CRIMES CIBERNÉTICOS: CRIMES REALIZADOS NO ÂMBITO VIRTUAL E A RELEVÂNCIA DA MANUTENÇÃO DE PROVAS

Joel Pitz[1]
Pablo Franciano Steffen[2]

"Diz-se que alguém é responsável criminalmente, pela prática de um ato reputado delituoso, quando deve responder por ele perante o poder social."[3]

Resumo

O presente artigo é um estudo abrangente sobre crimes cibernéticos, visando proporcionar ao leitor uma visão geral e fundamentada sobre o tema. Inicia-se com a evolução dos sistemas de informação e da Internet, abordando suas origens e desenvolvimentos até o momento atual, com dados e informações históricas relevantes. Prossegue-se com a classificação dos crimes cibernéticos, detalhando as características dos sujeitos do delito e fornecendo exemplos concretos, bem como, apresentado os crimes que derivaram destas evoluções tecnológicas. O artigo analisa ainda a definição da competência para o processamento e julgamento desses crimes, e finaliza com uma análise detalhada, dos artigos, da Lei 12.737/2012, que atualizou a legislação penal brasileira com relação aos delitos cometidos no ambiente virtual.

Palavras-Chave: Crimes Cibernéticos. Direito Penal. Direito Processual Penal.

Abstract

This article is a comprehensive study on cybercrime, aiming to provide the reader with a general and well-founded view of the topic. It begins with the evolution of information systems and the Internet, addressing their origins and developments up to the present, with relevant historical data and information. It continues with the classification of cybercrimes, detailing the characteristics of the subjects of the crime and providing concrete examples, as well as presenting the crimes that derived from these technological developments. The article also analyzes the definition of competence for the processing and judgment of these crimes, and ends with a detailed analysis of the articles of Law 12,737/2012, which updated Brazilian criminal legislation in relation to crimes committed in the virtual environment.

Keywords: Cybercrimes. Criminal Law. Criminal Procedural Law.

---

[1] Discente da 6ª fase do curso de Direito do Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí – UNIDAVI. E-mail: joel.pitz@unidavi.edu.br

[2] Advogado. Professor de Direito Penal, Direito Processual Penal e Direito Internacional do Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí – UNIDAVI. Mestre e Doutor em Ciência Jurídica pela Universidade do Vale do Itajaí – UNIVALI. E-mail: pablosteffen@unidavi.edu.br

[3] LEITE, Nelson Ferreira: O conteúdo jurídico da responsabilidade penal - Trabalho apresentado, em dezembro de 1962, no Curso de Especialização da Faculdade de Direito, cadeira de Direito Penal Comparado.

1 INTRODUÇÃO

Os crimes cibernéticos são caracterizados como condutas ilícitas praticadas por meio eletrônico, através da internet ou outras tecnologias da informação, abrangendo uma ampla gama de delitos, tais como: fraudes financeiras, roubo de identidade, pirataria de software e dados, ameaças, invasão de privacidade, ataques de negação de serviço (DDoS), chantagem, extorsão, tráfico de drogas e exploração sexual infantil, bem como, facilitou a prática de intimidação sistemática – cyberbullying. Esses delitos revelam uma crescente complexidade, uma vez que, seus autores frequentemente utilizam ferramentas e técnicas avançadas para ocultar sua identidade e localização real, o que dificulta a sua detecção e identificação, ou realizam perfis falsos com o intuito de disseminar ódio. Assim, a coleta de provas contundentes e periciais é imprescindível para a formalização da imputação penal nesses casos, contudo, a grande objeção nestes casos é ter prova irrefutável do crime.

O avanço da informática, especialmente ao longo da última década, inseriu-se de forma definitiva no cotidiano da população mundial, e o Brasil não foge à regra. A rápida evolução das tecnologias eletrônicas é surpreendente, com dispositivos sendo substituídos por versões mais modernas em intervalos cada vez menores. Esse crescimento acelerado trouxe inovações tecnológicas inimagináveis até o início dos anos 2000. Hoje, dispositivos como computadores, smartphones, tablets e outros estão conectados à internet praticamente ininterruptamente, nas mãos de grande parte da população mundial, o que facilita tanto o acesso a bens e serviços quanto a prática de crimes cibernéticos.

Posto que os benefícios advindos dessas tecnologias sejam incontestáveis – tendo facilitado a comunicação, reduzido barreiras geográficas e promovido avanços em diversos setores, como o produtivo e o informacional, esta ascensão veio seguido do aumento exponencial de crimes cometidos pelo meio digital. A sofisticação das técnicas criminosas, o anonimato proporcionado pelas redes e a rápida disseminação de informações dificultam a contenção e o combate a tais ilícitos, cujo demandam novas estratégias de investigação e regulação.

