DOSSIÊ

REVISTA DIREITO & DIALOGICIDADE

V. 9, N. 1 (2024) ISSN: 2178-826X

CRIMES CIBERNÉTICOS EM ASCENSÃO: UMA ANÁLISE SOBRE OS DESAFIOS PARA A PUNIÇÃO À LUZ DO CÓDIGO PENAL

CYBER CRIMES ON THE RISE: AN ANALYSIS OF THE CHALLENGES FOR PUNISHMENT IN LIGHT OF THE PENAL CODE

LICIA NEVES E SOUSA[1]
LUCAS NEVES E SOUSA[2]
JOSÉ LAURO POMPEU ALMEIDA[3]
BISMARCK OLIVEIRA BORGES[4]

RESUMO

O presente estudo pretende analisar quais desafios existem para aplicar sanções aos crimes cibernéticos à luz do código penal e outras legislações, tendo em vista o crescimento desenfreado dos crimes dessa natureza. Objetiva-se identificar os principais desafios encontrados no tocante ao combate dos delitos praticados no ambiente das redes e questionar se as medidas adotadas pelo ordenamento são suficientes para solucionar o problema. Para auxiliar nesse estudo foram adotadas bibliografias de autores renomados, bem como se analisou fontes e dispositivos normativos para embasar o desenvolvimento do texto. Em relação ao resultado e discussões, obteve-se que os desafios são vários, sobretudo por causa de uma legislação pouco específica e precisam serem sanados para reduzir a frequência que esses crimes são cometidos. Conclui-se que o ordenamento jurídico brasileiro precisa produzir normas específicas, preparar agentes e utilizar tecnologias com vistas aplicar de forma correta e proporcional as sanções aos crimes cibernéticos.

PALAVRAS-CHAVE: Crimes cibernéticos. Desafios. Código penal.

ABSTRACT

The present study intends to analyze what challenges exist in applying sanctions to cybercrimes in light of the criminal code and other legislation for cybercrimes, in view of the developed growth of crimes of this nature. The objective is to identify the main challenges encountered in combating crimes committed in the network environment and to question whether the measures adopted by the legal system are sufficient to solve the problem. To assist in this study, bibliographies of renowned authors were used, as well as sources and normative devices were analyzed to support the development of the text. Regarding the result and the investigation, we found that there are several challenges, mainly due to less specific legislation and need to be resolved to reduce the frequency with which these crimes are committed. It is concluded that the Brazilian legal system needs to produce specific standards, prepare agents and use technologies with a view to correctly and proportionately applying cybercrime assessments.

KEYWORDS: Cybercrimes. Challenges. Penal Code.

1 Graduando em Direito pela Universidade Regional do Cariri (URCA). E-mail: licia.neves@urca.br
2 Graduando em Direito pela Universidade Regional do Cariri (URCA). E-mail: lucas.neves@urca.br
3 Graduando em Direito pela Universidade Regional do Cariri (URCA). E-mail: lauro.almeida@urca.br
4 Orientador. Professor especialista da Universidade Regional do Cariri. E-mail: bismarck.borges@urca.br

1. INTRODUÇÃO

Hodiernamente, a tecnologia possibilita sua utilização para diversas finalidades e permite a interação com outros usuários em virtude da conectividade global por meio de computadores e outros dispositivos com acesso à rede. À medida que a tecnologia é desenvolvida, os crimes cibernéticos adquirem mecanismos informáticos capazes de obterem vantagens indevidas, sobretudo pela rede facilitar o surgimento de atos delituosos. Assim, essas condutas criminosas praticadas no âmbito da rede devem ser combatidas em razão dos danos gerados aos afetados.

O presente trabalho objetiva analisar quais dificuldades existem para os crimes virtuais sejam punidos com base no código penal e em outras legislações, tendo em vista que tais atos ilícitos são praticados em um ritmo cada vez maior ao utilizar o desenvolvimento da tecnologia para finalidades indevidas, sendo necessário adotar medidas de enfrentamento pelo fato das consequências decorrentes de tais atos serem graves às vítimas.

Explica Damásio e Milagre (2016, p. 48) que os crimes cibernéticos resultam das transformações tecnológicas e, por afetarem direitos como a privacidade e causarem diversos danos, aplicam-se os comandos do Código Penal e outras legislações para coibir a ocorrência de tais casos. Esses autores conceituam-no como crime ou contravenção penal cometido por via eletrônica com base na utilização de computadores e dispositivos com acesso à rede.

