# CIBERCRIMES
# INOVAÇÕES E O COMBATE EM CONSONÂNCIA COM O ORDENAMENTO JURÍDICO BRASILEIRO

# CYBERCRIMES
# INNOVATIONS AND COMBAT IN LINE WITH THE BRAZILIAN LEGAL SYSTEM

Elivaldo José Macedo[1]
Caroline Gomes Macêdo [2]
Rose Kelly da Silva Lobo[3]

## RESUMO

Este artigo tido como objetivo analisar as inovações e o combate ao cibercrime de acordo com o ordenamento jurídico brasileiro. Buscamos identificar quais os benefícios e malefícios que surgem com o advento da Internet, apontando os tipos de crimes relacionados ao ambiente virtual, em observância ao Direito Penal, discutimos de forma ampliada tais crimes conforme a legislação Brasileira, segundo inovações e as conquistas, por fim apontamos os desafios da legislação brasileira em acompanhar a intensa e rápida evolução dos crimes virtuais. Realizamos uma análise crítica sobre o Cibercrime no Brasil através de pesquisa bibliográfica, tendo como embasamento as novas doutrinas e legislações e suas eficácias. Nossa metodologia foi através do método qualitativo, apoiando-se em técnicas de coletas de dados. Sendo realizada uma pesquisa bibliográfica exploratória, com intuito de proporcionar mais informações sobre o referido tema. A referida pesquisa foi embasada nas doutrinas do Direito Brasileiro, jurisprudências e demais legislações que regulamentem acerca da relação entre os Cibercrimes, além de pesquisas em diversos sites de informativos. A partir desta discussão, concluímos que o ordenamento jurídico brasileiro tem oferecido ferramentas importantes para o combate aos cibercrimes, mas também necessita de inovações para acompanhar a evolução desta criminalidade. Ao concluirmos este artigo, vimos que à uma necessidade de conhecimento por parte dos usuários da internet no Brasil, para com as doutrinas penais, essa necessidade tem que ser suprida pelo Estado.

Palavras-chave: Cibercrime. Ordenamento Jurídico Brasileiro. Inovações Tecnológicas. Prevenção e Combate.

## ABSTRACT

This article aims to analyze the innovations and the fight against cybercrime according to the Brazilian legal system. We seek to identify the benefits and harms that arise with the advent of the Internet, pointing out the types of crimes related to the virtual environment, in compliance with Criminal Law, we discuss such crimes in an expanded way according to Brazilian legislation, according to innovations and achievements, finally we point out the challenges of Brazilian legislation in keeping up with the intense and rapid evolution of virtual crimes. We carried out a critical analysis of Cybercrime in Brazil through

[1]. Graduando do Curso de Bacharel em Direito pela Universidade Luterana do Brasil - Centro Universitário luterano de Santarém – ULBRA. E-mail: macedoelivaldo@gmail.com

[2] Doutora em Biotecnologia pela Universidade Federal do Pará – UFPA. Docente do Curso de Medicina da Universidade do Estado do Pará – UEPA. Coorientadora deste trabalho. E-mail: carolgomesmacedo@hotmail.com

[3] Advogada. Especialista em Ciências Criminais pela Universidade Federal do Pará – UFPA. Professora de Direito Material e Processual Penal. Docente do Curso de Direito da Universidade Luterana do Brasil e orientadora deste trabalho. E-mail: rkellylobo@hotmail.com

bibliographical research, based on new doctrines and legislation and their effectiveness. Our methodology was through the qualitative method, relying on data collection techniques. An exploratory bibliographical research was carried out, in order to provide more information on the aforementioned topic. This research was based on the doctrines of Brazilian Law, jurisprudence and other legislation that regulate the relationship between Cybercrimes, as well as research on various information sites. From this discussion, we conclude that the Brazilian legal system has offered important tools to combat cybercrime, but also needs innovations to follow the evolution of this crime. As we concluded this article, we saw that there is a need for knowledge on the part of internet users in Brazil, regarding criminal doctrines, this need has to be met by the State.

Keywords: Cybercrime. Brazilian legal system. Technological Innovations. Prevention and Combat.

## INTRODUÇÃO

Vivemos em um mundo cada vez mais perigoso e hostil. Se no passado todos os ataques eram físicos e havia fronteiras demarcando os Estados, hoje assistimos à globalização do mundo, onde já não existem fronteiras físicas no sentido clássico da palavra.

O mundo tornou-se uma pequena aldeia onde o que acontece num lugar é logo conhecido em lugares mais remotos (PINTO, 2011).

As inovações advindas das mídias digitais possibilitaram maior liberdade e máxima igualdade individual (ALVES; DINIZ; CASTRO, 2020).

Um computador pode desempenhar três papéis muito diferentes na cena do crime: pode ser o alvo direto de um criminoso; pode ser uma ferramenta essencial para a prática de um crime; pode ser um valioso repositório de evidências para investigações (MPF, 2013).

Esses crimes são particularmente perigosos porque podem ser cometidos anonimamente e de qualquer lugar do mundo.

Se a conduta descrita ocorrer por meio cibernético, ela pode se manifestar, por exemplo, em redes sociais, blogs, mensagens em aplicativos de comunicação instantânea, correspondência eletrônica, etc., em ambiente digital (BARRETO; BRASIL, 2016).

Neste contexto, é necessário criar mecanismos de prevenção e combate ao cibercrime. O ordenamento jurídico brasileiro tem sido uma ferramenta importante nesse processo, pois estabelece as regras a serem seguidas na punição dos infratores.

O cibercrime é um dos maiores desafios para a segurança jurídica atualmente. Ao longo dos anos, os avanços tecnológicos criaram novas formas de crimes que podem ser cometidos a partir da Internet.

Em 2003, foi criado o Comitê Gestor da Internet (CGI.br) para gerenciar os recursos da rede. Este comitê é composto por membros do governo, setor empresarial, academia, etc. (BEZERRA; AGNOLETTO, 2020).

O tema se desenvolve no argumento de que a compreensão a respeito dos crimes cibernéticos e suas legislações atuais, auxiliam na reflexão de estudos e meios de combatê-los, de forma eficaz. Por isso, a importância em conhecer suas classificações, buscando identificar quais os crimes virtuais praticados, e de que formas, tipos e precauções, são mais praticados e como a legislação brasileira os trata tais delitos. Neste sentido justifica-se o proposito desta pesquisa em buscar a aplicabilidade das leis em questões e a eficácia na redução dos crimes virtuais.

Um elemento da luta contra a guerra cibernética é a pesquisa relacionada a projetos de redes mais seguras. A Internet está agora com quarenta anos, praticamente na meia-idade, mas nada mudou desde o seu início. É claro que a largura de banda aumentou, assim como a conectividade sem fio e a proliferação de dispositivos móveis (CLARKE; KNAKE, 2015).

## 2 A HISTÓRIA DO COMPUTADOR

O primeiro computador digital programável feito nos Estados Unidos foi o *Automatic Sequence Controlled Calcutator* (ASCC), que ficou conhecido como Harvard Mark I. Construído pela IBM, em 1944, em uma parceria com a Universidade de Harvard, ele foi o primeiro de uma série de computadores concebidos por Howard H. Aiken (1900 – 1973) (VILLAÇA; STEINBACH, 2014).

> *Eletronic Numerical Integrator and Calculator* (ENIAC), muitos consideram ser o ENIAC, criado em 1946 pelos cientistas norte-americanos John Eckert e John Mauchly, como o primeiro computador a ser fabricado, contudo, o mesmo era imenso e ocupava diversas salas da Universidade da Pensilvânia e consumia uma quantidade grande de energia. A partir deste ponto as evoluções ocorrem de forma acelerada com destaque para as principais: 1951 - lançamento do UNIVAC – primeiro computador vendido comercialmente; anos 60 – o transistor substitui as válvulas, proporcionando uma redução no tamanho das máquinas; anos 70 – Microprocessador; 1981 – Computador com “mouse” e interface gráfica; 1982 – Computador pessoal; 1989 – Linguagem HTML (*Hyper Text Markup Language*); 1996 – Google (buscador); 2001 – Wikipédia (enciclopédia *on-line*); atualmente – *Facebook - Iphone - Ipad - Twitter, Skype, WhatsApp* (BEZERRA; AGNOLETTO, 2020).

Desde a criação do computador, ainda a base de válvulas e vácuo, na década de 1940, seguida por sua difusão nos idos de 1980, e, posteriormente, com a popularização da internet na década seguinte, com a criação do sistema *World Wide Web* (WWW), essas ferramentas vêm desenhando o novo rosto da sociedade: sua face virtual, gerando o que alguns denominam “Sociedade da Informação” (ESTEFAM, 2022).

## 3 COMO FUNCIONA A INTERNET?

A Internet nasceu de um projeto governamental chamado Advanced Research Projects Agency Network (ARPANET). Nas décadas de 1960 e 1970, surgiram outras iniciativas

semelhantes utilizando diferentes protocolos, como Mark I (Reino Unido), CYCLADES (França), Merit Network, Tymnet e Telenet (Estados Unidos). (BRASIL, MPF/SP, 2006).

O princípio em comum entre estas redes era o de comutação de pacotes, um método que possibilita a transmissão de dados em meios de comunicação sem a necessidade de canais dedicados para cada conexão (BRASIL; MPF/DF, 2016).

