

OS CRIMES VIRTUAIS E A EVOLUÇÃO DA LEGISLAÇÃO PENAL BRASILEIRA

CYBERCRIMES AND THE EVOLUTION OF BRAZILIAN PENAL LEGISLATION

Gustavo Henrique Barbosa Kochem¹
Matheus Behling Portela²

RESUMO

O processo de globalização vem acompanhado de uma série de evoluções tecnológicas, desencadeadas pela Revolução Industrial. Com o advento da internet, uma série de mudanças começaram a ser registradas em toda a sociedade. No entanto, assim como a internet trouxe uma série de benefícios em inúmeros campos da sociedade, muitas pessoas passaram a utilizar esse novo recurso tecnológico para a prática de impunidades. O aumento do compartilhamento de informações pela rede de internet e de computadores chamou atenção de criminosos, que viram nela uma oportunidade de cometer delitos contra os usuários. Esse novo formato de crime, denominado Crime Virtual, Crime Cibernético ou Cybercrime, tomou proporções significativas nos últimos anos, fazendo com que o Poder Judiciário visse a necessidade de tomar providências legais sobre eles. Sendo assim, o presente artigo apresenta um panorama geral sobre a evolução do ordenamento jurídico brasileiro em relação aos crimes virtuais, enfatizando os últimos dispositivos legais aprovados em território nacional, que visam aumentar a segurança dos usuários da internet.

Palavras-chave: Crimes Cibernéticos; Direito Penal; Evolução Tecnológica.

ABSTRACT

The globalization process is accompanied by a series of technological developments, triggered by the Industrial Revolution. With the advent of the internet, a series of changes began to be registered throughout society. However, just as the internet brought a series of benefits in countless areas of society, many people began to use this new technological resource to practice

¹ Acadêmico do Curso de Bacharelado em Direito pelo ISEPE Rondon – Contato: gustavoh2535@gmail.com

² Docente do curso de Bacharelado em Direito do ISEPE Rondon. Especialista em Direito Ambiental pela Universidade Cruzeiro do Sul (2021). Graduado em Direito pela Faculdade de Ensino Superior de Marechal Cândido Rondon (2018) – Contato: matheusportela@gmail.com

impunity. The increase in information sharing over the internet and computer networks caught the attention of criminals, who saw it as an opportunity to commit crimes against users. This new format of crime, called Virtual Crime, Cybercrime or Cybercrime, has taken on significant proportions in recent years, making the Judiciary see the need to take legal action against them. Therefore, this article presents a general overview of the evolution of the Brazilian legal system in relation to virtual crimes, emphasizing the latest legal provisions approved in the national territory, which aim to increase the security of internet users.

Keywords: Cybercrimes; Criminal Law; Technological evolution.

1. INTRODUÇÃO

O avanço da Era Digital e, consequentemente, da internet, aumentou de forma significativa as formas de comunicação e compartilhamento de informações entre os usuários, estejam eles fisicamente próximos ou não. Essa nova realidade atribuída à globalização trouxe à tona um novo conceito: o ciberespaço. Esse novo espaço de socialização começou a tomar proporções significativas, de modo que os problemas de socialização existentes no mundo físico, passassem a ser também um problema no espaço virtual (Marra, 2019).

Frente a essa nova realidade tecnológica, surge a necessidade de estabelecer novos princípios jurídicos, uma vez que os existentes no ordenamento jurídico não são suficientes para cobrir os novos delitos cometidos com a utilização de ferramentas tecnológicas. De Gois (2022, p. 9) explica que com o rápido compartilhamento de dados, “o universo jurídico começou a adotar medidas, criando normas que visem à preservação da privacidade do indivíduo que utiliza a internet, conferindo a ele o tratamento adequado quanto à utilização de seus dados”.

Com o advento da internet e seus benefícios, surge também a possibilidade de criminosos cometerem infrações de forma anônima, o que abriu um leque de oportunidades para que indivíduos mal-intencionados pudessem usar as redes de forma a prejudicar outros usuários.

Com o passar do tempo, e o constante aumento na prática desses crimes, eles passaram a ser chamados de crimes cibernéticos, ou crimes virtuais, atingindo uma parcela cada vez maior da população, e exigida do Poder Judiciário alterações na legislação, uma vez que, até pouco

tempo atrás, esses crimes eram inexistentes e, por tanto, não previsto pela lei (Brito, 2020).

Nesse contexto, o presente artigo tem como objetivo analisar a evolução dos dispositivos legais que atuam sobre os crimes cometidos em ambiente virtual. Traz a descrição das leis específicas criadas a partir de casos relatados, bem como as atualizações sofridas pelo Código Penal brasileiro.

A fim de contextualizar o leitor sobre o assunto discutido, a revisão bibliográfica apresenta o contexto histórico do surgimento e da evolução da internet no âmbito mundial, dando ênfase no território nacional. Na sequência, os crimes cibernéticos são definidos e caracterizados para, por fim, serem analisados sob o olhar do ordenamento jurídico brasileiro.

2. REVISÃO BIBLIOGRÁFICA

2.1 O ADVENTO DA INTERNET

A internet, mundialmente conhecida por suas contribuições em todos os campos, teve seus primeiros registros nos Estados Unidos, durante a Guerra Fria, no início da década de 70, naquela época chamada de “Arpanet”. Criada pelo Departamento de Defesa norte-americano, a internet surge como um sistema de comunicação entre diversos centros de pesquisa militar, com o objetivo de transmitir dados e informações durante o período de guerra (Maues; Duarte; Cardoso, 2018).