No presente trabalho, foi analisada e pontuado o marco inicial das ferramentas tecnológicas, a evolução histórica dos computadores, desde sua controversa criação até o surgimento da inteligência artificial (I.A) e o desenvolvimento das máquinas e aparelhos que conhecemos atualmente. O estudo, igualmente, percorreu a história da internet, com especial atenção ao seu desenvolvimento no Brasil, que se iniciou no final da década de 1980 e se expandiu significativamente hodiernamente. A obra ainda classifica os crimes cibernéticos em duas categorias principais: crimes cibernéticos próprios**,** que são aqueles que só podem ser cometidos no ambiente virtual, e crimes cibernéticos impróprios, que são delitos comuns, mas que se utilizam da internet como meio facilitador. A classificação dos sujeitos ativos (criminosos) e passivos (vítimas) também foi tratada, assim como as diferenças entre hackers – indivíduos que utilizam suas habilidades tecnológicas com intuito construtivo ou, pelo menos, não destrutivo – e crackers – que agem com o intuito de causar prejuízos.

Em seguida, em âmbito estritamente jurídico, foi delimitada a questão da competência para processar e julgar os crimes cibernéticos. A análise de competência leva em consideração se o delito em questão afeta bens ou interesses da União, suas autarquias ou empresas públicas, o que, neste caso, atrairia a competência da Justiça Federal, conforme previsto na Constituição Federal. Nos demais casos, a competência será da Justiça Estadual**.** Também foi analisado qual seria o foro competente, ou seja, a localidade onde o processo deve ser

iniciado, considerando, sobretudo, o local da consumação do delito ou da obtenção das provas.

A pesquisa também realizou um exame aprofundado da Lei 12.737/2012, amplamente conhecida como Lei Carolina Dieckmann, em referência ao caso que motivou sua criação. Esta lei introduziu os artigos 154-A e 154-B ao Código Penal Brasileiro[4], tipificando o crime de invasão de dispositivo informático, além de promover alterações em outros dispositivos legais, como os artigos 266[5] (relacionado à interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos ou de utilidade pública) e 298[6] (que trata da falsificação de documentos públicos e privados). O estudo jurídico realizado detalhou as implicações desses dispositivos legais no contexto da repressão e combate aos crimes cibernéticos no Brasil.

Para a elaboração deste trabalho, foi utilizado o método de pesquisa indutivo, e técnica de pesquisa bibliográfica, com o levantamento de dados em obras especializadas, artigos científicos, decisões jurisprudenciais e monografias. O objetivo principal foi oferecer uma visão abrangente e didática acerca do tema, de modo a proporcionar ao leitor uma compreensão aprofundada e clara das nuances que envolvem os crimes cibernéticos e seu tratamento no ordenamento jurídico brasileiro.

2 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A doutrina jurídica apresenta diversas classificações acerca da natureza dos crimes cibernéticos. Neste artigo, opta-se pela abordagem que os divide em **crimes cibernéticos próprios** e **crimes cibernéticos impróprios**[7].

Os crimes cibernéticos próprios são aqueles nos quais o agente, para a consumação do delito, necessita do uso imprescindível de um computador ou dispositivo informático. Em tais crimes, o computador figura como meio essencial de execução código, sendo o bem jurídico tutelado diretamente relacionado aos dados armazenados em sistemas computacionais ou redes. O crime é praticado e consumado[8] exclusivamente por meio de instrumentos informáticos. Um exemplo de crime cibernético próprio, previsto na legislação brasileira, é o crime de Invasão de Dispositivo Informático - artigo 154-A do Código Penal[9].

Por outro lado, os **crimes cibernéticos impróprios**[10] são aqueles em que, embora o computador possa ser utilizado como ferramenta para a prática delitiva, não se faz necessária à sua utilização exclusiva para a consumação do delito. Nesse caso[11], o bem jurídico atingido

---

[4] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 24.08.2024.
[5] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 24.08.2024.
[6] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 26.08.2024.
[7] PINHEIRO, Patrícia Peck. *Direito Digital*. 9. ed. São Paulo: Saraiva, 2019.
[8] PRADO, Luiz Regis. Curso de Direito Penal Brasileiro: Parte Especial - 14ª Ed. São Paulo: Revista dos Tribunais, 2015.
[9] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 14.09.2024.
[10] PINHEIRO, Patrícia Peck. *Direito Digital*. 9. ed. São Paulo: Saraiva, 2019.
[11] BITENCOURT, Cezar Roberto. Tratado de Direito Penal: Parte Especial, v.3, 14 ed., São Paulo: Saraiva Jur, 2018.

pode ser lesado de diversas formas, sem a exigência de uma conexão direta com o meio informático, transcendendo o universo digital e afetando o mundo físico. Exemplos de crimes impróprios, tipificados na legislação brasileira, incluem: calúnia, injúria, difamação, ameaça, furto, apropriação indébita, estelionato, dano, violação de direito autoral, pedofilia, e crimes contra a propriedade intelectual.

Nota-se que todos esses delitos podem ser cometidos sem a necessidade de um computador, mas, por outro lado, também podem ser perpetrados através do uso de dispositivos informáticos, configurando-se como crimes cibernéticos impróprios.

