**UNIVERSIDADE PRESBITERIANA MACKENZIE**

GIOVANNA VITÓRIA RODRIGUES CÂMARA

# CRIMES CIBERNÉTICOS:

A responsabilidade das plataformas digitais na prevenção e punição

São Paulo

2024

GIOVANNA VITÓRIA RODRIGUES CÂMARA

# CRIMES CIBERNÉTICOS:

A responsabilidade das plataformas digitais na prevenção e punição

São Paulo

2024

## RESUMO

Considerando a crescente presença da tecnologia na vida das pessoas e os desafios relacionados à segurança digital, objetiva-se analisar os crimes cibernéticos, dada sua ameaça crescente na sociedade contemporânea. Para tanto, procedeu-se a uma revisão bibliográfica e documental de artigos, monografias, livros, jurisprudências e legislações, utilizando como fontes bases de dados como Jusbrasil, Google Acadêmico e Biblioteca Digital do Mackenzie. A legislação brasileira, embora tenha evoluído com a Lei Carolina Dieckmann (Lei 12.737/12) e o Marco Civil da Internet (Lei 12.965/14), ainda carece de dispositivos mais eficientes para lidar com esses crimes. As plataformas digitais desempenham um papel crucial na preservação e aplicação de punições, mas a legislação atual não prevê uma responsabilidade direta dessas plataformas pelos crimes cibernéticos. A obtenção de provas de autoria é uma das principais dificuldades enfrentadas pelas autoridades, devido à complexidade desses crimes e à facilidade com que os criminosos podem ocultar sua identidade. Os resultados obtidos permitiram concluir que os desafios enfrentados pelas autoridades na investigação e punição dos criminosos cibernéticos são significativos, especialmente devido às dificuldades na obtenção de provas de autoria. Além disso, foi identificada a necessidade de uma legislação clara e atualizada que defina as responsabilidades das plataformas digitais e estabeleça consequências para o descumprimento das mesmas.



**Palavras-chave:** Crimes Cibernéticos, Segurança Digital, Legislação, Responsabilidade Das Plataformas Digitais.

# SUMÁRIO

1. INTRODUÇÃO ..... 5

2. CRIMES CIBERNÉTICOS ..... 6

3. DIFICULDADES NA OBTENÇÃO DE PROVAS DE AUTORIA ..... 10

4. REGULAÇÃO BRASILEIRA ..... 12

5. PAPEL DAS PLATAFORMAS DIGITAIS NA PRESERVAÇÃO E APLICAÇÃO DE PUNIÇÃO NO PROCESSO DE RESPONSABILIDADE ..... 14

6. CONCLUSÃO ..... 16

REFERÊNCIAS ..... 16

## 1. INTRODUÇÃO

Os crimes cibernéticos têm se tornado uma preocupação cada vez mais presente na sociedade contemporânea, à medida que a tecnologia avança e a dependência das plataformas digitais aumenta. Estes crimes abrangem uma ampla gama de atividades ilícitas, como hacking, *phishing*, fraudes online, *cyberbullying*, entre outros, causando prejuízos financeiros, danos emocionais e violações de privacidade para indivíduos e organizações em todo o mundo (Pereira, 2023).

No entanto, um dos aspectos mais complexos na abordagem dos crimes cibernéticos é a questão da responsabilidade das plataformas digitais na prevenção e punição desses delitos. Plataformas como redes sociais, serviços de mensagens, lojas online e provedores de serviços têm sido frequentemente apontadas como facilitadoras desses crimes, seja permitindo a disseminação de conteúdo ilegal, seja por não adotarem medidas suficientes para impedir atividades criminosas em suas plataformas (Bispo; Bindo, 2021).

A discussão sobre a responsabilidade das plataformas digitais ganhou ainda mais destaque com o aumento de casos de disseminação de desinformação, discurso de ódio, cyberbullying e violações de direitos autorais online. A pressão pública e governamental para que essas plataformas assumam uma postura mais proativa na identificação, prevenção e punição de crimes cibernéticos tem aumentado significativamente (Menin, 2023).

No entanto, a definição clara das responsabilidades das plataformas digitais nesse contexto é complexa e suscita debates acalorados. Enquanto alguns defendem que essas plataformas devem ter uma responsabilidade direta na prevenção e punição dos crimes cibernéticos que ocorrem em seus domínios, outros argumentam que isso pode levar a uma censura excessiva e minar a liberdade de expressão na internet (Menin, 2023).

