UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE CIÊNCIAS PENAIS

GABRIEL GUAZZELLI BESTETTI

OS DESAFIOS DO DIREITO NO COMBATE AOS CRIMES VIRTUAIS

Porto Alegre
2023

Gabriel Guazzelli Bestetti

OS DESAFIOS DO DIREITO NO COMBATE AOS CRIMES VIRTUAIS

Trabalho de conclusão de curso apresentado como requisito parcial para a obtenção do grau de bacharel em Direito da Universidade Federal do Rio Grande do Sul

Orientador: Professor Dr. Ângelo Roberto Ilha da Silva

Porto Alegre
2023

CIP - Catalogação na Publicação

Bestetti, Gabriel Guazzelli
OS DESAFIOS DO DIREITO NO COMBATE AOS CRIMES VIRTUAIS / Gabriel Guazzelli Bestetti. -- 2023.
54 f.
Orientador: Professor Dr. Ângelo Roberto Ilha da Silva.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Direito, Curso de Ciências Jurídicas e Sociais, Porto Alegre, BR-RS, 2023.

1. Crimes cibernéticos. 2. Crimes virtuais. 3. Crimes digitais. 4. Direito penal. 5. Legislação penal. I. Ilha da Silva, Professor Dr. Ângelo Roberto, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Gabriel Guazzelli Bestetti

OS DESAFIOS DO DIREITO NO COMBATE AOS CRIMES VIRTUAIS

Trabalho de conclusão de curso apresentado como requisito parcial para a obtenção do grau de bacharel em Direito da Universidade Federal do Rio Grande do Sul.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____
Prof. Dr. Ângelo Roberto Ilha da Silva
Orientador

_____
Prof. Dr. Mauro Fonseca Andrade

_____
Prof. Dr. Danilo Knijnik

RESUMO

Os avanços da internet representam um grande marco social, sendo hoje um dos principais e mais importantes meios de comunicação. No entanto, com seu crescimento, cresceu também o número de crimes praticados neste meio. Diante deste fato busca-se responder o seguinte problema de pesquisa: Quais são os crimes cibernéticos previstos no Brasil e quais as maiores limitações encontradas pelos poderes executivo, legislativo e judiciário quanto ao controle desta modalidade criminosa? Sendo objetivo deste estudo abordar os crimes cibernéticos e sua evolução no ordenamento jurídico brasileiro e demonstrar se existem limitações para caracterizar estes crimes conforme a legislação pertinente. Para tanto, foi utilizada a metodologia de revisão narrativa da literatura. A elaboração deste estudo permitiu concluir que a legislação penal com fulcro em combater os cibercrimes passou por uma gama de inovações desde que estes crimes surgiram no ordenamento jurídico. No entanto, mesmo com tantas evoluções ainda existem falhas no que se refere à preparação para lidar com estes crimes diante da capacidade dos criminosos de esquivar-se das investigações, o que traz dificuldades na condenação.

Palavras-chave: Crimes cibernéticos; crimes virtuais; crimes digitais; direito penal; legislação penal.

ABSTRACT

The advances of the internet represent a significant social milestone, being today one of the primary and most important means of communication. However, with its growth, the number of crimes committed in this environment has also increased. Faced with this fact, the following research problem is addressed: What are the cybercrimes foreseen in Brazil and what are the major limitations encountered by the executive, legislative, and judicial powers in controlling this criminal modality? The objective of this study is to address cyber crimes and their evolution in the Brazilian legal system and to demonstrate whether there are limitations in characterizing these crimes according to the relevant legislation. For this purpose, the methodology of narrative literature review was used. The elaboration of this study allowed us to conclude that the criminal legislation aimed at combating cyber crimes has undergone a range of innovations since these crimes emerged in the legal system. However, even with so many developments there are still flaws in terms of preparedness to deal with these crimes given the ability of criminals to evade investigations, which brings difficulties in securing convictions.

Keywords: Cyber crimes; virtual crimes; digital crimes; criminal law; criminal legislation.

SUMÁRIO

1. INTRODUÇÃO

A criação da internet marcou um grande avanço dentro do contexto do mundo globalizado. A cada dia que passa, mais pessoas utilizam-se da internet como meio de informação, para lazer, estudos e até mesmo para fazer compras. Com a popularização dos meios de comunicação digital, como leciona Cunha e Sergl[1], a internet passou a estabelecer novos processos que são reconfigurados a cada novidade no meio do acesso ao conhecimento e desempenham um importante papel dentro da atual conjuntura social, onde as pessoas fazem parte de uma era digitalizada.

Um levantamento realizado pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação em 2020 apontou que, com a pandemia de COVID-19 que chegou ao Brasil no início do mesmo ano, o número de pessoas nas redes aumentou significativamente. A pesquisa revelou um aumento na proporção de usuários de Internet na comparação com 2019, sobretudo entre os moradores das áreas rurais, onde 20% a mais de pessoas passaram a usar internet. Entre os habitantes com 60 anos ou mais o aumento foi um pouco menor, chegando a 14%, entre aqueles com Ensino Fundamental o aumento foi de 13 %, entre as mulheres os índices aumentaram 12% e nas classes mais baixas o aumento foi de 10%[2].

A COVID-19 surgiu no final de 2019 na cidade de Wuhan, província de Hubei, na República Popular da China, e disseminou-se pela Ásia e demais continentes rapidamente, contaminando milhares de pessoas, tornando-se o que conhecemos como a pandemia do coronavírus[3].

Frente à gravidade da doença, o Ministério da Saúde apontou a necessidade de um lockdown, uma vez que este vírus tem uma capacidade de

---

[1] SERGL, M & CUNHA, G. A relação entre o indivíduo pós-moderno, o consumo e a internet das coisas. **Revista Tecnologia e Sociedade**, v 16, n 39, p. 41-56, 2019. p.02.

[2] CETIC, Indicadores. 2021. Disponível em: https://cetic.br/pt/pesquisa/domicilios/indicadores/

[3] Chate R C, et al. Presentation of pulmonary infection on CT in COVID-19: **initial experience in Brazil. J Bras Pneumol**, v.46, n.2, 2020. p.01

disseminação gigante, e é de alta letalidade, principalmente para indivíduos do grupo de risco, levando pessoas de todo mundo a dependerem das redes de internet para se comunicar, trabalhar e estudar[4].

Todo este crescimento das redes traz uma gama de vantagens para os usuários, proporcionando cada vez mais praticidade e facilidade nas tarefas do dia a dia e conectando pessoas em todas as partes do mundo, permitindo novas formas de acesso à informação e entretenimento, além de ampliar os meios de comunicação através das chamadas redes sociais.

O número de pessoas conectadas a essas redes sociais aumenta de forma constante. Em 2020, as redes sociais alcançaram uma taxa de aumento de 40% no uso em plataformas como Facebook, WhatsApp e Instagram, de acordo com a pesquisa do Statista[5].

Da mesma forma, o número de cibercrimes vem aumentando ao longo dos anos. De acordo com o Senado Federal[6], os cibercrimes fazem parte da realidade mundial desde a década de 1990, no entanto, antes do crescimento do uso de internet e das redes sociais estes crimes eram mais comuns nas camadas mais profundas da internet, a Deep Web e a Dark Web. Porém, a evolução das redes de acesso comum e o maior número de usuários fizeram desta um alvo de interesse dos cibercriminosos, aumentando ainda mais a necessidade de regulamentar a punição destes crimes.

Sendo assim, este estudo busca responder os seguintes problemas de pesquisa: Quais são os crimes cibernéticos previstos no Brasil e quais as maiores limitações encontradas pelos poderes executivo, legislativo e judiciário quanto ao controle desta modalidade criminosa?

Neste contexto, trabalha-se com a hipótese de que no Brasil a evolução tecnológica favorece a comunicação, a liberdade de expressão e traz inúmeras

---

[4] CORREIA, M; RAMOS, R F & BAHTEN, L. Os cirurgiões e a pandemia do COVID-19. **Revista do Colégio Brasileiro de Cirurgiões**, v. [s.i] n. [s.i]. p. 1 – 6. 2020, p.03

[5] STATISTA. Number of internet and social media users worldwide. Disponível em: https://www.statista.com/statistics/617136/digital-population-worldwide/

[6] Senado Federal. Aprovada adesão do Brasil a convenção sobre crimes cibernéticos online. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico

benfeitorias na sociedade, mas também possibilita o aumento da prática de diversas formas de condutas maliciosas, que necessitam ser discutidas e punidas para garantir a segurança de toda sociedade em âmbito virtual.

O objetivo geral da pesquisa é abordar os crimes cibernéticos e sua evolução no ordenamento jurídico brasileiro, bem como demonstrar se existem limitações para caracterizar estes crimes conforme a legislação pertinente. Para atingi-lo definiu-se como objetivos específicos discorrer acerca da evolução da internet e dos cibercrimes no Brasil; discorrer acerca dos crimes de ódio; crimes contra a honra; o dano informático; o estelionato; a pornografia infantil e o estupro virtual, e demonstrar a evolução da legislação de controle dos crimes cibernéticos no Brasil até o ano de 2022.

Este estudo justifica-se pelo fato de que atualmente, a internet tem sido utilizada para inúmeras finalidades, sendo habitualmente utilizada para atividades comerciais e comunicação rápida entre pessoas em diversos lugares no mundo, o que torna, também, este meio propício para a prática de diversos tipos de crimes. Assim, é indispensável discutir a magnitude dos mesmos, suas modalidades e as medidas de contenção presentes no ordenamento jurídico, bem como se existem limitações para contê-los e quais seriam. A escolha do tema foi motivada pelo perceptível crescimento da internet e o aumento da ocorrência de cibercrimes, fazendo deste um tema atual e que apresenta uma grande relevância social.

Tanto as medidas de prevenção como as medidas de penalização são importantes no controle dos casos de crimes virtuais. Desta maneira, visa-se contribuir com o tema apontando a problemática atual e as possíveis estratégias para controle desta adversidade.

Para tal, foi realizada uma pesquisa através do método de revisão de literatura que consiste na busca de um conteúdo científico específico, com análise e descrição dos resultados. A literatura engloba todo material relevante com o tema, como artigos, livros, documentos, sites, teses, periódicos, entre outros.

Especificamente, baseia-se na revisão narrativa, que tem como característica a não utilização de critérios explícitos e sistemáticos para a realização de buscas, análises e descrições. Neste tipo de metodologia, não se

aplicam estratégias complexas. Tanto a seleção de pesquisas quanto a interpretação dos resultados podem variar de acordo com a subjetividade do pesquisador.

A fim de subsidiar o levantamento bibliográfico acerca do escopo deste estudo, como fontes de pesquisa foram utilizadas as bases de dados do Google Acadêmico, revistas jurídicas, doutrinas, jurisprudências e outros sites que disponibilizaram assuntos relacionados ao tema. Os termos de busca utilizados foram: cibercrimes; crimes cibernéticos; legislação e internet. Assim, foram selecionados apenas artigos e documentos que, após a leitura, apresentavam conteúdo relevante.

O primeiro tópico tem o escopo de conceituar internet e crimes cibernéticos, bem como contar um pouco de suas histórias para que se possa futuramente discorrer acerca dos crimes virtuais em espécie e quais os maiores desafios do combate deste tipo de crime.

Já o segundo tópico visa discorrer acerca das classificações e dos tipos de crimes cibernéticos uma vez que já se discutiu sobre suas origens e conceitos.

Por fim, no terceiro tópico, será analisada a legislação existente acerca dos crimes cibernéticos, a fim de apontar os avanços legislativos percebidos nos últimos anos, em especial a Lei nº 14.155 de 2021, por ser considerada um marco legislativo no que tange ao combate dos cibercrimes.

2. A HISTÓRIA DA INTERNET E DOS CRIMES CIBERNÉTICOS NO BRASIL

O presente capítulo tem o escopo de conceituar internet e crimes cibernéticos, bem como contar um pouco de suas histórias para que se possa, então, discorrer acerca dos crimes virtuais em espécie e quais os maiores desafios no seu combate.