3 DA VIOLÊNCIA ELETRÔNICA DERIVADA DO BULLYING (CYBERBULLYING) E O LINCHAMENTO VIRTUAL

Com a rápida expansão e imediatismo da internet[12] e o uso generalizado das redes sociais no século XXI, surgiu uma nova violência: o cyberbullying. Trata-se de uma forma de agressão eletrônica que, apesar de ser uma extensão do bullying tradicional, ocorre no ambiente virtual por meio de ataques que podem incorporar difamação, insultos, ameaças, entre outras práticas. De modo que, a velocidade e o alcance da internet transformaram o que antes eram pequenos incidentes locais em grandes ondas de linchamento virtual[13], que muitas vezes se originam[14] em plataformas como Instagram, TikTok, X (Twitter), WhatsApp, Facebook, entre outras.

Contudo, o avanço[15] dessas práticas para o ambiente digital traz um dilema ético e legal, mesmo que, todos os seres humanos tenham o direito à liberdade de expressão[16], conforme previsto no Artigo 19 da Declaração Universal dos Direitos Humanos[17], esse direito não é absoluto. A liberdade de emitir opiniões e divulgar informações deve sempre ser equilibrada com o respeito à dignidade da pessoa humana, garantida pelo Artigo I da Declaração Universal dos Direitos Humanos[18] e pela Constituição Brasileira em seu artigo 1º, inciso III[19]. O que vê-se, muitas vezes, é o uso distorcido desse direito para justificar atos de

---

[12] ROSSINI, Augusto Eduardo De Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

[13] JUS BRASIL. Linchamento Virtual: Você conhece? Disponível em: https://www.jusbrasil.com.br/artigos/linchamento-virtual-voce-conhece/912335410, acessado em 25.09.2024.

[14] FILHO, Valmor H., Revista VEJA, Agora é crime: cyberbullying alarma o Brasil, 2º país no mundo em casos, Governo dá importante passo ao criminalizar ataques virtuais, um problema que está perto de se tornar uma epidemia entre os jovens. Disponível em: https://veja.abril.com.br/brasil/agora-e-crime-cyberbullying-alarma-o-brasil-2o-pais-no-mundo-em-casos, acessado em 19.09.2024.

[15] SZNICK, Valdir. Novos Crimes e Novas Penas no Direito Penal. São Paulo: Livraria e Editora Universidade de Direito, 1992.

[16] BITENCOURT, Cezar. Tratado de Direito Penal Volume 2, 19 edição. SaraivaJur, 2019.

[17] Declaração Universal dos Direitos Humanos, adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948 - UNICEF. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos, acessado em 15.09.2024.

[18] Declaração Universal dos Direitos Humanos, adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948 - UNICEF. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos, acessado em 16.09.2024.

[19] BRASIL, Constituição da República Federativa do Brasil, de 05 de outubro de 1988. Brasília: Senado, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, acessado em 16.09.2024.

violência moral, humilhação pública e incitação ao ódio[20], o que transforma a vítima em alvo de julgamentos sumários, sem qualquer chance de defesa.

Assim, os linchamentos virtuais, que se assemelham ao linchamento físico tradicional, ocorrem quando um indivíduo é exposto e humilhado publicamente nas redes sociais. Como destaca o sociólogo e professor José Martins de Souza[21] em sua obra *Linchamentos: a justiça popular no Brasil*, a vítima assume o papel de "bode expiatório", sendo sacrificada por uma multidão de agressores virtuais que, muitas vezes, nem a conhecem pessoalmente. Esses atos, além de moralmente reprováveis, configuram diversas práticas criminosas tipificadas no Código Penal Brasileiro[22], como Calúnia - artigo 138[23], Difamação - artigo 139[24] e Injúria artigo 140[25]. Mais grave ainda, podem incitar ao suicídio ou à automutilação, o que é previsto no artigo 122[26] do Código Penal como crime de Induzimento ou Instigação ao Suicídio[27].

É comum que, em defesa dessas práticas, invoquem o direito à liberdade de expressão. No entanto, o Princípio da Dignidade da Pessoa Humana atua como um contrapeso a esse argumento, limitando as manifestações de opinião quando elas violam a integridade física, psicológica e moral do outro. A internet[28], ao contrário do que muitos imaginam, não é um território sem lei. As vítimas de cyberbullying têm o direito à reparação pelos danos sofridos, como preconiza o artigo 186 e 944 do Código Civil[29], que estabelece que aquele que, por ação ou omissão, cause danos a outra pessoa, deve indenizá-la.

Os efeitos do linchamento virtual podem ser devastadores. Relatos de vítimas mostram que muitas delas nunca mais voltam a ter uma vida normal após serem expostas ao escárnio público. Algumas necessitam de tratamento psicológico intenso, como mostram diversas reportagens sobre o tema. Nesse sentido, o cyberbullying e o linchamento virtual não são apenas "brincadeiras de mau gosto"[30], mas ações de profunda violência emocional e psicológica.

A prática, muitas vezes, vai além de insultos[31], alcançando a criação de perfis falsos[32] – os famosos "fakes" – usados para propagar mentiras, difamar e manipular a imagem da

---

[20] LOURENÇO, Ana, O que motiva os linchamentos Virtuais, e quais as consequências desses ataques no mundo real. Disponível em: https://super.abril.com.br/tecnologia/o-que-motiva-os-linchamentos-virtuais/, acessado em 25.09.2024.

[21] SOUZA, José Martins de. Linchamentos: a justiça popular no Brasil. 1. ed. São Paulo: Contexto, 2011.