Nesse sentido, o desafio reside em encontrar um equilíbrio entre a responsabilidade das plataformas digitais na prevenção e punição dos crimes cibernéticos e a preservação da liberdade de expressão e privacidade dos usuários. Políticas de uso responsável, investimento em tecnologias de segurança cibernética, cooperação com as autoridades e educação digital são algumas das medidas que podem ser adotadas para enfrentar esse desafio de forma eficaz. Além disso, é fundamental que haja uma legislação clara e atualizada que defina as responsabilidades das

plataformas digitais e estabeleça consequências para o descumprimento das mesmas (Pereira; Medeiros; Barros, 2024)

A pesquisa realizada constitui uma revisão bibliográfica e documental abrangente, que incluiu a análise de diversos tipos de materiais, tais como artigos científicos, monografias, livros, jurisprudências e legislações relacionadas ao tema dos crimes cibernéticos. Esses materiais foram coletados em fontes diversas, incluindo o Jusbrasil, Google Acadêmico e a Biblioteca Digital da Universidade Presbiteriana Mackenzie.

No processo de seleção dos materiais a serem analisados, foram estabelecidos critérios específicos. Dentre eles, deu-se preferência a obras de doutrina e estudos publicados em língua portuguesa, considerando uma janela temporal de análise dos últimos 20 anos.

Essa abordagem metodológica permitiu uma análise ampla e atualizada do tema, fornecendo uma base sólida para a compreensão dos diferentes aspectos relacionados aos crimes cibernéticos, suas implicações legais e suas repercussões na sociedade contemporânea.Sendo assim, neste trabalho abordaremos todos os conceitos de crimes cibernéticos, os desafios no combate aos crimes cibernéticos, as legislações contemporâneas, o papel das plataformas digitais tanto na preservação, quanto na punição durante o processo de responsabilização e por fim, as dificuldades para obtenção de provas.

## 2. CRIMES CIBERNÉTICOS

Os crimes cibernéticos têm registrado um aumento concomitante com a propagação da internet, com novos aplicativos e sites. As condutas ilícitas praticadas por agentes nesse domínio virtual revelam que, a cada dia que passa, há uma maior sofisticação e consolidação.

Ações dessa natureza ilícita exibem diversas nomenclaturas, portanto, vale ressaltar que todas essas denominações diferentes irão apresentar a mesma natureza intrínseca deste crime. Logo, os autores Antonelli e Almeida (2011, p.3) determinam sobre as diversas terminologias:

> existem várias nomenclaturas utilizadas para designar um crime praticado através de um computador conectado à Internet, dentre elas pode-se citar: crimes virtuais, [...], crimes cibernéticos, cibercrimes, entre outras. Desta maneira, para este labor, será utilizado ‘crime cibernético’ (Antonelli; Almeida, 2011, p.3).

A conexão com o mundo virtual se dá predominantemente por meio de computadores, conectados ou não a internet, manifestando-se por meio de diversas formas e podendo ocorrer a qualquer hora e lugar (Silva; Lima, 2018). Há diversos autores que conceituam os crimes

cibernéticos de suas próprias maneiras, alguns apresentam mais riquezas em suas definições e outros buscam atingir a definição de forma sucinta. Tendo como exemplo, o Fabrízio Rosa:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O „Crime de Informática“ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o Crime de Informática "pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos 10 crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública etc. (Rosa, 2002, p. 53).

Em comparação quanto ao autor Sergio Marcos Roque, a definição desses delitos tem sido como "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

De acordo com Crespo (2015, s/p), em seu estudo existem duas categorias para a classificação dos crimes cibernéticos, sendo elas denominadas como crimes digitais próprios e crimes digitais impróprios:

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio.

Assim os crimes cibernéticos próprios são aqueles que, por definição, só podem ser realizados no âmbito digital, em outras palavras, a execução do crime e a consumação dão-se nessa esfera virtual. No livro Fundamentos de direito Penal Informático, da Marco Tulio Viana; "São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)" (Viana, 2003, p. 32).

Já os crimes cibernéticos impróprios estão tipificados no Código Penal, haja vista que, infringem diversas leis e regulamentações, incluindo, porém, não podendo se limitar a violação dos bens jurídicos comuns, a dignidade da pessoa humana, dentre diversas outras (Tormen, 2018)

Em relação aos indivíduos envolvidos em crimes cibernéticos, vale ressaltar que existem dois termos utilizados para nomear esses sujeitos, sendo eles conhecidos como sujeitos ativos e passivo, tendo a doutrina de Harakemiv para expor o conceito:

> No crime em questão, adicionado ao Código Penal pela Lei 12.737/12, considera-se que pode incorrer como sujeito ativo qualquer pessoa, já que o seu tipo penal não exige nenhuma qualidade especial do seu agente, sendo, portanto, um crime comum.Quanto ao sujeito passivo dos crimes informáticos considera-se que possa ser qualquer pessoa que utilize ou não o meio eletrônico, podendo existir mais de um indivíduo desde que tenham seus bens jurídicos ameaçados ou lesados pela mesma conduta delituosa, como por exemplo, uma série de e-mails contendo o mesmo conteúdo viral cujo objetivo é lesar quem os recebe (Harakemiv; Vieira, 2014, p.424).