A sociedade passa por constantes evoluções e revoluções, e, dentre elas, algumas se destacam. No período mais recente da nossa história, passamos por uma grande revolução, a Revolução Digital, entendida como "o movimento de inserção na sociedade de novas tecnologias e serviços que utilizam desenvolvimentos recentes e que modificam a forma como o cotidiano cidadão progride".[7]

Os computadores e a internet surgiram para facilitar o cotidiano das pessoas. As tarefas, que antes eram realizadas em espaços de tempo muito longos, passaram a ser realizadas quase de forma instantânea. O computador é uma máquina que armazena e transforma informações, sob o controle de instruções predeterminadas.

Os benefícios da internet são gigantescos. O tráfego de informações que passam pelas redes diariamente proporciona aos internautas grande comodidade nas cidades com problemas de mobilidade ou num lugar longínquo do planeta desde que conectado à internet. Quem está conectado tem a sensação de inteiração e convivência.

A internet que conhecemos hoje passou por uma longa jornada até se tornar a rede pública que usamos para navegar, tendo iniciado como mecanismo criado por militares.

No ano de 1962, em pleno auge da Guerra Fria, um grupo de pesquisadores americanos vinculados a uma instituição militar decidiu dar vida a um sistema imune a bombardeios, que fosse capaz de interligar muitos

[7] SYDOW, S T. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. p. 7. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf. Acesso em: 22 jul. 2023.

computadores, permitindo o intercâmbio e o compartilhamento de dados entre eles[8].

Levaram pelo menos sete anos para que tal projeto saísse do papel, dando origem à primeira versão desse sistema que se chamava ARPANET (Advanced Research Projects Agency ou Agência de Projetos de Pesquisa Avançada), e sua principal característica era não possuir um comando central, de modo que, em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando[9].

A ideia de seu criador era construir uma rede em que cada equipamento seria relativamente autônomo e a comunicação se daria de modo distribuído. Com uma organização desse tipo, pedaços da rede que não fossem afetados por uma agressão poderiam manter-se em operação. Esse projeto recebeu o nome de ARPANET e deu origem à internet que conhecemos atualmente.

O nome Internet que conhecemos hoje surgiu na década seguinte, quando a tecnologia desenvolvida passou a ser usada para conectar universidades americanas entre si, e depois também institutos de pesquisa sediados em outros países. A ideia central, porém, permaneceu a mesma: uma espécie de associação mundial de computadores, todos interligados por meio de um conjunto de regras padronizadas que especificam o formato, a sincronização e a verificação de erros em comunicação de dados.

Comercialmente, no Brasil, a internet passou a ser utilizada na década de 1990, quando a Agência Nacional de Telecomunicações (Anatel), com o objetivo de regulamentar o uso de meios da Rede Pública de Telecomunicações e os Serviços de Conexão à Internet, através da Norma 004/1995, regulamentou seu uso:

> Internet é o nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores.[10]

---

[8] LINS, B F E. **A evolução da Internet: uma perspectiva histórica**. Brasília: Associação dos Consultores Legislativos e de Orçamento e Fiscalização Financeira da Câmara dos Deputados. 2013. p.22

[9] Ibdem. p.23

[10] BRASIL. **Portaria nº 148, de 31 de maio de 1995**. Disponível em: https://www.cgi.br/portarias/ano_numero/1995/148/ Acesso em: 06 ago. 2023.

Naquele ano, em Nota Conjunta divulgada pelo Ministério das Comunicações e pelo Ministério da Ciência e Tecnologia, foram passadas para a sociedade em geral as primeiras informações a respeito da introdução da internet no Brasil. A nota pública conjunta afirmava que: “O Governo considera de importância estratégica para o País tornar a INTERNET disponível a toda a Sociedade, com vistas à inserção do Brasil na Era da Informação”.[11]

É a partir deste momento que surge a internet que conhecemos hoje e é inegável que a Tecnologia da Informação e Comunicação (TIC) está cada vez mais presente na rotina das empresas e da maioria da população urbana.

De um ponto de vista histórico, Porter e Millar definem a relevância da cadeia de valor desde muito antes da mesma tomar tamanha proporção. Os autores já apontavam, dez anos antes da internet ser conhecida no Brasil, que ela geria novos negócios inteiros, muitas vezes de dentro das operações existentes na própria empresa, além de criar vantagens competitivas e mudar a estrutura da indústria, alterando as regras de competição[12]. Tais características foram, em grande parte, as responsáveis pela propagação das novas tecnologias.

No mesmo sentido, o estudo de Ianni já apontava que a internet era fruto das novas tecnologias, dentre elas a informática, a eletrônica e as telecomunicações. Se utilizada com sabedoria, levaria a uma nova ordem organizacional do tempo e do espaço, envolvendo capitais, pessoas e informações, dando ensejo a uma revolução tecnológica e gerando um impacto indiscutível no processo de globalização[13].

Atualmente, as pessoas estão acostumadas com a internet. Na verdade, a maioria da população já não sabe viver sem TIC, seja para trabalhar, para realizar compras, para se divertir, para se comunicar, para realizar vendas;

---

[11] Ibdem

[12] PORTER, M E. & MILLAR, V E. How information gives you competitive advantage. Harvard Business Review, Boston, Jul/Aug 1985, p. 02

[13] IANNI, O. Globalização: novos paradigmas das ciências sociais. **Estudos avançados**. v. 8, n. 21, 1994, p.149

enfim, uma infinidade de possibilidades é viável graças ao universo virtual em que a sociedade está inserida hoje em dia.

Informações do Instituto Brasileiro de Geografia e Estatística [IBGE] apontam que 82,7% dos domicílios brasileiros utilizam a internet; ou seja, a grande maioria da população está navegando, seja pelo celular, pelo computador, pelo tablet, pela tv, pelo console ou até mesmo pela geladeira[14].

Tamanha é a proporção tomada pela internet que a mesma passou a ser considerada um Direito Humano, de acordo com a Organização das Nações Unidas (ONU). O acesso à internet é um direito fundamental para a informação, porém enseja proteção das ações danosas e das falhas de segurança a que estão sujeitos os usuários, ante a grande habilidade tecnológica de internautas mal-intencionados, em especial dos *hackers* e *crackers*, que, em razão de seus conhecimentos técnicos, podem impedir, com um único ataque, o acesso de milhares ou milhões de internautas a serviços disponibilizados por meio da internet.

Os benefícios da internet são indiscutíveis. O trânsito de informações e transações através da web promove uma grande comodidade nas cidades com problemas de mobilidade ou em lugares longínquos do planeta.

Frente a este fato, o Ministério Público Federal (MPF) aponta que, devido à nova realidade, a tecnologia vem evoluindo em uma escala inigualável. No entanto isso não resulta apenas em melhorias para os padrões de vida mundiais, mas também facilita a consecução de diversas modalidades criminosas, entre elas a criação de um dos crimes mais infames da sociedade moderna: a pornografia infantojuvenil[15].

Assim sendo, é possível observar que, apesar dos benefícios, o uso crescente da internet abre espaço para práticas obscuras neste ambiente diferenciado. A disseminação de cibercrimes, que se tornam cada dia mais

---

[14] Instituto Brasileiro de Geografia e Estatística [IBGE]. Internet já é acessível em 90,0% dos domicílios do país em 2021. **IBGE**. 2021. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021.

[15] BRASIL. MINISTÉRIO PÚBLICO FEDERAL. **Crimes cibernéticos**.2° ed. Editora 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.

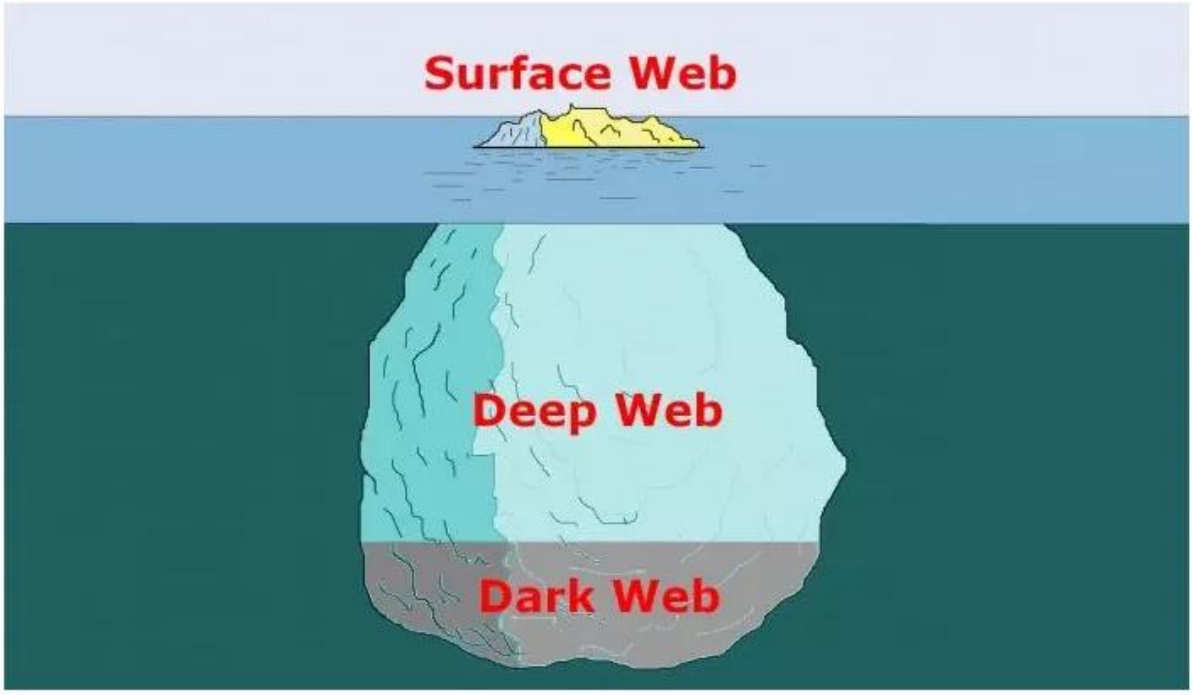
comuns, apresenta riscos iminentes para todos os usuários das redes de informação.

Apesar de a internet já existir há bastante tempo e ter conquistado um espaço gigantesco na vida de todos os indivíduos, ainda restam muitos desafios, pois estes crimes são praticados em um espaço diferente do espaço físico em que vivemos, o que muitas vezes acaba trazendo dificuldades para os agentes públicos acerca da investigação do crime, por exemplo.

Este espaço é chamado de Ciberespaço e, conforme explica um documento elaborado pela Escola de Magistrados da Justiça Federal, não abrange um espaço físico ou geográfico, mas representa uma construção social feita à imagem e semelhança do mundo em que vivemos. O ciberespaço conecta redes, equipamentos e principalmente pessoas.

Costuma-se dividir o ciberespaço em três camadas que se assemelham a um *Iceberg* (FIGURA 1): o primeiro espaço consiste na internet que todos temos acesso e é conhecida como internet pública; a segunda camada é a Deep Web e a terceira consiste na Dark Web.

Figura 1: As camadas da internet[16]



[16] Deep web e Dark Web: qual a diferença? **Tecnoblog**. 2019. Disponível em: https://tecnoblog.net/responde/deep-web-e-dark-web-qual-a-diferenca/

Este primeiro espaço consiste na internet que usamos diariamente, onde o acesso é livre para todos os usuários. No entanto, existem outras duas camadas mais profundas do ciberespaço, a Deep Web e a Dark Web, dois objetos distintos que muitas vezes são vistos congêneres pois são comumente utilizados para práticas criminosas.

A Deep Web representa uma camada exponencial de dados que não deveriam ser acessados e uma pluralidade de materiais oriundos de práticas criminosas, com qualidade substancial. Os conteúdos da Deep Web permanecem escondidos, mas, vez ou outra são encontrados e a invisibilidade é dissipada[17]. Para se ter acesso aos mesmos, o indivíduo precisa conhecer ou encontrar a URL correta, cadastrar-se ou realizar pagamentos para acesso, ou, ainda, utilizar mecanismos de busca específicos que demonstrem resultados. Acredita-se que esta dificuldade em acessar os dados da Deep Web contribua para a prática de crimes neste ambiente[18].

