B1 ISSN: 2595-1661

ARTIGO

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg

Cibercrimes na legislação brasileira: reflexos atuais da lei n 14.811/24

Cybercrimes in brazilian legislation: current reflections of law n 14.811/24

DOI: 10.55892/jrg.v8i18.2242
ARK: 57118/JRG.v8i18.2242

Recebido: 05/06/2025 | Aceito: 10/06/2025 | Publicado *on-line*: 11/06/2025

Eduarda Nasser Siqueira[1]
https://orcid.org/0009-0003-4925-1513
http://lattes.cnpq.br/1168060626478485
Centro de Ensino Superior de Palmas, TO, Brasil
E-mail: eduardasiqueiranasser@gmail.com

Iara Carolina Lima Gonçalves[2]
https://orcid.org/0000-0001-5996-5681
http://lattes.cnpq.br/4319123220159020
Centro de Ensino Superior de Palmas, TO, Brasil
E-mail: iara.carolina130@gmail.com

Resumo

Com o advento da tecnologia, tivemos uma mudança significativa no modo de interação e convivência humana, visto que, com a globalização, não existem mais restrições geográficas, possibilitando que os laços afetivos se permaneçam firmes e sólidos, mesmo diante da distância dos continentes e nações. Apesar da humanidade ter demonstrado um avanço acelerado com o auxílio da tecnologia, também surgiram novas modalidades de crimes, porém, adaptadas dentro meio digital, ora denominados por: *cibercrimes*. Os crimes virtuais consistem em condutas antijurídicas que são praticadas valendo-se dos meios da tecnologia e da informação para consumação do delito. Neste contexto, com a avanço na modernização dos meios de comunicação, foi possível observar um aumento exponencial na quantidade de usuários que ingressaram no *ciberespaço*, e por consequência direta, uma extrema vulnerabilidade social ante a falta de regulamentação legislativa sobre as redes.

Palavras-chave: Internet; Cibercrime; Lei nº 14.811/24.

Abstract

With the advent of technology, there has been a significant change in the way humans interact and live together, since globalization means that there are no longer any geographical restrictions, making it possible for emotional ties to remain firm and solid, even when continents and nations are far apart. Although humanity has made rapid progress with the help of technology, new types of crime have also emerged, but

[1] Graduação em andamento em DIREITO pelo Centro de Ensino Superior de Palmas
[2] Advogada e Servidora Pública. Mestre em Desenvolvimento Regional pela Universidade Federal do Tocantins (UFT), Professora Universitária desde 2015, leciona as disciplinas de Ética Geral e Profissional, Direito Ambiental, Direito Civil, Direito do Consumidor, Direito Previdenciário, Direito Tributário e Direito Constitucional.

adapted to the digital environment, now known as cybercrime. Cybercrime consists of unlawful conduct that is carried out using the means of technology and information to commit the crime. In this context, with the advance in the modernization of the means of communication, it has been possible to observe an exponential increase in the number of users who have entered cyberspace, and as a direct consequence, extreme social vulnerability in the face of the lack of legislative regulation on the networks.

Keywords: *Internet; Cybercrime; Law nº. 14.811/24.*

1. Introdução

Um dos maiores obstáculos enfrentados pela humanidade desde sempre residiu na ideia de conseguir unir as nações e os povos, independente da sua religião, crença pessoal, distância ou idioma, esse desejo foi almejado e tentado por muitos. Sendo que, a internet foi a única que conseguiu.

A união antes inalcançável dos povos, hoje é uma realidade graças a globalização, com o surgimento da internet tornou-se possível a interação entre as pessoas de localidades diferentes, e com o advento da tecnologia, nossa forma de viver foi totalmente transformada. Contudo, toda mudança vem acompanhada de efeitos positivos e negativos.

Por muitos anos as interações humanas somente eram possíveis através de diálogos pessoalmente, conversas por cartas, jornais, rádios e outros. Todavia, a internet trouxe uma nova forma de socialização, possibilitando a comunicação entre indivíduos do mundo todo, e por consequência direta, essa modernidade pode implicar em possíveis riscos aos usuários dos meios digitais.

A possibilidade do anonimato e a ausência de legislação que coibisse esse tipo de atividade serviu como combustível para criminosos por muito tempo, havendo discussões sobre a temática, principalmente em âmbito penal, onde não é permitida a interpretação "*in pejus"* em respeito ao princípio da legalidade, por expressa vedação legal do Código Penal Brasileiro:

> "Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

Assim como resta também disciplinado em nosso art. 5º, inciso XXXIX da Constituição Federal da República do Brasil de 1988, "Não havendo crime sem lei anterior que o defina".

Torna-se trivial afirmar que, nas relações de convívio no mundo real já existiam desavenças, contravenções e crimes, contudo, tais vivências também foram levadas para o âmbito digital, dando origem ao que denominamos de cibercrime ou crimes cibernéticos.

O termo "cibercrime" foi adotado da língua inglesa, sendo recepcionado pelo Brasil para conceituar todo e qualquer delito cometido valendo-se da tecnologia. O cibercrime é aquele que se utiliza dos meios digitais como forma de executar o crime, pouco importando a natureza do bem jurídico tutelado (podendo ser físico ou virtual).