No início da década de 90, tinha-se uma visão ampla, que haveria uma grande eclosão de números de usuários da Internet. Em 1990, haviam cerca de 2 milhões de pessoas conectadas à rede em todo o mundo (BRASIL, MPF/SP, 2006).

Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos (BRASIL; MPF/DF, 2016).

Existem pelo menos seis grandes vulnerabilidades no próprio design da Internet. A primeira delas é o sistema de endereçamento que descobre para onde ir a partir de um endereço específico. Os Provedores de Serviço de Internet (ISP) são às vezes chamados de carriers, porque são empresas que "carregam" o tráfego da Internet. (BRASIL, MPF/SP, 2006).

Outras empresas fazem terminais de computadores, roteadores, servidores, software, mas são os Provedores de Serviço de Internet que interligam todos eles (CLARKE; KNAKE, 2015).

No início do século XXI, em 2002, esse número passou para 604 milhões (Tabela 1) o número de usuários da internet em alguns Países, triplicou, em outros dobrou.

Tabela 1: Número de usuários da Internet no mundo no ano de 2002

| | País | Usuários da Internet | % | Data da Informação |
|---|---|---|---|---|
| 1 | Estados Unidos | 159,000,000 | 54,26 | 2002 |
| 2 | China | 59,100,000 | 4,55 | 2002 |
| 3 | Japão | 57,200,000 | 44,92 | 2002 |
| 4 | Alemanha | 34,000,000 | 41,25 | 2002 |
| 5 | Coréia do Sul | 26,270,000 | 54,06 | 2002 |
| 6 | Reino Unido | 25,000,000 | 41,48 | 2002 |
| 7 | Itália | 19,900,000 | 34,28 | 2002 |
| 8 | França | 18,716,000 | 30,97 | 2002 |
| 9 | Índia | 16,580,000 | 1,56 | 2002 |
| 10 | Canadá | 16,110,000 | 49,56 | 2002 |
| 11 | Brasil | 14,300,000 | 7,77 | 2002 |
| 12 | México | 10,033,000 | 9,56 | 2002 |
| 13 | Austrália | 9,472,000 | 47,57 | 2002 |
| 14 | Polônia | 8,880,000 | 22,99 | 2002 |

| | | | | |
|---|---|---|---|---|
| 15 | Taiwan | 8,590,000 | 37,76 | 2002 |
| 16 | Holanda | 8,200,000 | 50,25 | 2002 |
| 17 | Indonésia | 8,000,000 | 3,35 | 2002 |
| 18 | Malásia | 7,841,000 | 33,33 | 2002 |
| 19 | Espanha | 7,388,000 | 18,34 | 2001 |
| | Mundo | 604,111,719 | 4,74 | 2004 |

Fonte: *The Cia's World Factbook*

No entanto, no ano de 2018, segundo relatório criado pela Central Inteligence Agency (The CIA World Factbook, 2021-2022) esse número passou para 4,1 bilhões de usuários da internet, atingindo 53,9% da população mundial (Tabela 2).

Tabela 2: Número de usuários da Internet no mundo no ano de 2018

| | **País** | **Usuários da Internet** | **%** | **Data da Informação** |
|---|---|---|---|---|
| 1 | China | 751,886,119 | 54.3% | (July 2018 est.) |
| 2 | Índia | 446,759,327 | 34.45% | (July 2018 est.) |
| 3 | Estados Unidos | 285,519,020 | 87.27% | (July 2018 est.) |
| 4 | Brasil | 140,908,998 | 67.47% | (July 2018 est.) |
| 5 | Japão | 106,725,643 | 84.59% | (July 2018 est.) |
| 6 | Indonésia | 104,563,108 | 39.79% | (July 2018 est.) |
| 7 | México | 82,843,369 | 65.77% | (July 2018 est.) |
| 8 | Alemanha | 72,202,773 | 89.74% | (July 2018 est.) |
| 9 | Reino Unido | 61,784,878 | 94.9% | (July 2018 est.) |
| 10 | França | 55,265,718 | 82.04% | (July 2018 est.) |
| 11 | Coréia do Sul | 49,309,955 | 95.9% | (July 2018 est.) |
| 12 | Itália | 46,305,301 | 74.39% | (July 2018 est.) |
| 13 | Espanha | 42,478,990 | 86.11% | (July 2018 est.) |
| 14 | Canadá | 33,743,954 | 91% | (July 2018 est.) |
| 15 | Polônia | 29,791,401 | 77.54% | (July 2018 est.) |
| 16 | Malásia | 25,829,444 | 81.2% | (July 2018 est.) |
| 17 | Taiwan | 21,845,944 | 92.78% | (July 2018 est.) |
| 18 | Austrália | 21,419,302 | 86.55% | (July 2018 est.) |
| 19 | Holanda | 16,243,928 | 94.71% | (July 2018 est.) |
| | Mundo | 4.1 bilhões | 53.9% | (2019) |

Fonte: *The Cia's World Factbook*

As tabelas 1 e 2, mostram um cenário mundial dos dezenove Países, com maior número de usuários de internet, mais que duplicou.

O Brasil em 2002, já estava em décimo primeiro lugar no ranking mundial com 14.300.000, em 2018 o Brasil entra para era da tecnologia com grande destaque mundial, surgindo em quarto lugar com 140.908.998, atingindo 67,47% de sua população, tendo um crescimento de 89,85%, isso mostra rápida evolução no mundo tecnológico.

Os crimes cibernéticos atingiam em 2011, diariamente, 77 mil brasileiros, com um prejuízo anual de R$ 104 bilhões, segundo levantamento da Norton, Mas os números devem ser vistos com cautela, pois são muito variáveis de empresa para empresa (JESUS; MILAGRE, 2016).

## 4 OS CRIMES CIBERNÉTICOS

### 4.1 Formas mais comuns de criminalidade cibernética

#### 4.1.1 Crimes cibernéticos próprios

São aqueles em que sistemas computacionais, bancos de dados, arquivos ou terminais (como computadores, smartphones, tablets) são atacados por criminosos, geralmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou mesmo por meio de engenharia social. (O golpista faz com que a vítima forneça informações pessoais e/ou estratégicas). Aqui, o dispositivo informatizado e/ou seu conteúdo são alvo dos criminosos (BARRETO; BRASIL, 2016).

Onde o bem jurídico ofendido é a própria tecnologia da informação. Faltava legislação penal para esses crimes, e devido ao princípio da reserva criminal, não foi possível tipificar muitas práticas como criminosas, (JESUS, MILAGRE, 2016).

Eles também conhecidos como crimes de informática próprios, praticados por meio da informática; sem ela, a execução e consumação do crime são impossíveis. São tipos penais relativamente novos, pois surgiram com o desenvolvimento e expansão da informática, sendo a informática um bem protegido criminalmente, (TEIXEIRA, 2022).

#### 4.1.2 Crimes cibernéticos impróprios

São aqueles em que um aparato tecnológico serve de meio para a prática de um crime, possibilitando sua execução ou seu resultado. Aqui, apenas o veículo em que o crime é cometido envolve a tecnologia, enquanto alguns números típicos assumidos no Código Penal Brasileiro ou em leis penais especiais são suficientes, (BARRETO; BRASIL, 2016).

Em que a tecnologia da informação é um meio de atacar bens jurídicos já protegidos pelo Código Penal Brasileiro. A legislação penal é suficiente para esses crimes, pois grande parte da conduta corresponde a um dos tipos penais, (JESUS; MILAGRE, 2016).

Trata de crimes já previstos na legislação penal, que não são propriamente crimes informáticos. São crimes cometidos por meio de um sistema de computador, ou seja, todos os crimes que usam computadores como ferramenta para realizá-los, (TEIXEIRA, 2022).

#### 4.1.3 Algumas tipificações de formas de crimes cibernéticos comuns

A tabela 3 ilustra algumas formas de crimes cibernéticos mais comuns, com as suas respectivas tipificações: (MPF/DF, 2018)

Tabela 3: Algumas tipificações de formas de crimes cibernéticos comuns

| **Crime** | **Tipificação** |
|---|---|
| Estelionato e furto eletrônicos (fraudes bancárias) | arts. 155, §§ 3º e 4º, II, e 171 do CP |
| Invasão de dispositivo informático e furto de Dados | art. 154- A do CP |
| Falsificação e supressão de dados Armazenamento; produção; troca; Publicação de vídeos e imagens | arts. 155, 297, 298, 299, 313-A, 313-B do CP |
| contendo pornografia infantojuvenil | arts. 241 e 241-A, do ECA (Lei nº 8.069/1990) |
| Assédio e aliciamento de crianças | art. 241-D, do ECA (Lei nº 8.069/1990) |
| Ameaça | art. 147 do CP |
| Cyberbullying (veiculação de ofensas em blogs e comunidades virtuais) | arts. 138, 139, 140 do CP |
| Interrupção de serviço | art. 266, parágrafo 1º, do CP |
| Incitação e apologia de crime | arts. 286 e 287 do CP |
| Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional | art. 20 da Lei nº 7.716/1989 |
| Crimes contra a propriedade intelectual artística e de programa de computador | art. 184 do CP e Lei nº 9.609/1998 |
| Venda ilegal de medicamentos | art. 273 CP |

Fonte: MPF, 2018

## 4.2 Cibercrime

### 4.2.1 Etimologia e Conceito

Com o mundo mais tecnológico e globalizado, deslumbrado por seu progresso à velocidade da luz, a sociedade, ficou à mercê de novos tipos de crimes penais, antes vistos apenas na esfera tradicional, estes passaram também a ser praticados na esfera virtual como bem, crimes virtuais ou cibercrimes, assim chamados segundo ditam grandes doutrinadores do direito e também especialistas na área de tecnologia da informação.