Existe, ainda, uma camada mais profunda na internet, cuja criminalidade se dissemina livremente, chamada de Dark Web. As teorias acerca da Dark Web surgiram com uma tese de doutorado intitulada "*Distributed Decentralised Information Storage and Retrieval System",* criada pelo pesquisador Ian Clarke, na Edinburgh University, em 1995[19].

O grande índice de criminalidade na Dark Web se dá pelo fato de que Clarke desenvolveu um mecanismo para que as pessoas utilizassem esta camada mais profunda da Internet sem serem detectadas. Sua pretensão era distribuir gratuitamente o software criado para que qualquer pessoa pudesse

---

[17] VIGNOLI, R. G. A topografia da dark web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço. 2014. 153 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual de Londrina, Londrina, 2014. Disponível em: http://www.bibliotecadigital.uel.br/document/?view=vtls 000191992. Acesso em: 19 jul. 2023

[18] Ibdem

[19] BECKETT, A. The dark side of the internet: in the 'deep web', Freenet software allows users complete anonymity as they share viruses, criminal contacts and child pornography. The Guardian. Reino Unido, 26 Nov. 2009. Disponível em: https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. Acesso em: 04 ago. 2023.

conversar, ler ou configurar um site, até mesmo compartilhar arquivos anonimamente.

De acordo com Heaven[20], foi essa falta de rastreamento e a privacidade excessiva encontrada na Dark Web que fez dela um atrativo para a realização de crimes. Contudo, proporciona, também, uma navegação tranquila, sem observadores em busca do melhor cliente para a aquisição de seus produtos e com elevada privacidade. Além disso, dificulta a espionagem e a invasão de privacidade recorrentes na superfície, bem como o conhecimento por parte das empresas sobre quem visita suas páginas.

2.1 BREVES APONTAMENTOS SOBRE O CIBERCRIME E OS CIBERCRIMINOSOS

Com o crescimento do uso da internet e das redes, até mesmo em suas zonas mais seguras, a internet pública se depara com condutas que violam o ordenamento e apresentam algum tipo de ameaça aos bens jurídicos tutelados. Este tipo de crime é conhecido como cibercrime ou crimes cibernéticos.

Os crimes cometidos no ciberespaço são chamados atualmente de cibercrimes, uma vez que para alguns doutrinadores a expressão crime digital seria ampla demais. Por isso aposta-se no termo “Cibercrime”, que se refere às novas tecnologias. Por esta razão, é a nomenclatura utilizada pelo Acordo Internacional do Conselho da Europa[21].

Segundo Aras:

> Embora existam várias expressões para designar ou aludir aos ilícitos virtuais, as mais recorrentes são crimes informáticos ou crimes de informática, ou cibercrime, pontuando que “crimes telemáticos" ou "cibercrime" são expressões mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias[22]

[20] HEAVEN, D. Unpicking the mythologies around the dark web. **NewScientist**, v. 240, n. 3209-3210, p. 82-83, 2018.

[21] CRESPO, Marcelo Xavier de Freitas. **O cibercrime.** São Paulo: Saraiva, 2011.

[22] ARAS, Vladimir. Crime de Informática. Uma Nova Criminalidade. **Jus Navigandi**. Teresina, ano 6, n. 51, outubro de 2001. p. 06.

Existem diversas condutas ilícitas que podem ocorrer dentro do meio cibernético. Podem ocorrer desde condutas meramente antiéticas até a prática de crimes propriamente ditos, como conduta antijurídica, lesiva e punível[23].

Os crimes cibernéticos, em sua maioria, são crimes comuns cometidos com o auxílio de um computador ou outro meio tecnológico, entretanto, há algo além de uma nova ferramenta, de um novo meio, de um novo modus operandi para o cometimento de crimes[24].

Com o crescimento do uso da internet, é comum que tenha aumentado simultaneamente o número de crimes praticados nas redes. Pensando nisso, foi criado um sistema de denúncias para crimes cibernéticos, a *Safernet.*

A Safernet é responsável pelo monitoramento de denúncias de crimes virtuais e aponta que, em 2021, a Central de Denúncias recebeu e processou 150.095 denúncias anônimas envolvendo 71.095 páginas distintas ao redor do mundo. O número, segundo a Safernet, é 60,7% maior que no ano anterior[25].

> A Central Nacional de Denúncias de Crimes Cibernéticos da Safernet existe há 16 anos e é o hotline da Safernet Brasil, que recebe denúncias anônimas de crimes e violações contra os Direitos Humanos na Internet, que são encaminhados de forma transparente às autoridades. Caso você encontre imagens, vídeos, textos ou qualquer outro tipo de material que seja atentatório aos Direitos Humanos, faça a sua denúncia[26]

No mesmo sentido, Alexandre Junior aponta que:

> O Brasil está entre os principais centros de criminalidade praticados em meios cibernéticos ou cibercrimes. O nosso País está em segundo lugar na classificação mundial de fraudes bancárias online e malware financeiro, o que é um dado alarmante para os dias atuais. De acordo com a publicação do renomado Jornal, o número de ataques cibernéticos no Brasil cresceu, assustadoramente, em 197% (cento e

---

[23] KUNRATH, Josefa Cristina Tomaz Martins **A expansão da criminalidade no ciberespaço**. Feira de Santana: Universidade Estadual de Feira de Santana, 2017.

[24] FERREIRA, I. S. Direito & Internet: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: QuartierLatin. 2005.

[25] SAFERNET. Denúncias de neonazismo à Safernet aumentam 60% em um ano. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-neonazismo-safernet-aumentam-60-em-um-ano. Acesso em: 10 jun. 2023.

[26] Ibdem

> noventa e sete por cento) em 2014, e as fraudes bancárias online, 40% (quarenta por cento)[27]

Diante da alta tecnologia da internet atual, as relações que ocorrem no ciberespaço apresentam várias características, dentre as quais se destacam a instantaneidade, superando as barreiras de tempo e espaço; a aparente igualdade dos internautas, ressalvadas as condições pessoais quanto aos conhecimentos tecnológicos; a infinidade e diversidade de informações em texto, sons, imagens e a sensação de anonimato. No entanto, é possível que todas essas vantagens tornem a internet um lugar mais propício para a prática de crimes[28].

Os dados citados deixam clara a proporção tomada pelos crimes cibernéticos. Neste sentido, é importante observar que as condutas ilícitas praticadas no meio cibernético vêm gerando números preocupantes e são bastante diversas, passando por condutas antiéticas até a prática de crime propriamente considerado, como conduta antijurídica, lesiva e punível. São, portanto, incontáveis as condutas ilícitas possíveis de ocorrer no meio cibernético ou, através dele, abrangendo larga gama de delitos possíveis de se cometer na realidade física[29].

A autora aponta, ainda, que existem alguns procedimentos ilícitos que só podem ser realizados através dos meios eletrônicos, por sua especificidade, ou, como na maioria dos casos, porque o bem juridicamente relevante é fruto da uma relação gerada na rede e só existe nesse espaço imaterial[30].

Além disso, é importante observar que, das características das infrações penais cometidas fora do ambiente virtual, são identificadas as efetuadas através do uso de dispositivos tecnológicos. A Organização para Cooperação

---

[27] ALEXANDRE JUNIOR, J C. **Cibercrime:** um estudo acerca do conceito de crimes informáticos. Revista Eletrônica da Faculdade de Direito de Franca. v. 14, n.1, p. 341-351, 2019, p. 343.

[28] FURLANETO NETO, M; SANTOS, J E L; GIMENES, E V. Crimes na internet e inquérito policial eletrônico. São Paulo: EDIPRO, 2012.

[29] KUNRATH, Josefa Cristina Tomaz Martins **A expansão da criminalidade no ciberespaço**. Feira de Santana: Universidade Estadual de Feira de Santana, 2017

[30] Ibdem

Econômica e Desenvolvimento da Organização das Nações Unidas (OCDE), em 1983, trouxe a seguinte definição para os cibercrimes: “qualquer conduta ilegal, não ética, ou não autorizada que envolva processamento automático de dados e/ou a transmissão de dados”[31].

É diante disso que surge a necessidade de regulamentação da internet, pois desde a sua criação, uma das maiores discussões é a respeito da necessidade ou não de regulamentação desse ambiente que nasceu, a princípio, sem nenhum controle impositivo[32].

Após esta breve apresentação da evolução da internet no Brasil, bem como a definição de cibercrime, cabe discorrer brevemente sobre os cibercriminosos, ou seja, os indivíduos que praticam crimes em no ciberespaço. A importância de tal abordagem se dá pelo fato de que muitas pessoas desacreditam que crimes cometidos na internet são impunes, o que não condiz com a verdade.

Neste sentido, aquele que pratica conduta típica, antijurídica e culpável constitui os elementos de crime, e será processado, julgado e punido pela conduta praticada. O mesmo ocorre com o sujeito que pratica tal ato virtualmente, sem qualquer distinção oriunda do ambiente utilizado[33].

Os cibercriminosos, no entanto, têm a internet a seu favor, já que na grande maioria de suas práticas, estes criminosos se encontram muitas vezes em locais distintos, dificultando a sua localização.

> O carácter transfronteiriço destas infracções entra em conflito com a territorialidade das autoridades nacionais competentes para a aplicação da lei. As legislações nacionais estão confinadas a um território delimitado, pelo que se torna cada vez mais importante que exista legislação internacional[34].

---

[31] JESUS, D de; MILAGRE, J A. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

[32] PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2014

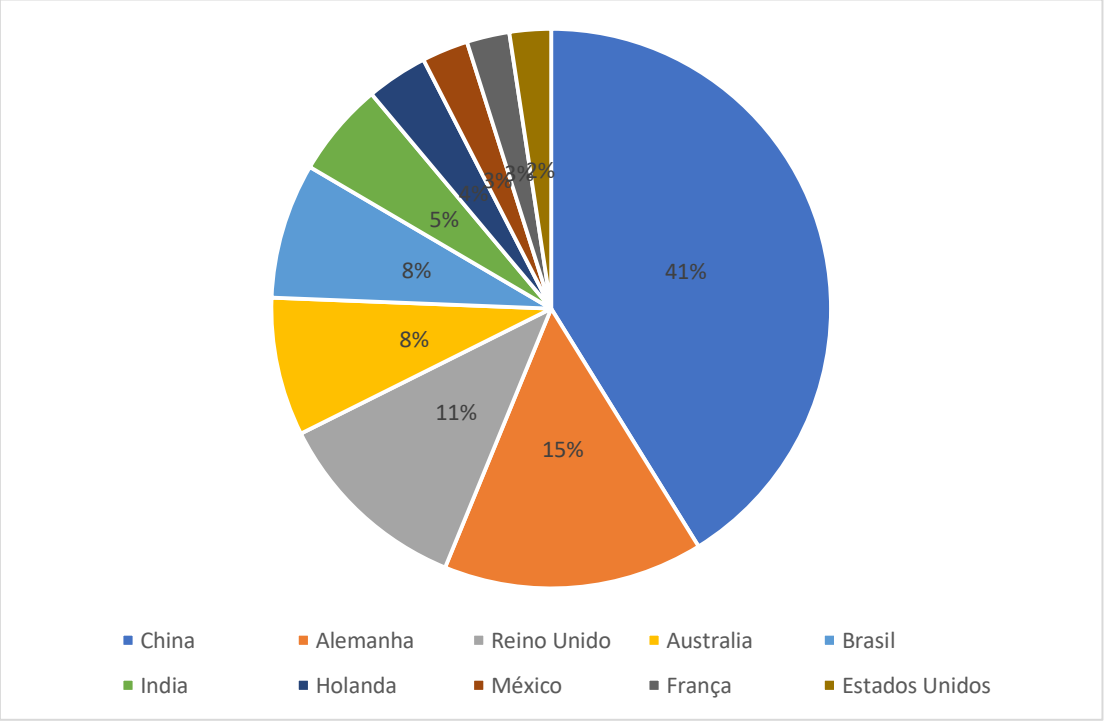
[33] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** Campinas, SP: Ed. Millennium, 2005.