Na década de 80, a Arpanet foi dividida em duas instituições, com objetivos diferentes, sendo a “MILNET (*Military Network*), dedicada exclusivamente à troca de dados militares, e a NSFNET (*National Science Foundation Network*), para uso acadêmico” (Alves, 2020, p. 32).

A partir daí, quando passou a ser chamada de “internet”, o seu uso expandiu-se para a comunicação entre órgãos estatais, universidades e laboratórios de pesquisa. Em 1982, as instituições acadêmicas aderiram fortemente o uso da internet em todo o território dos Estados Unidos, posteriormente, na Europa, seguindo para a Holanda, até alcançar todos os países do mundo (Barbosa, 2020).

Com o passar dos anos, no entanto, a internet deixou de ser de utilização exclusiva dos militares e do meio acadêmico, e passou a ser utilizada como meio de comunicação e transmissão de informações também entre a população em geral (Maues; Duarte; Cardoso, 2018).

No entanto, foi apenas no início da década de 90, de acordo com os autores, que a internet começou a tomar as proporções conhecidas atualmente, com o desenvolvimento da “www”. Barbosa (2020) explica que essa expansão teve início quando

[...] o cientista, professor e físico britânico Tim Berners-Lee desenvolveu um navegador ou browser como também é conhecido, a World Wide Web, o popular “www” que precede os sites, rede mundial de Computadores. A partir de então ela se popularizou pelo mundo com surgimento de novos browsers, muito conhecidos atualmente, como a internet Explorer, Mozilla Firefox, Google Chrome, Opera, dentre outros e consequentemente o aumento de usuários. Diante de tudo isso, começa a proliferar sites, chats e as famosas redes sociais (Barbosa, 2020, p. 11).

Durante todo esse processo, Maues, Duarte e Cardoso (2018) afirmam que o uso da internet no território brasileiro teve início, de fato, no ano de 1988, sendo nessa época utilizada apenas pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e pelo Laboratório Nacional de Computação Científica (LNCC) no Rio de Janeiro. Já a utilização da rede pela população em geral iniciou apenas no ano de 1991.

Antes sendo transmitida apenas por cabos de rede, a partir do ano 2000, começou a ser utilizado o sistema de Wi-Fi - “*Wireless Fidelity*”, ou seja, o acesso a internet por meio de sinal sem fio. Marra (2019) explica que esse novo sistema

representa uma inovação no meio de se comunicar, eis que é uma rede local de fácil instalação e mobilidade e que se vale de sinais de rádio, viabilizando ao acesso sem imposição de fronteiras entre os usuários. Aos computadores interligados na Rede, é atribuído um endereço singular, que representa um numerário de identidade, de localização, denominado TCP-IP (Marra, 2019, p. 149).

Tendo passado por inúmeros testes e melhorias, a comercialização da internet ganhou força nos anos que se seguiram. De acordo com Alves (2020), a internet alcançou seu auge no início do século XXI, passando a ser o principal meio de acesso a informação e comunicação entre as pessoas em todo o mundo. As pesquisas apresentadas mostram que, no ano de 2018, mais de quatro bilhões de pessoas eram usuárias da rede de internet, representando mais da metade da população mundial.

O aumento das possibilidades trazidas pelo avanço da internet, popularizou o conceito de “ciberespaço”. De Gois (2022) explica que o conceito de ciberespaço

descreve um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de sistemas de informação, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores embutidos. Ou seja, uma tecnologia digital ampla e interconectada, num ambiente complexo resultante da interação de pessoas, softwares e serviços na Internet por meio de dispositivos de tecnologia e redes a ela conectadas, que não existem de forma física (De Gois, 2022, p. 15).

O ciberespaço é definido, então, como o ambiente no qual ocorrem as interações virtuais, e que deve ser tratado como um novo formato de espaço social a ser analisado como tal.

Os benefícios atribuídos aos avanços tecnológicos e a facilidade de acesso a informação e comunicação trazida pela internet são imensuráveis. No entanto, diversos autores chamam atenção ao fato de que, ao mesmo tempo que esse crescimento acelerado do uso da internet trouxe melhorias para a sociedade, ele remete alguns perigos. Marra (2019, p. 50) atenta que “há de se observar que os espaços públicos de acesso são cada vez mais vulneráveis no que concerne à interceptação de dados, senhas e outras informações privativas do usuário. Há, portanto, o lançando de novos desafios quanto à segurança da Rede”.

Maues, Duarte e Cardoso (2018) também levantam esse alerta, uma vez que afirmam que

da mesma forma que se ampliam os usos benéficos da internet (principalmente econômico e social), também, começaram-se a criar meios deturpados de seu uso. Vale dizer que o mundo cibernético não é permeado apenas de benesses, vez que existem inúmeros fatores negativos que merecem destaque (Maues, Duarte e Cardoso, 2018, p. 169).

Nesse contexto, o capítulo a seguir apresentará, de forma detalhada, as ações de mau uso da internet que ficaram conhecidas mundialmente como “Crimes Virtuais”, e que receberam maior atenção dos órgãos competentes nos últimos anos, considerando o aumento no número de registros de crimes dessa natureza.