E quando mencionamos os crimes digitais a maioria das pessoas, erroneamente, podem acreditar que não estejam correndo riscos pelo fato de que utilizam seus computadores apenas com fins domésticos, fazendo trabalhos escolares, guardando arquivos pessoais, tais como: fotos de familiares e para se comunicar com algum amigo distante.

Contudo, é exatamente por isso que os usuários comuns são os maiores alvos desses criminosos, visto que são esses indivíduos que guardam seus arquivos

pessoais, senhas bancárias, informações sigilosas e não possuem uma grande proteção de software, demonstrando sua vulnerabilidade e facilidade para ocuparem o papel de vítima.

Ainda que você tenha um bom sistema de segurança que proteja seus documentos pessoais, nada impede que os agentes cometam crimes acessando seu dispositivo e enganando terceiros em seu nome, afim de eliminar a responsabilidade dele. Outro exemplo de cibercrime seria você tornar-se um alvo de difamação, injúria ou calúnia nas redes, comumente conhecido como "*cyberbullying*", não havendo necessidade da invasão ao seu dispositivo para consumar o delito.

Observe que nas relações reais já lidávamos diariamente com a figura de criminosos que se valiam da força ou destreza para conseguirem alcançar alguma vantagem ilícita com a vítima. Nesse diapasão, após o advento da internet, precisamos lidar com os mesmos delitos no ambiente virtual, onde se encontram cada vez mais camuflados pelo véu do anonimato, porém reais para efeitos de danos.

Esse artigo visa realizar uma pesquisa afim de iniciar um debate sobre essa nova modalidade de crimes, na intenção de demonstrar as possibilidades de sanções penais existentes e indenizações para vítimas dessa natureza delituosa, mencionando um pouco sobre seus conceitos e *"modus operandi"*.

2. CIBERCRIME: CONCEITO E LEGISLAÇÃO

O cibercrime ou crimes cibernéticos tratam-se de condutas tipificadas como antijurídicas cometidas no âmbito digital, ou valendo-se do acesso a computadores e internet.

Apesar de não ser unânime, a doutrina majoritária adere como conceito de crimes cibernéticos toda e qualquer conduta criminosa cometida através de computadores e dispositivos tecnológicos, bem como, atos que utilizem os meios digitais como forma de concretização.

Significa dizer que, em amplo sentido, o cibercrime engloba toda atividade criminosa que é exercida por meios informáticos para ser consumada, ou seja, todo ato que envolve tecnologia de modo independente ao que a lei está protegendo.
De acordo com Rossini (2004):

> […] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada pela própria pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, disponibilidade a confidencialidade (ROSSINI, 2004, p. 110).

Os primeiros casos de ataques no ciberespaço foram registrados no início de 1960, em meio a guerra fria, sendo que esses casos estavam ligados à espionagem e sabotagem das tropas inimigas. Contudo, a conscientização e estudos sobre o tema só tiveram início na década seguinte, e com os passar dos anos as ações criminosas virtuais escalonaram, fazendo com que finalmente o assunto fosse tratado com a importância que merecia.

A Convenção de Budapeste, ou Convenção de Crimes Cibernéticos adotada pelo Brasil em 16 de dezembro de 2021 definiu alguns comportamentos como crimes cibernéticos, por exemplo o acesso ilegal de dados, interceptação ilícita, violação de dados pessoais, invasão e interferência de sistema, uso indevido de aparelhagem e similares.

Apesar da tecnologia e seus ambientes digitais fazerem parte do dia a dia das pessoas, o legislador somente passou a adotar medidas que coibissem as condutas ilícitas, após a promulgação da Constituição da República Federativa do Brasil em 1988, época em que foram surgindo outras normas que versavam sobre questões informática, pois finalmente o ciberespaço começou a ser verdadeiramente notado.

Segundo Lévy (2000) o conceito de ciberespaço se caracteriza como:

> O ciberespaço (que também chamarei de "rede") é o novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ele abriga, assim como os seres humanos que navega me alimentam este universo. Quanto ao neologismo "cibercultura", especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem conjuntamente com o crescimento do ciberespaço. O ciberespaço tem sua existência virtualmente, que logo após o surgimento da Internet passou a existir, passando a ser um meio de comunicação, sendo assim onde as pessoas podem interagir com outros usuários, até mesmo de longa distância, possibilitando o começo de amizades virtuais, a criação de comunidades, lives, dentre outros (Lévy, 200, p. 17).

Bem como nos demais delitos, os virtuais também se consumam com uma conduta em inobservância aos limites legais, classificando-se como um ato antijurídico, ilícito e culpável, podendo ser com dolo ou culpa. Contudo, a diferença entre os crimes comuns para os digitais reside no fato de que os cibercrimes são cometidos dentro do ciberespaço, ou seja, nos ambientes virtuais, o que dificulta a identificação dos agressores, mas não impossibilita o rastreamento desses indivíduos (Gentil, *et al*., 2018)

Um estudo publicado no ano de 2024 pela Universidade de Oxford foi responsável por classificar os 10 países que mais enfrentam ataques cibernéticos no mundo, sendo que, o Brasil ocupou o 9º lugar dentro do ranking mundial. O coautor do estudo, professor Federico Varese informou que a pesquisa realizada é o primeiro passo para traçar planos estratégicos de combate e prevenção, afim de repelir as condutas de modo mais certeiro.