Segundo a perspectiva de Cecílio da Fonseca Vieira Ramalho Terceiro (2009 *apud* Dullius, 2012, [n.p.]):

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência de seus autores e seus asseclas.

Em vista desse contexto, com as principais definições, classificações dos crimes cibernéticos e determinação dos sujeitos definidas, será de suma importância tratar nos tópicos seguintes, acerca das dificuldades para os agentes localizar e punir o sujeito ativo/passivo deste delito.

Na contemporaneidade, as pessoas acreditam na impossibilidade de responsabilizar os autores desses crimes, por se tratar de um ambiente virtual, haja vista que, os crimes cibernéticos necessitam de investigações especializadas e ações efetivas. Segundo Ferreira, a impunidade dos crimes cibernéticos:

> Por isso temos a sensação de impunidade, sendo um atrativo muito forte para o crescimento desse tipo de delito. As ameaças podem ser tanto por meio de monitoramentos não autorizados do sistema como a (DEP WEB), como através de ataques mais sofisticados por hackers (Ferreira, 2015, p.32).

Essa perspectiva de impunidade para este delito não se sustenta, os crimes virtuais são rastreáveis e nenhum fator impedirá que esses crimes virem objetos de investigação. Contudo, os

crimes cibernéticos são complicados, uma vez que podem ocorrer de todas as formas, horários e por qualquer pessoa, portando os agentes precisam apresentar aptidão ao se deparar com esse crime.

> A mesma Internet que representa avanços tecnológicos na comunicação, na informação, na ciência, no comércio, é também aquela que difunde uma noção equivocada de impunidade, seja pelo referido anonimato, seja pela dificuldade no rastreamento do autor, ou ainda, seja pela dificuldade de aplicação da legislação em vigor (Marra, 2019, n.p).

A lei 12.735/12 em seu artigo 4º, determina que os órgãos da polícia judiciária precisam dessas divisões habilitadas no combate dos crimes cibernéticos. Existem um número reduzido de estados brasileiros que possuem essa preocupação com a preparação do ambiente necessário para resolução das ocorrências desses delitos (Lima, 2021).

No Brasil, o preparo dos policiais para combater esses crimes, vem crescendo consideravelmente, no entanto, os autores desses delitos estão crescendo excessivamente mais rápido. Em 2020, o Governo do Estado de São Paulo, inaugurou a Divisão de Crimes Cibernéticos, composta de polícias especializados para atuar nesta divisão (Brasil, 2020)

Neste departamento, as investigações exigem uma série de processos, que não podem ser interferidos para conseguir chegar no autor do crime, uma vez que, os criminosos sempre utilizam de diversos métodos segundo suas habilidades para conseguir atingir os seus objetivos com camuflagens especificas (Brasil, 2020).

Os crimes cibernéticos ao decorrer dos anos demonstraram uma crescente significativa em relação aos seus autores, com muita destreza ao realizar o crime e conseguir entornar suas vítimas e pouca preocupação com o combate deste crime na mesma intensidade, rapidez e aptidão. Há um entendimento doutrinário que visa apontar o porquê do crescimento concomitante dos crimes cibernéticos na contemporaneidade:

> Entendemos que há três razões para o aumento de crimes digitais: 1ª) Crescimento dos usuários de Internet e demais meios eletrônicos (celular, atm etc.) principalmente junto à baixa renda (classes C e D) e que se tornam vítimas fáceis, pois ainda não possuem cultura de uso mais seguro. 2ª) Quanto mais pessoas no meio digital, os bandidos profissionais (quadrilhas) também migram, e então há maior ocorrência de incidentes. 3*) Falta de conscientização em segurança da informação, a maior parte das pessoas acha que nunca vai ocorrer com ela, empresta a senha, deixa o computador aberto e ligado, não se preocupa em usar as ferramentas de modo mais diligente, isso somado com uma dose de inocência potencializa as ocorrências (Pinheiro, 2021, p. 230).

Há um consentimento de que a internet viabilizou diversas novas formas de interações sociais, que infelizmente, proporcionaram o aumento dos crimes cibernéticos. A muito anos atrás esse pensamento já havia sido debatido pelo doutrinador Corrêa (2008, n.p), que dizia: "a Internet

é um paraíso de informações, e, pelo fato de estas serem riquezas, inevitavelmente atraem o crime. Onde há riqueza há crime".