Tais crimes são praticados pela internet, levando ao mal moderno, uma nova prática de uma sociedade tecnológica que se desenvolve a cada dia sem precedentes. Os crimes cibernéticos têm um termo amplo que inclui todos os crimes cometidos por meio de redes de computadores e mais especificamente pela internet.

A extensão da atividade criminosa e suas consequências sociais podem ser resumidas por uma tipologia de crimes cibernéticos, como pornografia infantil, furto de propriedade intelectual, ataques a redes de computadores e criminosos convencionais como nos casos em que as evidências existem em formato digital, (ALVES; DINIZ; CASTRO, 2020).

Então, não há sistemas seguros no Ciberespaço, apesar da terminologia militar apontar para a existência dos chamados sistemas seguros, isso pode levar ao equivoco de que tais sistemas são imunes a ataques no Ciberespaço. Não há sistemas imunes no Ciberespaço. Mesmo que o sistema esteja desconectado da Internet, ele pode estar ou ter sido comprometido durante a instalação de aplicativos ou obtidos com o software junto com o sistema operacional. Podemos dizer que são menos perigosos que os sistemas completamente abertos ou não classificados, mas não mais do que isso (MELO, 2011).

Cibercrime nada mais é do que qualquer ato em que um computador ou meios de tecnologia de informação é utilizado a realização de um crime ou em que um computador ou aparelho de informática é objeto de um crime.

O cibercrime está associado ao fenômeno do crime de informação, ações que violam direitos básicos, seja pelo uso de computadores para cometer atividades criminosas, seja como elemento do tipo jurídico da atividade criminosa, (JUNIOR, 2019).

Entendemos o cibercrime como um ato típico e ilegal cometido por meio ou contra a tecnologia da informação.

Baseia-se, portanto, no Direito de Informática, que é um conjunto de princípios jurídicos, normas e entendimentos decorrentes da atividade de informática, (JESUS; MILAGRE, 2016).

A Convenção de Budapeste em 2001, por sua vez, define cibercrime como os atos cometidos contra a confidencialidade, integridade e disponibilidade de sistemas, redes e dados de computadores, bem como uso fraudulento desses sistemas, redes e dados (BARRETO; BRASIL, 2016).

Sujeito ativo pode ser qualquer pessoa, independentemente de qualquer qualidade especial ou condição pessoal, sendo, portanto, crime comum. Você pode ser sujeito ativo inclusive funcionário público. Admite-se, sem dificuldades, a figura do concurso eventual de pessoas, (BITENCOURT, 2019).

Em contrapartida, o sujeito passivo é o proprietário ou dono do dispositivo informático que tenha sido comprometido ou atacado pelo sujeito ativo do crime; também será igualmente o titular do conteúdo contido no dispositivo comprometido ou atacado, mesmo que seja outra pessoa.

Por outro lado, o detentor do conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais sobre o dispositivo atacado ou comprometido também será responsável (§ 3º), (BITENCOURT, 2019).

4.2. 2 Combate ao Cibercrime no Brasil

4.2.2.1 Código Penal Brasileiro e legislação relativos a delitos informáticos

4.2.2.1.1 Estupro Coletivo e Corretivo

A Lei nº 13.718, de 24 de setembro de 2018, altera o decreto – Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal Brasileiro), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688/1941 (Lei das Contravenções Penais) (BRASIL. Lei nº 13.718/2018).

Trata-se de infração que protege, de maneira ampla, a dignidade sexual, ou seja, a dignidade humana no âmbito da sexualidade e, de modo específico, a liberdade sexual das pessoas, tanto assim que o dispositivo somente se aplica quando o sujeito passivo não aquiescer com o ato libidinoso praticado em sua presença (ESTEFAM, 2022).

A Importunação sexual, foi acrescida na Lei nº 13.718, de 24 de setembro de 2018, acrescentando os artigos: Art. 215 – A, com pena de reclusão, de 1 (um) a 5 (cinco) anos, se o ato não constitui crime mais grave. O art. 217 – A. Com pena de reclusão, de 8 (oito) a 15 (quinze) anos. Caput do artigo acrescido pela Lei nº 12.015/2009). (BRASIL. Lei nº 13.718/2018).

A Lei nº 13.718/2018 modificou a redação do art. 225 do Código Penal, estabelecendo que a ação penal nos crimes dos capítulos I e II é pública incondicionada. Assim, para os crimes de estupro praticados a partir de 25 de setembro de 2018, a ação penal não mais dependerá de representação da vítima (GONÇALVES, 2021).

O art. 226. Traz em seu verso: A pena é aumentada (Caput do artigo com redação dada pela Lei nº 11.106/2005). Seus incisos I de quarta parte, se o crime é cometido com o concurso de 2 (duas) ou mais pessoas; II, de metade, se o agente é ascendente, padrasto ou madrasta, tio, irmão, cônjuge, companheiro, tutor, curador, preceptor ou empregador da vítima ou por qualquer outro título tiver autoridade sobre ela; e IV, de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado; o inciso III, foi revogado pela Lei nº 11.106/2005, (PRATES, 2020).

O estupro coletivo, mediante concurso de 2 (dois) ou mais agentes; o estupro corretivo, para controlar o comportamento social ou sexual da vítima.” (Inciso acrescido pela Lei nº 13.718/2018), (BRASIL. Lei nº 13.718/2018).

O art. 234-A. versa: Nos crimes previstos neste Título a pena é aumentada: (Caput do artigo acrescido pela Lei nº 12.015/2009), os incisos I e II, foram vetados na Lei nº 12.015/2009, o inciso III, versa: de metade a 2/3 (dois terços), se do crime resulta gravidez; e com redação dada pela Lei nº 13.718/2018), (PRATES, 2020).

4.2.2.1.2 Estupro Virtual

A Lei nº 12.015, de 7 de agosto de 2009, altera o título VI da parte especial do decreto – Lei nº 2.848/1940 (Código Penal Brasileiro), e o art. 1º da Lei nº 8.072/1990, que dispõe sobre os crimes hediondos, nos termos do inciso XLIII do art. 5º da Constituição Federal e revoga a Lei no 2.252/1954, que trata de corrupção de menores. A Lei alterou a redação do artigo 213 do Código Penal Brasileiro (Estupro).

Entretanto, com as alterações promovidas pela lei mencionada, a nova redação desse crime se tornou “Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso” Art. 213, (BRASIL. Lei nº 12.015/2009).

O bem jurídico protegido, a partir da redação determinada pela Lei nº. 12.015/2009, é a liberdade sexual da mulher e do homem, ou seja, a faculdade que ambos têm de escolher livremente seus parceiros sexuais, podendo recusar inclusive o próprio cônjuge, se assim o desejarem, (BITENCOURT, 2019).

Analisando a nova redação dada ao caput do art. 213 do Código Penal, podemos destacar os seguintes elementos: a) o constrangimento, levado a efeito mediante o emprego de violência ou grave ameaça; b) que pode ser dirigido a qualquer pessoa, seja do sexo feminino ou masculino; c) para que tenha conjunção carnal; d) ou ainda para fazer com que a vítima pratique ou permita que com ela se pratique qualquer ato libidinoso (GRECO, 2017).

Houve um aumento do alcance na lei acerca do ato de estuprar, afirmando que não é necessário a existência do contato físico da vítima com o agressor. A presença da grave ameaça realizada pelo agente é essencial para a consumação do crime, a qual se apresenta através da possível exposição e divulgação de fotos e vídeos de cunho sexual. “Essa ação detém o objetivo de a constranger e a impor medo afim de que se efetive o ato libidinoso,” (ALVES; DINIZ; CASTRO, 2020).

4.2.2.1.3 Estelionato Eletrônico

O delito de estelionato, previsto no art. 171 do Código Penal Brasileiro, também seria alterado, para inserir uma disposição relativa àquele que difundisse, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado. "A pena seria a mesma do caput" (JESUS; MILAGRE, 2016).

Essa figura qualificada foi inserida no Código pela Lei nº 14.155/2021, entrando em vigor no dia seguinte ao de sua publicação. Em virtude de sua índole gravosa, não se aplica a fatos cometidos antes do início de sua vigência (ESTEFAM, 2022).

A Fraude eletrônica, é uma modalidade qualificada de estelionato e causa de aumento de pena a ele relativa, assim dizem os §§ 2º-A e 2º-B, introduzidos ao art. 171 do Código Penal através da Lei nº 14.155, de 27 de maio de 2021, verbis: § 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. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, 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 (BRASIL, Lei nº 14.155/2021).

As Causas de aumento de pena (art. 171, §§ 3º e 4º), pena do estelionato (caput, §§ 2º e 2º-A) aumenta-se de um terço quando figurar como sujeito passivo: Entidade de direito público.

No caso de Instituto de assistência social, Súmula 24 do STJ: "Aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da Previdência Social, a qualificadora do § 3º do art. 171 do Código Penal". (ESTEFAM, 2022)

4.2.2.1.4 Pedofilia

A lei nº 8.069, de 13 de julho de 1990, dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências (BRASIL. Lei Nº 8069/1990). Esta lei pune com maior rigor aqueles que, prevalecendo-se de sua função ou da relação de parentesco ou proximidade com a criança ou adolescente, a induz à prática das condutas que o dispositivo visa coibir.