Vale destacar que não há uma legislação específica no ordenamento jurídico brasileiro sobre os crimes cibernéticos, sendo previsto nos artigos no Código Penal, A Lei de Combate a Crimes Cibernéticos (nº 12.737/2012) e Marco Civil da Internet (Lei 12.965/2014), porém longe de abranger todas as situações que advindas de tal delito em comento.

Nesse sentido, não é fácil assegurar a aplicação integral dessas legislações anteriores. Os desafios são identificados principalmente quando se trata de fiscalização punição dos agentes que atuam de forma ilícita.

Em relação ao primeiro desafio, tem-se a dificuldade de adequar a legislação no ambiente da internet, já que é necessário capacitar e empreender ferramentas tecnológicas desenvolvidas para ser suficiente para realizar a atividade de monitoramento. Por outro lado, nota-se que o arcabouço jurídico não consegue acompanhar o ritmo de velocidade que os crimes são praticados no sentido de abranger determinadas situações não previstas na legislação.

Em suma, o presente estudo buscou analisar quais desafios existem para a aplicação de punições aos crimes cibernéticos com base no código penal, concomitantemente com outras legislações sobre o tema. Para tanto, analisou-se o conceito, classificação e as ferramentas utilizadas para o cometimento dos

delitos de tal natureza com vistas a fornecer melhores esclarecimentos acerca de como essas ações são praticadas e, sobretudo, as sanções correspondentes.

Os resultados obtidos indicam que, tendo em vista a bibliografia e as considerações de estudiosos utilizados neste estudo, o código penal e outros dispositivos legais atinentes a matéria do combate aos crimes cibernéticos não são suficientes e capazes de impedirem a frequência que esses crimes aparecem.

A discussão do tema em comento é fundamental para debater quais medidas podem ser criadas pelo legislador ante os desafios existentes para a punição dos crimes cibernéticos, já que cada vez mais é necessário restringir seu ritmo desenfreado. Com base nisso, urge estudos, pesquisas, coleta de dados e preparo de agentes para enfrentar o problema.

2. REFERENCIAL TEÓRICO

2.1 DA CONCEITUAÇÃO E CLASSIFICAÇÃO DE CRIMES CIBERNÉTICOS

Inicialmente, cumpre esclarecer que não há um consenso sobre a melhor denominação dos crimes cibernéticos, isto é, são várias as denominações dos crimes praticados em ambiente virtual. Leonardi destaca que as denominações existentes para esse delito, como crimes de computação, delitos de informática, abuso de computador, fraude informática, não conseguem abranger de forma genéricas todas situações dos crimes relacionados ao uso da tecnologia. Quanto a conceituação dos crimes cibernéticos, com base na contribuição de Pinheiro, tem-se que são

> Crimes digitais podem ser conceituados como 'condutas de acesso não autorizado a sistemas informáticos ou não, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direito autorais, incitação ao ódio e discriminação, escárnio religioso, divulgação de pornografia infantil, terrorismo, entre outros. (ARAÚJO apud LEONARDI ,2012, p. 499)

Ainda com base nos dois autores, apesar de haver diferentes modalidades de crimes cibernéticos (ou virtuais), o Código Penal limitou-se a abranger duas condutas: crimes de invasão de dispositivos informáticos e interrupção de serviço telemático, os demais são considerados crimes comuns cometidos com auxílio da web. Deve-se ter o cuidado de conceituar tal crime para fins de aplicação do tipo penal.

Para efeitos de aplicação do código penal, segundo Sanches e ngelo (2017) esclarece "faz-se necessária uma análise inicial, primeiramente, para verificar se é um cibercrime ou não, depois aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado, que é a prática de delitos cometida através da internet que pode ser enquadrada no Código Penal Brasileiro".

No tocante às legislações que versam sobre o tema dos crimes cibernéticos, deve-se destacar, segundo Francesco (2014) a lei "Lei Carolina Dieckmann" como ficou conhecida a Lei Brasileira nº 12.737/2012, dispositivo que trouxe alterações no Código Penal Brasileiro ao tipificar os chamados

"delitos ou crimes informáticos, acrescentando acresceu os artigos 154-A e 154-B e alterou os artigos 266 e 298 do Código Penal brasileiro.

Tal legislação surge em um momento de discussão sobre as consequências dos crimes cibernéticos na sociedade e a necessidade de puni-los, contribuindo com inovações conceituais e tipificação de novas condutas criminosas na rede.

