

COOPERAÇÃO INTERNACIONAL CONTRA O CIBERCRIME

INTERNATIONAL COOPERATION AGAINST CYBERCRIME

Xenofontes Curvelo Piló¹

Filipe Augusto Silva²

Deilton Ribeiro Brasil³

RESUMO- O presente trabalho visa demonstrar como a cooperação internacional combate o cibercrime. Diante dos fenômenos da Internet e da globalização, busca demonstrar a escalada da criminalidade através da rede e evidenciar que o cometimento de ilícitos, sem a necessidade da presença física do agente, dificulta, ou mesmo, afasta a possibilidade de uma persecução penal. Diante da mitigação de conceitos tradicionais, como jurisdição e soberania, procura demonstrar a necessidade de incremento da cooperação jurídica entre os Estados para prevenir e reprimir o cibercrime. A pesquisa foi realizada com respaldo em estudos e conferências internacionais que envolvem seu reconhecimento dentro de uma lógica, considerando parâmetros convencionais, constitucionais e infraconstitucionais. Realizou-se uma pesquisa bibliográfica e método crítico-discursivo, partindo da análise documental de tratados internacionais, além do procedimento de revisão bibliográfica.

Palavras-chave: Cibercrime; Cooperação Jurídica Internacional; Políticas internacionais

ABSTRACT- This work aims to demonstrate how international cooperation combats cybercrime. In view of the phenomena of the Internet and globalization, it seeks to demonstrate the escalation of crime through the network and to highlight that the commission of illicit acts, without the need for the physical presence of the agent, makes it difficult, or even eliminates the possibility of criminal prosecution. Given the mitigation of traditional concepts, such as jurisdiction and sovereignty, it seeks to demonstrate the need to increase legal cooperation between States to prevent and repress cybercrime. The research was carried out with support from international studies and conferences that involve its recognition within a logic, considering conventional, constitutional and infra-constitutional parameters. A bibliographical research and critical-discursive method were carried out, starting from the documentary analysis of international treaties, in addition to the bibliographical review procedure.

Keywords: Cybercrime; International Legal Cooperation; International policies

¹ Doutorando e Mestre em Proteção dos Direitos Fundamentais pela Universidade de Itaúna/MG. Bacharel em Direito, Especialização em Direito Público lato sensu pelo CEAJUFE, Especialização em Direito Público lato sensu pela Universidade de Itaúna/MG. Especialização em Ciências Penais lato sensu pelo Centro Universitário Newton Paiva, membro da ABJD - Associação Brasileira de Juristas pela Democracia. Advogado. xenopilo@yahoo.com.br. Currículo Lattes: <http://lattes.cnpq.br/8570712885711499>.

² Bacharel em Direito pela Universidade de Itaúna. Pós-graduado em Direito Penal e Processo Penal pelo Centro Universitário Newton Paiva. Mestre em Direito pelo Programa de pós-graduação Stricto Sensu da Universidade de Itaúna. Doutorando em Direito pelo Programa de pós-graduação Stricto Sensu da Universidade de Itaúna. Advogado. Juiz Leigo da Comarca de Santa Luzia/MG. E-mail: filipefhp@hotmail.com.

Introdução

Atualmente no mundo em que vivemos há um momento de alta influência da informática na vida humana moderna. A maioria das atividades laborais e comunicacionais são realizadas, de alguma forma, com auxílio ou dependência da internet e sistemas informáticos em geral.

As relações humanas e os serviços, em sua grande maioria e intensidade, foram afetados pela introdução da internet e modificações consideráveis foram observadas na forma como esses serviços são prestados e as relações sociais estabelecidas. Os serviços públicos fundamentais para o cidadão são geridos por meio da internet. Os transportes, o comércio, as atividades financeiras, negociais e bancárias são continuamente modificados e aprimorados por meio da rede mundial de computadores.

O cibercrime não se trata de um fato negável nos nossos dias, dada a expansão da internet em tudo que fazemos. Assistimos à ampliação dos canais de fornecimento dos bens pela internet, adotando as empresas este meio por excelência para conseguirem dar respostas às necessidades do consumidor. Cibercrime constitui o ato tipificado por lei como crime e que seja cometido com a ajuda de um computador ou outro sistema informático adotando uma nova vida no ciberespaço.(GUEDES, 2021).

A autora continua afirmando que, atualmente é comum a pratica de crimes no ambiente de nuvem, sendo que, inclusive nesses casos, estamos diante de crimes cibernéticos considerando que são utilizados dispositivos informáticos para acessar esse ambiente. Crimes virtuais, crimes cibernéticos, cibercrimes, delito informático, delito 2.0, delito virtual, infocrimes, computer crimes, são varias nomenclaturas utilizadas pela doutrina para se referir a atos ilícitos cometidos por meio de artefatos tecnológicos.

Com toda essa inserção social no meio digital, os crimes do mundo real não estariam distantes do mundo paralelo virtual, o cometimento de crimes por meio da internet, que cada dia mais ameaça o cidadão por meio do chamado cibercrime. Seja por meio de roubo de informações, seja para vendas de produtos ilegais, ou publicações com informações falsas prejudiciais.