Desse modo, além do combate aos crimes cibernético ser uma dificuldade atual devido a necessidade de preparo especializado, a diversas dificuldades que os agentes apresentam para obtenção de provas de autoria, pois os recursos precisam ser imensuráveis e infinitos para conseguir localizar os criminosos, a seguir será demonstrado as dificuldade e facilidades na obtenção dessas provas.

## 3. DIFICULDADES NA OBTENÇÃO DE PROVAS DE AUTORIA

É indiscutível que a tecnologia simplificou diversos aspectos do nosso dia a dia. Contudo, junto com as vantagens, vieram os desafios dos crimes cibernéticos, os quais demonstram diversas complexidades na resolução. Lidar com esses crimes, será necessário de agentes especializados capazes de enfrentar aparelhos altamente sofisticados, considerando que os criminosos estão em constantes aprimoramento de suas habilidades (Pereira, Oliveira, Junior, 2021). Os autores Jesus e Milagre (2016), ressaltam que:

> Entretanto, a progressiva mutação tecnológica dificulta o combate a esses crimes, que estão em constante alinhamento com as novas tecnologias. Assim, com o uso incontido e indiscriminado da internet, alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos roubar informações criptografadas, como já havia sido feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão (Jesus; Milagre, 2016, n.p).

Há diversas etapas necessárias para identificação de autores nos crimes cibernéticos, sendo necessário todo um processo para verificação da verdadeira autoria no crime, pois as técnicas de anonimato são avançadas, há criptografia para ocultar identidade, entre outras diversas possibilidades para ocultar a identidade do autor, ou até mesmo atribuir a culpa a terceiros inocentes. (Pereira, Oliveira, Junior, 2021) O Fernado Tourinho Filho (2009), ressaltou seu entendimento sobre a veracidade dos fatos:

> Antes de mais nada, estabelecer a existência da verdade; e as provas são os meios pelos quais se procura estabelecê-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos. É o instrumento de verificação do *thema probandum*. (Tourinho, 2009, P. 522).

A Comissão Parlamentar de Inquérito, conhecida como CPI, realizou algumas audiências com intuito de ouvir os delegados da Polícia Federal sobre esses crimes virtuais na perspectiva da dificuldade em rastrear e punir os autores, por exemplo nos crimes de publicação de vídeos e fotos intimas, como relato no caso da atriz Carolina Dieckman (Canuto, 2015). Segunda essas audiências, as dificuldades apresentadas nas investigações são:

> A dificuldade se deve ao fato de que a velocidade de obter as informações com as empresas não ocorre na velocidade da internet. O chefe do Serviço de Repressão a Crimes Cibernéticos da PF, Elmer Vicente, explicou que a investigação começa com a identificação do endereço IP do computador de onde partiu o crime, que é dado pelo provedor de serviço. O próximo passo é conseguir, com o provedor de internet, o nome do usuário do IP. Segundo Elmer, no entanto, há duas grandes dificuldades. A primeira é que, curiosamente, algumas empresas não aceitam a requisição de informações da polícia pela internet. Outra dificuldade é que, se antes algumas empresas concediam informações por meio de requisição policial, com o marco civil da internet, as empresas geralmente cedem os dados apenas por meio judicial. (Agência Câmara De Notícias, 2015)

Dessa forma, como podemos observar nos crimes cibernéticos, existe uma imensidão de pessoas que podem praticar esses crimes, algumas consideradas com habilidades especiais e outras apenas indivíduos que possuam um computador com acesso à internet. As pessoas que não possuem tais conhecimentos para dificultar a operação, deixam as provas de autoria com acesso fácil, e com toda a recuperação de dados de dispositivos eletrônicos, os registros de atividades online, entre outros fatos, acabam sendo mais fáceis do autor ser identificado. (Pereira, Oliveira, Junior, 2021)

Normalmente, o endereço de IP (protocolo de internet) demonstra o titular da rede disponível no imóvel, esse IP é um identificador único atribuído a cada dispositivo conectado a uma rede de computadores, fornecendo a localização e atividades online. No entanto, os agentes necessitam tomar cuidado, pois em média de pessoas por domicílio pode variar entre 2 e 3 pessoas, então ainda que tenham uma localização, precisam agir conforme todos os procedimentos para conseguir localizar o indivíduo autor do crime (Pereira, 2023).

As dificuldades na obtenção de provas nos crimes cibernéticos destacam a importância contínua de revisões e atualizações nas legislações brasileiras, garantindo uma abordagem eficaz e equilibrada na investigação desses delitos, visando o bom convívio da sociedade. Com base nos dados atuais é possível ressaltar diversos exemplos de crimes realizados com mais frequência por esses criminosos, conforme dispostos no Código Penal Brasileiro, sendo eles os crimes contra a honra (arts. 138, 139 e 140 CP), crimes contra o patrimônio e crimes sexuais, necessitando, desse modo, de legislações mais eficientes nesses determinados delitos (Brasil, 1940).