2.2. CRIMES VIRTUAIS OU CYBERCRIMES: CONTEXTUALIZAÇÃO

Antes de mais nada, é necessário apresentar a denominação do termo “crime”. No ordenamento jurídico brasileiro, o termo “crime” é definido como “uma conduta humana que é descrita como tal na lei penal, e que é considerada ilícita e passível de punição pelo Estado” (Mocinho, 2023, p. 5).

Essa definição está prevista do artigo 1º da Lei nº 2.848, de 7 de dezembro de 1940, o Código Penal Brasileiro, que diz "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (Brasil, 1940).

Ou seja, o crime pode ser definido como uma conduta contrária ao ordenamento jurídico, que atente contra a vida, a liberdade, a propriedade, a integridade física e moral, e dignidade da pessoa humana, ou qualquer outro bem jurídico tutelado pelo Estado. Mocinho (2023) explica ainda que

o Código Penal Brasileiro estabelece que para que uma conduta seja considerada criminosa, é necessário que estejam presentes os seguintes elementos: tipicidade, ilicitude e culpabilidade. A tipicidade diz respeito à adequação da conduta ao tipo penal descrito na lei, ou seja, é preciso que a conduta esteja prevista como criminosa em lei. A ilicitude, por sua vez, diz respeito à contrariedade da conduta aos valores jurídicos protegidos pelo ordenamento jurídico. Por fim, a culpabilidade exige que o agente tenha consciência da ilicitude de sua conduta e que possua capacidade para agir de forma diferente (Mocinho, 2023, p. 6).

Dentre os tipos de crime tipificados pelo Código Penal, o que tem ganhado mais destaque nos últimos anos, com o advento da internet e o avanço das tecnologias, é o Crime Virtual, podendo ser conhecido como crime cibernético, digital, eletrônico, cybercrimes, fraudes eletrônicas, delitos computacionais (Lucchesi; Hernandez, 2018).

Vários autores apresentam definições para o termo. Dentre eles, Brito (2020, p. 4) define os crimes virtuais, também conhecidos como Crimes Cibernéticos ou Cybercrimes, de acordo com a INTERPOL, como sendo “a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na internet. Ainda, pode se dizer que são crimes com utilização de computadores e internet, com fins de fraudar sistemas de comunicação, segurança de computadores e redes corporativas”.

Marra (2019), também discute a tipificação do crime virtual abordada por diversos

autores, e conclui que

crime virtual é a conduta típica, ilícita e culpável que preenche os pressupostos de crime ou de contravenção penal, ocorrida com dolo ou culpa, perpetrada por pessoa física ou jurídica por meio da informática, seja na Rede Mundial de Computadores ou não, e que vai de encontro à segurança do sistema informático, o qual deve observar a integridade, desimpedimento e a privacidade de indivíduos e entidades (Marra, 2019, p. 153).

Cabe destacar, na fala da autora, que os crimes virtuais não precisam, necessariamente, estar ligados à Rede Mundial de Computadores, uma vez que podem ocorrer por meio de outros sistemas informáticos ligados à internet (Marra, 2019).

Os crimes cibernéticos podem acontecer nas mais diversas esferas criminais. Dos Santos, Martins, Tybucsh (2017) citam que os principais crimes cibernéticos identificados no Brasil são

a pornografia infantil, pirataria, fraude e golpes, sabotagem informática, difamação, calúnia, injúria, dano, estelionato, crimes contra o sistema financeiro, ameaça, interceptação do fluxo de dados em tráfego por serviço de telecomunicação, apologia de crime ou de criminoso, violação de direito autoral, tráfico de substâncias estupefacientes, rufianismo, entre outros (Dos Santos; Martins; Tybucsh, 2017, p. 7).

Maues, Duarte e Cardoso (2018) destacam também os crimes de pornografia, adulta e infantil, da prática de racismo, fraudes em contratos eletrônicos, crimes contra a honra, furtos de informações pessoais e/ou bancárias, dentre outros. Nesses últimos, os infratores são popularmente conhecidos como “hackers”.

O termo “hacker”, conforme explicam Lucchesi e Hernandez (2018), está relacionado ao indivíduo que invade sistemas informáticos, furta senhas e informações pessoais de outros usuários e/ou propaga vírus e cavalos de tróia por meio da rede. Além desse termo, os autores sinalizam que existem mais três ramificações de infratores, sendo “b) cracker, sabota e pirateia programas de computador; c) “lammer”, conhecimentos limitados de informática, sem potencial ofensivo; d) “spammer” invade a privacidade de outrem por meio de mensagens eletrônicas, entre outros não relevantes a este artigo” (Lucchesi; Hernandez, 2018, p. 5).

Marra (2019) explica que os crimes virtuais podem ser classificados de três maneiras: puros, mistos e comuns. De acordo com a autora,

o crime informático puro é o que se encontra relacionado ao sistema de informática, isto

é, o sujeito ativo pretende apenas corromper os dados do computador do sujeito passivo, tais como o "software" e o "hardware" e, assim, é percebido nos vírus que contaminam um computador, por exemplo. Já o crime de informática misto, diz respeito à violação do bem jurídico diferente do sistema, porém este é instrumento inerente à consumação do delito, como ocorre no caso do furto eletrônico a contas bancárias online. E, por último, o crime informático comum é aquele que está previsto na lei penal e pode ou não ocorrer com o uso do computador, a exemplo da pedofilia, do racismo e do cyberbullying (Marra, 2019, p. 153).

