se e afastando-se da Alemanha: Curt Nimuendajú como parte de redes transnacionais de antropólogos*. Horizontes Antropológicos, FapUNIFESP (SciELO), 2022. DOI: 10.1590/s0104-71832022000100007.

SILVA, Vanderlan Francisco da; RAMOS, Helmano. *Fontes digitais: a digitalização de processos-crimes e as mortes no presídio do Serrotão (1991-2008)*. Convergências: estudos em Humanidades Digitais, Instituto Federal de Ciência e Tecnologia de Goiás, 2023. DOI: 10.59616/cehd.v1i03.307.

SILVEIRA, Renato de Mello Jorge. *op. cit.*, p. 17.

SOUZA, Gabriela Soares de; DANTAS, Flávia Gonçalves Barros. *Crimes conexos e a competência do juiz singular no crime de latrocínio*. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 8, 2023. Disponível em: http://dx.doi.org/10.51891/rease.v9i8.10908.

SOUZA, Wadim Passos Ferreira de; WESLEY. *A convenção de Budapeste e seus reflexos sobre a competência para o processo e julgamento dos crimes cibernéticos no Brasil*. Revista Judicial Brasileira, Escola Nacional de Formação e Aperfeiçoamento de Magistrados, 2023. DOI: 10.54795/rejubesp.dirdig.219.

SPERBER, Suzi Frankl; ZILIOTI, Ariana. *O caos sacro, uma análise do sagrado em "O homossexual ou a dificuldade de se expressar" de Copi*. Terceira Margem, Universidade Federal do Rio de Janeiro, 2021. Disponível em: http://dx.doi.org/10.55702/3m.v25i46.41968.

UNODC. *UNODC*. Fonte: United Nations Office on Drugs and Crime. Disponível em: https://www.unodc.org/lpo-brazil/pt/covid19/cibercriminalidade-e-desinformacao.html.