Portanto, a seguir, será abordado as configurações apresentadas nas legislações brasileiras que embaçam os direitos das vítimas após sofrerem esses crimes, tais legislações são fundamentais para lidar com crimes cibernéticos, estabelecendo regras juntamente com as penalidades quando descumprir a regra.

## 4. REGULAÇÃO BRASILEIRA

Atualmente, as regulamentações dos crimes cibernéticos estão sendo debatidas e reformuladas, visto que na Constituição Federal no seu artigo 5º, XXXIX, demonstra que: “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal” (Tormen, 2018).

Há duas normativas que caracterizam as condutas criminosas no ambiente virtual, sendo elas sancionadas em 2012, modificando o Código Penal e implementando outras diversas penas para os crimes que não apresentavam uma tipificação pré-estabelecida (Crimes..., 2024).

Em primeiro lugar, a Lei 12.737/12, conhecida como Lei Carolina Dieckman, foi um início importante para as normatizações desses crimes. A atriz que teve seu nome atribuído a lei, porque foi vítima de crime invasão de dispositivo informático, realizado por meio da internet, tendo o conteúdo pessoal levado a público, dentre muitas ameaças com intuito de extorsão, sem nenhum amparo legal (Fachini, 2023).

> 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 (Brasil, 2012).

Como mencionado acima, esse artigo teve intuito de tipificar os crimes de invasão de dispositivos informáticos, haja vista que, esse crime não apresentava legislação no Código Penal. O artigo seguinte, 154-B estabelece que as condutas criminosas alçadas neste artigo, apenas procederão por intermediário de representação do ofendido, sendo uma ação penal publica, condicionada a representação da vítima (Cabette, 2025).

> 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, 1940).

Após um período, a Lei 12.965/14, conhecida como o Marco Civil da Internet, que regulamentou os direitos e deveres dos cidadãos brasileiros, tendo um papel importante na base

teórica sobre as relações digitais, normatizando a utilização da internet no Brasil e assegurando que todos desfrutem em conformidade com os princípios da Constituição Federal (Santos, 2016).

> A situação pré-Marco Civil era de completa ausência de regulamentação civil da internet no país. Ao contrário do que alguns entusiastas libertários poderiam achar, a ausência de leis nesse âmbito não representa a vitória da liberdade e do laissez-faire. Ao contrário, gera uma grande insegurança jurídica, uma das razões é que juízes e tribunais, sem um padrão legal para a tomada de decisões sobre a rede, acabam decidindo de acordo com regras muitas vezes criadas ad hoc, ou de acordo com as suas próprias convicções, resultando em inúmeras decisões judiciais contraditórias (Lemos, 2014, p. 10).

Dessa forma, ao observar a lei mencionada, fica evidente as subdivisões em cinco capítulos. Tendo como primeiro capítulo as disposições preliminares, ou seja, ressaltar que a Lei observará todos princípios e garantias na utilização da internet, e os fundamentos que devem ser observados na empregabilidade deste uso (Brasil, 2014).

A segunda capítulo da Lei vai abordar os direitos e garantias dos usuários, sendo importante a determinação expressa para evitar ambiguidades. Já o capítulo seguinte, por sua vez, vai ressaltar um enfoque aos serviços de distribuição da internet e às suas aplicações, sendo divido em quatro seções centrais, relacionadas a neutralidade de rede, proteção aos registros, dados pessoas e comunicações privadas, a responsabilidade dos fornecedores por danos decorrentes do conteúdo de terceiros e requisição judicial de registros (Brasil, 2014).

Por fim, o capítulo quarto e quinto alçam as ações do poder público e disposições finais. Então, o Marco Civil é atualmente a lei que visa abordar todos os requisitos necessários para estabelecer as regras e regulamentos para conviver nesta nova era digital, visando adotar uma legislação “principiológica”, ou seja, ter como ponto central os direitos, fundamentos e objetivos na utilização da internet (Santos, 2016).

Cabe ressaltar, ademais, que o Marco Civil não conseguiu completar as diversas lacunas identificadas no sistema, principalmente ao tratar dos crimes cibernéticos, tendo em vista que, o Marco Civil não é uma lei exclusiva voltada para esses crimes, e que por se tratar de um assunto extremamente atual, diversas mudanças estão sendo debatidas e tendem a sofrer mudanças.

