FACULDADE CRISTO REI - FACCREI

O *CYBERBULLING* E SUAS TRANSFORMAÇÕES NA SOCIEDADE ATUAL NA PERSPECTIVA DA LGPD

https://doi.org/10.47820/recima21.v4i1.4565

PUBLICADO: 11/2023

CORNÉLIO PROCÓPIO/2023

SAMUEL DE OLIVEIRA SOTH
CYRO JOSÉ JACOMETTI SILVA

O *CYBERBULLING* E SUAS TRANSFORMAÇÕES NA SOCIEDADE ATUAL NA PERSPECTIVA DA LGPD

CYBERBULLYING AND ITS TRANSFORMATIONS IN TODAY'S SOCIETY FROM THE PERSPECTIVE OF THE LGPD

EL CIBERACOSO Y SUS TRANSFORMACIONES EN LA SOCIEDAD ACTUAL DESDE LA PERSPECTIVA DE LA LGPD

Trabalho de conclusão de curso apresentado ao Curso de Direito da Faculdade Cristo Rei de Cornélio Procópio – PR como requisito parcial para obtenção do grau e do diploma de bacharel em Direito.

Professor(a)-Orientador(a): Dr. Cyro José Jacometti Silva

CORNÉLIO PROCÓPIO/2023

TERMO DE APROVAÇÃO

SAMUEL DE OLIVEIRA SOTH
CYRO JOSÉ JACOMETTI SILVA

O *CYBERBULLING* E SUAS TRANSFORMAÇÕES NA SOCIEDADE ATUAL NA PERSPECTIVA DA LGPD

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharel em Direito da Faculdade Cristo Rei de Cornélio Procópio – PR, como requisito à obtenção do grau e do diploma de Bacharel em Direito.

CORNÉLIO PROCÓPIO/2023

RESUMO
O presente artigo científico, por meio de pesquisa doutrinária, faz uma análise dos crimes cibernéticos com ênfase no *cyberbullying* e sua correlação com o crime contra honra, pelo Direito Penal Brasileiro. Pontua sobre a proteção legal das atividades nas redes cibernéticas e as questões legais no Brasil, a legislação penal e a responsabilidade dos provedores. Com o advento da pandemia Covid-19, também houve uma expansão da utilização das plataformas educacionais, logo, se intensificou o uso da rede, algo que também será analisado. Ao final da pesquisa, percebe-se a importância da prevenção e proteção no quesito das redes e todos os recursos midiáticos, em relação aos crimes contra honra, uma vez que são os mais praticados e de difícil punibilidade pelo seu *modus operandi.*

PALAVRAS-CHAVE: Crimes Cibernéticos. Honra. Direito penal. Internet.

ABSTRACT
This scientific article, through doctrinal research, analyzes cybercrimes with an emphasis on cyberbullying and its correlation with crimes against honor under Brazilian Criminal Law. It points out the legal protection of activities in cyber networks and legal issues in Brazil, criminal legislation and the responsibility of providers. With the advent of the Covid19 pandemic there was also an expansion in the use of educational platforms, and the use of the network soon intensified, something that will also be analyzed. At the end of the research, we can see the importance of prevention and protection in terms of networks and all media resources, in relation to crimes against honor, since they are the most practiced and difficult to punish due to their modus operandi.

KEYWORDS: *Cyber Crimes. Honor. Criminal law. Internet.*

RESUMEN
Este artículo científico, a través de la investigación doctrinal, realiza un análisis de los delitos cibernéticos con énfasis en el ciberacoso y su correlación con los delitos contra el honor, por el Derecho Penal Brasileño. Señala la protección legal de las actividades en redes cibernéticas y las cuestiones legales en Brasil, la legislación penal y la responsabilidad de los proveedores. Con la llegada de la pandemia de Covid-19, también hubo una expansión en el uso de plataformas educativas, por lo que se intensificó el uso de la red, algo que también se analizará. Al final de la investigación, se percibe la importancia de la prevención y protección en términos de redes y todos los recursos mediáticos en relación a los delitos contra el honor, ya que son los más practicados y difíciles de sancionar por su modus operandi.