Segundo Varese:

> "Esperamos expandir o estudo para que possamos determinar se características nacionais como nível educacional, penetração da internet, PIB ou níveis de corrupção estão associadas ao crime cibernético. Muitas pessoas pensam que o crime cibernético é global e fluido, mas este estudo corrobora a visão de que, assim como as formas de crime organizado, ele está inserido em contextos específicos",

Com a realização do mencionado estudo, foi possível identificar que cada país presente no ranking precisa lidar com cibercrimes diferentes, e que o comportamento dos criminosos varia conforme a realidade específica da nação. O Brasil, maior economia da América Latina, tem testemunhado um aumento em ataques direcionados aos setores financeiros e instituições governamentais.

2.1 TIPOS DE CRIMES CIBERNÉTICOS

Conforme explorado, o cibercrime será consumado quando o agente se valida de um meio tecnológico para atingir ou causar dano à vítima. Imperioso destacar que dentre as infinitas possibilidades de comportamentos dentro do ciberespaço, podemos rastrear e mencionar as condutas mais frequentes no Brasil.

Dentre os comportamentos mais frequente conforme registros, são:

> 1) *Hacking* (ocorre quando o indivíduo consegue acesso não autorizado aos sistemas e as informações do alvo, com a intenção de roubar, alterar ou destruir dados);
> 2) *Phishing* (técnica utilizada para conseguir acesso as informações financeiras e números de cartões da vítima, ocorrem por meio de e-mails e mensagens falsas se passando por entidades confiáveis, com intuito de ludibriar o usuário a fornecer seus dados;
> 3) Fraude ou Roubo (Os cibercriminosos obtêm informações através do vazamento de dados online, e se passam pela vítima com intuito de realizarem empréstimos ou aplicarem golpes em terceiros utilizando os dados adquiridos ilegalmente);
> 4) *Cyberbullying* e Assédio (Consiste na utilização do ciberespaço para disseminar discursos de ódio ou intimidações e ameaças à vítima).
> Conforme mencionado, dentro do âmbito digital podemos encontrar uma infinidade de comportamentos que se configuram como cibercrimes, contudo, os quatro mencionados são os mais comuns.

3. LEGISLAÇÃO BRASILEIRA: BASES LEGAIS E REGULAMENTAÇÃO DOS CRIMES VIRTUAIS

Este tópico será responsável por apresentar as legislações vigentes mais importantes no Brasil a fim de demonstrar quais foram as normas responsáveis por alterarem o formato de combate aos crimes virtuais.

Principalmente por que apenas no final da década de 90 que surgiram as discussões sobre o *Bullying*, pois antes desse período, não existia nenhum dispositivo legal que coibisse esse tipo de intimidação.

Insta mencionar que essas leis foram as primeiras que versaram exclusivamente sobre essa modalidade de *cybercrime*, demonstrando um evidente avanço legislativo.

3.1 LEI DOS CRIMES CIBERNÉTICOS Nº 12.737/2012 OU LEI CAROLINA DIECKMANN

No ano de 2011 a atriz brasileira Caroline Dieckmann foi alvo de um crime digital, após o seu computador de uso doméstico ter sido invadido, os responsáveis conseguiram acesso à 36 fotos intimas da atriz, oportunidade em que, usaram essas imagens para extorquir a brasileira.

Apesar da tentativa de chantagem, a atriz se negou a realizar o pagamento que os cibercriminosos estavam pedindo, ocasião em que suas fotos foram divulgadas na internet, gerando uma repercussão nacional sobre o caso. Veja o que disse a atriz em sua rede social após 10 anos do ocorrido:

> “Em 2011 eu passei por um processo doloroso. A minha intimidade foi invadida e isso gerou uma grande discussão pública. Eu tive fotos roubadas e fui extorquida: ou eu pagava ou as minhas fotos seriam publicadas. Eu me recusei a pagar o dinheiro pedido pelos criminosos e eu tive essas fotos íntimas divulgadas na internet. Tudo isso gerou tanta discussão, que se fez urgente a criação de uma lei que protegesse as pessoas, principalmente as mulheres porque são as principais vítimas de crimes na internet”.

Importante destacar que até o ano de 2011 não existia nenhum dispositivo legal que regulamentasse sobre os crimes de informática, contudo, após o caso da atriz brasileira, o assunto ganhou uma maior notoriedade. Ocasião em que no mesmo ano do ocorrido, 6 deputados federais apresentaram um projeto de lei que versava sobre a invasão de dispositivos eletrônicos e o uso das informações obtidas ilegalmente.

Os responsáveis por invadirem o dispositivo da atriz foram localizados e indiciados por furto, extorsão qualificada (exigir dinheiro em troca de não divulgar as fotos) e difamação, sendo que não houve condenação pela invasão, isso por que não existia nenhum dispositivo legal que definisse a conduta como criminosa. Conforme já mencionado, nossa Constituição veda sanção por ato criminoso sem lei anterior que o defina, “não há crime sem lei anterior que o defina”, localizado em seu art. 5º, inciso XXXIX.

A Lei Nº 12.737 foi responsável por definir invasão de dispositivo como crime, previsto no art. 154-A e 154–B do Código Penal, e apesar dos criminosos terem respondido pelo furto, hoje já existe diferenciação entre os dois dispositivos legais.