Desse modo, segundo estudos fica evidente que os legisladores estão admitindo as particularidades dos crimes cibernéticos com a atual incidência criminal no Brasil. Sendo importante a busca das melhores alternativas para solucionar os problemas decorrentes deste delito na sociedade, com aperfeiçoamento dos dispositivos de persecução (Minski, 2018).

## 5. PAPEL DAS PLATAFORMAS DIGITAIS NA PRESERVAÇÃO E APLICAÇÃO DE PUNIÇÃO NO PROCESSO DE RESPONSABILIDADE

Cada capítulo abordado anteriormente tinha como objetivo principal enfatizar a responsabilidade das plataformas digitais, tanto na preservação, quanto na punição direta, que poderia ser empregado por tais responsáveis. Primeiramente, vamos ressaltar as punições que essas plataformas podem ou não aplicar no processo desses crimes.

Com relação aos provedores, o Marco Civil (lei 12.965/14) regulamentou em sua legislação diversos deveres que obrigatoriamente precisam ser realizados, com intuito de contribuir com a Justiça, quando for necessário. No entanto, como ressaltado anteriormente, essa lei demonstra alguns aspectos controvertidos na implementação de casos reais, principalmente ao tratar dos crimes cibernéticos (Minski, 2018).

O artigo 19° do Marco Civil, define qual modelo de responsabilidade que opera conteúdo de terceiro, haja vista que, segundo doutrinadores essas plataformas digitais não “criam” esses aplicativos, apenas indicam a utilização conforme as buscas pessoais. Esse artigo demonstra os seguintes aspectos:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (Brasil, 2014).

Dessa forma, o intuito deste artigo é alçar a responsabilização das plataformas digitais, ressaltando que apenas serão responsabilizados por conteúdos que causarem danos a terceiros, no instante receberem uma ordem judicial e não apresentarem as medidas cabíveis, no tempo necessário.

Entretanto, houve discussões sobre o STF sobre a inconstitucionalidade deste artigo, pois há discordância em precisar de ordem judicial para retirar o conteúdo das redes sociais após ser notificado, uma vez que, os processos são extremamente demorados e duradouros. Mas essas discussões não obtiveram sucesso demonstrando que, a responsabilidade conforme a legislação é subsidiária, não sendo necessário qualquer supervisão no conteúdo desenvolvido por terceiros. (Alves, 2020)

A legislação brasileira não prevê nenhum tipo de responsabilização direta das plataformas digitais para os crimes cibernéticos, o presidente da Comissão de Privacidade, Proteção de Dados

e Inteligência Artificial de seccional de São Paulo da Ordem dos Advogados do Brasil, Solano de Camargo, demonstra ser necessário o debate sobre as responsabilidades das plataformas, haja vista que, os criminosos vão se aproveitar da pouca dificuldade ofertada para praticar esses crimes e as plataformas não terão como preocupação a atuação direta nas ocorrências, já que não sofrem nenhum tipo de responsabilização imediata (Xavier, 2023).

O advogado Solano de Camargo, ressaltou acreditar na importância de ampliar o debate, em evidências nos casos sem governança necessária pelas plataformas digitais, com intuito de controlar as ações dos criminosos, as palavras do jurista foram:

> Embora as plataformas não sejam responsáveis pelas ações de seus usuários, elas desempenham um papel importante ao facilitar a comunicação e interação entre eles. Por isso, elas devem ser responsabilizadas por não tomarem medidas para prevenir a prática de crimes através de seus recursos (Xavier, 2023).

Segundo o Luiz Augusto Filizzola D'Urso, o presidente da Comissão Nacional de Cibercrimes da Associação Brasileira dos Advogados Criminalista, há uma extrema falta de dedicação das plataformas para diminuir quaisquer condutas criminosas de seus sistemas, acreditando no "desinteresse" das plataformas (Xavier, 2023).

> Isso pode ser justificado em razão das leis. Hoje não há como trazer a responsabilidade por eventual coautoria ou por omissão dessas plataformas para esses golpes aplicados porque as leis afastam a responsabilidade. Na esfera cível, nós temos o Marco Civil da Internet afastando por completo a responsabilidade, no artigo 19, sobre conteúdo publicado por seus usuários, mesmo que ele seja ilícito, com a exceção da pornografia (artigo 21) (Xavier, 2023).

Assim, podemos considerar que não haverá responsabilidade direta para as plataformas digitais prevista em lei. As responsabilidades são no âmbito civil, com a reparação do dano causado a vítima, sendo ele moral ou material, e na esfera penal, pois as legislações abordadas no decorrer desta pesquisa demonstram as sanções atribuídas aos criminosos, segundo o crime atribuído ao Código Penal de 1940 e a Lei n° 12.737/12.