[22] CAPEZ, Fernando. Curso de Direito Penal. Parte Geral, v.1, 15 ed. São Paulo: Saraiva, 2011.

[23] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 16.09.2024.

[24] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 16.09.2024.

[25] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 16.09.2024.

[26] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 16.09.2024.

[27] JUS BRASIL. Induzimento, instigação e auxílio ao suicídio pelos meios digitais. Disponível em: https://www.jusbrasil.com.br/artigos/induzimento-instigacao-e-auxilio-ao-suicidio-pelos-meios-digitais/1445315086 ,acessado em 26.09.2024.

[28] SILVA, Rita de Cássia Lopes da. Direito Penal e sistema informático: Problemas fundamentais. Dissertação Mestrado, Universidade Estadual de Maringá, Maringá, 2002.

[29] BRASIL, Código Civil, de 10 de janeiro de 2002. LEI Nº 10.406,2002. Disponível em: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm, acessado em 17.09.2024.

[30] NODARI, Luana, O que é bullying virtual ou cyberbullying? Perguntas e respostas sobre o bullying na internet. Disponível em: https://psicologaluananodari.com.br/o-que-e-bullying-virtual-ou-cyberbullying-perguntas-e-respostas-sobre-o-bullying-na-internet/, acessado em 26.09.2024.

[31] DONEDA, Danilo. *Direito à Privacidade e Proteção de Dados Pessoais: A Função e os Limites da Autodeterminação Informativa*. 2. ed. Rio de Janeiro: Renovar, 2011.

vítima. Essas práticas, embora digitais, deixam rastros e provas, que podem ser utilizadas pela vítima em vias judiciais. Medidas simples, como a captura de telas e o registro das postagens ofensivas, podem ser cruciais na identificação dos autores. Em casos mais complexos, o auxílio de autoridades policiais especializadas em crimes cibernéticos é essencial para rastrear e responsabilizar os infratores.

Além dos impactos psicológicos[33] e criminais, o cyberbullying também afeta a honra e a imagem das vítimas, atingindo diretamente sua vida social e profissional. Grupos que ridicularizam, divulgam informações[34] falsas ou humilham pessoas online não oferecem espaço para que essas vítimas exerçam seu direito ao contraditório e à ampla defesa, ambos garantidos pela Constituição Brasileira. Esse contexto gera uma injustiça irreparável e atenta contra a integridade moral e pessoal dos indivíduos.

Entre os tipos de crimes mais comuns praticados nesse ambiente digital estão a Calúnia, que consiste em acusar falsamente alguém de cometer um crime; a Difamação, que envolve atribuir a alguém um fato que ofende sua reputação, seja ele verdadeiro ou não; e a Injúria, que é a ofensa direta à dignidade ou ao decoro da pessoa. Ademais, compartilhar "nudes" ou outras informações não autorizadas, configura crimes como difamação ou injúria, que, dependendo do caso, é tratada como um delito grave, especialmente se envolver menores de idade[35], como previsto no Estatuto da Criança e do Adolescente em seus artigos 241, 241-A e 241-B, do Estatuto da Criança e do Adolescente (ECA)[36].

Ou seja, embora o direito à liberdade de expressão seja fundamental, ele não pode servir de escudo e se sobressair nas práticas que desrespeitam a dignidade alheia. Linchamentos virtuais, cyberbullying e outros crimes digitais ultrapassam os limites da legalidade e da ética, gerando consequências não apenas no campo penal, mas também na esfera civil, no caso de reparação de danos e responsabilidade Civil. A internet não é um espaço livre de responsabilidades; pelo contrário, exige o uso consciente e responsável das ferramentas de comunicação, principalmente no que é divulgado, comentado ou doutrinado.

Assim, é importante lembrar: se alguém, efetuar-lhe o convite para integrar algum grupo cuja intenção seja ridicularizar, ofender outra pessoa, ou até mesmo para dissipar jogos suicidas[37], com o intuito de induzimento, instigação ou auxílio ao suicídio, como foi o caso da "Baleia Azul"[38], recuse-se imediatamente. A participação em tais grupos, mesmo que de forma passiva, pode resultar em implicações legais sérias, e os danos causados às vítimas

---

[32] MILAGRE, José Antônio; DE JESUS, Damásio. Manual de Crimes Informáticos, 1 edição. Saraiva, 2016.

[33] PORFÍRIO, Francisco, Brasil Escola, Cyberbullying. Disponível em: https://brasilescola.uol.com.br/sociologia/cyberbullying.htm#:~:text=Consequ%C3%AAncias%20do%20cyberbullying,O%20cyberbullying%20pode&text=Assim%20como%20ocorre%20com%20o,ansiedade%20e%20s%C3%ADndrome%20do%20p%C3%A2nico. Acessado em 26.09.2024.

[34] AMARAL, Mariana Valente do. *Crimes Digitais e a Responsabilização no Direito Brasileiro*. São Paulo: Thomson Reuters, 2021.

[35] BRASIL, Decreto legislativo nº 28 de 14/09/1990, e do Decreto nº 99.710 de 21/12/1990, a Convenção sobre direitos da Criança adotada pela Assembleia Geral das Nações Unidas. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm, acessado em 26.09.2024.