PALABRAS CLAVE: *Delitos cibernéticos. Honor. Derecho penal. Internet.*

SUMÁRIO

INTRODUÇÃO

O advento da era digital trouxe consigo uma série de mudanças profundas na nossa sociedade que revolucionaram a forma como comunicamos e partilhamos informação. O surgimento da Internet e das redes sociais promoveu um mundo conectado onde pessoas de diferentes partes do mundo podem comunicar em tempo real, partilhar experiências e expressar as suas opiniões. No entanto, esta revolução tecnológica também trouxe consigo desafios significativos, e um deles que ganhou espaço na última década é o *cyberbullying.*

O *cyberbullying* é um fenômeno que evoluiu como uma manifestação perturbadora da sociedade digital. Refere-se ao uso da Internet e das tecnologias de comunicação para assediar, difamar, ameaçar ou insultar indivíduos. Essa forma de comportamento criminoso ocorre por diversos meios, incluindo mídias sociais, mensagens instantâneas, *e-mail,* fóruns *on-line* e outros canais de comunicação digital. Na sua essência, o *cyberbullying* visa prejudicar a reputação, a integridade emocional e a dignidade das vítimas, muitas vezes com consequências graves.

Ao longo dos anos, o *cyberbullying* evoluiu e assumiu novas formas e está a tornar-se um problema crescente em todo o mundo. Em particular, este artigo centrar-se-á na análise do *cyberbullying*, centrando-se nos crimes contra a honra, mais especificamente no crime de injúria, apontando como esta manifestação digital de comportamentos nocivos afeta a vida das vítimas e da sociedade como um todo.

No contexto do *cyberbullying*, o insulto é uma expressão de desrespeito e calúnia que ocorre quando indivíduos utilizam plataformas digitais para proferir palavras, gestos, escritos ou quaisquer outros meios simbólicos que ofendam a dignidade ou a decência de alguém. A análise do *bullying* é crucial porque revela como o *cyberbullying* pode assumir muitas formas e quão devastador pode ser o seu impacto sobre aqueles que são visados.

Este artigo também examinará os impactos mais amplos do *cyberbullying* e do *bullying* na sociedade, para além das vítimas individuais. A propagação de mensagens ofensivas pode minar a confiança nas interações digitais, tornando a Internet um ambiente menos seguro para todos. Além disso, esse comportamento pode gerar conflitos, ações judiciais e até violência no mundo real.

Para resolver o problema do *cyberbullying* e dos danos no ciberespaço, é essencial que os governos, as empresas tecnológicas, os educadores e a sociedade em geral trabalhem em conjunto em estratégias de prevenção e combate. Devem ser promulgadas e aplicadas leis adequadas para responsabilizar aqueles que cometem estes crimes, enquanto as empresas tecnológicas devem implementar políticas rigorosas e mecanismos de denúncia eficazes. Além disso, a sensibilização do público para os danos causados pelo *cyberbullying* e pelas invectivas é essencial para prevenir este comportamento prejudicial.

Em suma, o *cyberbullying* e os crimes de honra, como a difamação, colocam desafios significativos na nossa sociedade digital. Este artigo explorará detalhadamente como estes fenómenos afetam as vítimas e a sociedade como um todo, e como é necessário um esforço coordenado para criar um ambiente online mais seguro e respeitoso para todos.

1.CRIMES CIBERNÉTICOS

Os crimes cibernéticos são uma categoria de crimes em rápida expansão que ocorrem no espaço virtual da Internet e envolvem o uso de computadores, redes e dispositivos conectados para cometer atividades ilegais.

De acordo com a Pesquisa Global sobre Fraudes e Crimes Econômicos 2022 da PwC, disponível em seu site, “cerca de 46% das organizações estrangeiras sofreram invasões *hackers* nos últimos 24 meses. No Brasil, este percentual é de 62%”.