Os artigos 154-A e 154-B são responsáveis por tipificar como crime a conduta de invasão, pouco importando se houve subtração, adulteração ou destruição de dados, bastando a mera invasão ao dispositivo eletrônico (computador, smartphone e outros) para consumar a conduta. Enquanto o furto qualificado será consumado com o ato de obter vantagem ilícita, ou subtração da informação desejada, pouco importando para esse dispositivo se houve invasão ao computador ou smartphone, pois o intuito é punir a transferência de dados ilegalmente.

Insta salienta que a criação da Lei Carolina Dieckmann foi um marco nacional e hoje serve de parâmetro para proteção de milhares de usuários, contribuindo com o avanço na criação de dispositivos legais sobre cibercrimes.

3.2 MARCO CIVIL DA INTERNET OU LEI Nº 12.965/2014

Posteriormente a promulgação da lei nº 12.737/2012 tivemos a promulgação do Marco Civil da Internet, lei nº 12.965/2015 sendo a primeira lei no país que versava especificamente sobre o meio digital, com o pleno intuito de definir princípios, direitos e obrigações para o uso nas redes de internet do Brasil.

Antes do Marco Civil da Internet existir os temas eram tratados em observância à Constituição Federal de 1988, referentes à invasão de privacidade, proteção de dados pessoais e liberdade de expressão, mas com o advento do Marco Civil, tais temas finalmente estavam definidos.

> No artigo 2º, apresenta seus fundamentos (respeito à liberdade de expressão, a pluralidade e a diversidade, a finalidade social da rede, entre outros); no artigo 3º, a Lei elenca um rol exemplificativo de princípios (proteção da privacidade, responsabilização dos agentes de acordo com suas atividades, e mais alguns); no artigo 4º, explica os objetivos da Lei (promoção do direito de acesso à internet a todos, do acesso à informação, ao conhecimento, e outros); e no artigo 5º, que discorre sobre alguns conceitos (por exemplo, explica que internet é o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes) (BRASIL, 2014).

Vale destacar que uma das maiores importâncias do Marco Civil foi a o reconhecimento do direito de acesso à internet para todos, previsto no Art. 4º da referida lei. Apesar de parecer um mero detalhe, esse direito reconhecido gerou grandes impactos em políticas públicas que foram posteriormente desenvolvidas.

Assim, "O Marco Civil da Internet é uma resposta do Poder Legislativo Brasileiro aos conflitos inerentes à sociabilidade humana, surgidos com a disseminação da sociedade da informação", mencionaram Barreto Júnior e César (2017, p. 84).

No art. 4º do Marco Civil, restou definido o uso da internet no Brasil como sendo direito de acesso a todos, tratando-se de uma determinação extremamente importante quando restou definido outro aspecto basilar dessa lei, a neutralidade da rede, que foi consagrada em seu art. 9º, da seguinte forma:

> "Art. 9º - O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação".

O princípio versa sobre o dever do provedor do sinal de internet tratar de maneira igualitária todos os seus contratantes. Sendo vedado o privilégio de determinados dados ou empresas.

A neutralidade de rede possui finalidade de impedir práticas abusivas e discriminatórias por parte dos provedores. Pois fundamenta-se no princípio isonômico supramencionado. Por exemplo, imagine um cenário em que um provedor de streaming forneça dois pacotes para o consumidor com preços diferentes, mas de maneira deliberada, prejudique a entrega de conexão para os assinantes do plano mais barato, afim de deixar os vídeos mais lentos e travando, com objetivo de induzir uma migração para o pacote mais caro.

Esse princípio demonstra extrema importância para garantir a livre escolha do acesso à internet, sem que haja manipulações comerciais.

Na definição do professor Pedro Henrique Soares Ramos:

> "A neutralidade da rede é um princípio de arquitetura de rede que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de maneira isonômica, não os discriminando em razão do seu conteúdo ou origem".

O Marco Civil da Internet é tido como um grande exemplo para todos, principalmente ao analisarmos o procedimento adotado para a sua redação, o projeto não inovou apenas sobre o tema abordado, mas no processo da própria criação também.

Em outubro de 2009 foi realizada a primeira consulta pública de elaboração do Marco Civil, que consistia na participação ativa de vários setores para a criação do projeto. No ano de 2011 foi proposta a primeira versão do texto, após inúmeras participações na plataforma online de consulta pública, chegando a ter mais de 1.200 comentários sobre o que deveria ser abordado na lei regulamentadora.

Ainda no ano de 2011 o texto do projeto foi apresentado à Câmara dos Deputados e a proposta novamente passou por diversas audiências públicas, ouvindo todos os segmentos da sociedade, sendo eles: sociedade civil, empresariados e representantes governamentais.

Não obstante aos segmentos ouvidos, pela primeira vez na história, um projeto de lei também recebeu contribuições pela internet, mais especificamente pelo aplicativo Twitter, atual "X".