[36] BRASIL, Lei 8.069/90. Brasília: Senado,13 de julho de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm, acessado em 17.09.2024.

[37] BRASIL, Lei 13.968/19. Brasília: Senado, 26 de dezembro de 2019. Disponível em: https://legis.senado.leg.br/norma/31881858#:~:text=Altera%20o%20Decreto%2DLei%20n%C2%BA,aux%C3%ADlio%20a%20quem%20a%20pratique.&text=DIREITO%20PENAL%20 , acessado em 26.09.2024.

[38] G1, RAMAL, Andrea, Entenda o 'Jogo da Baleia Azul' e os riscos envolvidos. Disponível em: https://g1.globo.com/educacao/blog/andrea-ramal/post/entenda-o-jogo-da-baleia-azul-e-os-riscos-envolvidos.html, acessado em 18.09.2024.

podem ser irreversíveis. O linchamento virtual e estes atos, não estão protegidos pelo princípio da liberdade de expressão, sobretudo, quando envolve discursos de ódio ou incitação à violência. A dignidade da pessoa humana é um valor inalienável e deve ser respeitado em todas as esferas, inclusive no mundo digital.

4 SUJEITOS DO CRIME E COMPETÊNCIA JURISDICIONAL EM CRIMES CIBERNÉTICOS

Nos crimes cibernéticos, o sujeito[39] ativo pode ser qualquer pessoa que utilize a internet e a tecnologia da informação para cometer ilícitos. Esses sujeitos variam amplamente em termos de conhecimento técnico e periculosidade:

Pessoas Comuns: Indivíduos sem conhecimentos técnicos avançados e que cometem crimes cibernéticos simples, como a divulgação não autorizada de informações e imagens ou ridicularização e ofensa de outra pessoa nas redes sociais. Esses crimes, apesar de serem graves, não exigem habilidades técnicas sofisticadas, mas ainda configuram ofensas sérias à honra, moral e privacidade das vítimas.

Indivíduos com Conhecimento Técnico Avançado: São aqueles que necessariamente, precisam de habilidades especializadas em informática e segurança cibernética. Estes, podem executar ataques mais complexos, como invasões de sistemas pessoais, corporativos e governamentais. Análogo a isso, o ataque à Sony Pictures em 2014[40], foi utilizado um malware extremamente sofisticado que era indetectável por programas antivírus comuns[41]. Isso demonstra a capacidade de indivíduos com conhecimento técnico profundo para causar danos significativos[42].

Hackers e Crackers[43]: Preliminarmente, é importante distinguir entre hackers, que aplicam seus conhecimentos para fins legais e éticos, e “crackers”, que usam habilidades similares para atividades ilícitas. A terminologia "cracker" foi criada pelos hackers para diferenciar aqueles que utilizam seus conhecimentos para quebrar sistemas de forma ilegal, esses frequentemente possuem habilidades técnicas equiparadas aos hackers, mas com intenções prejudiciais.

A identificação desses sujeitos é frequentemente realizada através do IP[44] (*Internet Protocol*), que funciona como uma identidade virtual para cada dispositivo conectado à internet. Porém, a identificação pode ser complicada e desafiadora, pois os provedores de internet podem não armazenar essas informações por muito tempo ou podem exigir

---

[39] CEZAR, Dimas. *Direito Penal e Crimes Cibernéticos*. Editora Forense, 2016.

[40] TECNOBLOG, CÂMARA, Júlio, Tudo o que você precisa saber sobre os ataques e vazamentos sofridos pela Sony Pictures. Disponível em: https://tecnoblog.net/especiais/sony-pictures-ataque-hacker-tudo-sobre/, ce4ssado em 26.09.2024.

[41] FOLHA DE SÃO PAULO. ROMANI, Bruno. Entenda o caso da invasão hacker à Sony Pictures. Disponível em: https://temas.folha.uol.com.br/futuro-digital/seguranca-e-o-mundo-digital/hack-do-seculo-caso-sony-chama-atencao-para-seguranca-de-dados.shtml ,acessado em 26.09.2024.

[42] G1, REUTERS, Ataque contra a Sony Pictures deve custar US$ 100 mi, diz especialista. Disponível em: https://g1.globo.com/tecnologia/noticia/2014/12/ataque-contra-sony-pictures-deve-custar-us100-mi-diz-especialista.html, acessado em 18.09.2024.

[43] Bittencourt, Edson. *Crimes Cibernéticos e a Sociedade da Informação*. Editora Juruá, 2017.

[44] Bessone, Patricia. *Direito e Tecnologia: O Impacto da Tecnologia na Sociedade e no Direito*. Editora Método, 2020.

autorização judicial para divulgá-las. Ademais, com o vasto conhecimento técnico utilizado, é possível mascarar ou alterar o IP, dificultando a rastreabilidade.

Já o sujeito passivo, em crimes cibernéticos, pode ser qualquer pessoa ou entidade, que tenha seus direitos ou bens jurídicos afetados, portanto, inclui-se tanto pessoas físicas quanto jurídicas. A vítima desses crimes pode ter sua honra, moral, privacidade e outros direitos prejudicados por ações perpetradas online.