Já quanto a classificação de crimes cibernéticos, duas são aceitas majoritariamente pela doutrina: crimes próprios (ou puro) e crime misto (ou impuro). Conforme menciona Anderson Soares Furtado Oliveira exige-se que o crime seja cometido dentro do ambiente virtual.

Nas palavras do autor acerca do crime cibernético próprio:

> Só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço". Ou seja, exige-se que o crime seja cometido dentro do ambiente virtual. (OLIVEIRA,2009, p.33).

Já em relação aos crimes impróprios: crimes cibernéticos impróprios, assevera Aires José Rover (2009, p.33):

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.

Desse modo, tal crime não necessariamente tem sua consumação na rede, na medida em que pode ser praticada por meio de outro meio, isto é, não se utiliza da rede diretamente.

Assim, é fundamental em primeiro momento tomar conhecimento sobre o conceito e classificações para que seja possível evidenciar o nível de dificuldade existente para enquadrar a conduta delituosa ao tipo penal previsto, tendo em vista que as disposições normativas atuais são escassas e limitadas quanto a essa função de subsunção do fato à norma jurídica.

A próxima seção irá analisar quem é o sujeito ativo e passivo dos crimes cibernéticos.

2.2 DO SUJEITO ATIVO E PASSIVO DOS CRIMES CIBERNÉTICOS

Outro ponto crucial para o entendimento aprofundado sobre os crimes cibernéticos é saber quem é o sujeito ativo e passivo. Em relação ao sujeito ativo, ante a dificuldade de identifica-lo por ser um crime em que o autor não o realiza de modo presencial, surge a necessidade de especificar entre determinados grupos, em destaque o hacker e o cracker.

Para Michaelis (2009), o significado literal da palavra hacker, segundo tradução do dicionário quer dizer "pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados". Nesse sentido, estes são usuários que detêm vasto conhecimento informático que utilizam para diversas finalidades, não necessariamente para práticas ilícitas.

Almeida et al (2015, p.226) considera:

> Com isso entende-se que hacker é apenas o gênero, e as espécies de hackers podem variar de acordo com as práticas, uma das espécies são os crackers; essa palavra foi criada no ano de 1985, por hackers que não concordavam com a utilização do termo hacker pela imprensa para definir técnicos ou usuários de computadores que incorressem em ações ilegais ou que causassem transtornos para outras pessoas. Os hackers e os crackers geralmente são muito parecidos em relação ao vasto conhecimento aprofundado em informática, sendo que a principal distinção é a finalidade que suas práticas resultam, posto que os hackers realizam atividades positivas, não criminosas, enquanto a motivação dos crackers é criminosa em sua essência, agindo, normalmente e premeditadamente, com objetivo criminoso de obter vantagens ilícitas.

Percebe-se que o sujeito ativo é aquele que utiliza de seus conhecimentos técnicos para cometer crimes, conforme visto acima, em essência são os crackers.

Já em relação ao sujeito passivo, isto é, sujeitos afetados pelas ações criminosas no ambienta da rede de internet, abrange-se uma totalidade sendo possíveis qualquer pessoa física ou jurídica.

Almeida et al (2015, p.227) aduz:

> Quando falamos de um crime específico, logo sabemos quem é o sujeito ativo e passivo da conduta quem realizou e em quem recaiu a ação ou omissão. Contudo, no caso dos crimes virtuais, de forma generalizada, a única afirmação cabível é que será sempre uma pessoa física ou jurídica ou uma entidade titular seja pública ou privada titular do bem jurídico tutelado, sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado enfim o que sofre a ação. Portanto, o sujeito passivo da infração penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, haja vista poder, por exemplo, ter seus bens desviados, seu patrimônio deteriorado ou mesmo ter informações violadas. Ambas são capazes de determinar a ação do agente criminoso.

Ainda com base no autor, percebe-se que esses crimes tendem a se perpetuarem na sociedade, tendo em vista que são escassos canais de denúncia e de orientações para não serem vítimas, ainda que existindo, uma grande parcela da sociedade não denuncia porque acredita que os infratores serão impunes em razão dos desafios que existem para a punição desses crimes.