O Marco Civil da Internet demonstrou inovação no tema discutido e na sua forma de procedibilidade, garantindo a participação ampla e popular, indo em consonância com o que a própria lei 12.965/2014 define em seu art. 4º, inciso I:

> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;

3.3 CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste, ou Convenção de Crimes Cibernéticos foi firmada no ano de 2001, mas foi adotada pelo Brasil somente em 16 de dezembro de 2021. A presente convenção visa conceituar alguns comportamentos dentro do meio digital, tais como: o que são crimes cibernéticos, acesso ilegal de dados, interceptação ilícita, violação de dados, interferência de sistema, uso indevido de aparelhagem e outros. Assim, aduz Júlio César Alexandre Júnior:

> "O principal destaque do Tratado é a definição de cibercrime (Capítulo I), tipificando-os como infrações contra sistemas e dados de tecnologias da informação (Capítulo II, Título I), infrações relacionadas com computadores (Capítulo II, Título II), infrações relacionadas com o conteúdo, pornografia infantil (Capítulo II, Título III), infrações relacionadas com a violação e direitos autorais (Capítulo II, Título IV), cujas proposituras estão adentradas em Direito Penal Material. (ISSN 1983-4225 – V.14, 2019, pág. 6)".

A Convenção de Budapeste consiste na criação de uma rede de cooperação digital com efeitos entre os participantes do tratado, os quais se comprometem a prestar assistência mútua no combate aos crimes cibernéticos e com o constante avanço da tecnologia, a adesão desse acordo torna-se imprescindível.

Um dos principais benefícios da Convenção Budapeste consiste na facilitação e celeridade na obtenção de dados pessoais de determinados usuários em investigações transnacionais. Isso por que, na ausência desse tratado, quando um país necessita de informações que estão armazenadas em bancos de dados de outra nação, torna-se necessário o envio de uma carta rogatória. Documento que não garante uma resposta, muito menos efetiva ou rápida.

Ponto em que manifesta o diferencial desse tratado, pois impõe o dever de cooperação entre os Estados signatários da Convenção de Budapeste, assegurando a disponibilização de dados de maneira eficaz e tempestiva. Justamente pela internacionalização da Internet, a tomada de decisões rápidas é extremamente importante, pois se a informação não for combatida rapidamente, poderá alcançar escala mundial em questão de minutos, dificultando sobremaneira seu combatimento e responsabilização.

Importante destacar que embora a Convenção aborde sobre o conceito de cibercrime e na forma como os seus signatários irão realizar sua colaboração, ela não se responsabiliza por aplicar ou quantificar a pena, possibilitando que cada país legisle e aplique sanções de acordo com sua soberania. Não havendo uma internacionalização da pena.

Convenção de Budapeste em seu Art. 2º:

> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador.

4. *CYBERBULLYING*: MODALIDADES E EFEITOS.

O *cyberbullying* trata-se da mais nova modalidade de *bullying* cometida dentro do meio virtual, importante mencionar que essa atividade criminosa é uma das formas mais famosas de cibercrimes.

Com o crescimento exponencial, avanço da tecnologia e democratização do acesso a internet os comportamentos mais conhecidos do *bullying* virtual são aqueles cometidos contra a honra, sendo eles: injúria, difamação e até mesmo a calúnia.

O que mais espanta os pesquisadores é que os praticantes desse tipo de delito são em sua grande maioria adolescentes, jovens que se escondem por baixo do véu do anonimato proporcionado pela internet, “os praticantes de *cyberbullying* em sua maioria são adolescentes, não sendo possível traçar o seu perfil, pois os seus ataques ficam no ambiente virtual uma vez que as vítimas não os denunciam” (SILVA, 2010 apud REIS; GOING, 2024).

Neste contexto, as famílias desenvolvem um papel essencial no combate ao comportamento punível desses jovens. O Estatuto da Criança e do Adolescente em seu art. 4º dispõe que é dever da família, da sociedade e de toda a comunidade zelar e preservar pela saúde, vida e educação desses jovens.

> Há uma relação direta entre as interações no contexto virtual, o *cyberbullying* e o *bullying*. A forma como a família e a escola fazem a mediação contribuem para a resolução do problema ou não, em alguns casos até pioram a agressão entre as crianças e adolescentes. Mas se a escola e os pais tratam o tema punindo as práticas agressivas e promovem orientações seguras, nota-se a redução do *bullying* (MANDIRA, 2017 apud REIS; GOING, 2024).

É nítida a importância da parceria entre familiares e entidades de ensino para coibirem as agressões cometidas entre os adolescentes, tais como o *cyberbullying*, pois havendo inércia das partes, os resultados alcançados podem ser depressão, crise de pânico, fobia social, medo, baixa autoestima, irritabilidade e sentimento de frustação.

> Um adolescente de 13 anos, morador de Guarujá, no litoral de São Paulo, lembrou os momentos de tristeza de quando enfrentava o *cyberbullying* e o *bullying* no ambiente escolar. “Eu postava fotos e me xingavam de gordo, bolo fofo, saco de areia, baleia, entre outras coisas”, desabafou o garoto. Ele os demais alunos da rede municipal de ensino receberam palestras sobre o tema para orientar os problemas causados pela prática e como se proteger. *(Portal G1, Santos, 2022).*

Por trata-se de um crime virtual a vítima fica refém dos agressores independentemente de onde esteja podendo ser na escola, na sua casa, durante as férias. Em contrariedade ao que ocorria antigamente, com a possibilidade da vítima se afastar do seu agressor.

Outro tipo de *cyberbullying* que está cada vez mais popular chama-se “cancelamento”, consistindo na prática de um grupo de pessoas se juntarem para cometerem uma espécie de linchamento virtual sob a vítima.