Diante de todo o exposto, cabe explanar que a competência[45] para julgar[46] crimes cibernéticos nem sempre é tão intuitiva quanto parece. Embora a Justiça Federal seja normalmente associada a crimes envolvendo a internet devido à sua grande repercussão de natureza interestadual e internacional, a competência[47] é determinada com base na territorialidade[48] e na natureza do delito, de modo que cabe a:

Justiça Federal: Julgar crimes cibernéticos que envolvem elementos de internacionalidade, ou seja, se um crime cibernético afeta bens jurídicos em outros países ou se o delito tem repercussão internacional, ele pode ser julgado pela Justiça Federal, desde que os países envolvidos sejam signatários de tratados internacionais, conforme o artigo 109 da Constituição Federal[49].

Justiça Estadual: Se o crime cibernético não ultrapassar as fronteiras do Brasil e não tiver impacto internacional, a competência será da Justiça Estadual, cujo, analisará o crime de acordo com as regras de territorialidade, o local onde o crime foi consumado ou onde o bem jurídico foi afetado.

Exceção do STJ: O Superior Tribunal de Justiça (STJ)[50] estabelece uma exceção para crimes contra a honra cometidos online, de modo que, determinou que a competência pode ser fixada pelo local onde o provedor de internet, que hospedou o conteúdo ilícito, está localizado, com o intuito de facilitar a identificação e julgamento dos responsáveis pelos conteúdos ofensivos.

A legislação penal brasileira, historicamente obsoleta para lidar com crimes cibernéticos em sua totalidade, haja vista a facilidade com que a tecnologia vem adentrando na sociedade, recebeu um importante avanço com a promulgação da Lei 12.737, de 2012, conhecida como Lei Carolina Dieckmann[51], cuja surgiu em resposta a um notório caso de violação de privacidade[52] envolvendo a atriz brasileira, que posteriormente deu nome à

---

[45] JUS BRASIL. STJ analisa competência para os chamados crimes informáticos (crimes virtuais = cybercrimes): competência territorial do local de hospedagem do site. Disponível em: https://www.jusbrasil.com.br/noticias/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site/2659329. acessado em 26.09.2024.

[46] BRASIL, CC 121215/PR, Rel. Ministra Alderita Ramos de Oliveira (desembargadora convocada do TJ/PE), TERCEIRA SEÇÃO, julgado em: 12/12/2012, DJe 01/02/2013.

[47] Greco, Luís Roberto. *Direito Penal: Parte Geral*. Editora Impetus, 2020..

[48] BRASIL, Código de Processo Penal, de 3 de outubro de 1941. DECRETO-LEI Nº 3.689,1941.Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm , acessado em 26.09.2024.

[49] BRASIL, Constituição da República Federativa do Brasil, de 05 de outubro de 1988. Brasília: Senado, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, acessado em 18.09.2024.

[50] Souza, Renato. *A Justiça e os Crimes Cibernéticos: Jurisprudência e Competência*. Editora Saraiva, 2019.

[51] G1, GRAELL e VINCAX, Fernanda, Marcus, Lei Carolina Dieckmann completa 10 anos como marco no combate a crimes cibernéticos. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/12/02/lei-carolina-dieckmann-completa-10-anos-como-marco-no-combate-a-crimes-ciberneticos.ghtml, acessado em 19.09.2024.

[52] Almeida, Marcos. *Crimes Cibernéticos e a Nova Lei 12.737/2012: Aspectos Práticos e Teóricos*. Editora Lumen Juris, 2018.

legislação, a Lei 14.155, de 2021, as jurisprudências e as doutrinas, como fontes da lei, de forma análoga.

A Lei 12.737/12[53] introduziu novos dispositivos legais e modificou artigos do Código Penal para abordar mais efetivamente os crimes praticados na esfera digital, a qual, acrescentou os artigos 154-A e 154-B ao Código Penal[54] e alterou os artigos 266 e 298 do referido, de modo que, o artigo 154-A, posteriormente, foi, novamente, alterada pela Lei 14.155/21[55], refletindo a necessidade de uma resposta legal mais robusta e atualizada[56] aos desafios dos crimes cibernéticos.

5 CONSIDERAÇÕES FINAIS

Os crimes realizados no âmbito virtual têm se proliferado de maneira alarmante na sociedade, revelando, assim, uma crescente interdependência entre a tecnologia e as práticas ilícitas. A evolução acelerada das tecnologias digitais, que trouxe inovações significativas para a comunicação, acesso à informação e otimização de tempo, também abriu novas portas para a prática de delitos cibernéticos, incluindo fraudes, roubos de identidade, e crimes como o cyberbullying, linchamento virtual e o popularmente conhecido *"cancelamento".*[57] Esses delitos, ao explorar o anonimato e a facilidade de acesso à internet, apresentam desafios significativos e únicos para a detecção e a responsabilização dos infratores.

