

DESAFIOS DA APLICAÇÃO DA LEGISLAÇÃO PENAL BRASILEIRA AOS CIBERCRIMES

LUCCHESI, M.P.B¹; TIZZO, L.G.L.²

Palavras-chave: Cibercrimes. Desafios. Legislação.

INTRODUÇÃO

A internet se tornou o meio mais poderoso de comunicação ao redor do mundo. Surgindo com esse objetivo em 1960, inicialmente em prol das Forças Armadas, sendo utilizada para a junção de computadores mundialmente interconectados, comunicando-se através de protocolos que eram tidos como organizadores das mensagens de dados.

Ameleto Masini Neto (2025) afirma que antes da internet ser o meio de comunicação mais utilizado e ter todo o alcance que tem atualmente, ela começou a ser desenvolvida durante a Guerra Fria e com o passar do tempo, com a evolução da rede e dos computadores, inevitavelmente a internet chegou ao uso individual.

Essa evolução nos meios de comunicação criou um Direito Penal com inseguranças e riscos, passando a ser chamado de “Direito Penal de Emergência”. Nessa nova formação da sociedade de se comunicar, buscar notícias, ter acessos quase que ilimitados à diversos conteúdos e informações, a prevenção passou a pautar a política criminal.

O Direito Penal de emergência surgiu de atitudes não pensadas levando ao uso simbólico desse ramo do Direito, que encontra certas dificuldades em alcançar as violações digitais (Neto,2025).

“Importante frisar que esta grande rede não tem um único controlador, na verdade, é uma realidade sem fronteiras, trazendo mil questões para um mundo que historicamente se divide.” (Cavalcante, 2012, p.3).

Para Ameleto Masini Neto (2025), mesmo com todos os benefícios que a internet traz para a sociedade, há também os perigos que essa rede deixa à mercê dos indivíduos, gerando uma originalidade que dá luz à assuntos importantes em face da investigação de infrações cometidas nesse ambiente não tangível e que excede a linha de tempo e espaço.

¹ Maria Paula Bueno Lucchesi. Acadêmica do Curso de Bacharelado de Direito da Faculdade de Apucarana – FAP. Apucarana – Pr. 2025.

² Luis Gustavo Liberato Tizzo. Orientador da pesquisa. Docente Mestre do Curso de Bacharelado de Direito da Faculdade de Apucarana – FAP. Apucarana – Pr. 2025.

OBJETIVO

Compreender as dificuldades existentes na aplicação da legislação penal no que tange os crimes cibernéticos.

MÉTODO

Tratou-se de uma pesquisa utilizando o método dedutivo onde, a partir de uma relação entre premissas, tirou-se uma conclusão e método histórico, onde a pesquisa analisou acontecimentos, processos e instituições do passado para verificar a sua influência na sociedade atualmente.

CONCEITO DE CRIMES CIBERNÉTICOS

Os crimes cibernéticos ou *cybercrimes* são definidos como “qualquer condutas típicas e antijurídicas realizadas por meio de computadores, sistemas de informática ou dispositivos móveis informáticos” (Neto, 2025, p. 21).

Os primeiros *cybercrimes*, de acordo com Ameleto Masini Neto (2025), aconteceram em 1960 quando foi registrado o uso dos computadores para práticas de espionagem, sabotagem etc. Porém foi em 1980 que esses delitos começaram a se potencializar.

Dentro do estudo das tipologias dos crimes cibernéticos, a primeira subdivisão é a que diferencia as “ofensas focadas no computador” das “ofensas assistidas pelo computador”. A primeira categoria fala sobre os crimes que seu alvo é a própria estrutura eletrônica, abrangendo a rede mundial de computadores e sem a qual, essas infrações não ocorreriam, à título de exemplo cita-se a invasão de dispositivo informático de uso alheio, conectado à rede de computadores. A segunda categoria refere-se a ofensas cometidas antes da internet, tais ofensas independem da rede, porém, no caso concreto, consubstanciam-se em atos assistidos por ela. Como por exemplo extorsão cibernética, furto mediante fraude eletrônica etc. (Neto, 2025).

Os crimes cibernéticos podem ser próprios, impróprios, mistos e mediatos ou indiretos. Sendo *cybercrimes* próprios, aqueles onde o bem jurídico tutelado pela norma penal é a inviolabilidade dos dados ou informações. Os crimes cibernéticos impróprios são aqueles que utilizam o computador como ferramenta para o cometimento do crime. Por sua vez, os crimes cibernéticos mistos são delitos

derivados do acesso não autorizado a sistemas informáticos. Já os crimes mediatos ou indiretos, são os crimes em que o delito-fim não é no âmbito informático, porém herdou essa característica de uma violação por meio tecnológico para poder ser consumado (Lopes, Santos, Teixeira, 2021. p. 126).