[34] KUNRATH, Josefa Cristina Tomaz Martins **A expansão da criminalidade no ciberespaço**. Feira de Santana: Universidade Estadual de Feira de Santana, 2017

Como já dito anteriormente, o número de crimes cometidos pela internet demonstra um constante aumento em seus índices, ao mesmo passo que os cibercriminosos parecem estar cada dia mais atentos às novas tecnologias e formas de cometer seus crimes de uma maneira que dificulte a atuação legal.

Dados preocupantes foram divulgados no relatório Internet Crime Complaints Center de 2022, onde o Brasil apareceu como o quinto país com maior prejuízo econômico gerado por cibercrimes, como demonstra o gráfico a seguir:

Gráfico 1: Países com maior prejuízo econômico gerado por cibercrimes



Assim, é possível concluir que o crescimento imensurável da internet desde seu surgimento, tornando-a um dos principais meios de comunicação da atualidade, trouxe inúmeras vantagens para a sociedade. Entretanto, esta evolução também trouxe consigo os crimes cibernéticos, que nos últimos anos vêm crescendo e gerando preocupação, dada a sua complexidade.

3. AS CLASSIFICAÇÃO E OS TIPOS DE CRIMES CIBERNÉTICOS

Existem dúvidas e impasses doutrinários acerca da classificação destes crimes, no entanto, para a realização deste trabalho serão utilizadas as teorias de Furlaneto e Guimarães[35]. Nesta classificação os crimes cibernéticos são classificados em Puros, Mistos e Comuns. Além da classificação de Ferreira e Greco Filho, que se preocupam em subdividi-los em próprios e impróprios. A escolha das teorias se deu pelo fato de serem as mais adotadas dentre os doutrinadores do direito cibernético.

3.1 CLASSIFICAÇÃO DOS CRIMES CIBERNETICOS

Primeiramente, classificam-se como crimes cibernéticos puros aqueles cujo principal objetivo é atingir diretamente o sistema de informações, seja através da invasão de sistemas e computadores de forma não autorizada, obtendo acesso a dados ou informações secretas ou destruindo computadores com o uso de softwares mal-intencionados chamados de vírus[36].

Por sua vez, nos crimes cibernéticos comuns, a internet e os sistemas de informação não são os objetos do crime, mas sim meros meios, isso é, a Internet é utilizada apenas como meio para que se possa realizar determinado delito que já se enquadra na Lei Penal. A Internet é vista apenas como mais um meio para realização deste delito[37].

Nos crimes cibernéticos mistos, observa-se que a finalidade do indivíduo que pratica o crime não é prejudicar o sistema de informação digital, mas este ainda é um meio essencial para a consumação do ato.

---

[35] FURLANETO NETO, M; GUIMARÃES J. A C. Crimes na internet: Elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003

[36] Ibdem

[37] Ibdem

Já Ferreira e Greco Filho adotam a classificação que divide os crimes cibernéticos em crimes próprios, condutas praticadas contra os bens jurídicos informáticos; e crimes impróprios, condutas praticadas contra os bens jurídicos tradicionais, como abordado a seguir[38] [39].

No que tange à classificação como próprios ou impróprios, conforme explica Túlio Lima Vianna, os crimes cibernéticos próprios são aqueles que só podem ser praticados através do uso de internet, ou seja, a execução do crime e a consumação ocorrem nesse meio, trata-se de tipos novos em que o bem jurídico tutelado é a própria internet. São os crimes praticados contra os dados da vítima obtidos em seus meios de comunicação digital, seja computador, tablet ou smartphone. Neste sentido, o autor aponta que "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)."[40]

Já os crimes cibernéticos impróprios, são aqueles que são tipificados no Código Penal, uma vez que não violam o sistema de informações e sim os bens jurídicos comuns tutelados pelo CP. Estes crimes ferem a dignidade da pessoa humana.

Com relação ao patrimônio tutelado, existe dificuldade para reconhecer os crimes cibernéticos impróprios, pois não se pode tipificar a informação armazenada como um bem material, pois trata-se de bens imateriais, insuscetíveis de apreensão como objeto.

Vianna cita um exemplo que nos permite elucidar a informação:

> Um exemplo de crime cibernético impróprio são os crimes de transferência de valores em contas bancárias realizadas por terceiros através da violabilidade do sistema de informações dos bancos, no qual os criminosos utilizam-se dos sistemas informáticos apenas como animus operandi, ou seja, furtando dinheiro da conta da vítima através de um sistema interligado à internet[41].

---

[38] GRECO FILHO, V. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim, São Paulo: IBCCrim, n. 95, ano 8, out. 2000. p. 5.

[39] FERREIRA, I. S. Direito & Internet: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: QuartierLatin. 2005, p. 72.

[40] VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro, Editora Forense. 2009. p.43.

[41] Ibdem. p.44.

Uma vez abordadas as principais classificações dos crimes cibernéticos pela doutrina falar-se-á acerca de seus tipos, ou seja, quais são os crimes cibernéticos respaldados pelo ordenamento jurídico brasileiro.

3.2 TIPOS DE CRIMES CIBERNÉTICOS

Salienta-se que, devido ao grande número de pessoas que navegam nas redes de internet e a imensurável quantidade de dados nas redes, fica impossível descrever todas as possibilidades de atos ilícitos que podem ser praticados. No entanto, busca-se descrever a seguir os mais comuns previstos no ordenamento jurídico.

É importante observar que, à medida que a realidade virtual se torna mais acessível, a ocorrência de interações criminosas entre usuários aumenta também. Globalmente, o número de indivíduos que interagem no mundo virtual é estimado em dezenas de milhões e, como resultado do aumento, é fundamental que se passe a regulamentar cada vez mais atitudes praticadas neste ambiente que seriam consideras crimes fora do mundo virtual também.

3.2.1 Crimes de ódio

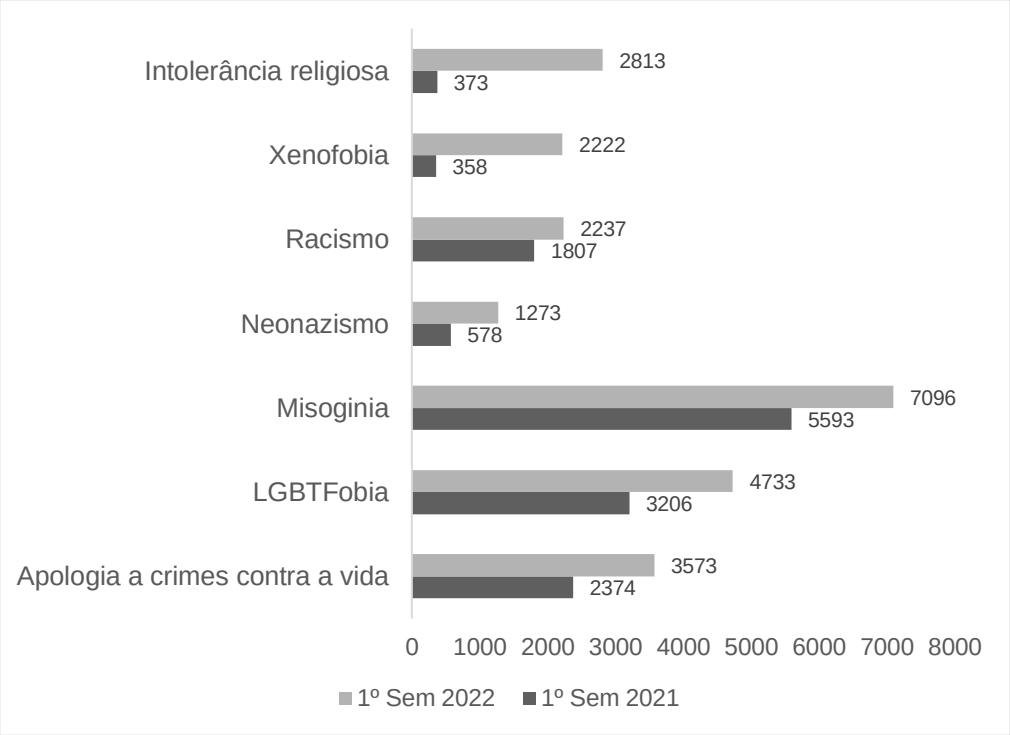
Os crimes de ódio dizem respeito a crimes cometidos diretamente contra um grupo de pessoas ou uma única pessoa devido a características da sua identidade, seja pela sua raça, cor, religião, deficiência, orientação sexual ou origem nacional, sendo que estes ataques são habitualmente marcados por grande violência[42].

Os indicadores da Central Nacional de Denúncias da Safernet registraram mais denúncias de racismo, LGBTfobia, xenofobia, neonazismo, misoginia, apologia a crimes contra a vida e intolerância religiosa no primeiro semestre de

[42] CHENG, W. The phenomenon of hate crimes. **Journal of Applied Social Psychology**, n. [S.l], v.43, 2013.

2022, em relação ao mesmo período do ano anterior[43], conforme verificado no gráfico abaixo.

Gráfico 2: Incidência de crimes de ódio (2021 – 2022)[44]



Os dados supramencionados permitem observar que o crime que mais se destacou foi o crime de misoginia. A misoginia refere-se a um sentimento de ódio, desprezo ou preconceito em relação às mulheres com base em seu gênero. Implica em uma atitude negativa e hostil em relação às mesmas, bem como uma crença na sua inferioridade em relação aos homens.

A misoginia pode se manifestar de várias maneiras, desde atitudes sutis e discriminatórias até comportamentos mais evidentes e agressivos. Pode ser encontrada em diferentes contextos sociais, culturais e geográficos, e pode

[43] SAFERNET. CRIMES NA WEB: Crimes de ódio têm crescimento de até 650% no primeiro semestre de 2022. **SAFERNET**. 2022. Disponível em: https://new.safernet.org.br/content/crimes-de-odio-tem-crescimento-de-ate-650-no-primeiro-semestre-de-2022. Acesso em: 10 jul. 2023.

[44] Ibdem

influenciar a forma como as mulheres são tratadas na sociedade, bem como as oportunidades que lhes são oferecidas[45].

É importante observar que a misoginia é um problema grave e prejudicial que afeta a igualdade de gênero e o respeito a todas as pessoas, independentemente de seu gênero. Nos últimos anos, houve um foco maior no combate à misoginia e na promoção da igualdade de gênero em todo o mundo.

Cabe mencionar que, apesar de misoginia ainda não ser considerada crime, foi proposto o projeto de Lei 890/23 que prevê a punição por crimes resultantes de discriminação ou preconceito por práticas misóginas. O projeto em tela define misoginia como discriminação, preconceito, propagação do ódio ou aversão praticados contra mulheres por razões da condição de sexo feminino[46].

Além da misoginia, a LGBTfobia ou homofobia também apresenta índices alarmantes no que se refere ao total dos crimes de ódio praticados no ciberespaço em 2022. Este crime consiste no ódio ou discriminação contra indivíduos que se identificam como lésbicas, gays, bissexuais, transgêneros ou outras orientações ou gênero não heteronormativos. Este tipo de discriminação pode manifestar-se de diversas formas, como abuso verbal, violência física, exclusão social, tratamento desigual e até mesmo restrições legais aos direitos dos indivíduos LGBTQ+[47].

É importante notar que o termo homofobia deve ser entendido não apenas como ódio, mas também os preconceitos sistêmicos, culturais e sociais que contribuem para a marginalização das pessoas LGBTQ+.