> É o caso de Larissa Ribeiro*, uma influenciadora digital do noroeste do Rio Grande do Sul. A influencer conta que foi alvo da prática do cancelamento ao postar seus treinos de academia no Instagram. Na época do ocorrido, um de seus vídeos viralizou na rede e foi motivo de diversas mensagens e comentários de cunho pejorativo, de homens e mulheres. Ela explica que depois do episódio desenvolveu uma grande insegurança ao se expor e postar em suas redes sociais. “Depois desse evento, virei outra pessoa. Antes, eu postava bastante, não ligava, era bem tranquila. Agora, sou super insegura de postar qualquer coisa”, explica. Ela notou diversos prejuízos na sua saúde mental e começou a fazer psicoterapia. “Fiquei bem ansiosa, tive crise de ansiedade naqueles dias, foi bem difícil”, relata.

É incontestável que atualmente o *cyberbullying* demonstra um poder danoso muito maior do que aqueles comportamentos que conhecíamos, pois a internet possibilita que a agressão ocorra em massa, independente do lugar e horário.
Sem mencionarmos o fato de que com o avanço da tecnologia, as agressões se tornam cada vez piores, não obstante a esta realidade, tivemos uma recente alteração em nosso Código Penal, ainda no ano deste artigo, em 2025, a Lei nº 15.123 foi sancionada, criando uma circunstância agravante na pena em caso de crimes de violência psicológica contra a mulher praticada com o uso das Inteligências Artificiais (IA).

Esse tipo de crime psicológico pode ocorrer através de manipulação, humilhação, chantagem, constrangimento, ridicularização ou de qualquer outra maneira que cause prejuízos psíquicos à vítima.
Um dos crimes mais conhecidos nesta modalidade, são denominados por *Deepfakes:* consistindo na prática de se valer das novas IA ’s para manipularem imagens e vídeos com a voz ou rosto da vítima, a fim de constrangê-la, sendo um crime comumente associado à criação de falso conteúdo pornográfico, simulando nudez, no intuito de amedrontar e ameaçar a vítima.

4. LEI FEDERAL Nº 14.811/2024 – LEI DO *CYBERBULLYING*

Em 12 de janeiro de 2024 foi sancionada a Lei n 14.811/2024, responsável por instituir medidas de proteção à criança e ao adolescente nos estabelecimentos educacionais e similares, com o intuito de prevenir e combater aos crimes digitais.
A lei foi responsável por modificar vários dispositivos legais, sendo eles: o Código Penal, Estatuto da Criança e do Adolescente (ECA) e a Lei dos Crimes Hediondos, isso porque, a presente norma trata-se de uma resposta à crescente preocupação social quanto aos impactos do *cyberbullying* e da violência digital ante a ausência de dispositivos legais que versassem sobre a temática.

A lei supracitada foi responsável por acrescentar ao Código Penal o art. 146 - A, e 146 – A, parágrafo único, tipificando em nosso ordenamento jurídico, como criminosa, a prática do *bullying*. (BRASIL, 2024). *Vultus*:

> Art. 146 - A - **Intimidar sistematicamente**, individualmente ou em grupo, **mediante violência física ou psicológica**, uma ou mais pessoas, de modo **intencional e repetitivo**, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:
> Pena - multa, se a conduta não constituir crime mais grave.

Ressalta-se que, o *bullying* e o *cyberbullying* consistem em condutas de intimidação, cujo o objetivo principal reside em humilhar, diminuir ou insultar a vítima.

Contudo, para que restem configurados os crimes em questão, a conduta deverá ser sistemática, ou seja, não pode ser executada de modo eventual.
Neste viés, vejamos o que disse a Ana Maria Cavalier Simonato:

> "Pela leitura do novo dispositivo legal, percebe-se que no crime de *bullying* e *cyberbullying* a conduta de intimidação exercitada contra a vítima (que pode ser uma violência física ou psicológica) deve ser sistemática, ou seja, não pode ser uma conduta eventual (apenas um ato), podendo, ainda, ser praticada, individualmente ou em grupo.
> Para a prática do crime de *bullying* e *cyberbullying* também não é necessária uma motivação evidente a prática da conduta delituosa, podendo o ilícito se dar por atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais".

Importante mencionar que a Lei nº 13.185/2015, conhecida como Lei *Antibullying* também disserta sobre as escolas precisarem adotar medidas de conscientização, prevenção e combate ao *bullying*, além de também abordar sobre o conceito de *bullying*. Vejamos:

> "Toda ação repetitiva ou intencional, que ocorre sem motivação evidente, praticada por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as pessoas envolvidas". (BRASIL, 2015)

Conforme exposto ao longo do artigo em baila, o cyberbullying trata-se da modalidade virtual da conduta do bullying, razão pela qual, a Lei Federal também abordou sobre essa forma de execução, determinando de maneira assertiva, uma punição mais grave quando o agente se valida dos dispositivos virtuais para cometer o ato criminoso.
Vejamos o que diz o art. 146, § único da Lei nº 14.811/24:

> **Intimidação sistemática virtual (*cyberbullying*)**
> Parágrafo único. Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos **on-line** ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:
> Pena - reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave".