Outros autores ainda classificam os crimes virtuais como próprios e impróprios. Dos Santos e De Paula (2023) explicam que

os crimes próprios são aqueles que o computador é o objeto para prática do delito tendo a prática e a consumação no âmbito virtual como invasão, modificação ou ataques de hackers. Já os impróprios são os que utilizam o computador e internet para intermédio de delitos que reproduzem efeitos na “vida real” como por exemplo a falsificação de documento (Dos Santos; De Paula, 2023, p. 9).

Em relação ao processo de denúncia e investigação dos crimes virtuais, De Freitas, Gonçalves e Torres (2023, p. 303) explicam que os profissionais responsáveis observam alguns pontos importantes que ajudam na identificação dos criminosos em ação, e que “essas análises buscam localizar o dispositivo utilizado nos crimes para identificar o delinquente, a busca consiste na verificação de informações e detalhes repassados pelas vítimas, ligando os pontos fáticos ocorridos no contexto virtual”.

Dentre os diversos crimes virtuais caracterizados, os que mais se destacam são: invasão de dispositivo para roubo de informações, Cyberbullying, Crimes contra honra e Pornografia infantil. Além disso, a disseminação de vírus como *phishing*, *spam* (*Sending and Posting Advertisement in Mass*) ou *malware*, também se destacam entre os usuários da internet. Barbosa (2020) explica que

Phishing são conversas ou mensagens falsas com links fraudulentos que ocorre através de e-mail de spam ou outras formas de comunicação que são enviadas no atacado com o intento de induzir aqueles que recebem, a fazer algo que prejudique a segurança pessoal ou da organização onde trabalham. [...] a mensagem de *Spam* promove um produto ou serviço com o intuito de que a pessoa se interesse e acaba acessando o link fraudulento. Mas em outros casos, o objetivo é apenas propagar uma história falsa, e ao clicar, as informações de dados financeiros e pessoais são roubadas. Os *malwares* são softwares maliciosos instalados sem permissão do usuário. Vírus, cavalos de Tróia, spywares e ransomwares estão entre os diferentes tipos de malwares (Barbosa, 2020, p. 15).

Outros autores apresentam explicações resumidas sobre os principais tipos registrados de crimes virtuais. Lucchesi e Hernandez (2018) explicam que, derivado do termo “bullying”, que remete a ação daquele que “(...) maltrata ou violenta de forma constante outras pessoas por motivos supérfluos”, o “cyberbullying” trata da mesma forma de agressão, só que no ambiente virtual, por meio de redes sociais, mensagens de texto, dentre outras. Os autores destacam que “embora no cyberbullying as agressões não sejam físicas, as consequências são tão ou até mais graves que as praticadas no bullying, pois os abusos têm cunho psicológico, mas, em situações extremas, podem chegar ao dano físico” (Lucchesi e Hernandez, 2018, p. 6).

Ainda segundo os autores, as ações que se enquadram no cyberbullying são: ataque às características físicas da vítima, ameaças de morte, publicação de informações pessoais que constringam a vítima, dentre outras, que atinjam a imagem e a autoestima do indivíduo agredido (Lucchesi; Hernandez, 2018).

Já os crimes contra a honra são aqueles que atingem a integridade moral da pessoa humanos, ou seja, a dignidade da pessoa. Ele pode incluir o desrespeito ao nome ou a fama de alguém, por exemplo. Maues, Duarte e Cardoso (2018), explicam que tais crimes os mesmo que estão previstos no Código Penal quando praticados em meio físico: calúnia (art. 138), difamação (art. 139) e injúria (art. 140).

Os autores ainda apontam outros crimes cometidos no meio virtual, que podem ser identificados pelo Código Penal, quando afirmam

é oportuno abordar sobre outros crimes comuns no âmbito virtual, ameaça (art. 147, CP); fraude bancárias por meio de Internet Banking ou clonagem de cartão Internet Bank-ing (art. 155, § 4º, inciso II, CP); comentar, em chats, e-mails e outros, de forma negativa, sobre raças, religiões e etnias (preconceito ou discriminação art. 20 da Lei n. 7.71/89); enviar, trocar fotos de crianças nuas (pedofilia art. 247 da Lei n. 8.09 /90, o Estatuto da Criança e do Adolescente - ECA); exploração sexual cibernética contra crianças e adolescentes (art. 241-A c/c art. 241-E, do Estatuto da Criança e do Adolescente- ECA); falsa identidade virtual (art. 307, CP) e a venda de medicamento pela Internet (art. 273, § 1º, CP) (Maues; Duarte; Cardoso, 2018, p. 176).

Outro formato de crime que preocupa bastante os usuários da internet são os crimes de pornografia, principalmente envolvendo menores de idade. Esses crimes, de um modo geral, não acontecem em redes de domínio público, mas em locais que não fazem parte dos buscadores

comuns, e são destinados especificamente para o cometimento desses e outros delitos, popularmente conhecida como *darkweb*.

Essa parcela da internet, de acordo com Sato (2019),

Se traduz na parcela não indexada da internet utilizada para a prática de cybercrimes, extremismo, terrorismo, divulgação de conteúdo ofensivo, popularização de imagens de homicídios, estupros e, igualmente, reduto de organizações criminosas dedicadas à proliferação de materiais pedopornográficos (Sato, 2019, p. 169).