Tamanho é o impacto da homofobia na vida da população LGBTQ+ que, em junho de 2019, o Supremo Tribunal Federal (STF), através da Ação Direta

---

[45] MOTERANI, G M B, Carvalho, F M De. Misoginia: A Violência Contra A Mulher Numa Visão Histórica e Psicanalítica. **Avesso do avesso** v.14, n.14, p. 167-178, novembro 2016

[46] Proposta que criminaliza misoginia começa a tramitar no Senado. **AGÊNCIA SENADO**. 2023. Disponível em: https://www12.senado.leg.br/noticias/materias/2023/03/07/proposta-que-criminaliza-misoginia-comeca-a-tramitar-no-senado. Acesso em: 16 ago. 2023.

[47] TAGLIAMENTO, G.; SILVA, S. S. C. da; SILVA, D. B. da; MARQUES, G. de S.; HASSON, R.; SANTOS, G. E. dos. Minha dor vem de você: uma análise das consequências da LGBTfobia na saúde mental de pessoas LGBTs. **Cadernos de Gênero e Diversidade**, *[S. l.]*, v. 6, n. 3, p. 77–112, 2021.

de Inconstitucionalidade por Omissão (ADO) nº 26, de relatoria do ministro Celso de Mello, decidiu em favor da criminalização da LGBTfobia de forma equiparada ao racismo, até o Congresso Nacional elaborar legislação específica sobre o tema[48].

Além destes, percebeu-se um aumento significativo no que se refere aos crimes de xenofobia, racismo e neonazismo praticados virtualmente, se comparado aos dados do ano anterior. A soma total do aumento dos crimes de ódio praticados no ciberespaço no ano de 2022, se comparados a 2021, chega a 650%, segundo a Safernet[49].

3.2.2 Crimes contra a honra

A Internet cada vez mais vem assumindo um papel de importante ferramenta no que diz respeito à liberdade de expressão de ideias e informações. Com o crescimento desenfreado das redes sociais, as pessoas cada vez mais expõem seus pensamentos e ideias na internet, porém existem situações em que esta exposição pode acarretar num ilícito penal contra a honra de outrem, qual seja, calúnia, difamação ou injúria.

Antes mesmo de se discutir os crimes contra a honra na internet, cabe definir a honra. Para a doutrina, podemos definir a honra como objetiva e subjetiva, sendo que a primeira diz respeito à opinião social acerca dos atributos físicos, intelectuais, morais de cada um. O indivíduo tem algo que permeia na sociedade, ou seja, é aquela que se refere diretamente a índole do sujeito na vida social[50].

---

[48] STF enquadra homofobia e transfobia como crimes de racismo ao reconhecer omissão legislativa Supremo Tribunal Federal. 2019. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=414010. Acesso em: 16 ago. 2023.

[49] SAFERNET. CRIMES NA WEB: Crimes de ódio têm crescimento de até 650% no primeiro semestre de 2022. **SAFERNET**. 2022. Disponível em: https://new.safernet.org.br/content/crimes-de-odio-tem-crescimento-de-ate-650-no-primeiro-semestre-de-2022. Acesso em: 10 jul. 2023.

[50] CAPEZ, F. Curso de direito penal 2: Parte especial, 19. ed. São Paulo, Saraiva, 2019.

Por outro lado, a honra subjetiva se refere à opinião do sujeito a respeito de si mesmo sobre os atributos supramencionados, ou seja, a visão de cada um sobre si mesmo, sem importar a opinião de terceiro[51].

Isso posto, é importante salientar que, embora o direito à liberdade de expressão esteja previsto na carta magna, o mesmo não deve violar a honra de outrem, seja ela objetiva ou subjetiva, sob o risco de violar a legislação penal.

Os crimes contra a honra, muitas vezes se confundem entre si devido à falta de conhecimento social; de forma interpretativa poderíamos dizer que esta confusão é a mesma que ocorre entre os crimes de roubo e furto[52]. Neste sentido, os crimes contra a honra estão dispostos no Código Penal da seguinte maneira:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos. (...)
> § 3º - Admite-se a prova da verdade, salvo:
> I - Se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível[53];

A calúnia tutela a honra objetiva, ou seja, é a ideia de que a sociedade passará a ter sobre o outro indivíduo, alusivo às questões supramencionadas que seja da pessoa em si. Como explica Capez, no crime de calúnia o autor atribui a outrem a prática de um determinado fato delituoso frente à sociedade, afetando diretamente sua honra[54].

> O vocábulo “calúnia” tem sua origem etimológica na expressão latina calomniae, significando o ato praticado por alguém visando a desacreditar terceira pessoa publicamente, através de acusações falsas. O que, vulgarmente, diferencia a calúnia de seus sinônimos são duas características que lhe são próprias: a gravidade maior da acusação feita e a falsidade da imputação. A gravidade da calúnia é de tal monta que o teólogo, Archibald Joseph Marcistyrn, estudioso dos anjos, afirmou que o termo “diabo” tem origem grega, nascido de

[51] Ibdem

[52] GRECO, R. **Curso de direito penal**. 24 ed. São Paulo: Atlas, 2022

[53] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

[54] CAPEZ, F. **Curso de direito penal 2:** Parte especial, 19. ed. São Paulo, Saraiva, 2019

> diabolos, que significa “caluniador”. A dedução é imediata: por ser caluniador o anjo decaído passou a ser conhecido por uma de suas características negativas. Historicamente, como figura típica autônoma, com significado próprio, aparece pela primeira vez no direito francês, que lhe dá uma menção de subespécie, passando a tratar, separadamente, a calúnia e a injúria. Até então, desde Código de Manu, as ofensas estavam todas englobadas no termo genérico “injúria” [55]

No que compete à ação nuclear do crime de calúnia, é importante apontar que a pessoa que, sabendo da calúnia, faça a divulgação da mesma, também incorre no mesmo crime, conforme descrito no Art. 138, supra, do Código Penal, não importando, por exemplo, o meio utilizado para a propagação do crime. É bastante comum que se utilize da internet para a prática deste crime, onde ocorre a propagação das chamadas *Fake News*[56].

Outro crime contra a honra praticado na internet é a difamação, prevista no CP em seu art. 139:

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa. Exceção da verdade
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções[57].

A origem da palavra é mais uma vez decifrada por Aranha:

> Difamar tem sua origem etimológica no termo latino diffamare, significando literalmente falar mal de alguém. Das derivações, difamador ou difamante, significa que o que difama, e difamatória, representando o conter uma difamação. Em sentido vulgar tem como significado tirar a boa fama ou desacreditar publicamente, como indicam os dicionaristas. A difamação somente ganhou contornos como figura típica, só se destacou como figura isolada, no Código atual, pois o de 1830 e o de 1890 só falavam na calúnia e na injúria. Na verdade, das três figuras típicas contra a honra a difamação foi a última a ganhar contornos próprios... foi no direito canônico que surgiu a primeira referência expressa sobre difamação, pois diffamatio era definido como detractio famae alterius pública su coram multis facta et cum directa vel indirecta intentione alterius infamian in publicum

[55] ARANHA, A. J. Q. T. C. Crimes contra a honra. São Paulo: Saraiva, 2000, p. 59

[56] GRECO, R. Curso de direito penal. 24 ed. São Paulo: Atlas, 2022.

[57] BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

> propalandi, para se tornar figura típica com a lei francesa de 17 de maio de 1819, a qual oficializou o termo diffamation. Era prevista como a imputação de um fato determinado que porte atteinte à l'honneur ou à la considération de la personae ou du corps auquel le fait est imputé. Como se disse ao início, entre nós surgiu com o código atual, pois os anteriores a incluíam como uma das formas da injúria. A difamação é um minus em relação a calúnia, mas um majus no tocante a injúria. Tratase, na verdade, de uma figura intermediária, no sentido da gravidade, entre os crimes contra a honra[58].

Assim como no caso do crime anterior, a difamação tutela a honra objetiva, já que, conforme explica Capez, este crime tem por base a atribuição de fato a outrem que ofenda a reputação do ofendido fazendo menção direta às qualidades físicas, intelectuais, e morais, de forma que afete a forma que o indivíduo ofendido é visto em seu meio de convivência.[59]

Sendo assim, extrai-se da explicação do doutrinador Fernando Capez que a difamação é composta por dois fatores: em um primeiro momento deve ocorrer a imputação de fato que necessariamente seja ofensivo à honra de outrem e, por fim, é necessário que este mesmo fato falsamente imputado seja levado a uma terceira pessoa, caracterizando assim a difamação.

O terceiro e último crime contra a honra a ser abordado é a injúria, este crime está previsto no CP em seu art. 140 da seguinte forma:

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - Quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - No caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3 o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa.[60]

---

[58] ARANHA, A J Q. T.C. **Crimes contra a honra**. São Paulo: Saraiva, 2000

[59] CAPEZ, F. **Curso de direito penal 2**: Parte especial, 19. ed. São Paulo, Saraiva, 2019,

[60] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

O crime de injúria, diferente dos demais, diz respeito diretamente à honra subjetiva do sujeito ofendido, ou seja, a visão que este tem de si mesmo. Porém, como aponta Capez, a honra objetiva, ou seja, o valor que o indivíduo goza na sociedade, também pode ser afetada, no entanto, no caso da injúria esta ofensa é indiferente à configuração do crime[61].

A injúria recebe algumas subclassificações doutrinárias, conforme destaca-se a seguir:

> De acordo com a classificação doutrinária, a injúria pode ser: (i) imediata – quando é proferida pelo próprio agente; (ii) mediata – quando o agente se vale de outro meio para executá-la (p. ex., de uma criança); (iii) direta quando se referem ao próprio ofendido; (iv) oblíqua – quando atinge alguém estimado pelo ofendido (p. ex., "seu 25 irmão é um ladrão"); (v) indireta ou reflexa – quando, ao ofender alguém, também se atinge a honra de terceira pessoa; (vi) equívoca – quando por meio de expressões ambíguas; (vii) explícita – quando são empregadas expressões que não se revestem de dúvidas. A injúria também pode ser implícita, irônica, interrogativa, simbólica, truncada.[62]

A consumação do crime de injúria, por sua vez, se dá quando o ofendido toma ciência da imputação, neste caso se trata de delito formal, ou seja, o crime se consuma quando o sujeito passivo toma ciência da imputação ofensiva, independentemente de o ofendido sentir-se ou não atingido em sua honra subjetiva, sendo suficiente, tão só, que o ato seja revestido de idoneidade ofensiva[63].

Além dos crimes contra a honra, existem diversos outros crimes que podem ser praticados na internet, como por exemplo o furto de dados na internet, abordado a seguir.

3.2.3 Dano informático

O crime de dano informático está previsto no artigo 163 do Código Penal, tendo o patrimônio de uma empresa ou pessoa física como bem jurídico tutelado,

---

[61] GRECO, R. **Curso de direito penal**. 24 ed. São Paulo: Atlas, 2022, p. 442

[62] CAPEZ, F. **Curso de direito penal 2**: Parte especial, 19. ed. São Paulo, Saraiva, 2019

[63] Ibdem

e é cometido por quem destrói, inutiliza ou deteriora patrimônio alheio; este patrimônio, por sua vez, pode tratar-se de dados que possuam qualquer espécie de valor.

> Art. 163. (...)
> I - com violência à pessoa ou grave ameaça;
> II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave
> III - contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos;
> IV - por motivo egoístico ou com prejuízo considerável para a vítima: Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência[64].

Conforme aponta Rogério Greco, este crime permite a tentativa e consuma-se a partir da divulgação e distribuição de vírus, através de acessos não autorizados a sistemas computacionais, dentre outras formas que possam violar dados que integrem a propriedade de outrem, cuja consumação se dá no momento do resultado.

3.2.4 Estelionato

O estelionato é um dos crimes que mais ocorre no ambiente do ciberespaço. De acordo com dados da Polícia Civil do Distrito Federal, em 2020 foram registradas 9.529 queixas de estelionato praticado através da internet, sendo o mais comum dentre os crimes cibernéticos registrados.

Este crime está disposto no art. 171 do Código Penal:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa[65]

Ademais, em seu § 3º, o artigo estabelece que a pena será aumentada de um terço, na situação em que o crime for cometido em detrimento de entidade

---

[64] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

[65] Ibdem

de direito público ou de instituto de economia popular, assistência social ou beneficência.