Em qualquer caso, o eventual "consentimento" da vítima e/ou o fato de já ter se envolvido em situações similares no passado é absolutamente irrelevante para caracterização do crime, aplicando-se entendimento semelhante ao consignado na Súmula nº 593, do STJ (DIGIÁCOMO; DIGIÁCOMO, 2020).

Em parte, o desiderato da novel lei teve por finalidade a alteração das penas, o que se deu no cenário dos arts. 240 e 241, ambos com outra redação. Sob outro aspecto, criaram-se figuras novas, buscando penalizar aqueles que mantêm fotos e outros registros de menores de 18 anos, envoltos em cenas pornográficas ou de sexo explícito (NUCCI, 2018).

No caso de divulgação de cena de sexo envolvendo criança ou adolescente, inclusive em situações de estupro de vulnerável (com vítimas menores de 14 anos), não se aplica o art. 218-C, que é expressamente subsidiário, mas o art. 241-A do ECA, cuja pena é mais grave (JESUS, 2020).

Assim expressa o art. 241-A (Incluído pela Lei nº 11.829/2008). Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (DIGIÁCOMO; DIGIÁCOMO, 2020).

O Art. 241-B (Incluído pela Lei nº 11.829/2008), traz em seu bojo: Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (DIGIÁCOMO; DIGIÁCOMO, 2020).

O delito se consuma com a prática de qualquer dos comportamentos previstos no art. 234, caput, parágrafo único, do Código Penal. Tratando-se de crime plurissubsistente, torna-se possível o raciocínio relativo à tentativa, (JESUS, 2020).

Análise do núcleo do tipo, simular significa representar ou reproduzir algo com a aparência de realidade. O objeto da conduta é a participação de criança ou adolescente em cena de sexo explícito ou pornográfica.

O Art. 241-C (Incluído pela Lei nº 11.829/2008). Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa, (NUCCI, 2018).

> O dispositivo merece críticas, pois só visa crianças, não havendo a tipificação do crime quando as condutas aqui descritas envolver menores. Para tipificação do crime em questão, basta a utilização de "qualquer meio de comunicação" para prática das condutas descritas no dispositivo, não sendo necessária a efetiva prática do ato sexual (que se ocorrer, por sinal, importará na prática de "estupro de vulnerável", tipificado no art. 217-A, do Código Penal, que por ser um crime mais grave, segundo alguns julgados, "absorverá" o crime previsto neste dispositivo, que neste caso será considerado o "crime-meio"), (DIGIÁCOMO; DIGIÁCOMO, 2020).

“O tipo incriminador é inédito e corretamente inserido no Estatuto da Criança e do Adolescente pela Lei nº 11.829/2008”, (NUCCI, 2018).

De acordo com o art. 241-E do ECA, “para efeito dos crimes previstos nesta Lei, a expressão ‘cena de sexo explícito ou pornográfica’ compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais”, (ESTEFAM, 2022).

O art. 241-E, de acordo com o ECA, compreende-se dentre as cenas de sexo explícito ou pornográfica quaisquer situações que retratem o menor em atividades sexuais explícitas, reais ou simuladas, ou exibam seus órgãos genitais para fins primordialmente sexuais (JESUS, 2020).

4.2.2.1.5 Violação de segredo profissional

Para a ocorrência do delito é imprescindível um vínculo entre o exercício de atividade privada e o conhecimento do segredo. É um crime doloso, consistente na presença de elementos cognitivos (consciência) e voluntário (vontade) que possibilitem a ação do agente. Portanto, é necessário, a intenção de revelar o segredo capaz de causar danos. A modalidade culposa não é permitida (MACHADO, 2017).

O Código Penal Brasileiro, protege o sigilo profissional. Há casos em que a aquele que se torna confidente de segredos, em razão de função, ministério, ofício ou profissão, tem o dever legal de protegê-los do público.

Isso ocorre nas hipóteses, de o criminoso confessar em sua defesa a autoria de um crime, ou de um paciente revela a seu médico doença grave e contagiosa de que o aflige, ou de alguém confessar a seu sacerdote a prática de ato indecoroso, ou de o dono de um cofre revelar ao serralheiro o seu segredo, etc. (JESUS, 2020).

O objetivo do tipo penal é punir aquele que, meio de suas atividades exercida, obtém um segredo e, à vez de ocultá-lo, revelar a terceiros, possibilitando assim dano a outrem. Neste tipo penal, ao contrário do que acontece com o anterior, o segredo pode se concretizar oralmente.

O Art. 154. Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de 3 (três) meses a l (um) ano, ou multa, (ESTEFAM, 2022).

4.2.2.1.6 Crime funcional (Servidor Público ou Equiparado)

A Lei n. 9.983/2000 acrescentou o § 1º ao art. 327, que equipara a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, nos seguintes termos: equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública, (BITENCOURT, 2019).

Causa de aumento da pena, caso o agente dos delitos previstos nos arts. 293 e 294 seja funcionário público (ver art. 327, CP), a pena deve ser aumentada em um sexto (art. 295, CP). Por outro lado, exige-se que o funcionário tenha utilizado, de algum modo, as facilidades proporcionadas pelo seu cargo, (NUCCI, 2019).

4.2.2.1.7 Pornografia de vingança;

A Lei nº 13.718, de 24 de setembro de 2018, altera o decreto-Lei nº 2.848/1940 (Código Penal Brasileiro), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir estupro coletivo e estupro corretivo como razões para aumento de penas; Isso é revogada dispositivo do Decreto-Lei nº 3.688/ 1941 (Lei das Contravenções Penais), (BRASIL. Lei nº 13.718/2018).

Protege-se a dignidade sexual, a honra e a intimidade das pessoas e, ainda, a paz pública. O dispositivo legal tipifica duas condutas. A primeira delas consiste na divulgação de cena envolvendo estupro ou estupro de vulnerável e é nesse contexto que se tutela, além da honra e da intimidade das vítimas desses crimes, a paz pública, porque o fato poderia incentivar terceiros a fazer o mesmo, (ESTEFAM, 2022).

A publicação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia está disciplinada pelo Art. 218-C. do Código Penal Brasileiro. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática, uma f otografia, vídeo ou outra gravação audiovisual que contenha cena de estupro ou de estupro de uma pessoa vulnerável; ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

O aumento de pena esta elencado no § 1º. A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação, (JESUS, 2020).

4.2.2.1.8 Violência psicológica

A Lei nº 13.772, de 19 de dezembro de 2018, altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal Brasileiro), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado, (BRASIL. Lei nº 13.772/2018).

Deve-se destacar que a Lei nº 13.772/2018, também modificou a Lei Maria da Penha, a fim de incluir a "violação da intimidade" da mulher como situação configuradora de violência psicológica (art. 7º, inciso II, da Lei nº 11.340/2016), (ESTEFAM, 2022).

Registro não autorizado da intimidade sexual, denominação jurídico acrescentada pela Lei nº 13.772/2018. Este capítulo foi introduzido no Código Penal pela Lei nº 13.772, de 19 de dezembro de 2018. O único delito deste capítulo é "não autorizado registro da intimidade sexual (art. 216-B), (GONÇALVES, 2021).

4.2.2.1.9 Ciberstalking

A Lei nº 14.132, de 31 de março de 2021. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848/1940 (Código Penal Brasileiro), que regulamenta o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688/1941 (Lei das Contravenções Penais), (BRASIL. Lei nº 14.132/2021).

Como ensina Luciana Gerbovic, "Stalker é o perseguidor, alguém que escolhe uma vítima por diversos motivos e a assedia persistentemente, por meio de atos persecutórios – direta ou indireta, presencial ou virtual – sempre contra a vontade da vítima. Em outras palavras, stalker é aquele que promove uma "caça" física ou psicológica contra alguém" (apud, GRECO, 2022).

> O Art. 147-A do Código Penal Brasileiro, diz que: Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. § 1º A pena é aumentada de metade se o crime é cometido: I – contra criança, adolescente ou idoso; II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código; III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. § 3º Somente se procede mediante representação.

4.2.2.1.10 Cyberbullying

4.2.2.1.10.1 Conceito

De origem inglesa e ainda não está traduzido no Brasil, é usado para qualificar comportamentos agressivo na escola, é praticado tanto por meninos quanto por meninas (SILVA, 2010).

Para Silva (2015). O bullying "é um fenômeno tão antigo quanto a própria instituição chamada escola". No entanto, o assunto tornou-se objeto de estudo científico apenas no início da década de 1970.

Tudo começou na Suécia, onde grande parte da sociedade manifestava preocupação com a violência entre alunos e suas consequências no ambiente escolar. Em pouco tempo, a mesma onda de interesse espalhou para todos os outros países escandinavos. (SILVA, 2010)

Segundo o Ministério Púbico Federal (MPF, 2013), "o cyberbullying é um fenômeno que surgiu com o aparecimento da Internet e a popularização das redes sociais." No ambiente virtual, a violência se revela pelas intimidações, ridicularizações, humilhação e ameaças, mensagens ou fotos, muitas vezes adulteradas, enviadas à vítima e/ou publicadas na rede e visualizadas por um número incalculável de pessoas no espaço público, causam prejuízos isso é difícil de reparar porque algo postado na internet, mesmo que removido, poderia ser resgatado por qualquer pessoa no mundo que pudesse replicar o conteúdo novamente, perpetuando a perseguição.