Ainda de acordo com a autora, de *darkweb* é uma parte da internet de difícil rastreio, fazendo com que as equipes de investigação tenham ainda mais dificuldade na localização e identificação dos autores e, conseqüentemente, no combate (Sato, 2019).

Vários autores atentam, ainda, ao fato de que, dentre os crimes cometidos pelos usuários da *darkweb*, os mais recorrentes são os crimes contra a dignidade sexual de crianças e adolescentes, por meio do compartilhamento de vídeo e fotos de cunho pornográfico. Pires (2018) afirma que esses crimes, já conhecidos e praticados de forma física, passam agora a ser praticados na forma virtual, e passam a fazer parte da atividade criminosa conhecida por “ciberpedofilia”, aumentando de forma significativa a recorrência dos casos, devido à facilidade de compartilhamento de informações proporcionada pela internet.

No Brasil, a SaferNet³, uma associação civil de direito privado, recebe e analisa os registros de crimes virtuais registrados no país. De acordo com a associação, no ano de 2023 foram registradas 75% a mais de denúncias do que em 2022, conforme mostra a Figura 1.

Outra instituição responsável pelas denúncias, em parceria com a Safetnet, é o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Esse centro é responsável por receber e analisar os registros de incidentes criminais cometidos por meio da rede de computadores, e também auxiliar nas decisões legais propostas para sanar os tais problemas.

De acordo com a página CERT.br (2024), de janeiro à abril desse ano foram registrados 146.386 incidentes de crimes cibernéticos cometidos contra dispositivos da rede nacional de computadores, incluindo todas as categorias possíveis de registro.

³ Disponível em: <https://new.safernet.org.br/>.

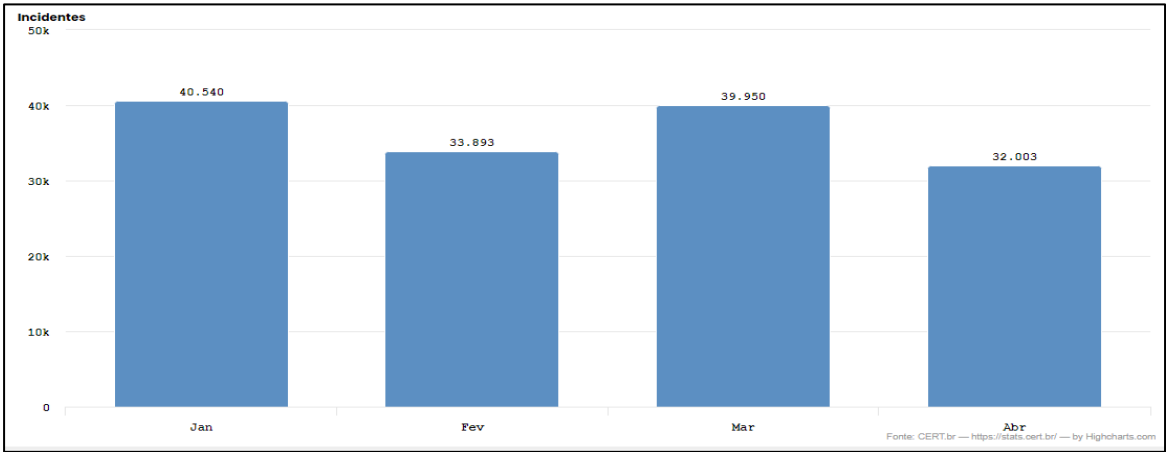
Figura 1: Denúncias novas recebidas pela Safernet 2022/2023.

2022/2023	2022	2023	VARIAÇÃO %
Imagens de abuso e exploração sexual infantil	40.572	71.867	77,13%
Xenofobia	4.030	14.196	252,25%
Intolerância religiosa	764	993	29,97%
Tráfico de pessoas	342	380	11,11%
Neonazismo	1.104	1.114	0,00%
Apologia e Incitação a crimes contra a vida	4.054	4.041	0,00%
Racismo	2.804	2.233	-20,36%
LGBTfobia	3.807	1.501	-60,57%
Misoginia (violência ou discriminação contra mulheres)	8.734	3.706	-57,56%
Outros crimes	1.922	1,282	-33,30%

Fonte: Safernet (2024)

Nesse contexto, com o registro de cada vez mais crimes atrelados ao ambiente virtual, exigindo que o ordenamento jurídico brasileiro promova alterações que sejam capazes de suprir as necessidades das vítimas e, principalmente, penalizar os infratores de acordo com o crime cometido.

Figura 2: Incidentes de Crimes Cibernéticos registrados ao Cert.br de janeiro a abril de 2024.



Fonte: CERT.br (2024)

No capítulo a seguir, será exposta a evolução da legislação brasileira em relação aos crimes virtuais, desde o início da preocupação do Poder Judiciário com essa nova realidade, até as atualizações mais recente dos dispositivos legais, em especial no que tange ao Código Penal.

2.3. A ADEQUAÇÃO DA LEGISLAÇÃO PENAL BRASILEIRA

Conhecida como “Era Digital” ou “Era da informática”, o século XX trouxe para o ordenamento jurídico brasileiro uma série de desafios relacionados aos meios de comunicação digital, uma vez que houve, desde os primórdios, a necessidade de pensar em leis que atendessem às necessidades do novo cenário (Lucchesi e Hernandez, 2018).

De acordo com relatos, o surgimento da primeira lei de proteção relaciona ao uso de computadores surgiu no ano de 1998, a Lei nº 9.609, que “Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências” (BRASIL, 1998).