Neste sentido, Rogério Greco explica que, desde o surgimento das relações sociais, o homem muitas vezes se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens de forma errônea.[66]

A prática de estelionato no ciberespaço ocorre quando a conduta do agente que pratica o crime busca induzir ou manter a vítima em erro, e com isso, obtendo vantagem ilícita, para si ou para outrem.

Diversas são as condutas dos estelionatários na internet, o desafio é tipificá-las como estelionato. Diante disso, o legislador previu como meio executório a fraude com o objetivo de obter consentimento da vítima, iludi-la para que voluntariamente entregue o bem; o agente leva a vítima a erro ou induz que ela continue praticando um erro que ocasione em vantagem para o sujeito ou outra pessoa de seu interesse.[67]

No ambiente virtual, a conduta do estelionatário pode ocorrer de diversas formas como: encaminhar e-mails falsos, levando o usuário a clicar em links que o direcionam a um site falso com o objetivo de apropriar-se dos seus dados bancários para adquirir para si os valores na conta da vítima, e fazer compras com o cartão da vítima cujos dados foram obtidos ilegalmente através da internet.

3.2.5 Pornografia infantil

O crime de pornografia infantil é um dos mais graves praticados no ciberespaço, e, assim como a pornografia, faz parte de um mercado bilionário. De acordo com o relatório da SaferNet Brasil referente a 2018, o Brasil registrou

[66] GRECO, R. **Curso de direito penal.** 24 ed. São Paulo: Atlas, 2022

[67] CAPEZ, F. **Curso de direito penal 2**: Parte especial, 19. ed. São Paulo, Saraiva, 2019

um total de 133.732 queixas referentes a delitos cometidos no ciberespaço, 110% a mais em relação ao ano anterior[68].

Dentre as queixas, a SaferNet aponta que o principal crime denunciado foi a pornografia infantil, apontando ainda que, nos últimos quatorze anos que antecederam o relatório, mais de 4,1 milhões de denúncias anônimas foram contabilizadas contra 790 mil endereços eletrônicos por divulgarem conteúdo inapropriado na internet[69].

O elemento subjetivo do tipo é o dolo, o qual ocorre quando o agente tem a finalidade de expor ao público, ou comercializar o objeto material do crime, sendo neste caso de cunho sexual infantil. Importante salientar que, como dispõe Pinheiro, não é necessário que alguém venha a ter acesso ao material para ocorrer a consumação do crime, basta somente a disponibilização do material e a possibilidade de que alguém venha a ter acesso ao mesmo[70].

Há, ainda, a necessidade se fazer uma distinção entre a Pedofilia e a Pornografia Infantil: na primeira, não existe divulgação de conteúdo, mas sim uma perversão sexual, na qual o adulto experimenta sentimentos eróticos com crianças e adolescentes. Já, na Pornografia Infantil, não é necessária a ocorrência da relação sexual entre adultos e crianças, mas sim, a comercialização de conteúdo sexual envolvendo menores[71].

No Estatuto da Criança e do Adolescente, Lei 8.069/90, que estabelece em seus artigos 240 e seguintes algumas penalidades para o sujeito que divulga ou comercializa imagens e vídeos envolvendo menores em cena de sexo, observa-se:

> Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica:
> Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa.
> Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracena com criança ou adolescente.

[68] SAFERNET. Brasil registrou uma alta de 109,95% em denúncias de crimes na internet em 2018. 2019. Disponível em: https://www.jornalopcao.com.br/ultimas-noticias/brasil-registrou-uma-alta-de-10995-em-denuncias-de-crimes-na-internet-em-2018-163701/

[69] Ibdem.

[70] PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2014

[71] INELLAS, G. C. Z. **Crimes na Internet**, 2. ed. São Paulo: Editora Juarez de Oliveira, 2009

> Art. 241 – Fotografar ou publicar cena e sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão de 1 (um) a 4 (quatro) anos[72].

Acerca da aplicação do art. 241 do ECA a crimes praticados na internet destaca-se que o Supremo Federal já entende que sua aplicação se dá também para os crimes cujo local de consumação seja a Internet, tendo em vista que o crime se caracteriza pela simples publicação, sendo indiferente o meio utilizado para tal[73].

Além disso, Pinheiro aponta que, para efetuar a localização do agente que praticou uma das condutas previstas nos referidos dispositivos, muitas vezes é necessária a quebra de sigilo, tendo em vista que será preciso rastrear o endereço IP daquele que praticou o ilícito. Após conseguir localizar o culpado é necessário que sejam analisadas as provas eletrônicas por uma perícia técnica rigorosa, para serem aceitas nos processos[74].

3.2.6 Estupro virtual

O estupro virtual é uma modalidade de cibercrime que vem sendo bastante debatida nos últimos tempos. Este debate se dá pelo fato de que existem correntes as quais defendem o entendimento de que é possível haver o estupro pelo meio virtual, mas há outros posicionamentos que entendem ser impossível a existência desta modalidade criminal, haja vista que a presença física do agressor seria indispensável para tal prática[75].

Importante salientar que o crime de estupro está disposto no art. 213 do Código Penal que o qualifica como o ato de “constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que

---

[72] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

[73] PINHEIRO, P P. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2014

[74] Ibdem

[75] BARBOSA, C de F. Penal, Processo Penal, Criminologia e Novas Tecnologias: A caracterização jurídica do estupro virtual. **COPENDI**. 2021. Disponível em: http://conpedi.danilolr.info.

com ele se pratique outro ato libidinoso: Pena - reclusão, de 6 (seis) a 10 (dez) anos”[76].

Levando em consideração o referido texto trazido pelo ordenamento penal brasileiro, alguns estudiosos defendem que não há necessidade de contato ou presença física para a ocorrência do crime.

> No caso em que o autor, ameaçando divulgar vídeo íntimo da vítima, a constrange, via internet, a se auto masturbar ou a introduzir objetos na vagina ou no ânus, tem-se estupro, pois a vítima, mediante grave ameaça, foi constrangida a praticar ato libidinoso diverso da conjunção carnal. Portanto, o estupro virtual configura-se quando o autor se vale da internet para praticar em desfavor da vítima a conduta descrita no art. 213 do Código Penal[77].

Salienta-se que a denominação estupro virtual ainda gera certa estranheza na sociedade, tendo em vista que, para muitos, para ser configurado o crime de estupro, deve-se obrigatoriamente haver conjunção carnal, como disposto anteriormente na Lei 12.15/2009.

No entanto, tal lei foi alterada e, assim, passou a ser possível o enquadramento deste estupro virtual no trecho onde compreende: “constranger alguém mediante grave ameaça” e “a praticar outro ato libidinoso”. Diante desta mudança permitiu-se entender como ato libidinoso todo o ato capaz e suficiente de satisfazer o desejo sexual de um indivíduo.

Por fim, cabe mencionar que o primeiro caso de condenação por estupro virtual se deu no Rio Grande do Sul através do Habeas Corpus (HC) n° 478.310 – PA que entendeu que o contato físico não é algo prescindível para a ocorrência do crime de estupro conforme a ementa a seguir:

> HABEAS CORPUS. ESTUPRO DE VULNERÁVEL. QUALQUER ATO DE LIBIDINAGEM. CONTATO FÍSICO DIRETO. PRESCINDIBILIDADE. CONTEMPLAÇÃO LASCIVA POR MEIO VIRTUAL. SUFICIÊNCIA. ORDEM DENEGADA.
> 1. É pacífica a compreensão, portanto, de que o estupro de vulnerável se consuma com a prática de qualquer ato de libidinagem ofensivo à dignidade sexual da vítima, conforme já consolidado por esta Corte Nacional.

---

[76] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

[77] GUIMARÃES, A. S. Estupro Virtual. **Direito penal em contexto**. 2018. Disponível em: http://www.direitopenalemcontexto.com.br/estupro-virtual/. Acesso em: 4 ago. 2023

> 2. Doutrina e jurisprudência sustentam a prescindibilidade do contato físico direto do réu com a vítima, a fim de priorizar o nexo causal entre o ato praticado pelo acusado, destinado à satisfação da sua lascívia, e o efetivo dano à dignidade sexual sofrido pela ofendida.3. No caso, ficou devidamente comprovado que o paciente agiu mediante nítido poder de controle psicológico sobre as outras duas agentes, dado o vínculo afetivo entre eles estabelecido. Assim, as incitou à prática dos atos de estupro contra as infantes (uma de 3 meses de idade e outra de 2 anos e 11 meses de idade), com o envio das respectivas imagens via aplicativo virtual, as quais permitiram a referida contemplação lasciva e a consequente adequação da conduta ao tipo do art. 217-A do Código Penal[78].

No entanto, como apontado pelo promotor do caso em tela, é fundamental que a legislação brasileira passe por atualização para melhor atender os crimes cibernéticos, tendo em vista que, com o aumento e evolução das tecnologias, cada vez mais modalidade destes crimes vem sendo praticadas.

[78] RIO GRANDE DO SUL. Superior Tribunal de Justiça. Habeas Corpus nº 478.310 - PA. Relator: Ministro Rogerio Schietti Cruz. Rio Grande do sul. 09 de fevereiro de 2021. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201802976418&dt_publicacao=18/02/2021. Acesso em: 16 ago. 2023.

4. A LEGISLAÇÃO DE CIBERCRIMES E SUAS LIMITAÇÕES

A primeira legislação brasileira a abordar a ocorrência de crimes virtuais foi a Lei 9.609 de 19 de fevereiro de 1998, cujo objetivo era dispor sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País.

Esta regulamentação substituiu a Lei 7.646 de 18 de dezembro de 1987 que também dispunha sobre a propriedade intelectual, mas não mencionava os crimes cometidos em espaço virtual, sendo assim, a nova legislação apresentou considerações inovadoras acerca da tecnologia virtual.

A referida lei tipificou o primeiro crime virtual acerca de proteção aos direitos de autor e do registro de programas virtuais, de garantias aos usuários de programas de computador, de contratos de licença de uso virtual, comercialização e transferência de tecnologia, e neste contexto trouxe à baila a primeira tipificação:

> Art. 12. Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral[79].

Ainda, tal legislação foi complementada pela Lei nº 9.610/1998, cujo principal objetivo é dedicar-se extensamente à questão dos direitos autorais, sendo que esta deveria ser aplicada a tudo que sua antecessora se fizesse omissa[80]. Muitos anos se passaram e somente em 2012 uma nova legislação totalmente voltada para os crimes cibernéticos foi aprovada.

---

[79] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

[80] SIQUEIRA, M. S. et al. Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13. 2017. p. 122

Para suprir tal necessidade, o Congresso Nacional aprovou a Lei 12.737 de 30 de novembro de 2012, que dispôs acerca da tipificação criminal de delitos informáticos e alterou o Código Penal. Esta lei ficou conhecida como “Lei Carolina Dieckmann”. Naquele ano, a atriz teve seu computador invadido por criminosos popularmente chamados de *hackers,* que divulgaram 36 fotos íntimas de Carolina, causando um grande transtorno e constrangimento à mesma.

A inovação legislativa trazida pela Lei 12.737/2012 introduziu no Código Penal a tipificação do crime de invasão de dispositivo informático, cujo art. 154-A passou a vigorar naquele ano da seguinte forma:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita; § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput[81]

Vale ressaltar que, em casos de o crime ser cometido contra políticos ou resultar em prejuízo financeiro, a pena pode sofrer aumento, ao passo que a propriedade é fortemente defendida pelo ordenamento jurídico brasileiro. Também podem ocorrer crimes como furto de dados em cartões de débito e crédito, com o risco de falsificação dos mesmos pelos criminosos. A lei que altera o Código Penal tem ainda o intuito de proibir a produção, divulgação ou propagação do uso de softwares ou equipamentos que tenham o objetivo de invadir aparelho informático alheio.