Cabe ressaltar que há medidas que são adotadas pelas plataformas digitais em relação a preservação, como por exemplo, a coleta de evidências, alçada no Marco Civil, artigo 10 da Lei 12.965/14. As evidências nos processos penais, são consideradas o meio mais importante da ciência processual, para vincular a culpa ou inocência do agente, tendo a idoneidade e validade de prova apurados para obtenção do resultado do processo, dentro do devido processo legal e com todas as garantias individuais (Sodré, 2012).

## 6. CONCLUSÃO

À luz de todas os aspectos apresentados, fica evidente que as preservações vindas das plataformas, deveriam ser mais eficientes, para demonstrar diminuição nas porcentagens destes crimes. Atualmente, há uma certa dificuldade nas relações de crimes cibernéticos e a dificuldade em obter evidências lícitas e suficientes para comprovar a autoria e a materialidade dos fatos, devido as facilidades para alterar dados na internet, como alteração de endereços eletrônicos (Sodré, 2012).

Além disso, há falta de cooperação entre autoridades e vítimas, contribuindo na incerteza durante o processo de resolução dos crimes. Sendo necessário retornar ao assunto de legislações eficientes, agentes habilitados e equipamentos com capacidade, com intuito de tornar cada etapa desse processo mais ágil e fácil. Ou seja, policiais capacitados vão conseguir lidar com as vítimas desses crimes, os computadores acabaram ajudando na eficiência em comparação com o criminoso e legislações competentes junto com a responsabilidade das plataformas digitais diminuíram a quantidade desses crimes e possíveis criminosos.

## REFERÊNCIAS

ALVES, N. **O artigo 19 do Marco Civil da Internet é constitucional?**. De 2020. Disponível em: https://www.jusbrasil.com.br/artigos/o-artigo-19-do-marco-civil-da-internet-e-constitucional/787278083. Acesso em: 10/01/2024.

BISPO, A; BINTO, E.V. Crimes Cibernéticos: Da Ineficácia Da Lei Carolina Dieckmann Na Prática De Crimes Virtuais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 11, p. 354-369, 2023.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União, Rio de Janeiro, RJ, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm\. Acesso em: 29 abr. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em:

CABETTE, E. **Crime de invasão de dispositivo informático**. Disponível em: https://www.jusbrasil.com.br/artigos/crime-de-invasao-de-dispositivo-informatico-artigo-154-a-cp/153070617/amp. Acesso em: 10/01/2024.

CANUTO, L C. **CPI constata dificuldade em rastrear e punir crimes de internet.** Câmara dos Deputados, agosto de 2015. Disponível em: https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e- punir-crimes-de-internet/. Acesso em:

CARLETTI, G. A. **Responsabilidade civil dos provedores de aplicação que utilizaram criptografia no combate de crimes cibernéticos comedidos em suas plataformas.** 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/30219. Acesso em: 10/01/2024.

CORRÊA, G. **Aspectos jurídicos da internet**. Saraiva, 2008.

CRESPO, M **Crimes Digitais: do que estamos falando?** Disponível em: http://canalcienciascriminais.com.br/ artigo/crimes-digitais-do-que-estamos-falando/. Acesso em: 10/01/2024.

D'URSO, L A. F. **Cibercrime: perigo na internet**. Publicado em 2017. Disponível em http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/. Acesso em: 10/01/2024.

FACHINI, T. **Lei Carolina Dieckmann: Tudo o que você precisa saber sobre.** Disponível em:https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/. Acesso em: 10/01/2024.

FERREIRA, É. **Internet Macrocriminalidade e Jurisdição Internacional**. 1 edição (ano 2007), 1 reimpr. Curitiba: Juruá, 2010.

**Governo do Estado inaugura Divisão de Crimes Cibernéticos.** Portal do Governo, 18/12/2020. Disponível em: https://www.saopaulo.sp.gov.br/spnoticias/governo-do-estado-inaugura-divisao-de-crimes-ciberneticos-2/. Acesso em: 10/01/2024.

HARAKEMIW, R A; VIEIRA, T. **Crimes Cibernéticos. Anais do 2o Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais, 2014.** Disponível em: http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-an%C3%A1lise-do- processo-investigat%C3%B3rio-e-desafios-enfrentados. Acesso em: 10/01/2024.

HUMBERTO L. ANTONELLI, E. G. ALMEIDA. **A Internet e o Direito: Uma abordagem sobre cibercrimes.** EGOV. 2011. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/a_internet_e_o_direito_uma_abordagem_sobre_cibercrimes.pdf. Acesso em: 10/01/2024.