Com a finalidade específica de compreender melhor os desafios enfrentados pelo direito penal transnacional, considera-se a teoria das relações internacionais globais e as questões práticas inerentes à sua implementação de sua governança, e como essas tendências mais amplas são discernidas. Essas observações estão ligadas para ilustrar as formas pelas quais os entes internacionais modernos têm tido dificuldades em assumir as funções de prover segurança para o domínio transnacional.

2- A Eficácia das Políticas Internacionais no Combate ao Cibercrime

Os desenvolvimentos tecnológicos das últimas décadas proporcionaram uma verdadeira revolução nas formas de interação social, com recursos à tecnologia, usuários do mundo inteiro passaram a ter uma maior produção, com mais eficiência, uma comunicação mais rápida e econômica, vindo a interagir virtualmente independente de seus distanciamento.

O mundo assiste atualmente a um fenômeno que mudou as relações entre todas as nações e que tem sido nomeado de globalização econômica e informacional, que propõem mudanças no concerto das relações da economia e das políticas internas e externas. A internet tem sido um espaço virtual de convergência e concentração, sem precedentes, das mais variadas formas de informação, comunicação, comercialização de produtos, serviços e entretenimento.

Entretanto, estes desenvolvimentos tecnológicos, relacionados com aplicações de internet trouxeram novos problemas, quer para seus utilizadores, quer para as instituições policiais e judiciais. O cibercrime é uma das maiores ameaças enfrentadas pela sociedade moderna, impactando indivíduos, empresas e governos em todo o mundo. Com a crescente digitalização e dependência da tecnologia, o alcance e a sofisticação dos cibercriminosos aumentaram significativamente. (CALDAS, 2024)

Continua o autor, o cibercrime abrange uma ampla gama de atividades ilícitas realizadas através da internet ou de sistemas de computador, destacamos ntre os principais tipos de cibercrime, fraude e roubo de identidade, ataques de

Malware, Phishing e Engenharia Social, espionagem cibernética, ataques DDoS (Distributed Denial of Service). A extensão do cibercrime é alarmante, com um aumento constante no número de incidentes e nas perdas financeiras associadas. Relatórios indicam que o cibercrime pode causar trilhões de dólares em danos anuais globalmente, afetando milhões de pessoas e empresas.

Para Emerson Wendt, o cibercrime representa uma ameaça global que transcende fronteiras nacionais, exigindo uma resposta coordenada e colaborativa entre os países. A natureza transnacional do cibercrime torna a cooperação internacional não apenas importante, mas essencial para enfrentar eficazmente esse desafio. A primeira ação de abrangência internacional do combate aos comportamentos delitivos via internet deu-se entre os anos de 1983 e 1985, quando um comitê, patrocinado pela Organisation for Economic Co-operation and development (OECD), discutiu sobre uma harmonização internacional das leis penais, de modo a combater os crimes econômicos cometidos com o uso de computador. (WENDT, 2021)

Ainda afirma o autor, outras iniciativas, apesar de não tratarem precisamente de cibercrimes, foram importantes para criar uma cultura de cooperação entre países e organismos internacionais, iniciar a abertura de barreiras burocráticas, facilitar a comunicação entre autoridades, permitir troca de informações mais célere, entre outras. Para a criação de uma efetiva justiça criminal internacional, faz-se necessária a existência de quatro elementos, ou seja, um ordenamento jurídico- para definir os tipos penais-, força policial para investigar os delitos, um sistema judiciário para aplicação da lei e um sistema prisional para punir e recuperar os condenados.

Carlos Hélder Mendes professa que cibercriminosos operam sem restrições geográficas, utilizando a internet para conduzir atividades ilícitas a partir de qualquer local do mundo. Isso significa que um ataque cibernético pode ser planejado e executado em um país, visando vítimas em múltiplas jurisdições. Sem uma cooperação internacional eficaz, os esforços de um país para investigar e processar cibercriminosos podem ser facilmente frustrados pela falta de jurisdição ou recursos.

A cooperação internacional facilita o compartilhamento de informações e inteligência entre as agências de aplicação da lei, governos e organizações do setor privado. Este compartilhamento é vital para identificar e rastrear cibercriminosos, entender suas técnicas e mitigar ameaças em tempo real. Redes de colaboração, como a Interpol e a Europol, desempenham um papel fundamental ao fornecer plataformas para o intercâmbio rápido e eficiente de informações críticas.(MENDES, 2020)

Pedro Zaniolo professa que os diferentes países possuem legislações e regulamentos variados em relação ao cibercrime, o que pode criar lacunas e inconsistências que os cibercriminosos exploram. A cooperação internacional promove a harmonização das leis e normas, estabelecendo um quadro jurídico comum que facilita a investigação e a punição dos crimes cibernéticos. A Convenção de Budapeste sobre Cibercrime é um exemplo notável de um esforço global para alinhar as legislações nacionais com padrões internacionais. (ZANIOLO, 2022)

Além de combater diretamente o cibercrime, a cooperação internacional contribui para o fortalecimento geral da cibersegurança global. Iniciativas colaborativas de pesquisa e desenvolvimento ajudam a criar novas tecnologias e métodos de defesa contra ameaças cibernéticas. A partilha de conhecimentos e a inovação contínua são essenciais para manter a segurança cibernética à frente das capacidades dos cibercriminosos.