Nesse viés a Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann, foi um marco importante na adaptação da legislação penal brasileira à realidade dos crimes cibernéticos, cujo com a inclusão dos artigos 154-A e 154-B ao Código Penal, juntamente com as modificações subsequentes, reflete uma tentativa de endereçar de maneira mais robusta os delitos praticados no ambiente digital. Portanto a contínua atualização das leis é de suma importância para enfrentar a grande agilidade de inovação dos crimes virtuais e garantir uma resposta e aparo legal eficaz.

A relevância da manutenção de provas em crimes cibernéticos não pode ser subestimada, haja vista que a natureza digital desses crimes exige uma abordagem meticulosa na coleta e preservação de evidências, pois a volatilidade e a facilidade de alteração dos dados digitais tornam a manutenção de provas uma tarefa complexa e crítica e muitas vezes impossível. A eficácia da investigação e a possibilidade de uma condenação criminal dependem da integridade e da preservação das provas coletadas, portanto as medidas como o armazenamento seguro de logs, a preservação de dados, a consciência no uso das redes digitais e a utilização de técnicas forenses especializadas são fundamentais para garantir que as evidências não sejam comprometidas.

---

[53] BRASIL, Lei 12.737/12. Brasília: Senado, 30 de novembro de 2012. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm, acessado em 18.09.2024.

[54] BRASIL, Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acessado em 19.09.2024.

[55] BRASIL, Lei 14.155/21. Brasília: Senado, 27 de maio de 2021. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1, acessado em 19.09.2024.

[56] Furtado, Edmilson. *Crimes Cibernéticos: Análise da Lei 14.155/2021 e suas Alterações no Código Penal*. Editora Dialética, 2021.

[57] JUS BRASIL. O cancelamento Virtual e o impacto jurídico. Disponível em https://www.jusbrasil.com.br/artigos/o-cancelamento-virtual-e-o-impacto-juridico/1197014184. Disponível em: https://www.jusbrasil.com.br/artigos/o-cancelamento-virtual-e-o-impacto-juridico/1197014184, acessado em 19.09.2024.

Além disso, a competência para julgar crimes cibernéticos deve ser cuidadosamente determinada, levando em consideração a natureza do delito e o impacto territorial ou internacional, visando a divisão entre a Justiça Federal e Estadual, bem como a coerência na aplicação de normas específicas para crimes contra a honra e outros delitos cibernéticos, os quais, são aspectos essenciais para assegurar um julgamento justo e adequado.

Portanto, a luta contra os crimes cibernéticos exige uma combinação de apoio, atualização e avanços legislativos, estratégias eficazes de coleta e preservação de provas, uma abordagem consciente na sociedade sobre as consequências de seus atos praticados no meio digital, a utilização orgânica das redes sociais, a necessidade de autenticação e verificação de identidade nestas redes, e a coordenada entre diferentes competências nas jurisdições, são fundamentais. A compreensão e a adaptação contínua às mudanças tecnológicas e às novas formas de criminalidade digital são irrefutáveis para garantir a proteção dos direitos e a justiça no ambiente digital.

6 REFERÊNCIAS

ALMEIDA, Marcos. Crimes Cibernéticos e a Nova Lei 12.737/2012: Aspectos Práticos e Teóricos. Editora Lumen Juris, 2018.

AMARAL, Mariana Valente do. *Crimes Digitais e a Responsabilização no Direito Brasileiro*. São Paulo: Thomson Reuters, 2021.

BESSONE, Patricia. *Direito e Tecnologia: O Impacto da Tecnologia na Sociedade e no Direito*. Editora Método, 2020.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal Volume 2, 19 edição. SaraivaJur, 2019.

_____. Tratado de Direito Penal: Parte Especial, v.3, 14 ed., São Paulo: Saraiva Jur, 2018.

BITTENCOURT, Edson. *Crimes Cibernéticos e a Sociedade da Informação*. Editora Juruá, 2017.

BRASIL, Código Civil, de 10 de janeiro de 2002. Lei nº 10.406,2002.

_____. Código Penal, de 7 de dezembro de 1940. DECRETO-LEI Nº 2.848,1940.

_____. Código de Processo Penal, de 3 de outubro de 1941. DECRETO-LEI Nº 3.689,1941.

_____. Constituição da República Federativa do Brasil, de 05 de outubro de 1988. Brasília: Senado, 1988.

_____. Lei 8.069/90. Brasília: Senado,13 de julho de 1990.

_____. Lei 12.737/12. Brasília: Senado, 30 de novembro de 2012.

_____. Lei 13.968/19. Brasília: Senado, 26 de dezembro de 2019.

_____. Lei 14.155/21. Brasília: Senado, 27 de maio de 2021.

_____. CC 121215/PR, Rel. Ministra Alderita Ramos de Oliveira (desembargadora convocada do TJ/PE), TERCEIRA SEÇÃO, julgado em: 12/12/2012, DJe 01/02/2013.

_____. Decreto legislativo nº 28 de 14/09/1990, e do Decreto nº 99.710 de 21/12/1990, a Convenção sobre direitos da Criança adotada pela Assembleia Geral das Nações Unidas.

CAPEZ, Fernando. Curso de Direito Penal. Parte Geral, v.1, 15 ed. São Paulo: Saraiva, 2011.