Ante o exposto, entende-se que a informática, além de permitir a realização de novas infrações, pode potencializar as já existentes.

DESAFIOS DA APLICAÇÃO DA LEGISLAÇÃO PENAL

No que tange a internet e sua constante evolução, Emerson Wendt (2021) ressaltar os principais aspectos considerados desafiadores, tanto para a segurança pública quanto para a investigação dos cibercrimes.

Apesar de ser possível realizar o enquadramento típico de boa parte das condutas que causam prejuízos aos usuários da internet, ainda existem casos em que não há uma previsão penal que possa promover um enquadramento específico que se encaixe da melhor maneira aos crimes cibernéticos, de uma forma que possa evitar questionamentos jurídicos. À título de exemplo, Wendt (2021) cita a alegação de que a conduta não configura crime por não haver previsão legal que o defina.

Embora a legislação atual não abranja todas as possíveis especificidades de cada caso que envolva um crime cibernético, Emerson Wendt (2021) dá luz para a evolução jurídica que acompanhou o desenvolvimento dos cibercrimes, sendo a principal realizada em 2012, onde o plenário da Câmara dos Deputados aprovou a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann.

Wendt (2021) afirma que houve avanços significativos no ordenamento jurídico do Brasil no que se refere aos cibercrimes, entretanto, com a velocidade que a internet e os usuários se desenvolvem, torna-se desafiador para que os legisladores e a segurança pública acompanhem essas evoluções de modo eficaz. Dessa forma, a falta de capacitação de policiais, Ministério Público e do judiciário, representa um grande desafio, a ponto de haver possibilidades de cibercriminosos não serem punidos.

Importante frisar que os recursos tecnológicos permitem que os sujeitos ativos dos crimes cibernéticos, mesmo que espalhados por diferentes localidades, podem se comunicar com rapidez e realizar ações criminosas, até mesmo de forma anônima, dificultando assim a investigação desses crimes. Essas dificuldades não se

trata do desconhecimento dos processos investigativos, nem tão somente são referentes às possíveis brechas da legislação. As dificuldades acontecem quando o investigador se depara com o tráfego de pacotes encriptados ou protegidos pelos provedores de conteúdo (Wendt, 2021).

Mesmo com os avanços jurídicos contra os cibercrimes, é possível afirmar, de grosso modo, que muitos dos usuários não possuem conhecimento da dimensão dos riscos que correm todos os dias com a utilização da internet e das redes sociais.

Por isso, Emerson Wendt (2021) pontua que é mais importante conscientizar o usuário para que seja capaz de compreender a necessidade de utilizar a internet com segurança ao invés de munir esses usuários de recursos tecnológicos avançados que tem por objetivo tornar a utilização da internet mais segura.

CONSIDERAÇÕES FINAIS

O principal motivo para a elaboração desse trabalho se fundamentou na necessidade de entender melhor a forma como a evolução da internet não acompanha a evolução jurídica e legislativa do Brasil.

Se o uso e os recursos da internet avançam tão rápido como é possível que a legislação seja aplicada com eficácia?

Conclua-se que a capacitação de todos aqueles que, profissionalmente, se deparam com os crimes cibernéticos (policiais, advogados, membros do Poder Judiciário e do Ministério Público) é essencial para que haja sucesso em qualquer atividade que busque enfrentar os desafios que o acesso ilimitado a internet sobrepõe à sociedade.

Além disso, é fundamental que tenha um aprimoramento na legislação que trata sobre esses delitos, de modo que ajude a diminuir sua incidência, por beneficiar a punição dos cibercriminosos.

Também se entende que o trabalho isolado dos órgãos que representam a persecução penal não é o suficiente sem uma ação governamental fundamentada na unificação de propósitos e objetivos em comum.

Por fim, importante frisar a importância da conscientização dos usuários para que possam, além de ter o conhecimento desses crimes, prestar atenção na forma com que utilizam a rede mundial de computadores, para que assim consigam navegar pela internet de forma mais assertiva e segura.

REFERÊNCIAS

NETO, Ameleto Masini. **Crimes Cibernéticos**. Indaiatuba, SP: Editora Foco, 2025.

CAVALCANTE, W.F. **Crimes Cibernéticos**: noções básicas de investigação e ameaça na internet. 2013. Disponível em:

<https://jus.com.br/artigos/25743/crimesciberneticos> Acesso em: 29 set 2025.

LOPES, Alan Moreira, SANTOS, Keila Dos, TEIXEIRA, Tarcisio. **Direito Digital**: teórica e prática. São Paulo, SP: 1 ed. Tirant lo Blanch, 2021.

WENDT, Emerson. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro, RJ: 3 ed. Brasport, 2021.