3- Desafios na Cooperação Jurídica Internacional para Combater o Cibercrime

O cibercrime não respeita fronteiras nacionais, permitindo que criminosos operem de qualquer lugar do mundo e atinjam vítimas em múltiplas jurisdições. Essa característica intrínseca do cibercrime cria desafios significativos para a aplicação da lei, que está frequentemente limitada pelas fronteiras nacionais. A cooperação jurídica internacional é essencial para fechar essas lacunas, mas enfrentar a complexidade das leis e sistemas jurídicos variados pode ser um grande desafio. Cada país possui seu próprio conjunto de leis e regulamentações que governam a cibersegurança e a cibercriminalidade. Essas

diferenças podem criar obstáculos significativos para a cooperação internacional. O que é considerado crime cibernético em um país pode não ser em outro, e as penalidades podem variar amplamente. Harmonizar essas leis e encontrar um terreno comum é uma tarefa desafiadora, mas necessária para uma colaboração eficaz. (CASELLI, 2022)

Continua o autor os procedimentos jurídicos e a burocracia também representam desafios importantes. O processo de obtenção de assistência jurídica de outro país pode ser demorado e complicado, muitas vezes envolvendo múltiplas etapas e aprovações. Além disso, os requisitos legais para a coleta e troca de evidências digitais podem variar, complicando ainda mais a cooperação. A confiança entre nações é um fator crucial para uma cooperação jurídica eficaz. Sem confiança mútua, os países podem relutar em compartilhar informações sensíveis ou em colaborar plenamente em investigações transnacionais. Construir e manter essa confiança exige esforços contínuos de diplomacia cibernética, bem como a participação em acordos e tratados internacionais.

O futuro da cooperação jurídica internacional para combater o cibercrime depende da capacidade dos países de adaptar suas políticas e práticas às mudanças rápidas no ambiente digital. Isso inclui a adoção de novas tecnologias, o fortalecimento de acordos internacionais e a melhoria contínua da capacitação dos profissionais envolvidos. A inovação e a flexibilidade serão essenciais para enfrentar os desafios emergentes e garantir uma resposta coordenada e eficaz às ameaças cibernéticas.

4- CONSIDERAÇÕES FINAIS

A globalização não significa, em absoluto, o bem-estar globalizado. Os sistemas de informação globalizados acomodam um número crescente de ofensas transnacionais. A crescente ameaça do cibercrime exige uma resposta coordenada e robusta que transcenda fronteiras nacionais. A cooperação internacional emergiu como um componente crucial na luta contra o cibercrime, destacando a necessidade de esforços conjuntos e harmonizados entre nações, organizações internacionais, e o setor privado. A natureza global do cibercrime, onde criminosos podem operar a partir de qualquer lugar e atacar vítimas em múltiplas jurisdições, sublinha a importância vital da cooperação internacional.

Nenhum país, por mais avançado que seja em termos de tecnologia e legislação, pode combater eficazmente o cibercrime de forma isolada. A colaboração entre nações permite o compartilhamento de informações, recursos e expertise, criando uma frente unida contra ameaças cibernéticas.

A cooperação internacional contra o cibercrime é um esforço contínuo e dinâmico que requer a colaboração de múltiplos atores em diversas frentes. Embora existam desafios significativos, as oportunidades para fortalecer a cibersegurança global são imensas. Ao trabalhar juntos, compartilhando informações, recursos e melhores práticas, as nações podem criar um ambiente cibernético mais seguro e resiliente, protegendo indivíduos, empresas e infraestruturas críticas contra as ameaças cibernéticas.

Referencias

CALDAS, Felipe de Ornelas. Crimes Cibernéticos, e a insuficiente legislação brasileira. Lumen Juris. Rio de Janeiro. 2024

CASELLI, Guilherme. Manual de Investigação Digital. Editora Juspodium. São Paulo 2022.

GUEDES, Inês Sousa. Gomes, Marcus Alan de Melo. Cibercriminalidade- Novos desafios, ofensas e soluções. Ed. Pactor- Lisboa/Portugal. 2021

MENDES, Carlos Hélder C. Furtado. Tecnoinvestigação Criminal- Entre a proteção de dados e a infiltração por software. Editora Juspodium. São Paulo 2020.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos- Ameaças e procedimentos de investigação. Rio de Janeiro. Brasport. 2021

ZANIOLO, Pedro Augusto. Crimes Modernos. O impacto da tecnologia no direito. Editora Juspodium. São Paulo 2022.