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

LIMA, C. **Crimes cibernéticos: o lado obscura da rede.** Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2419/1/CLÁUDIO%20VIEIRA%20GUIMARÃES%20LIMA%20-%20TCC.pdf. Acesso em: 15/02/2024. (Usei a pág 21)

MARRA, F. Desafios do Direito na Era da Internet: uma breve análise sobre os crimes cibernéticos. **Campo Jurídico,** v. 7, n. 2, p. 145–167, 12 dez. 2019. Disponível em: http://fasb.edu.br/revista/index.php/campojuridico/article/view/289. Acesso em: 15/02/2024

MENIN, M et al. **A responsabilidade civil por cyberbullying praticado por crianças e adolescentes**. v. 18, n.1, 2023.

MINSKI, B. H. Z. **Crimes cibernéticos e a responsabilidade dos provedores: uma análise conceitual e legislativa sob a ótica da sociedade de informações e do risco**. Disponível em: https://acervodigital.ufpr.br/xmlui/bitstream/handle/1884/62274/BRUNO%20HENRIQUE%20ZANETTE%20MINSKI.pdf?sequence=1&isAllowed=y . Acesso em: 10/01/2024.

PEREIRA, A V. Censo 2022: **Brasil tem menos de três moradores por domicílio**. Disponível em: https://www.correiobraziliense.com.br/brasil/2023/06/amp/5105291-censo-2022-brasil-tem-menos-de-tres-moradores-por-domicilio.html. Acesso em: 10/01/2024.

PEREIRA, D. **A Investigação de Crimes Através de Meios Eletrónicos pela GNR**. 2023. Tese de Doutorado.

PEREIRA, M. A. C. et al. **Crimes cibernéticos e os desafios ao direito brasileiro**. Disponível em: https://repositorio.animaeducacao.com.br/items/3af94ab5-cc04-4818-a75a-5a53c920ada3. Acesso em: 10/01/2024.

PEREIRA, W; MEDEIROS, N; BARROS, R. Crimes digitais e os limites da liberdade de expressao na internet no brasil (direito). **Repositório Institucional**, v. 2, n. 2, 2024.

PINHEIRO, P. **Direito digital.** 7. ed. São Paulo: Saraiva Educação, 2021.

PINHEIRO, P. P. **Direito digital.** 7. ed. São Paulo: Saraiva Educação, 2021.

RAMALHO TERCEIRO, C. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi,** Teresina, a. 6, n. 58, ago. 2002. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=3186. Acesso em: 10/01/2024.

ROSA, F. **Crimes de Informática**. Campinas: Bookseller, 2002. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-cibernéticos. Acessado em: 10/01/2024.

ROSSINI, A. E de S. **Informática, telemática e direito penal.** São Paulo: Memórias Jurídica, 2004. ROSSINI, 2004, p. 110-113.

SANTOS, V. W. **Neutralidade da rede e o Marco Civil da Internet no Brasil: atores, políticas e controvérsias**. 2016. Tese (Doutorado em Direito) – Universidade Estadual de Campinas, Campinas, p. 148-149. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/321453/1/Santos_ViniciusWagnerOliveira_D.pdf. Acesso em: 10/01/2024.

SARLET, I. W. **Inteligência Artificial, Proteção de Dados Pessoais e Responsabilidade na Era Digital-Série Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação**. Saraiva Educação SA, 2022.

SILVA, J.; LIMA, M. **Os principais cibercrimes praticados no Brasil**. 2018. Disponível em: https://editorarealize.com.br/artigo/visualizar/48488. Acesso em: 10/01/2024.

SODRÉ, L. **Dificuldade na colheita de elementos de autoria e materialidade dos crimes.** Disponível em: https://dspace.uniceplac.edu.br/bitstream/123456789/1717/1/Ludmilla%20Gonçalo%20da%20Silva%20Sodré%20.pdf. Acesso em: 10/01/2024.

SYDOW, S T. **Curso de Direito Penal Informático – Parte Geral e Especial.** 4. ed. rev. e atua. – São Paulo: Editora JusPodivm 2023. 880p.

TORMEN, C.. **Crimes cibernéticos: (im)possibilidades de coerção**.Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4078.pdf. Acesso em: 10/01/2024.

TOURINHO FILHO, F. **Código de Processo Penal Comentado**: v1. 12. ed. rev. e atual. São Paulo, 2009.

VIANNA, T. **Fundamentos de Direito Penal Informático.** Rio de Janeiro: Forense, 2003. Disponível em: https://ambitojuridico.com.br/edicoes/revista- 191/crimes-ciberneticos-phishing/. Acesso em: 10/01/2024.

XAVIER, R. **Responsabilidade das plataformas por crimes patrimoniais precisa ser discutida**. 10 de setembro de 2023. Disponível em: https://www.conjur.com.br/2023-set-10/responsabilidade-redes-crimes-patrimoniais-discutida/. Acesso em: 10/01/2024.