4.2.2.1.10.2 As formas de bullying

Verbal (insultar, ofender, falar mal, colocar apelidos pejorativos, "zoar"), física e material (bater, empurrar, beliscar, roubar, furtar ou destruir pertences da vítima), Psicológica e moral (humilhar, excluir, discriminar, chantagear, intimidar, difamar), Sexual (abusar, violentar, assediar, insinuar), virtual ou Ciberbullying (bullying realizado por meio de ferramentas tecnológicas: celulares, filmadoras, internet etc.), (SILVA, 2010).

4.2.2.1.10.3 Aspectos Jurídico-Penais Relacionados ao Ciberbullying

O bem jurídico protegido pela tipificação do crime de calúnia é, para quem aceita esta divisão, a honra objetiva, ou seja, a reputação da pessoa, ou seja, é o conceito que os demais membros da sociedade têm a respeito do indivíduo, relativamente a seus atributos morais, éticos, culturais, intelectuais, físicos ou profissionais, (BITTENCOURT, 2019).

Calúnia Art. 138. Valor protegido (objetividade jurídica). Honra objetiva, ou seja, a reputação o bom nome da pessoa. "É o conceito da vítima perante o meio social." Tipo objetivo (ESTEFAM, 2022).

A calúnia ocorre com a falsa atribuição a alguém de fato definido como crime. Imputar (ação nuclear) significa atribuir, ou seja, contar um fato inserindo uma pessoa como responsável. É preciso que este fato seja tipificado como ato criminoso (JESUS, 2020).

Se a lei julgar isso como contravenção penal, não haverá calúnia, mas difamação (que consiste na atribuição de outros fatos ofensivos à honra). Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa. (ESTEFAM, 2022)

Difamar significa desacreditar publicamente uma pessoa, prejudicar sua reputação. Nesse caso, o tipo penal foi deliberadamente repetitivo. Difamar já significa atribuir algo vergonhoso a outrem, embora a descrição abstrata feita pelo legislador tenha deixado claro que dentro da infração penal do art. 139, não se trata de qualquer fato inconveniente ou negativo, mas sim um insulto à sua reputação. (NUCCI, 2019)

> De todas os crimes elencados no Código Penal Brasileiro voltados à proteção da honra, a injúria, em sua forma básica é considerado menos grave. Por mais paradoxal que pareça, a injúria torna-se a mais grave infração penal contra a honra quando consiste na utilização de elementos referentes à raça, cor, etnia, religião, origem ou à condição de pessoa idosa ou portadora de deficiência, sendo denominada, aqui, de injúria preconceituosa, cuja pena a ela equiparável à pena prevista para o crime de homicídio culposo, é ainda mais grave, porque no caso de homicídio culposo é imposto uma pena de detenção, de 1 (um) a 3 (três) anos, e na injúria preconceituosa uma pena de reclusão, de 1 (um) a 3 (três) anos e multa, sendo discutida sua proporcionalidade comparativamente às demais infrações penais (GRECO, 2017).

O crime de injúria art. 140 do Código Penal Brasileiro, protege a honra subjetiva, ou seja, o sentimento que cada pessoa tem de qualidades físicos, morais ou intelectuais. “É um crime que atinge a autoestima da vítima, sua autoestima. a injúria, o agente não contam, mas atribui uma qualidade negativa ao outro.” (GONÇALVES, 2021)

O parágrafo único do art. 140 da Lei de Execução Penal obriga o juiz, caso não tenha revogado o livramento condicional, na hipótese facultativa, que advirta o liberado ou exaspere as condições. “Ao não revogar, o juiz é obrigado a advertir o liberado ou tornar mais severas as condições impostas na sentença concessiva,” (JESUS, 2020).

#### 4.2.2.1.11 Ciberterrorismo

##### 4.2.2.1.11.1 Conceito

Ciberterrorismo, atos baseados em motivação política, ideológica ou social e operações de *hacking* com o objetivo de causar danos graves (perda de vidas humanas, danos económicos, ataques ou ameaças a sistemas informáticos, redes e informações relevantes nelas armazenadas) para o efeito de intimidação, ou coagir um governo (PINTO, 2011).

Pode ser um ataque físico com o objetivo de destruir nós computorizados de infraestrutura crítica (internet, telecomunicações) ou redes elétricas de um país ou cidade. O ciberterrorismo é semelhante ao cibercrime, mas é uma versão mais extrema do cibercrime com piores consequências (PINTO, 2011).

4.2.2.1.11.2 Aspectos Jurídico-Penais Relacionados ao Ciberterrorismo.

A Lei nº 13.260 de 16 de março de 2016, regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e Lei nº 12.850, de 2 de agosto de 2013 (BRASIL. Lei nº 13.260/2016).

No campo doutrinário, é muito difícil definir com precisão e objetividade o fenômeno do terrorismo. Grande parte dessa dificuldade está enraizada na própria natureza do ato, que assume diferentes formas dependendo do país, motivação e métodos.

A razão desse problema tem três aspectos: o primeiro é que o terrorismo, como o crime organizado, muda constantemente de aspecto de acordo com as condições históricas, culturais e geográficas. Outra razão é o enquadramento no tipo penal, pois cada figura típica requer abstração conceitual, definição precisa, abrangência geral e aplicação no tempo. (REVISTA JURÍDICA, 2017).

4.2.2.1.12 Deep Web e Dark Web

4.2.2.1.12.1 Conceito

Para o MPF a *Deep Web*, parte da Internet fechada, utilizada para comunicações e troca de arquivos de forma anônima (não é indexada por mecanismos de busca comuns).

Acessada através de aplicativos da “Rede TOR” (The Onion Rout), que elimina os rastros do acesso (BRASIL, MPF, 2015).

Em 1996, Paul Syverson e outros militares do Laboratório Central da Marinha dos Estados Unidos para Segurança de Computadores, com a ajuda da *Darpa* (www.darpa.mil), desenvolveram um software livre de rede aberta capaz de estabelecer uma comunicação resistente a ataques e análises dos pacotes de dados trafegados e, ainda, que não permitisse ser descoberta a origem do acesso. Assim nascia o projeto Tor (BARRETO; WENDT; CASELI, 2017).

Estatísticas mostram que somente 10% da Internet é acessível, o restante está na *Deep Web*. Ela é usada para práticas ilícitas como: Venda de Drogas, Vendas de armas, Documentos falsos, Pedofilia. (MPF, 2015).

Na Operação *DirtyNet*, uma operação inédita no Brasil com infiltrações de policiais na *Deep Web* usando malwares para comprovação de delitos, constatou-se a troca de arquivos de pornografia infantil que ocorria utilizando o aplicativo GIGATRIBE (rede P2P privada). Com o resultado desta operação, houve a criação de um fórum sobre pedofilia controlado pela Polícia Federal para rastreamento de suspeitos (MPF, 2015).

Existem diversas possiblidades de preservação do conteúdo investigado na *Deep Web*. Os mais acessíveis estão: Preservação via printscreen – através desta sistemática, haverá materializado o conteúdo do site em forma de um arquivo de imagem (BARRETO; WENDT; CASELI, 2017).

Diferente da *Deep Web*, a *Dark Web* ou *Darknet* é uma rede fechada, usada para compartilhar conteúdo de forma anônima. Seu acesso é permitido mediante o uso de softwares específicos, como o TOR Project, o Freenet e a rede I2P (2017) ou outras dezenas de redes secretas e criptografadas. (BRASIL, TRF 3ª REGIÃO, 2017)

4.2.2.1.13 Validade Jurídica das Evidências Digitais Colidas na Web

A Lei nº 14.382, de 27 de junho de 2022, Dispõe sobre o Sistema Eletrônico dos Registros Públicos (SERP); altera as Leis: Lei nº 4.591/1964, Lei nº 6.015/1973 (Lei de Registros Públicos), Lei nº 6.766/1979, Lei nº 8.935/1994, Lei nº 10.406/2002 (Código Civil Brasileiro), Lei nº 11.977/2009, Lei nº 13.097/2015, e Lei nº 13.465/2017; e revoga a Lei nº 9.042/1995, e dispositivos das Leis: Lei nº 4.864/1965, Lei nº 8.212/1991, Lei nº 12.441/2011, Lei nº 12.810/2013, e Lei nº 14.195/2021, (BRASIL, Lei nº 14.382/2022).

Dos atos processuais em meio eletrônico. A sistematização dos atos processuais no CPC/2015 veio complementar as disposições previstas na Lei nº 11.419/2006. Vale ressaltar que, além de estender a prática eletrônica aos atos notariais e de registro, o CPC/2015 estabelece que, ainda que os autos sejam apenas parcialmente virtuais, todos os atos processuais deverão ser produzidos, comunicados, armazenados e validados por meio eletrônico. Em outras palavras, os autos físicos coexistirão com os autos virtuais, (DONIZETTI, 2018).

O art. 193 do CPC de 2015 prevê que “os atos processuais podem ser totais ou parcialmente digitais, de forma a permitir que sejam produzidos, comunicados, armazenados e validados por meio eletrônico, na forma da lei”. (TEIXEIRA, 2022)

4.2.2.1.14 Invasão de dispositivo informático.

O art. 154-A contém, ainda, forma qualificada, aplicável quando a conduta resultar na obtenção de conteúdo de comunicações eletrônicas privadas (e-mails), segredos comerciais ou industriais (patentes, planos de negócio, estratégias comerciais), informações sigilosas definidas em lei ou o controle remoto do dispositivo (JESUS, 2020).