É nítido que estamos presenciando um momento histórico no ordenamento brasileiro, pois, cada vez mais, o legislador tem se preocupado com a proteção dos bens jurídicos dentro do ambiente virtual. Sendo que, com a promulgação da Lei nº 14.811/24 reconhecendo o *bullying* e o *cyberbullying* como conduta criminosa, por consequência direta, proporciona uma maior segurança aos usuários e vítimas, principalmente, às crianças e adolescentes.

Cumpre destacar que, além da preocupação do ordenamento criar um ambiente mais seguro, a aplicação de medidas pedagógicas e políticas de prevenção evidencia que, além da intenção de punir, o Estado tem buscado maneiras de conscientizar, prevenir e educar sobre os efeitos desses atos criminosos.

Outras modificações significativas da referida normativa federal encontram-se no interior da Lei nº 8.072/90, comumente conhecida por Lei de Crimes Hediondos. Isto pois, as condutas de induzimento, instigação ou auxílio ao suicídio e/ou automutilação tornaram-se inafiançáveis, impossíveis de anistia, graça ou indulto quando cometidas por meio de rede de computadores, art. 122, caput e § 4º da Lei nº 8.072/90. Bem como, no Estatuto da Criança e do Adolescente onde restou positivado

como criminosa a conduta de intermediar, ou facilitar a pornografia infantil, previstos no art. 240, inciso I e II do ECA.

Vale mencionar que a tomada de decisões, bem como, a implementação de políticas públicas que se preocupem com essa temática depende de modo direto da cobrança da sociedade, não devendo ser visto apenas como obrigação das escolas, pais e professores. A sociedade, como um todo, precisa estar vigilante, devendo procurar maneiras de coibir e conscientizar sobre as possíveis problemáticas deste tema.

5. CONSIDERAÇÕES FINAIS

Conclui-se que, um dos maiores obstáculos da humanidade resta superado, a globalização já é uma realidade, independente da sua religião, crença pessoal, distância ou idioma, esse desejo foi almejado e resta definitivamente alcançado.
As interações não possuem mais restrição geográfica e os laços afetivos hoje possuem a possibilidade de permanecerem firmes e sólidos, mesmo diante da distância dos continentes e nações.

Com o advento da tecnologia, houveram mudanças, e assim como com toda mudança essa também veio acompanhada de efeitos positivos e negativos. Com base integralmente no que fora demonstrado no artigo em baila, constata-se que os avanços da tecnologia têm refletido diretamente na nossa forma de estabelecer, manter, comandar, conscientizar e encerrar laços uns com os outros.

Embora a modernização e globalização mundial estejam proporcionando incontáveis benefícios à população moderna, incumbiram a nós, de maneira indireta, o ônus de adotar comportamentos preventivos que visem zelar pela integridade física e psíquica dos usuários, principalmente quanto aos grupos mais vulneráveis.

A proteção digital hoje tem se tornado uma necessidade, tal qual, qualquer outra forma de segurança já conhecida. Antigamente, os alvos mais almejados eram as figuras públicas e personas que demonstravam relevante poder econômico, contudo, atualmente, os crimes digitais atingem preferencialmente pessoas comuns, pois são esses indivíduos que não possuem poder aquisitivo e, intelectual, para buscarem os meios de combate equiparados aos ataques virtuais.

Visto que, são os usuários comuns que guardam arquivos pessoais, senhas bancárias, informações sigilosas em seus respetivos aparelhos eletrônicos, mas não possuem uma proteção de software. Portanto, conclui-se que, o combate aos crimes virtuais não deve se limitar apenas à esfera repressiva, como deve, se estender para as ações preventivas, no intuito de conscientizar a população e apresentar mecanismos de como se proteger virtualmente.

Já dizia Albert Einstein: *“Se tornou aparentemente óbvio que nossa tecnologia excedeu nossa humanidade”.*

Incontestavelmente a tecnologia veio para ficar, contudo, a empatia humana tem sido superada pela falsa sensação de liberdade irrestrita, bem como, pelo suposto anonimato que as redes proporcionam. Razão pela qual, regras são necessárias, pois sem elas, voltaríamos a viver como selvagens.

6. REFERÊNCIAS

ALEXANDRE JÚNIOR, Júlio César. Revista Direito Franca. Disponível em: https://revista.direitofranca.br/index.php/refdf/issue/view/50. Acesso em: 04 maio 2025.

BARRETO JUNIOR, Irineu Francisco; CÉSAR, Daniel. *Marco civil da internet e neutralidade da rede: aspectos jurídicos e tecnológicos*. Revista Eletrônica do Curso de Direito da UFSM, v. 12, n. 1, 2017, p. 65-88. Disponível em: https://periodicos.ufsm.br/revistadireito/article/download/23288/pdf/127381. Acesso em: 04 maio 2025.

BRASIL, *Lei nº 14.811, de 12 de janeiro de 2024 (Lei do Bullying).* Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 01 de junho de 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 maio 2025.

BRASIL. *Decreto-Lei nº 3.914, de 9 de novembro de 1941*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm. Acesso em: 03 maio 2025.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 03 maio 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 maio 2025.

BRASIL. *Lei nº 8.069, de 13 de julho de 1990 (ECA)*. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 maio 2025.

BRASIL. *Ministério da Justiça*. Convenção de Budapeste é promulgada no Brasil. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 05 maio 2025.