> Ocorre que, atualmente muitos dos crimes praticados ainda não são divulgados, seja por conta da não disseminação dessas informações ou pela falta de denúncias, como, por exemplo: grandes empresas evitam a divulgação sobre possíveis ataques virtuais ou mesmo invasões para não demonstrarem fragilidade quanto à segurança, e quanto às pessoas físicas vemos que por falta da devida punibilidade aos infratores e a falta de mecanismos de denúncia, apesar de já existirem, as vítimas acabam não denunciando o que facilita a propagação desses crimes.

Assim, fica evidente que a coletividade se enquadra como sujeito passivo, podendo ser vários os sujeitos afetados. A próxima seção irá analisar os desafios para a punição dos crimes cibernéticos.

2.3 DOS DESAFIOS PARA A PUNIÇÃO DOS CRIMES CIBERNÉTICOS

Vale destacar que os órgãos de combate aos crimes virtuais no Brasil, no tocante à punição aos crimes cibernéticos, são poucos eficazes em razão das dificuldades operacionais existentes no sentido de prevenir e ser superior ao ritmo de cometimento dos crimes.

Miranda (2013) pontua tal dificuldade no tocante a atuação da polícia em crimes de computação: crimes dessa natureza requer investigação especializada e ação efetiva. Infelizmente, não existem no Brasil policiais preparados para combater esse tipo de crime, faltando, pois, visão, planejamento, preparo e treinamento".

Não bastasse isso, as medidas adotadas têm apresentado dificuldade para identificar os sujeitos, pois os criminosos tem a facilidade de esconder identidade, apagando o IP e mascarando a sua localização com o uso de VPN, trazendo grande dificuldade na investigação e punição dos referidos crimes.

Frota e Paiva (2017) destaca que tais ferramentas tecnológicas que dificultam a localização do usuário causam empecilhos para as investigações policiais. Para agravar mais ainda a situação, mesmo que os órgãos de inteligência possuam acesso ao IP, exige-se autorização policial para poder acessar de forma indireta. Ou seja, um entrave que própria legislação cria.

Além disso, é perceptível as dificuldades da penalização dos sujeitos cometedores desses crimes cibernéticos, como diz Carvalho (2013) "é evidente que há desafios no processo investigatório desses crimes virtuais, como por exemplo, a resistência dos provedores em fornecer dados de usuário e local de acesso, alegando que essas informações são sigilosas.

Wendent e Jorge (2013) destacam que a apuração dos crimes virtuais por meio de processos investigatórios possui entraves legais, pois se exige ordem judicial para a quebra desse sigilo, destacando.

> Os crimes virtuais ocorrem principalmente em redes sociais, sendo que nesse meio as condutas, mais praticadas, tipificadas no Código Penal Brasileiro são as do art.138 (Calúnia), art.139 (Difamação), art.140 (Injúria), art.147 (Ameaça), e art. 307 (Falsa Identidade), cuja autoria pode ser investigada buscando-se o IP de criação da página de perfil falso e o IP de postagem das mensagens ofensivas. A materialidade do delito virtual deve ser preservada mediante a impressão e salvamento das páginas, que contém o conteúdo ofensivo e, ainda, deve requerer ao provedor a retirada do conteúdo em até 24 horas, com sua preservação em dispositivos de armazenamento, para continuar a auxiliar nas investigações do autor do crime. Entretanto, também é exigida a ordem judicial na quebra de sigilo telemático para aquisição de dados pessoais do criminoso junto ao provedor de acesso, assim como nos outros procedimentos de investigação.

Enquanto isso, a quantidade de criminosos que se aproveitam do desenvolvimento desenfreado das tecnologias e entraves criados pela própria legislação quanto ao processo de investigação possibilitou o surgimento e ampliação de ataques a bens jurídicos tutelados pela legislação penal.

Um estudo realizado por Ângelo (2002) concluiu que o aumento dessas ações na internet decorre destes fatores: "proliferação de ferramentas gratuitas para ataques, as poucas leis para a prevenção dos crimes digitais e o crescente índice de grupos organizados para explorar oportunidades para o cibercrime são as principais causas apontadas pelo estudo para o aumento dessas ações na internet"

Como visto acima, o presente texto pretende analisar os desafios para a aplicação das punições previstas no código penal no tocante aos crimes dessa natureza, bem como pontua se são suficientes e capazes de inibirem a atuação dos criminosos.

Percebe-se de um modo geral que o Direito em si possui limitações para abranger as diversas situações e modalidades de crimes cibernéticos que são praticados na internet, de forma que há dificuldades para o enquadramento da conduta ao tipo penal e, em alguns casos, carece de punições aos agentes. Em resumo, as palavras do seguinte autor são claras a respeito de tais dificuldades.