Esta figura típica do art. 154-A – invasão de dispositivo informático – insere-se no contexto dos crimes contra a liberdade individual, bem jurídico mediato a ser tutelado. (NUCCI, 2019)

A fim de antecipar a possibilidade de punir os cibercriminosos que disseminarem vírus ou spyware pela rede ou atacarem equipamentos de informática alheios, a referida lei introduziu no artigo 154-A do Código Penal o crime denominado “invasão de dispositivo informático”, (GONÇALVES, 2021).

Crime qualificado, § 3º. Se 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: Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (BITTENCOURT, 2019)

Se em razão da invasão ocorrer o controle remoto não autorizado do dispositivo invadido – ou mesmo a obtenção de conteúdo de comunicações eletrônicas privadas (como os e-mails), informações sigilosas, segredos comerciais ou industriais –, a pena passa a ser de reclusão, e não de detenção. Nestas hipóteses, aumenta-se a pena se houver divulgação, comercialização ou transmissão a terceiro, de forma gratuita ou não, dos dados ou informações obtidas, nos termos dos §§ 3º e 4º do art. 154-A do Código Penal. (TEIXEIRA, 2022).

No § 5º. Aumenta-se a pena de um terço à metade se o crime for praticado contra: I – Presidente da República, governadores e prefeitos; II – Presidente do Supremo Tribunal Federal; III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (JESUS, 2020)

De acordo com o art. 154-B do CP, nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (ESTEFAM, 2022)

A ação penal, conforme determinação contida no art. 154-B, incluído também pela Lei nº 12.737/2012, será de iniciativa pública condicionada à representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, ou contra empresas concessionárias de serviços públicos (GRECO, 2017).

O objeto material desta infração penal é o serviço telegráfico, radiotelegráfico, telefônico, telemático ou de informação de utilidade pública. Sua disciplina é o art. 266 do Código Penal Brasileiro. Pena: detenção, de 1 (um) a 3 (três) anos, e multa. A Lei nº 12.737/2012, que criou nova figura penal no § 1º, também acrescentou novo bem jurídico, qual seja, a proteção do serviço telemático, bem como de informação de utilidade pública. "Na verdade, referido diploma legal acrescentou um novo parágrafo, e renumerou o parágrafo único que passou a ser o § 2º deste artigo." (BITTENCOURT, 2019)

### 4.3 Os desafios da legislação brasileira em acompanhar a intensa e rápida evolução dos crimes virtuais.

A origem da tentativa de regulamentação legislativa sobre os assuntos ligados a internet começa com a Ordem dos Advogados do Brasil (OAB) em 1999 com uma comissão criada especialmente para redigir um modelo para a lei a ser apresentada ao Congresso Nacional. Contudo, tratava-se de uma regulamentação de comércio eletrônico (validade de documentos eletrônicos e assinatura digital), (BEZERRA; AGNOLETTO, 2020, pág. 15).

A Lei nº 12.735 de 30 de novembro de 2012, altera o Decreto-Lei nº 2.848/1940 ( Código Penal Brasileiro), o Decreto-Lei nº 1.001/1969 (Código Penal Brasileiro Militar), e a Lei nº 7.716/1989 (define os crimes resultantes de preconceito de raça ou de cor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências, (BRASIL, Lei nº 12.735/2012).

O projeto substitutivo do senador Eduardo Azeredo agregou num único texto as propostas apresentadas no Projeto de Lei da Câmara dos Deputados 89/2003 e nos Projetos de Lei do Senado Federal 76/2000 e 137/2000. O projeto substitutivo modifica a legislação penal brasileira: Decreto-Lei nº 2.848/1940 (Código Penal Brasileiro); Decreto-Lei nº 1.001/1969

(Código Penal Brasileiro Militar) e as Leis Federais: Lei nº 7.716/1989 e Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente) e Lei nº 10.446/2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, ou que sejam praticadas contra sistemas informatizados e similares e dá outras providências (MOLITOR; VELAZQUEZ, 2017).

O conteúdo do projeto de Azeredo segue definições estabelecidas internacionalmente pela Convenção de Budapeste (2001), ratificada por 43 países da Comunidade Europeia e pelos Estados Unidos, em vigor a partir de 2007 (GOUVEIA, 2007).

Além disso, a Lei nº 12.735/2012 no art. 5º, determinou que a Lei nº 7.716/1989, passasse a conter o inciso II no § 3º do art. 20, para obrigar que a prática, a indução ou incitação de discriminação, ou preconceito de raça, cor, etnia, religião ou procedência nacional, praticados por intermédio dos meios de comunicação social ou publicação de qualquer natureza, tenham a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio (CRESPO, 2016) .

A Lei n° 12.737 de 30 de novembro de 2012. Denominada de Carolina Dickmann, dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848/1940 (Código Penal Brasileiro); e dá outras providências.

Foi elaborada justamente com este escopo, ou seja, muito mais do que “homenagear” uma atriz, surgiu para colmatar relevantes lacunas existentes no ordenamento jurídico (ESTEFAM, 2022).

Bens juridicamente protegidos são a liberdade individual e o direito à intimidade, configurados na proteção da inviolabilidade dos dados e informações existentes em dispositivo informático (GRECO, 2022).

Neste sentido, a Lei nº 12.737/2012 pretendeu criminalizar a criação e disseminação de vírus computacional, os ataques tipo Denial of Service (DoS) e, ainda, o chamado hacking (invasão a sistemas), entre outras condutas.

A lei inseriu os arts. 154-A e 154-B no Código Penal Brasileiro, criando a “invasão de dispositivo informático” e regulamentando sua ação penal, que será condicionada à representação como regra e, no caso de prática em desfavor da Administração Pública, será pública incondicionada (CRESPO, 2016).

A Lei n° 12.965 de 13 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O Marco Civil inicia-se com o comando legal de que nele se estabelecem os princípios, garantias, direitos e deveres para o uso da internet no Brasil. Primeiramente, há que se

ressaltar que tal comando pressupõe um equívoco do legislador e uma total dissonância do sistema jurídico em que se insere o Marco Civil. Quem estabelece princípios, garantias, direitos e deveres para quaisquer usos e tecnologias é a Constituição Federal do Brasil.

O Marco Civil "é uma legislação infraconstitucional que deveria implementar e regulamentar a Constituição. Contudo, não é isso que ocorre" (GONÇALVES, 2017).

Uma das funções do Marco Civil Brasileiro é gerar segurança jurídica, oferecendo base legal ao Poder Judiciário quando se deparar com questões envolvendo internet e tecnologia da informação, evitando-se decisões contraditórias sobre temas idênticos, o que era muito comum (JESUS; MILAGRE, 2014).

A Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

A Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder.

A proteção aos direitos fundamentais é bastante evidente no art. 2° da LGPD, que pode ser relacionado ao texto constitucional brasileiro no que concerne ao conteúdo, haja vista que a Constituição Federal Brasileira é pautada na proteção aos direitos fundamentais. Entre os artigos constitucionais destacáveis, pode-se citar: art. 3°, I e II; art. 4°, II; art. 5°, X e XII; art. 7°, XXVII; e art. 219 (PINHEIRO, 2018).

A divergência entre doutrinadores, a LGPD se preocupa e versa apenas e tão somente sobre o tratamento de dados pessoais. Ou seja, não atinge diretamente dados de pessoa jurídica, documentos sigilosos ou confidenciais, segredos de negócio, planos estratégicos, algoritmos, fórmulas, softwares, patentes, entre outros documentos ou informações que não sejam relacionadas a pessoa natural identificada ou identificável.

Toda essa miríade de outros tipos de informações ou documentos encontram tutela em distintos diplomas legais, como a Lei de Propriedade Industrial (Lei nº 9.279/1996), a Lei de Direitos Autorais (Lei nº 9.610/1998) e a Lei de Software (Lei nº 9.609/1998), apenas para citar alguns exemplos (MALDONADO; BLUM, 2020).

A Lei nº 13.441, de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Nela previsto, elenca as seguintes regras para que possa efetivamente ocorrer a mencionada infiltração.

> Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal Brasileiro) , obedecerá às seguintes regras: I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público; II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas; III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial. § 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo. § 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se: I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão; II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão. § 3º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios. (BRASIL, Lei nº 13.441/2017).

Sujeitos ativo e passivo: Podem ser qualquer pessoa; Elemento subjetivo: É o dolo; Objetos material e jurídico: O objeto material é o dispositivo informático; o objeto jurídico é a inviolabilidade da intimidade e da vida privada das pessoas; Classificação: Trata-se de crime comum (pode ser cometido por qualquer pessoa) (NUCCI, 2019).

Art. 190-B. As informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo (incluído pela Lei nº 13.441/2017). Parágrafo único. Antes da conclusão da operação, o acesso aos autos será reservado ao juiz, ao Ministério Público e ao delegado de polícia responsável pela operação, com o objetivo de garantir o sigilo das investigações.” (incluído pela Lei nº 13.441/2017).

Art. 190-C. Não comete crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848/1940 (Código Penal Brasileiro). Parágrafo único. O agente policial infiltrado que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados.” (incluído pela Lei nº 13.441/2017).