Além disso, a referida lei atualizou os artigos 266 e 298 do Código Penal nos seguintes termos:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

[81] BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

> § 2º aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública. [82]

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012) Vigência
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012) Vigência Falsidade ideológica [83]

Existiu uma grande polêmica acerca da tramitação e da promulgação de tal lei, que acabou gerando um certo atraso para outras leis de teor semelhante. Diante desta explicação, faz-se necessário apontar que, apesar de ser legislação de suma importância no combate aos crimes cibernéticos, diante da dimensão das evoluções tecnológicas, a lei ainda está muito aquém de suprir todas as necessidades que este tipo penal pode requerer[84].

Assim, em 2014 foi promulgada a Lei nº 12.965, de 23 de junho de 2014, conhecida popularmente como Marco Civil da internet, cujo principal objetivo é estabelecer instruções do uso da internet em todo o território nacional, como garantias, direitos e deveres de cada um perante a evolução tecnológica.

Seus artigos 1º e 3º demonstram suma importância para o uso da internet que conhecemos hoje, pois trazem seus princípios e garantias. Ademais, frente à preocupação com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários no uso da internet, o legislador garantiu expressamente no Marco Civil esses dois direitos constitucionais, condição para o pleno exercício do direito a acesso à rede mundial de computadores[85].

Neste sentido, esta lei tem por objetivo estabelecer limitações de uso da internet, e alcançar direitos, garantias e deveres relativos à rede mundial de

---

[82] Ibdem

[83] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

[84] SIQUEIRA, M. S. et al. Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13. 2017. p. 122

[85] TEIXEIRA, T. **Marco civil da internet**: comentado. 1ªed. São Paulo: Almerinda. 2016. p. 120

computadores, com base no direito fundamental à privacidade, além de estabelecer a proteção de dados pessoais dos usuários.

Esta lei realmente foi um grande marco para delimitar o uso da internet. No entanto, como indica Siqueira, ela está longe de atender todas as necessidades trazidas pelo crescimento da internet no Brasil, uma vez que tal legislação não abrange todo o campo de atuação dos criminosos da internet, restando inúmeras lacunas a serem supridas por outras legislações[86].

Um exemplo desta lacuna bastante comum no cotidiano da sociedade, é o que diz respeito aos contratos firmados no âmbito da internet. Neste sentido, destaca-se o entendimento de Vedovate:

> Sem dúvida alguma, a internet é um dos meios mais eficazes para a celebração de contratos. Hoje são milhares de contratos fechados por essa via, de forma que obedecem aos princípios da publicidade, da vinculação, da veracidade, da não-abusividade entre outros. No ordenamento jurídico brasileiro não existe normatização específica sobre os contratos realizados sob essa égide. No entanto, o Código Civil e o Código de Defesa do Consumidor sanam, em parte, os conflitos atinentes a respeito desse tema, faltando uma norma específica que assegure os asseios da comunidade virtual.[87]

Neste contexto, observa-se que o ordenamento atual não tem sido o bastante para coibir as inúmeras práticas ilícitas passíveis de prática virtual. Dado o fato de que a internet, com sua vasta amplitude, permite constantemente a criação de novos tipos penais, muitas vezes as autoridades do sistema jurídico não têm o suporte, o preparo e as habilidades necessárias para resolução dos casos de crimes virtuais.

4.1 A LEI Nº 14.155 DE 2021 E O COMBATE AOS CRIMES CIBERNÉTICOS

Como supramencionado, as leis promulgadas até o presente momento deixaram de suprir as necessidades da sociedade e do ordenamento jurídico atual frente ao constante crescimento da internet, que atualmente é algo indispensável para todos.

---

[86] Ibdem

[87] VEDOVATE, L. L. V. Contratos Eletrônicos. **INTERTEMAS**. v. 10, n. 10. Presidente Prudente, 2005, p.13.

Neste sentido, em 27 de maio de 2021 foi promulgada a Lei 14.155, que regulamenta os crimes cibernéticos de forma mais gravosa. Buscando atender às necessidades da realidade atual, esta lei é responsável por:

> Alterar o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato[88].

Durante o período da pandemia do COVID-19 no Brasil, os índices de crimes praticados em âmbito virtual foram elevados. As denúncias de crimes pela internet quase triplicaram de 2019 para 2020, e em 2021 não foi diferente. O País passou a ocupar a quinta posição entre os países com maior número de crimes virtuais.

Além disso, destaca-se o constante crescimento dos inúmeros ilícitos penais que passaram a ocorrer. Vão desde ameaças simples, a delitos de racismo, pornografia infantil, estelionato, entre outros. Importante destacar que os cibercrimes ou crimes virtuais, segundo a doutrina, são “aqueles em que a tecnologia foi utilizada como ferramenta-meio ou alvo-fim da atividade criminosa no meio ambiente computacional da sociedade complexa da informação e comunicação”.[89]

Sendo assim, a Lei 14.155/21, veio para trazer maior rigidez às penas dos delitos de furto e estelionato perpetrados no cerne digital, incluindo computadores, celulares e tablets. Modifica a Lei 2.828 do Código Penal, endurecendo as punições nos casos de invasão de dispositivo, furto qualificado e estelionato cometidos nesse ambiente, com conexão ou não à internet[90].

As alterações trazidas para o Código Penal com a promulgação da Lei 14.155/21 buscam atualizá-lo mediante as mudanças que ocorrem no mundo, principalmente sobre os crimes relacionados ao ambiente digital, incluindo uma

---

[88] BRASIL. Lei nº 14.155, de 27 de maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10259.htm

[89] PINHEIRO, P P; GROCHOCKI, L R. Noções de Direito Cibernético. In: VELHO, Jesus Antônio. Tratado de computação forense. Campinas, SP: Millennium, 2016.

[90] TEIXEIRA, T. **Marco civil da internet**: comentado. 1ªed. São Paulo: Almerinda. 2016

responsabilização penal mais gravosa para quem cometer delitos específicos. Além disso, o texto incrementa um aumento de pena que, antes, eram excessivamente brandas[91].

Neste sentido, o art. 154-A foi inserido no ordenamento jurídico pela Lei Carolina Dieckmann e sofreu importantes alterações, passando a vigorar com uma pena mais dura e deixando de ocupar o rol dos delitos com menor potencial ofensivo, definidos pela Lei 10.259/01 como: “infrações de menor potencial ofensivo, para os efeitos desta lei, os crimes a que a lei comine pena máxima não superior a 2 (dois) anos, ou multa”.[92]

Com o aumento da pena, o crime passou a ocupar o rol dos crimes com médio potencial ofensivo, o que na prática significa que, se preso em flagrante, o autor do delito será submetido a lavratura de auto de prisão em flagrante e não mero termo circunstanciado de ocorrência, como ocorre com os crimes de menor potencial ofensivo, além de, claro, a pena ser mais gravosa.

Além disso, este delito não mais é julgado pelo Juizado Especial Criminal e não mais admite transação penal. Contudo, como sua pena não excede 4 anos, ainda é possível o arbitramento de fiança pelo Delegado de Polícia, a suspensão condicional do processo e o acordo de não persecução penal.

O § 1º do referido dispositivo trata, por sua vez, de um tipo penal praticado por quem realiza quaisquer das condutas nele previstas, seja ela produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. Note-se que não basta que a conduta delitiva possibilite a invasão, mas que o agente tenha praticado o comportamento com o intuito de permitir que isso aconteça.

O tipo demanda dolo específico, não bastando para sua prática a intenção de realizar a conduta nele prevista. Deveras, exige-se que o agente saiba que está, por exemplo, fornecendo um programa que será utilizado por um

---

[91] MIRABETE, Júlio F e FABBRINI, Renato N./ Manual de direito penal: parte especial: arts. 121 a 234-B do CP – volume 2, 36° edição, São Paulo, Atlas, 2021

[92] BRASIL. Lei no 10.259, de 12 de julho de 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10259.htm

terceiro, para a invasão de um dispositivo. Portanto, a norma em análise representa uma exceção à teoria monista, pois o auxílio material é criminalizado de forma autônoma, o que permite a punição do agente, ainda que não ocorra a subsequente e visada invasão de dispositivo informático[93].

Isso posto, o crime de invasão de dispositivo informático contará com o aumento de pena, se, do ato delitivo, decorre prejuízo econômico para a vítima. Logo, se quem comete o delito invadir o aparelho da vítima e, estando em posse de suas fotos íntimas, ameaça divulgar as imagens, acaso esta não lhe transfira certa quantia, o jurista estará diante de uma hipótese de extorsão e não de simples invasão de sistema informático. Nesse caso, a realização da transação bancária será exaurimento da extorsão e não hipótese de incidência da aludida majorante. A majorante, assim, é um reforço à punição do caput, que não desconstitui o fato deste ser residual/subsidiário em relação a outros tipos.

O parágrafo seguinte, por sua vez, aumentou a pena em situações nas quais:

> Da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.[94]

Neste caso, a pena passou de 6 meses a 2 anos para uma pena mais dura de 2 a 5 anos. Da mesma forma que as penas anteriores, a nova pena do dispositivo não retroage. No entanto, a pena prevista para o delito atende o requisito objetivo para oferta de acordo de não persecução penal, conforme previsto na Lei do Pacote Anticrime.

Importante mencionar, que além de alterações, a nova legislação também criou modalidades de crimes para atender às atuais necessidades da sociedade, como é o caso do furto qualificado pela fraude eletrônica. Tal crime está alocado no art. § 4º-B:

---

[93] FIGUEIREDO, Beatriz Ferreira; DA CRUZ, Maria José Amorim. Racismo recreativo e injúria racial: uma análise jurisprudencial do animus jocandi. Revista Estudantil Manus Iuris, v. 1, n. 2, p. 199-213, 2020.

[94] 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

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo [95].

Esta norma é uma interessante hipótese de qualificadora da qualificadora, ou seja, uma norma chamada de super qualificadora, pois aumenta a pena mínima do crime de furto previamente qualificado pelo delito de fraude.

O crime de furto está previsto no art. 155, caput do Código Penal:

> Furtar, como se sabe, é subtrair, para si ou para outrem, coisa alheia móvel (art. 155, caput do Código Penal). Praticará, assim, a modalidade qualificada em análise, quem subtrair coisa alheia móvel para si ou para outrem, mediante fraude eletrônica, conforme descrita no art. 155, § 4º-B.[96]

O art. 155, § 4º-B, além de mencionar o meio para execução, realça a uma especial importância o instrumento empregado, sendo este o furto de fraude eletrônica.

Além deste, a Lei 14.155/2021 criou causas de aumento específicas para esta modalidade de crime, a teor do art. 155, § 4º-C e seus incisos:

> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – Aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. [97]

Da leitura do dispositivo, extrai-se que o legislador instituiu como causa de aumento de pena a relevância do resultado gravoso, prevendo, logo em seguida no inciso I, majoração decorrente da prática do crime por via da

---

[95] Ibdem

[96] Ibdem

[97] BRASIL. Lei no 10.259, de 12 de julho de 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10259.htm

utilização de servidor mantido fora do território nacional e, no inciso II, incremento de sanção concernente a características das vítimas.

Por fim, além de criar a modalidade de furto mediante fraude eletrônica, a referida lei também positivou o estelionato mediante fraude eletrônica, no art. 171, § 2º-A. Cabe mencionar que o estelionato por si está previsto no art. 171 do Código Penal nos seguintes termos:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. Deveras, no estelionato, o delinquente enganar a vítima, através do emprego de artifício, ardil, ou qualquer outro meio fraudulento, fazendo com que ela lhe entregue, de bom grado, uma vantagem ilícita.[98]

Neste contexto, o art. 171, § 2º-A, dispõe que a pena do estelionato se agrava quando a fraude empregada pelo agente é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.[99]

Apesar de tal legislação trazer muitos avanços para o combate dos crimes cibernéticos, estes ainda se mostram pequenos frente aos avanços dessa modalidade criminal.

Como muitos criminosos agem com o mínimo de suspeita possível, aproveitando o mundo tecnológico a seu favor, o qual permite que atuem de forma anônima e silenciosa, há grandes dificuldades em investigar e punir esses crimes. Dessa forma, fica mais difícil identificar tais agentes pois usam

---

[98] Ibdem

[99] Ibdem

dispositivos tecnológicos em locais públicos e possuem a capacidade de agir de forma anônima[100].