No entanto, nota-se que essa lei não prevê penalidade ou multa para os crimes digitais em geral. Sendo assim, na ausência de uma legislação específica, o indivíduo que praticar algum crime de natureza digital deverá ser julgado com base no Código Penal, descrito na Lei nº 2.848/40, tendo a pena determinada de acordo com a tipificação do crime cometido.

Ainda sem ter uma legislação específica destinada aos crimes virtuais, alguns deles podem ser tipificados pela redação original do Código Penal. Por exemplo, os crimes virtuais já caracterizados anteriormente como impróprios, ou seja, o crime cibernético que tem como objetivo invadir um site ou rede pública para acesso à dados confidenciais, para posteriormente divulga-los, está previsto no Art. 153, § 1º do Código Penal, que prevê “Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de um a quatro anos e multa” (Brasil, 1940).

No entanto, Acha (2018) explica que, com os registros cada vez mais constantes de crimes realizados por meios digitais, o Direito Penal, que até então, regulamentava crimes cometidos no mundo físico, com limitações territoriais, se obriga a repensar novos modelos e formas de sancionar leis que visem à regulamentação dos crimes digitais.

Com isso, o Código Penal passou a incluir atualizações relacionadas aos crimes virtuais, com o intuito de atender às novas necessidades da sociedade frente aos avanços da tecnologia. Com crescimento dos crimes virtuais no Brasil, o ordenamento jurídico teve que estabelecer uma série de leis com tipificações penais, para delitos informáticos e enquadrar a essa nova realidade (Dos Santos; De Paula, 2023).

No ano de 2012, duas importantes leis entraram em vigor no país: a Lei nº 12.735 (Lei Azeredo) e a Lei nº 12.737 (Lei Carolina Dieckmann), as duas sancionadas em 30 de novembro de 2012 (Mauer; Duarte; Cardoso, 2018). Os autores explicam que,

a Lei nº 12.735/2012 (conhecida como Lei Azeredo) estabelece a obrigatoriedade de interrupção imediata de mensagens com conteúdo racista além de retirá-las de qualquer meio de comunicação e a criação das delegacias virtuais. [...] O intuito da lei foi alterar o Código Penal, o Código Penal Militar e a lei contra o racismo (Lei nº 7.716/89) (Mauer; Duarte; Cardoso, 2018, p. 172).

Já a Lei nº 12.737/12 (Lei Carolina Dieckmann), recebeu o nome da atriz global Carolina Dickmann, teve a sua motivação no vazamento de fotos íntimas da atriz pelo ex-marido. Na época os agentes criminosos foram punidos pelos crimes de extorsão, difamação e furto, mas não pela invasão de computador, uma vez que não existia um dispositivo legal para tal. Daí, a atualização da legislação que recebeu o nome da vítima (Mauer; Duarte; Cardoso, 2018).

De Gois (2022) apresenta de Lei Carolina Dickmann por meio de um quadro (Figura 3) que facilita a compreensão do disposto. Além disso, destaca-se que a presente lei altera o Art. 154 do Código Penal, em seus artigos 266 e 298, e acrescentou os Art. 154-A e 154-B, que preveem os crimes de caráter digital, e dispõe

Art. 154-A. 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.
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 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**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 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.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

§ 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.

Art. 154-B. 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 (Brasil, 2012).

Cabe destacar, no entanto, que a Lei em questão, em seu artigo 154-B prevê que o crime é tipificado apenas quando há representação da vítima, ou seja, não podendo ser mediante denúncia de terceiros.

Maues, Duarte e Cardoso (2018) apontam que o avanço da necessidade de atenção aos crimes cometidos no meio virtual corrobora para a criação da área do Direito Digital, e explicam que

o Direito Digital surge com o estabelecimento da internet e todas as suas situações sociais, políticas, econômicas e jurídicas. Essa disciplina consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos do Direito que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as áreas (Maues, Duarte e Cardoso, 2018, p. 172).

Figura 3: Exposição da Lei nº 12.737/12

Crime	Pena	Exemplo
Invadir dispositivo alheio, conectado ou não a rede de computadores, mediante violação de segurança com o fim de obter informações sem autorização	Detenção de três meses a um ano e multa	Invadir computador para roubar conteúdos sem consentimento do dono
Agravantes	Pena	Exemplo
Roubo de informação em que causa prejuízo econômico	Aumenta a pena de detenção de três meses a um ano e quatro meses	Criminoso rouba conteúdo sigiloso de uma pessoa e apaga a informação, causando perda de dinheiro
Obtenção de conteúdo de comunicações privadas de forma não autorizada	Aumenta a pena de detenção de seis meses a dois anos e multa	Roubar conteúdo de e-mail ou controlar computadores tomando-os zumbis
Divulgação e comercialização de conteúdo roubado de dispositivo informático	Reclusão de oito meses a três anos e quatro meses	Roubar informações sigilosas e vender ou divulgar na internet

Fonte: De Gois (2022, p. 39).

Nos anos que se seguiram, outras leis foram sendo sancionadas com o auxílio dos estudos direcionados ao direito digital. No ano de 2013, o decreto nº 7.962, de 15 de março, dispõe sobre a regulamentação do comércio eletrônico, preenchendo lacunas do Código de Defesa do Consumidor, que não traz regulamentação específica acerca das compras online. Esse novo decreto exige, então, que as páginas de comércio eletrônico disponham de informações detalhadas sobre a procedência da loja, as informações sobre os produtos, dentre outros dados, que permitam que o consumidor acione o vendedor caso tenha qualquer problema com sua compra (Dos Santos; Martins; Tybucsh, 2017).