BRASIL. *Ministério da Justiça*. Crimes digitais. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais. Acesso em: 03 maio 2025.

CÂMARA DOS DEPUTADOS. Conheça a evolução dos crimes cibernéticos. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos/. Acesso em: 03 maio 2025.

CRUZ, Diego; RODRIGUES, Juliana. *Crimes cibernéticos e a falsa sensação de impunidade*. Revista Científica Eletrônica do Curso de Direito, 13 ed. jan. 2018.

CYBLE. *Top countries facing cybercrime threats*. Disponível em: https://cyble.com/blog/top-countries-facing-cybercrime-threats/. Acesso em: 02 maio 2025.

DAMÁSIO, José Antonio. *Manual de Crimes Informáticos*. São Paulo: Saraiva, 2016.

DEFENSORIA PÚBLICA DO ESTADO DO CEARÁ. *Lei Carolina Dieckmann – 10 anos*. Disponível em: https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/. Acesso em: 03 maio 2025.

DESINFORMANTE. *Marco Civil da Internet*. Disponível em: https://desinformante.com.br/marco-civil-internet/. Acesso em: 04 maio 2025.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. *Direito penal esquematizado – parte geral*. 9. ed. São Paulo: Saraiva Educação, 2020.

G1. *Estudante xingado de "gordo e bolo fofo" compartilha sofrimento após ser vítima de bullying e cyberbullying*. Disponível em: https://g1.globo.com/sp/santos-regiao/noticia/2022/06/11/estudante-xingado-de-gordo-e-bolo-fofo-compartilha-sofrimento-apos-ser-vitima-de-bullying-e-cyberbullying.ghtml. Acesso em: 10 maio 2025.

GENTIL, Camila Queiroga et al. *Crimes virtuais*. Ciências Humanas e Sociais, Aracaju, v. 4, n. 3, p. 55-62, abr. 2019. Disponível em: https://experteditora.com.br/wp-content/uploads/2023/07/Crimes-virtuais.pdf. Acesso em: 02 maio 2025.

JUSBRASIL. *Lei 14.811/24 criminaliza o bullying e o cyberbullying*. Disponível em: https://www.jusbrasil.com.br/artigos/lei-14811-24-criminaliza-o-bullying-e-o-cyberbullying/
2142758107. Acesso em: 03 de junho de 2025,

JUSBRASIL. *Marco Civil da Internet: uma perspectiva sobre os crimes contra a honra em rede e a liberdade de expressão*. Disponível em: https://www.jusbrasil.com.br/artigos/marco-civil-da-internet-uma-perspectiva-sobre-os-crimes-contra-a-honra-em-rede-e-a-liberdade-de-expressao-da-sociedade/1548263642. Acesso em: 03 maio 2025.

KAMIMURA MURATA, Ana Maria Lumi; TORRES, Paula Ritzmann. *Publicações do IBCCRIM*. Disponível em: https://publicacoes.ibccrim.org.br/
index.php/boletim_1993/article/view/575/108. Acesso em: 05 maio 2025.

LÉVY, Pierre. *Cibercultura*. 2. ed. São Paulo: Editora 34, 2000.

NUCCI, Guilherme de S. *Curso de Direito Penal: Parte Geral: Arts. 1º a 120 do Código Penal*. v. 1. 8. ed. Rio de Janeiro: Forense, 2024. E-book. ISBN 9786559649228. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559649228/. Acesso em: 02 nov. 2024.

NUCCI, Guilherme de Souza. *Manual de direito penal*. 16. ed. Rio de Janeiro: Forense, 2020.

ONU BRASIL. *Brasil é o quarto país com mais usuários de internet do mundo, diz relatório da ONU*. Disponível em: https://brasil.un.org/pt-br/77784. Acesso em: 03 maio 2025.

OXFORD UNIVERSITY. *World-first cybercrime index ranks countries by cybercrime threat level*. Disponível em: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level. Acesso em: 02 maio 2025.

QUERO BOLSA. *Biografia de Albert Einstein.* Disponível em: https://querobolsa.com.br/enem/biografias/albert-einstein. Acesso em 11 de maio de 2025.

RAMOS, Pedro Henrique Soares. *Uma questão de escolhas: o debate sobre a regulação da neutralidade da rede no Marco Civil da Internet*. CONPEDI, 22., 2013. Anais.

REPOSITÓRIO MCTI. *Evolução da Internet no Brasil e no Mundo*. Disponível em: https://repositorio.mcti.gov.br/bitstream/mctic/5459/1/2000_evolucao_da_internet_no_brasil_e_no_mundo.pdf. Acesso em: 03 maio 2025.

REPOSITÓRIO MCTI. Página inicial. Disponível em: https://repositorio.
mcti.gov.br/handle/mctic/5459. Acesso em: 03 maio 2025.

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

SENADO FEDERAL. *Dez anos de vigência da Lei Carolina Dieckmann*. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em: 03 maio 2025.

SENADO FEDERAL. *Golpes digitais atingem 24% da população brasileira, revela Data Senado.* Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 03 maio 2025

TRIBUNAL DE JUSTIÇA DO CNJ. *Crimes digitais: o que são, como denunciar e quais leis tipificam como crime*. Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/. Acesso em: 03 maio 2025.