Além disso, a obtenção de provas e punição de crimes virtuais é dificultada pela falta de capacitação de profissionais dedicados ao combate a esses crimes, por isso é necessário que os mesmos se atualizem para melhor desempenharem suas funções[101].

Isso posto, conclui-se que, com o passar do tempo, a legislação acerca dos crimes cibernéticos se tornou necessária. Apesar de ter sofrido um grande avanço em 2012 com a implantação da famosa Lei Carolina Dieckmann, ela já não bastava para as necessidades sociais sendo promulgada a Lei nº 14.155 de 2021.

[100] SIQUEIRA, M. S. et al. Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13. 2017

[101] FROTA, Jessica Olívia Dias; PAIVA, Maria de Fátima Sampaio. Crimes virtuais e as dificuldades para combatê-los. 2017. Disponível em: https://flucianofeijao.com.br/novoo/wp-content/uploads/2018/11/ARTIGOS_CRIMES_VIRTUAIS\nDIFICULDADE.

5. CONCLUSÃO

A trajetória da internet, desde suas origens até sua posição atual como um dos principais pilares da comunicação contemporânea, é uma narrativa repleta de transformações e avanços tecnológicos sem precedentes. No entanto, essa evolução também trouxe à tona desafios inesperados, revelando a dualidade do ciberespaço como um terreno propício para a manifestação de variados delitos.

Entre os crimes que ganharam destaque nesse ambiente digital, merecem atenção os crimes de ódio, os ataques à honra, a disseminação de informações danosas, o estelionato, a alarmante propagação da pornografia infantil e o estupro virtual. A amplitude dessas transgressões reflete a complexidade do ambiente online e a necessidade de uma abordagem multifacetada para lidar com suas consequências.

Apesar de ser impossível abranger todos os tipos de cibercrimes, o presente estudo buscou discorrer sobre aqueles considerados mais graves ou com maior índice de ocorrências e dos impactos sociais associados a eles.

À medida que os cibercrimes floresceram com a proliferação da internet, as esferas legislativa, judiciária e executiva tomaram medidas conjuntas para combater essa modalidade delituosa. Um exemplo emblemático desse empenho é a promulgação da Lei n° 14.155 de 2021, um marco que se seguiu vinte anos após sua predecessora, a Lei nº 12.737, mais conhecida como a "Lei Carolina Dieckmann". Essa nova legislação representa uma resposta do sistema jurídico à constante evolução das práticas cibercriminosas e ao desafio de se manter à altura das inovações digitais.

No entanto, apesar das inúmeras mudanças e atualizações trazidas por essa lei recente, a batalha contra os cibercriminosos ainda é um território que demanda constante aperfeiçoamento. A habilidade dos mesmos em ocultar suas atividades por meio de dispositivos específicos destaca a necessidade de estratégias investigativas cada vez mais sofisticadas e da colaboração íntima com especialistas em segurança cibernética.

A disparidade entre a agilidade dos cibercriminosos e a preparação das equipes encarregadas de combatê-los é um desafio que requer atenção

contínua. Investimentos em capacitação, tecnologia e cooperação interdisciplinar são pilares cruciais para superar essa lacuna, permitindo que os profissionais da aplicação da lei estejam à altura dos desafios impostos pelas complexidades do ciberespaço.

Em última análise, a jornada para combater os cibercrimes é dinâmica e em constante evolução. A resposta a esses desafios exige não apenas atualizações regulares na legislação e nas táticas investigativas, mas também uma conscientização ampla sobre os riscos e melhores práticas de segurança cibernética em todos os níveis da sociedade. Ao unir esforços em âmbito público e privado, podemos criar um ambiente digital mais seguro, onde a tecnologia e a comunicação florescem em harmonia com a ética e a lei.

REFERÊNCIAS

ALEXANDRE JUNIOR, J C. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**. v. 14, n.1, p. 341-351, 2019.

ARANHA, A J Q. T. de C. **Crimes contra a honra**. São Paulo: Saraiva, 2000.

ARAS, V. Crime de Informática. Uma Nova Criminalidade. **Jus Navigandi**. Teresina, ano 6, n. 51, 2001.

BARBOSA, C de F. Penal, Processo Penal, Criminologia e Novas Tecnologias: A caracterização jurídica do estupro virtual. **COPENDI**. 2021. Disponível em: http://conpedi.danilolr.info.

BECKETT, A. The dark side of the internet: in the 'deep web', Freenet software allows users complete anonymity as they share viruses, criminal contacts and child pornography. The Guardian. Reino Unido, 26 nov. 2009. Disponível em: https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. Acesso em: 04 ago. 2023.

BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/Del2848compilado.htm

BRASIL. Lei n° 10.259, de 12 de julho de 2001. Dispõe sobre a instituição dos Juizados Especiais Cíveis e Criminais no âmbito da Justiça Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10259.htm

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10259.htm

BRASIL. MINISTÉRIO PÚBLICO FEDERAL. **Crimes cibernéticos**.2° ed. Editora 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.

BRASIL. **Portaria nº 148, de 31 de maio de 1995**. Disponível em: https://www.cgi.br/portarias/download/Portaria_148_1995.pdf. Acesso em: 06 ago. 2023.

CAPEZ, F. **Curso de direito penal 2**: Parte especial, 19. ed. São Paulo, Saraiva, 2019.

CHATE R C, et al. Presentation of pulmonary infection on CT in COVID-19: initial experience in Brazil. **J Bras Pneumol,** v.46, n.2, 2020.

CHENG, W. The phenomenon of hate crimes. **Journal of Applied Social Psychology**, n. [S.l], v.43, 2013.

CORREIA, M., RAMOS, R. F., & BAHTEN, L. Os cirurgiões e a pandemia do COVID-19. **Revista do Colégio Brasileiro de Cirurgiões**, v. [s.i] n. [s.i]. p. 1 – 6. 2020

CRESPO, Marcelo Xavier de Freitas. **O cibercrime.** São Paulo: Saraiva, 2011

FERREIRA, Ivette Senise. **Direito & Interne**t: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: QuartierLatin. 2005.

FROTA, Jessica Olívia Dias; PAIVA, Maria de Fátima Sampaio. Crimes virtuais e as dificuldades para combatê-los. 2017. Disponível em: https://flucianofeijao.com.br/novoo/wpcontent/uploads/2018/11/ARTIGOS_CRIMES_VIRTUAIS\nDIFICULDADE. Acesso em: 28 jul. 2023.

FURLANETO NETO, M; GUIMARÃES J. A C. Crimes na internet: Elementos para uma reflexão sobre a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003

FURLANETO NETO, M; SANTOS, J E L; GIMENES, E V. **Crimes na internet e inquérito policial eletrônico**. São Paulo: EDIPRO, 2012.

GRECO FILHO, V. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim, São Paulo: IBCCrim, n. 95, ano 8, out. 2000.

GRECO, R. **Curso de direito penal**. 24 ed. São Paulo: Atlas, 2022.

GUIMARÃES, A. S. Estupro Virtual. **Direito penal em contexto**. 2018. Disponível em: http://www.direitopenalemcontexto.com.br/estupro-virtual/. Acesso em: 4 ago. 2023

HEAVEN, D. Unpicking the mythologies around the dark web. **NewScientist**, v. 240, n. 3209-3210, p. 82-83, 2018.

IANNI, O. Globalização: novos paradigmas das ciências sociais**. Estudos avançados**. v. 8, n. 21, 1994

INELLAS, G. C. Z. **Crimes na Internet,** 2. ed. São Paulo: Editora Juarez de Oliveira, 2009, p. 129-130.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA [IBGE]. Internet já é acessível em 90,0% dos domicílios do país em 2021. IBGE. 2021. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 24 jun. 2023.

JESUS, D de; MILAGRE, J A. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

KUNRATH, Josefa Cristina Tomaz Martins **A expansão da criminalidade no ciberespaço**. Feira de Santana: Universidade Estadual de Feira de Santana, 2017

LINS, B F E. **A evolução da Internet: uma perspectiva histórica**. Brasília: Associação dos Consultores Legislativos e de Orçamento e Fiscalização Financeira da Câmara dos Deputados. 2013.

MIRABETE, J F e FABBRINI, R N. **Manual de direito penal**: parte especial: arts. 121 a 234-B do CP – volume 2, 36° edição, São Paulo, Atlas, 2021

MOTERANI, G M B, CARVALHO, F M De. Misoginia: A Violência Contra a Mulher Numa Visão Histórica e Psicanalítica. **Avesso do avesso** v.14, n.14, p. 167-178, novembro 2016

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2014.

PINHEIRO, P P; GROCHOCKI, L R. **Noções de Direito Cibernético**. In: VELHO, Jesus Antônio. Tratado de computação forense. Campinas, SP: Millennium, p. 535-564. 2016.

PORTER, M E. & MILLAR, V E. How information gives you competitive advantage. Harvard Business Review, Boston, Jul/Aug 1985.

Proposta que criminaliza misoginia começa a tramitar no Senado. **AGÊNCIA SENADO**. 2023. Disponível em: https://www12.senado.leg.br/noticias/materias/2023/03/07/proposta-que-criminaliza-misoginia-comeca-a-tramitar-no-senado. Acesso em: 16 ago. 2023.

RIO GRANDE DO SUL. Superior Tribunal de Justiça. Habeas Corpus nº 478.310 - PA. Relator: Ministro Rogerio Schietti Cruz. Rio Grande do sul. 09 de fevereiro de 2021. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201802976418&dt_publicacao=18/02/2021. Acesso em: 16 ago. 2023.

SAFERNET. Brasil registrou uma alta de 109,95% em denúncias de crimes na internet em 2018. 2019. **Safernet**. Disponível em: https://www.jornalopcao.com.br/ultimas-noticias/brasil-registrou-uma-alta-de-10995-em-denuncias-de-crimes-na-internet-em-2018-163701/ Acesso em: 10 ago. 2023.

SAFERNET. CRIMES NA WEB: Crimes de ódio têm crescimento de até 650% no primeiro semestre de 2022. **Safernet**. 2022. Disponível em: https://new.safernet.org.br/content/crimes-de-odio-tem-crescimento-de-ate-650-no-primeiro-semestre-de-2022. Acesso em: 10 jul. 2023.

SAFERNET. Denúncias de neonazismo à Safernet aumentam 60% em um ano. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-neonazismo-safernet-aumentam-60-em-um-ano Acesso em: 10 jun. 2023.

SERGL, M & CUNHA, G. A relação entre o indivíduo pós-moderno, o consumo e a internet das coisas. **Revista Tecnologia e Sociedade**, v 16, n 39, p. 41-56, 2019.

SIQUEIRA, M. S. et al. **Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito** – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13. 2017.

STF enquadra homofobia e transfobia como crimes de racismo ao reconhecer omissão legislativa Supremo Tribunal Federal. 2019. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=414010. Acesso em: 16 ago. 2023.

SYDOW, S T. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf. Acesso em: 22 jul. 2023.

TAGLIAMENTO, G.; SILVA, S. S. C. da; SILVA, D. B. da; MARQUES, G. de S.; HASSON, R.; SANTOS, G. E. dos. Minha dor vem de você: uma análise das consequências da LGBTfobia na saúde mental de pessoas LGBTs. **Cadernos de Gênero e Diversidade**, [S. l.], v. 6, n. 3, p. 77–112, 2021.

TEIXEIRA, T. **Marco civil da internet**: comentado. 1ªed. São Paulo: Almerinda. 2016.

VIANNA, T.L. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Editora Forense. 2009.

VEDOVATE, L. L. V. Contratos Eletrônicos. **INTERTEMAS**. v. 10, n. 10. Presidente Prudente, 2005

VIGNOLI, R. G. **A topografia da dark web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço**. 2014. 153 f. Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual de Londrina, Londrina, 2014. Disponível em: http://www.bibliotecadigital.uel.br/document/?view=vtls000191992. Acesso em: 17 jul. 2023.