Ainda em 2013, o Projeto de Lei nº 6.630 objetivou incluir no Código Penal o artigo 216-

B que passaria a “prever a pena de reclusão de um a três anos, além de multa, no caso de exposição pública da intimidade sexual, com aumento de um terço a metade na pena se o crime for cometido por motivo torpe, contra pessoa com deficiência ou menor de idade” (Stoco; Bach, 2018, p. 683). Esse PL só foi aprovado no ano de 2018, pela Lei nº 13.772, que altera o Código Penal e dispõe

Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes:

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo (Brasil, 2018).

Em 2014, entrou em vigor o que viria a ser o principal dispositivo legal relacionado ao ambiente virtual no país: o Marco Civil da Internet. A Lei nº 12.965, de 23 de abril de 2014, “Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil” (Brasil, 2014).

De acordo com Acha (2018, p. 212), a Lei do Marco Civil trouxe “a garantia da liberdade de expressão, privacidade e neutralidade da rede, intimidade dos usuários, inviolabilidade das comunicações, vedação da divulgação de dados pessoais, obrigatoriedade de guarda de registros de conexão e obrigação de retirada dos conteúdos infringentes”.

A partir daqui a legislação brasileira passou a se preocupar, principalmente, com o tratamento de dados pessoais compartilhados em rede, dando ênfase a divulgação não autorizada, ou repasse desses dados por parte de instituições. Com essa preocupação em crescente aumento, no ano de 2018 então a Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, que

Art. 1º - dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

No ano seguinte, a LGPD ainda sofreu algumas alterações pela Lei nº 13.853/19, que criou a Autoridade Nacional de Proteção de Dados (Brasil, 2019). Barbosa (2020) fala sobre a LGPD, e explica que, desde que entrou em vigor, ela deve ser cumprida dentro e fora do território

nacional, quando se tratar de pessoas que estejam em solo brasileiro. Além disso, o autor chama atenção ao fato de que a nova lei trouxe a obrigatoriedade do consentimento de tratamento de dados, ou seja, para que dados pessoais possam ser tratados, é fundamental que tenha o consentimento assinado pelo indivíduo. E o autor ainda destaca que,

essa proteção se estende também aos direitos do cidadão, que pode requerer que dados sejam apagados, pode desistir do consentimento, transferir dados para outro fornecedor de serviços, entre outros, além de que o tratamento de dados tem que ser feito respeitando alguns quesitos, como a finalidade e a necessidade, que devem ser acertados e informados ao cidadão antes de ter acesso aos dados (Barbosa, 2020, p. 21).

Ainda no ano de 2018, a já citada Lei nº 13.772/18 também tipificou a conduta do indivíduo que publica cenas de cunho sexual ou pornográfico, sem conhecimento dos envolvidos, conforme dispõe

Art. 218-B. Submeter, induzir ou atrair à prostituição ou outra forma de exploração sexual alguém menor de 18 (dezoito) anos ou que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, facilitá-la, impedir ou dificultar que a abandone: Pena - reclusão, de 4 (quatro) a 10 (dez) anos. § 1º Se o crime é praticado com o fim de obter vantagem econômica, aplica-se também multa (Brasil, 2018).

Depois da LGPD, o Código Penal sofreu uma nova alteração, agora pela Lei nº 14.155, de 27 de maio de 2021, que aparece para “tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet” (Brasil, 2021). A atualização do dispositivo legal prevê

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico (Brasil, 2021).

De acordo com os registros, essa foi a última atualização sofrida pelo Código Penal em relação aos crimes virtuais. No entanto, vários autores ainda defendem a necessidade de mais dispositivos legais destinados a esse fim, para que a fiscalização e penalização dos criminosos seja ainda mais eficaz.

8. CONCLUSÃO

Os avanços da tecnologia trouxeram inúmeros benefícios para o mundo da comunicação e da informação. No entanto, assim como qualquer outra mudança, essa também veio acompanhada por uma série de problemas.

A facilidade de compartilhamento de informações atraiu a atenção de malfeitores, e colaborou para o surgimento de uma nova forma de cometer crimes: os crimes virtuais.

Podendo agora agir de forma anônima na internet, os criminosos, popularmente conhecidos como hackers, passaram a atuar no roubo de dados e informações pessoais, prática de bullying virtual, vazamento de fotos e vídeos íntimos, fraudes bancárias, dentre outros delitos que são extremamente prejudiciais à sociedade de um modo geral.

Com toda essa facilidade de compartilhamento de informações, o Ciberespaço, ou seja, o mundo virtual, também tornou seus usuários mais vulneráveis, visto que, quanto mais dados compartilhados em rede, maior a possibilidade de violação, roubo ou utilização indevida de tais dados.

Frente a esse novo cenário, com o aumento dos casos registrados de ataques aos usuários das redes, o Poder Judiciário se vê frente a um impasse legislativo: a legislação brasileira não estava preparada para atender a crimes cometidos no ambiente virtual.

Com isso, os dispositivos legais passaram a sofrer uma série de alterações com o intuito de atender de forma mais eficaz as vítimas de crimes virtuais, bem como de punir de forma mais severas os infratores.