Art. 190-D. Os órgãos de registro e cadastro público poderão incluir nos bancos de dados próprios, mediante procedimento sigiloso e requisição da autoridade judicial, as informações necessárias à efetividade da identidade fictícia criada. Parágrafo único. O procedimento sigiloso de que trata esta Seção será numerado e tombado em livro específico.” (incluído pela Lei nº 13.441/2017).

Art. 190-E. Concluída a investigação, todos os atos eletrônicos praticados durante a operação deverão ser registrados, gravados, armazenados e encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado. Parágrafo único. Os atos eletrônicos registrados citados no caput deste artigo serão reunidos em autos apartados e apensados ao processo criminal juntamente com o inquérito policial, assegurando-se a preservação da identidade do agente policial infiltrado e a intimidade das crianças e dos adolescentes envolvidos." (incluído pela Lei nº 13.441/2017).

A Lei nº 14.132, de 31 de março de 2021. A perseguição de que trata o tipo penal nos remete ao denominado *stalking* (perseguindo). Sua finalidade "é a tutela da liberdade individual, abalada por condutas que constrangem alguém a ponto de invadir severamente sua privacidade e de impedir sua livre determinação e o exercício de liberdades básicas," (CUNHA, 2021).

O que se busca com a incriminação "é salvaguardar a liberdade pessoal, em primeiro plano, além da integridade psíquica e física das pessoas, tolhidas em sua tranquilidade quando são alvo de uma perseguição reiterada, que invade sua privacidade e prejudica seu bem-estar cotidiano" (ESTEFAM, 2022).

A Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848/1940 (Código Penal Brasileiro), 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/ 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

A Lei nº 12.737, de 30 de novembro de 2012, inseriu o art. 154-A ao Código Penal Brasileiro, havendo modificações em sua redação original trazida pela Lei nº 14.155, de 27 de maio de 2021, exigiu a presença dos seguintes elementos para efeitos de caracterização do delito de invasão de dispositivo informático: "a) o núcleo invadir; b) dispositivo informático alheio; c) conectado ou não à rede de computadores; d) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo; e) ou de instalar vulnerabilidades para obter vantagem ilícita" (GRECO, 2017).

## 5 CONSIDERAÇÕES FINAIS

Ao longo do presente trabalho, abordamos os temas relacionados às inovações e ao combate aos cibercrimes de acordo com o ordenamento jurídico brasileiro. Observou-se que a legislação brasileira vem se adequando às novas exigências, especialmente no que tange à criminalização dos atos cibernéticos. No entanto, o desafio das autoridades na prevenção e no combate aos cibercrimes é crescente, uma vez que estes crimes se caracterizam por serem

difíceis de serem detectados, muitas vezes com consequências irreversíveis para as vítimas. Assim, é necessária a realização de ações que visem promover a conscientização dos usuários, bem como a capacitação dos órgãos responsáveis pela investigação e aplicação da lei. Apesar da atual legislação brasileira não conseguir acompanhar as novas tecnologias emergentes, ela ainda é capaz de fornecer uma base sólida para a criminalização dos crimes cibernéticos e para a proteção das vítimas, permitindo que as autoridades responsáveis possam tomar as medidas necessárias e punir os criminosos. Portanto, é necessário que o Estado adote medidas mais eficazes e eficientes para o combate aos crimes cibernéticos, buscando o aperfeiçoamento constante da legislação em consonância com as novas tecnologias existentes, para ser possível proteger, de forma efetiva, os cidadãos brasileiros. Para a Escola de Magistrados da Justiça Federal da 3ª região, sugere em seu Caderno de Estudos 1, especializar os legisladores e dar expertise à magistratura, são medidas essenciais para combater esta nova onda de crimes tecnológicos, que infelizmente não parece diminuir a cada ano.

## 6 REFERÊNCIAS


ALVES, Marco Antônio; DINIZ, Thiago Dias de Matos; CASTRO, Viviane Vidigal de. **Criminologia e cybercrimes [Recurso eletrônico on-line] organização XI Congresso RECAJUFMG:** UFMG – Belo Horizonte; Coordenadores: Marco Antônio Alves, Thiago Dias de Matos Diniz e Viviane Vidigal de Castro – Belo Horizonte: UFMG, 2020.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet.** 1 Ed., São Paulo: Brasport, 2016.

BARRETO, Alesandro Gonçalves; WENDT, Emerson Wendt; CASELI, Guilherme Caselli. **Investigação Digital em Fontes Abertas, buscas de dados em rede sociais, coleta de informações na Deep Web, Análise de metadados**, BRASPORT, 2ª ed. 2017

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate ao Crime Cibernético** / Clayton da Silva Bezerra 1. ed.- Rio de Janeiro; Mallet Editora, 2020.

BITENCOURT, Cezar Roberto. **Código Penal comentado** / Cezar Roberto Bitencourt. – 10. ed. – São Paulo: Saraiva Educação, 2019.

BRASIL. **LEI Nº 12.015, de 7 de agosto de 2009.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm#:~:text=%E2%80%9CViola%C3%A7%C3%A3o%20sexual%20mediante%20fraude&text=Ter%20conjun%C3%A7%C3%A3o%20carnal%20ou%20praticar,a%206%20(seis)%20anos. Acessada em 17/02/2023

BRASIL. **LEI Nº 12.735, de 30 de novembro de 2012**. Disponível em

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acessado em 03/11/2022

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. Acessado em 03/11/2022

BRASIL. **Lei N° 12.965 de 13 de abril de 2014. Marco Civil da Internet.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 02/11/2022

BRASIL. **LEI Nº 13.441, de 8 de maio de 2017.** Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm#:~:text=LEI%20N%C2%BA%2013.441%2C%20DE%208,de%20crian%C3%A7a%20e%20de%20adolescente. Acessada em 17/02/2023

BRASIL. **LEI Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessada em 02/11/2022

BRASIL. **LEI Nº 13.718, de 24 de setembro de 2018.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acessado em 20/02/2023

BRASIL. **LEI Nº 13.772, de 19 de dezembro de 2018.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13772.htm#:~:text=Registro%20n%C3%A3o%20autorizado%20da%20intimidade%20sexual&text=Produzir%2C%20fotografar%2C%20filmar%20ou%20registrar,Par%C3%A1grafo%20%C3%BAnico. Acessado em 20/02/2023

BRASIL. **LEI Nº 14.132, de 31 de março de 2021.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acessada em 14/02/2023

BRASIL. **LEI Nº 14.155, de 27 de maio de 2021.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acessada em 17/05/2023.

BRASIL. **LEI Nº 14.382, de 27 de junho de 2022.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14382.htm. Acessada em 17/02/2023

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.

BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados **Investigação e prova nos crimes cibernéticos.** São Paulo: EMAG, 2017.

BRASIL. **REVISTA JURÍDICA** da Escola Superior do Ministério Público de São Paulo, ANO 6. V. 11, janeiro-junho 2017, Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-Juridica-ESMP-SP_n.11.pdf. Acessado em 10/02/2023

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos** / 2. Câmara de coordenação e revisão. – 3. ed. rev. e ampl. – Brasília: MPF, 2016.

BRASIL. Ministério Público Federal (MPF). **Atuação do Ministério Público Federal, COMBATE AOS CRIMES CIBERNÉTICOS, "Atuação_do_MP_no_combate_aos_crimes_cibernéticos INFANCIA_E_JUVENTUDE", Curso de capacitação para procuradores e juízes realizado pela. ESMPU, em 20 a 22/10/2015. - Curso sobre atuação do MPF no combate aos crimes cibernéticos**. Disponível em: https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf. Acessado em 16/09/2022;

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação: crimes cibernéticos.** 2 ed. rev. - Brasília: MPF/2ª CCR, 2013. Págs; 326 a 329.

BRASIL. Ministério Público Federal, Procuradoria da República no estado de SP, **Grupo de Combate aos Crimes Cibernéticos, CRIMES CIBERNÉTICOS MANUAL PRÁTICO DE INVESTIGAÇÃO, abril de 2006**. Disponível em: https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/ManuaL%20Pr%C3%83%C2%A1tico%20de%20Investiga%C3%83%C2%A7%C3%83%C2%A3o%20sobre%20Crimes%20de%20Inform%C3%83%C2%A1tica.PDF. Acessado em 17/02/2023

CLARKE, Richard A.; KNAKE, Robert K. **GUERRA CIBERNÉTICA, A Próxima Ameaça à Segurança e o que fazer a respeito**, Richard A. Clarke, Robert K. Knake. BRASPORT, 2015.

CRESPO, Marcelo Xavier de Freitas. **As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos,** Publicado por Canal Ciências Criminais, 2016. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/201526971/as-leis-n-12735-2012-e-12737-2012-e-os-crimes-digitais-acertos-e-equivocos-legislativos. Acessado em 03/11/2022

CUNHA, Rogério Sanches. **LEI 14.132/21: INSERE NO CÓDIGO PENAL O ART. 147-A, PARA TIPIFICAR O CRIME DE PERSEGUIÇÃO,** 01/04/2021, Rogério Sanches Cunha, São Paulo. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/04/01/lei-14-13221-insere-no-codigo-penal-o-art-147-para-tipificar-o-crime-de-perseguicao/. Acessado em: 13/02/2023

DONIZETTI, Elpídio. **Novo Código de Processo Civil Comentado** / Elpídio Donizetti – 3. ed. rev., atual. e ampl. – São Paulo: Atlas, 2018.