CEZAR, Dimas. *Direito Penal e Crimes Cibernéticos*. Editora Forense, 2016.

Declaração Universal dos Direitos Humanos, adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948 - UNICEF.

DONEDA, Danilo. Direito à Privacidade e Proteção de Dados Pessoais: A Função e os Limites da Autodeterminação Informativa. 2. ed. Rio de Janeiro: Renovar, 2011.

FILHO, Valmor H., Revista VEJA, Agora é crime: cyberbullying alarma o Brasil, 2º país no mundo em casos, Governo dá importante passo ao criminalizar ataques virtuais, um problema que está perto de se tornar uma epidemia entre os jovens. Disponível em: https://veja.abril.com.br/brasil/agora-e-crime-cyberbullying-alarma-o-brasil-2o-pais-no-mundo-em-casos.

FURTADO, Edmilson. Crimes Cibernéticos: Análise da Lei 14.155/2021 e suas Alterações no Código Penal. Editora Dialética, 2021.

FOLHA DE SÃO PAULO. ROMANI, Bruno. Entenda o caso da invasão hacker à Sony Pictures.

G1, GRAELL e VINCAX, Fernanda, Marcus, Lei Carolina Dieckmann completa 10 anos como marco no combate a crimes cibernéticos.

G1, RAMAL, Andrea, Entenda o 'Jogo da Baleia Azul' e os riscos envolvidos.

G1, REUTERS, Ataque contra a Sony Pictures deve custar US$ 100 mi, diz especialista.
GRECO, Luís Roberto. Direito Penal: Parte Geral. Editora Impetus, 2020.

JUS BRASIL. STJ analisa competência para os chamados crimes informáticos (crimes virtuais = cybercrimes): competência territorial do local de hospedagem do site. Disponível em https://www.jusbrasil.com.br/noticias/stj-analisa-competencia-para-os-chamados-crimes-informaticos-crimes-virtuais-cybercrimes-competencia-territorial-do-local-de-hospedagem-do-site/2659329.

_____. O cancelamento Virtual e o impacto jurídico. Disponível em https://www.jusbrasil.com.br/artigos/o-cancelamento-virtual-e-o-impacto-juridico/1197014184.

_____. Induzimento, instigação e auxílio ao suicídio pelos meios digitais. Disponível em: https://www.jusbrasil.com.br/artigos/induzimento-instigacao-e-auxilio-ao-suicidio-pelos-meios-digitais/1445315086.

_____. Linchamento Virtual: Você conhece? Disponível em https://www.jusbrasil.com.br/artigos/linchamento-virtual-voce-conhece/912335410.

LEITE, Nelson Ferreira: O conteúdo jurídico da responsabilidade penal - Trabalho apresentado, em dezembro de 1962, no Curso de Especialização da Faculdade de Direito, cadeira de Direito Penal Comparado.

LOURENÇO, Ana, O que motiva os linchamentos Virtuais, e quais as consequências desses ataques no mundo real.

MILAGRE, José Antônio; DE JESUS, Damásio. Manual de Crimes Informáticos, 1 edição. Saraiva, 2016.

NODARI, Luana, O que é bullying virtual ou cyberbullying? Perguntas e respostas sobre o bullying na internet. Disponível em: https://psicologaluananodari.com.br/o-que-e-bullying-virtual-ou-cyberbullying-perguntas-e-respostas-sobre-o-bullying-na-internet/.

PINHEIRO, Patrícia Peck. *Direito Digital*. 9. ed. São Paulo: Saraiva, 2019.

PORFÍRIO, Francisco, Brasil Escola, Cyberbullying. Disponível em: https://brasilescola.uol.com.br/sociologia/cyberbullying.htm#:~:text=Consequ%C3%AAncias%20do%20cyberbullying,O%20cyberbullying%20pode&text=Assim%20como%20ocorre%20com%20o,ansiedade%20e%20s%C3%ADndrome%20do%20p%C3%A2nico.

PRADO, Luiz Regis. Curso de Direito Penal Brasileiro: Parte Especial - 14ª Ed. São Paulo: Revista dos Tribunais, 2015.

RAMOS, Paulo; RAMOS, Magda Maria; BUSNELLO, Saul José. **Manual prático de metodologia da pesquisa**: artigo, resenha, projeto, TCC, monografia, dissertação e tese. Blumenau: Acadêmica, 2003, 84p.

ROSSINI, Augusto Eduardo De Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SILVA, Rita de Cássia Lopes da. Direito Penal e sistema informático: Problemas fundamentais. Dissertação Mestrado, Universidade Estadual de Maringá, Maringá, 2002.

SOUZA, José Martins de. Linchamentos: a justiça popular no Brasil. 1. ed. São Paulo: Contexto, 2011.

SOUZA, Renato. *A Justiça e os Crimes Cibernéticos: Jurisprudência e Competência*. Editora Saraiva, 2019.

SZNICK, Valdir. Novos Crimes e Novas Penas no Direito Penal. São Paulo: Livraria e Editora Universidade de Direito, 1992.

TECNOBLOG, CÂMARA, Júlio, Tudo o que você precisa saber sobre os ataques e vazamentos sofridos pela Sony Pictures.