No entanto, mesmo com as últimas mudanças realizadas no âmbito jurídico brasileiro, diversos autores ainda chamam atenção à necessidade da criação de mais dispositivos destinados à punir os criminosos, uma vez que a legislação atual ainda não se mostra completamente eficaz frente aos casos registrados.

9. REFERÊNCIAS

ACHA, Fernanda Rosa. Crimes Digitais: Uma necessária Releitura do Direito Penal à Luz das Novas Tecnologias. **LINKSCIENCEPLACE-Interdisciplinary Scientific Journal**, v. 5, n. 6, 2019. Disponível em: <http://revista.srvroot.com/linkscienceplace/index.php/linkscienceplace/article/view/621>. Acesso em: 01 mai. 2024.

ALVES, Matheus de Araújo. CRIMES DIGITAIS: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. **Dialética**, 2020. 148 p. Disponível em: https://www.google.com.br/books/edition/Crimes_Digitais/hxIFEAAAQBAJ?hl=pt-BR&gbpv=1&dq=crimes+era+digital&printsec=frontcover. Acesso em: 30 abr. 2024.

BARBOSA, Mateus Israel Alves Crivinel. **Crimes virtuais**: a evolução dos crimes cibernéticos e os desafios no combate. 2020. Trabalho de Curso (Bacharelado em Direito). Pontifícia Universidade Católica de Goiás. Goiânia – GO. 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105>. Acesso em: 30 abr. 2024.

BRASIL. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 30 abr. 2024.

BRASIL. **Lei nº 9.609**, de 19 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19609.htm. Acesso em: 30 abr. 2024.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 01 mai. 2024.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 30 abr. 2024.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 30 abr. 2024.

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. Acesso em: 02 mai. 2024.

BRASIL. **Lei nº 13.853**, de 8 de julho de 2019. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 30 abr. 2024.

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. Acesso em: 30 abr. 2024.

BRITO, Marcelo Matos *et al.* **Crimes cibernéticos e a recepção da lei no 12.737/2012 no Brasil**. 2020. Disponível em: <http://ri.ucs.br:8080/jspui/handle/prefix/4608>. Acesso em: 30 abr. 2024.

CERT.br. Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <https://www.cert.br/>. Acesso em: 10 mai. 2024.

DE FREITAS, Camila Cristina Gonzaga; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. **Revista JRG de Estudos Acadêmicos**, v. 6, n. 12, p. 296-311, 2023. Disponível em: <http://www.revistajrg.com/index.php/jrg/article/view/520>. Acesso em: 8 mai. 2024.

DE GOIS, Elisangela Cristine. **Direito fundamental da privacidade da intimidade com a evolução da internet: Lei Geral de Proteção de Dados no Brasil**. 2022. 87 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2022. Disponível em: <https://pantheon.ufrj.br/handle/11422/18820>. Acesso em 12 mai. 2024.

DOS SANTOS, Bianca Stefany Ribeiro; DE PAULA, Gil Cesar Costa. **CRIMES CIBERNÉTICOS NO BRASIL: invasão de dispositivo informático e estelionato virtual**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito). Pontifícia Universidade Católica de Goiás. Goiânia – GO. 2023. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6523>. Acesso em: 10 mai. 2024.

DOS SANTOS, Liara Ruff; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo In: **4º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede**. Santa Maria – RS. 2017. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf>. Acesso em: 01 mai. 2024.

LUCCHESI, Ângela Tereza; HERNANDEZ, Erika Fernanda Tangerino. Crimes Virtuais: cyberbullying, revenge porn, sextortion, estupro virtual. **Revista Officium: estudos de direito** – v.1, n.1, 2. Jul/dez, 2018. Disponível em: <https://facdombosco.edu.br/wp-content/uploads/2018/12/%C3%82ngela-Tereza-Lucchesi-Erika-Fernanda-Tangerino->

Hernandez-crimes-virtuais-Copia.pdf. Acesso em: 09 mai. 2024.

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. *Journal of Law and Sustainable Development*, v. 7, n. 2, p. 145-167, 2019. Disponível em: <https://ojs.journalsdg.org/jlss/article/view/51>. Acesso em: 01 mai. 2024.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. *Revista Científica da Faculdade Sete de Setembro*. v. 12 n. 18. 2018. Disponível em: <http://www.publicacoes.unirios.edu.br/index.php/revistarios/article/view/326>. Acesso em: 10 mai. 2024.

SATO, Gustavo Worcki. A INFILTRAÇÃO VIRTUAL DE AGENTES E O COMBATE À PEDOPORNOGRAFIA DIGITAL. ESTUDO DA LEI 13.441/2017 E LEI 13.964/2019. *J2-Jornal Jurídico*, v. 4, n. 1, p. 163-181, 2021. Disponível em: <https://www.revistas.ponteditora.org/index.php/j2/article/view/335/248>. Acesso em: 9 mai. 2024.

STOCO, I. M.; BACH, M. A MULHER COMO VÍTIMA DE CRIMES VIRTUAIS: A LEGISLAÇÃO E A JURISPRUDÊNCIA BRASILEIRA. *Caderno PAIC*, [S. l.], v. 19, n. 1, p. 679–698, 2018. Disponível em: <https://cadernopaic.fae.emnuvens.com.br/cadernopaic/article/view/311>. Acesso em: 08 maio. 2024.