> O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores. (PINHEIRO, 2009 apud DULLIUS, 2012, [n.p.]).

Assim, cabe dizer que o ordenamento jurídico brasileiro apresenta dificuldades para identificar, punir e prevenir a ocorrência dos crimes cibernéticos pelos fundamentos apresentados até então. Nesse sentido, urge criar um aparato legislativo, técnico e operacional para o combate a tais dessa natureza, uma vez que no Brasil pouco se avançou acerca da punição dos agentes envolvidos.

3 CONSIDERAÇÕES FINAIS

A presente pesquisa buscou analisar os desafios existentes para aplicar sanções previstas pelo código penal e outras legislações aos cometedores de delitos digitais no ambiente da rede. Para tanto, partiu-se do conceito e classificação dos crimes dessa natureza a fim de evidenciar a dificuldade existente para enquadrar a conduta delituosa ao tipo penal previsto, tendo em vista que as disposições normativas atuais são escassas e limitadas quanto a essa função de subsunção do fato à norma jurídica.

Ademais disso, especificou-se nesse presente estudo quem é o sujeito ativo e qual é o sujeito passivo. Referente ao sujeito ativo, apresentou-se a diferença entre *hacker* e *cracker*, cujo primeiro não

necessariamente é um infrator, pois no sentido literal da palavra como visto acima este é quem detém conhecimento técnico e informático sobre os sistemas e comandos virtuais.

Dito isso, os *crackers* são na essência do termo infratores que violam direitos tutelados pelo código penal utilizando as redes como meio para cometer crimes cibernéticos.

Por outro lado, também se evidenciou que são vários os desafios que surgem no momento de aplicar a punição aos infratores, como visto acima, não é fácil. No entanto, é fundamental que haja a criação de métodos e sistemas tecnológicos capazes de enfrentar esse ritmo desenfreado de cometimento de crimes, uma vez que violaram direitos essenciais, como a privacidade e os dados sensíveis aos usuários.

4 REFERÊNCIAS

ALMEIDA, Jessica de Jesus et al. **Crimes cibernéticos.** Caderno de Graduação-Ciências Humanas e Sociais-UNIT-SERGIPE, v. 2, n. 3, p. 215-236, 2015.

ARAÚJO, Cláudio Rodrigues. **Análise da aplicação do direito penal nos crimes virtuais**. Pensar Acadêmico, Manhuaçu, v. 19, n. 2, p. 494-511, maio-setembro, 2021.

BRASIL. Lei Nº 14.132, de 31 de Março de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acessado em: 02 nov 2023.

BRASIL. Lei Nº 14.155, de 27 de Maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acessado em: 05 nov de 2023.

DULLIUS, Aladio Anastácio. **Dos crimes praticados em ambientes virtuais.** 2012. Disponível em: http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html. Acesso em: 05 nov. 2023.

FERREIRA, Sarah Pereira. **Crimes cibernéticos: a ineficácia da legislação brasileira.** 2021.

FROTA, Jessica Olívia Dias; PAIVA, Maria de Fátima Sampaio. **Crimes virtuais e as dificuldades para combatê-los.** 2017. Disponível: https://flucianofeijao.com.br/novoo/wp-content/uploads/2018/11/ARTIGOS_CRIMES_VIR TUAIS\nDIFICULDADE. Acesso em 05 de outubro de 2023.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.
LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

LESSA, Isabella Maria Baldissera; VIEIRA, Tiago Vidal. **Crimes virtuais: análise do processo investigatório e desafios enfrentados**. 5º Simpósio de Sustentabilidade e Contemporaneidade nas Ciências Socias. jun 2017.

OTHON, Dante Pessoa; DAMASCENO, Ingrid Maria Santos das Neves. **Crimes cibernéticos: desafios enfrentados no processo investigatório.** 2023. Trabalho de Conclusão de Curso-Curso de Graduação em Direito- Universidade Potiguar- Rio Grande do Norte.

ROVER, Aires José. **Crimes de informática**. Disponível em: http://www.infojur.ufsc.br/aires/arquivos/CRIMES%20DE%20INFORMATICA%20public.pdf. Acesso em 05 nov 2023.

SOARES, Murilo Cesar. **Os Direitos Na Esfera Pública Mediática: a Imprensa como instrumento da Cidadania.** São Paulo: Cultura Acadêmica, 2012.