DIGIÁCOMO, Murillo José; DIGIÁCOMO, Ildeara Amorim. 1968 - **Estatuto da criança e do adolescente anotado e interpretado** / Murillo José Digiácomo e Ildeara Amorim Digiácomo - Curitiba. Ministério Público do Estado do Paraná. Centro de Apoio Operacional das Promotorias da Criança e do Adolescente, 2020. 8ª Edição.

ESTEFAM, André. **Direito Penal: Parte Especial – Arts. 121 a 234-C – v. 2** / André Estefam. 9. ed. São Paulo: SaraivaJur, 2022.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. **Direito Penal: Parte Geral** / André Estefam, Victor Eduardo Rios Gonçalves; coord. Pedro Lenza. 11. ed. São Paulo: SaraivaJur, 2022.

GONÇALVES, Victor Hugo Pereira. **Marco Civil da Internet comentado** / Victor Hugo Pereira Gonçalves. – 1. ed. – São Paulo: Atlas, 2017.

GONÇALVES, Victor Eduardo Rios. **Direito penal: parte especial** / Victor Eduardo Rios Gonçalves. / coord. Pedro Lenza. – 11. ed. – São Paulo: Saraiva Educação, 2021.

GOUVEIA, Flávia. **INTERNET - Tecnologia a serviço do crime, Notícias BR do Brasil**, Cienc. Cult. vol. 59 nº. 1 São Paulo Jan./Mar. 2007. Disponível em: http://cienciaecultura.bvs.br/pdf/cic/v59n1/a03v59n1.pdf. Acessado em 04/03/2023

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa** / Rogério Greco. – 14. ed. Niterói, RJ: Impetus, 2017.

GRECO, Rogério. **Código Penal: comentado** / Rogério Greco. – 11. ed. – Niterói, RJ: Impetus, 2017.

GRECO, Rogério. **Curso de direito penal: volume 2: parte especial: artigos 121 a 212 do Código Penal Brasileiro** / Rogério Greco. – 19. ed. – Barueri [SP]: Atlas, 2022.

JESUS, Damásio de. **Parte geral** / Damásio de Jesus; atualização André Estefam. – **Direito penal vol. 1**- 37. ed. – São Paulo: Saraiva Educação, 2020.

JESUS, Damásio de. **Parte especial: crimes contra a pessoa a crimes contra o patrimônio – arts. 121 a 183 do CP** / Damásio de Jesus; atualização André Estefam. **Direito penal vol. 2** – 36. ed. – São Paulo: Saraiva Educação, 2020.

JESUS, Damásio de. **Parte especial: crimes contra a propriedade imaterial a crimes contra a paz pública – arts. 184 a 288-A do CP** / Damásio de Jesus; atualização André Estefam. **Direito penal vol. 3** – 24. ed. – São Paulo: Saraiva Educação, 2020.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos** / Damásio de Jesus, José Antônio Milagre. – São Paulo: Saraiva, 2016.

JESUS, Damásio de; MILAGRE, José Antônio. **Marco Civil do Internet: comentários à Lei n. 12.965, de 23 de abril de 2014** / Damásio de Jesus, José Antônio Milagre. - São Paulo: Saraiva, 2014.

JUNIOR, Júlio César Alexandre. **CIBERCRIME: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS**, Júlio César Alexandre Júnior, Revista Eletrônica da Faculdade de Direito de Franca, ISSN 1983-4225 – v. 14, n. 1, jun. 2019. Disponível em: file:///C:/Users/FalconMac/Downloads/602-Texto%20do%20artigo-3194-1-10-20190726.pdf. Acessado em: 02/11/2022

LOBATO, Luisa; KENKEL, Kai Michael. **A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra, Contexto Internacional (PUC), Rio de Janeiro, vol. 37, no 2, maio/agosto, 1ª Revisão: 27/04/2015**, Luisa Lobato, Kai Michael Kenkel p. 629-660. Disponível em: https://old.scielo.br/pdf/cint/v37n2/0102-8529-cint-37-02-00629.pdf. Acessado em 12/02/2023

MACHADO, Costa. **Código Penal Interpretado: artigo por artigo, parágrafo por parágrafo.** Costa Machado, organizador: David Teixeira de Azevedo, coordenador. - 7. ed. - Barueri, SP: Manole, 2017.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]** / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**, 8ª Ed. Atlas, 2017.

MEDERO, Gema Sanchez. **CIBERCRIMEN, CIBERTERRORISMO Y CIBERGUERRA: LOS NUEVOS DESAFÍOS DELS. XXI. 239-267. REVISTA CENIPEC. 31. 2012. ENERO-DICIEMBRE.** Prof. Gema Sánchez Medero. ISSN: 0798-920. Disponível em: https://docplayer.es/4815190-Cibercrimen-ciberterrorismo-y-ciberguerra-prof-gema-sanchez-medero-prof-gema-sanchez-medero-cibercrimen-ciberterrorismo-y-ciberguerra.html; https://translate.google.com.br/?hl=pt-BR. Acessado em 08/11/2022

MELO, Pedro Jorge Pereira de. **A Ciberguerra. Estrutura Nacional para Enfrentar as Vulnerabilidades – uma Capacidade Autónoma ou Partilhada.** Pedro Jorge Pereira de Melo, Coronel de Transmissões, INSTITUTO DE ESTUDOS SUPERIORES MILITARES (CURSO DE PROMOÇÃO A OFICIAL GENERAL), Trabalho de Investigação Individual do CPOG 2010/11, Lisboa, IESM, 21 de junho de 2011. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/12017/1/TII_Cor%20Melo_CiberGuerra_21Jun2011_Final.pdf. Acessado em: 03/11/2022

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina**. BREVE PANORAMA SOBRE A LEGISLAÇÃO APLICADA NOS CRIMES ELETRÔNICOS, Revista de Direito, Governança e Novas Tecnologias Rev. de Direito, Organização Comitê Científico Double Blind Review pelo SEER/OJS**, | e-ISSN: 2526-0049| Maranhão | v. 3 | n. 2 | p. 81 –96| Jul/Dez. 2017.81. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/2589/pdf. Acessado em 13/11/2022

NUCCI, Guilherme de Souza. **Curso de direito parte especial: arts. 213 a 361 do código penal** / Guilherme de Souza Nucci. – 3. ed. – Rio de Janeiro: Forense, 2019.

NUCCI, Guilherme de Souza. **Estatuto da criança e do adolescente comentado** / Guilherme de Souza Nucci. 4ª ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2018.

PINTO, Marco Aurélio Gonçalves. **Teoria Relativista Do Ciberterrorismo, Academia Militar, Direcção de Ensino, Departamento de Estudos Pós-Graduados, Dissertação para a obtenção do grau de Mestre em Guerra da Informação,** Lisboa 2011, pág. vii. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf. Acessado em 16/09/2022.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD)** / Patrícia Peck Pinheiro. – São Paulo: Saraiva Educação, 2018.

PRATES, Marcia Maria Bianchi. BRASIL. **[Código penal (1940)]. Código penal e de processo penal** / Marcia Maria Bianchi Prates (organizadora). -- Brasília: Câmara dos Deputados, Edições Câmara, 2020.

SILVA, Ana Beatriz Barbosa. **Bullying: mentes perigosas nas escolas** / Ana Beatriz Barbosa Silva - [2. ed.] - São Paulo: Globo, 2015.

SILVA, Ana Beatriz Barbosa. **bullying, CARTILHA 2010 - JUSTIÇA NAS ESCOLAS**, Ana Beatriz Barbosa Silva, Conselho Nacional de Justiça, 1ª Edição, Brasília/DF – 2010

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico** / Tarcísio Teixeira. – 6. ed. – São Paulo: SaraivaJur, 2022.

**The CIA World Factbook 2021-2022**. Central Intelligence Agency, Skyhorse Publishing, 2021. Disponível em: https://pt.b-ok.lat/book/18331058/31c8ce. Acessado em: 17/09/2022

TRESCA, Laura; PERIN, Luiz. **Article 19. DA CIBERSEGURANÇA À CIBERGUERRA O DESENVOLVIMENTO DE POLÍTICAS DE VIGILÂNCIA NO BRASIL**, São Paulo, 2016. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2016/03/Da-Ciberseguranc%CC%A7a-a%CC%80-Ciberguerra-WEB.pdf. Acessado em 12/02/2023

VILLAÇA, Marco Valério Miorim; STEINBACH, Reginaldo. **BREVÍSSIMA HISTÓRIA DO COMPUTADOR E SUAS TECNOLOGIAS – PARTE I – DO OSSO DE LEBOMBO AOS COMPUTADORES ELETROMECÂNICOS**. Revista Ilha Digital, ISSN 2177-2649, volume 5, páginas 3 – 24, 2014. Disponível em: https://ilhadigital.florianopolis.ifsc.edu.br/index.php/ilhadigital/article/view/72/59. Acessado em 04/03/2023.

WENDT, Emerson. **INTELIGÊNCIA CIBERNÉTICA: DA CIBERGUERRA AO CIBERCRIME A (IN)SEGURANÇA VIRTUAL NO BRASIL** [recurso eletrônico] / Emerson Wendt. Livro digital. ISBN 978-85-64514-15-7. São Paulo: Editora Delfos, 2011.