Com a crescente dependência da sociedade da tecnologia e da Internet, esses crimes se tornaram um problema global que afeta países ao redor do mundo, incluindo, o Brasil.

> No ranking da América Latina e Caribe, o Brasil é o segundo com mais registros de ataques cibernéticos, com 103,1 bilhões de tentativas, um aumento de 16% em relação ao que foi registrado em 2021. No México, país que lidera o ranking, foram 187 bilhões de tentativas em 2022 (Moneylab, 2023)

Sendo um país com uma crescente população conectada à Internet, o Brasil não está imune aos efeitos do crime cibernético. Embora a era digital tenha trazido muitos benefícios, como a conveniência das transações *online*, a comunicação instantânea e o acesso à informação, também trouxe consigo riscos significativos, uma vez que os criminosos se adaptaram ao ambiente virtual para realizar atividades criminosas.

> Segundo o Anuário Brasileiro de Segurança Pública, os registros de vítimas de golpes de crimes digitais ultrapassaram 200 mil em 2022, representando um assustador aumento de 65,2% em relação ao ano anterior.
> Os números revelados pelo Anuário são baseados em dados oficiais de secretarias estaduais e órgãos de segurança, provenientes de 21 das 27 unidades federativas do país. Os estados de Bahia, Ceará, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e São Paulo, embora não estejam inclusos no levantamento, também enfrentam desafios significativos em relação à segurança digital. (International IT, 2023)

Os impactos do crime cibernético no Brasil são variados e multifacetados. A disseminação da Internet e o maior acesso à tecnologia levaram a uma série de problemas, incluindo:

A. Perdas financeiras: Um dos impactos imediatos do crime cibernético são as perdas financeiras. Ataques como fraude bancária, roubo de dados financeiros e esquemas de *phishing* podem levar a perdas substanciais para indivíduos e empresas. Isto não só afeta diretamente as vítimas, mas também tem consequências econômicas mais amplas.

A Kaspersky, Dmitry Bestuzhev (2021), uma das maiores empresas cibernéticas do mundo, divulgou um prognóstico de segurança na sua página de Comunicados para a Imprensa, divulgando 10 pontos sobre ataques cibernéticos, entre eles citou o “*boom*” do *infoteler*, o *ransomware* e o QR Codes, não esquecendo que estão chegando as criptomoedas e uma nova forma de trabalhar, pós pandemia.

> O infostealer é um vírus que rouba informações do seu computador com objetivo de **criar recompensa financeira** para cibercriminosos. Os ataques coletam dados bancários, logins, fotos e documentos.
> Com esses dados em mãos, os hackers podem chantageá-lo ou vender suas informações para outros golpistas.

> O ransomware é um malware capaz de bloquear o computador e criptografar arquivos. Com isso, o hacker assume o controle do aparelho e exige **recompensa em dinheiro** para ativar os serviços da máquina novamente.
> Caso a vítima prefira não ceder, os criminosos podem vazar os dados salvos no dispositivo.
> Com o uso dos QR Codes em alta, a prática de golpes por este formato também cresceu. Os criminosos substituem os códigos verdadeiros e modificam a URL.
> Sendo assim, **a vítima é direcionada para uma página falsa.** Além disso, os hackers podem utilizar os QR Codes para instalar aplicativos com vírus e infectar o seu computador ou celular (Leandro Miranda, 2023).

E ainda:

> As estatísticas de crimes cibernéticos apresentados pelo FBI mostram que um mínimo de 422 milhões de indivíduos foram afetados por crimes cibernéticos, com 800.944 reclamações registradas em 2022. FBI estima ainda que cerca de 33 bilhões de contas poderão ser violadas em 2023, com o custo dessas violações está projetado para atingir 10,5 trilhões de Dólares Norte Americanos até 2025, sendo que 80% dos crimes cibernéticos relatados são geralmente atribuídos a ataques de *phishing*. (Maputo, 2023)

B. Invasão de privacidade: As violações de sistemas e a exposição de dados pessoais são grandes preocupações num mundo cada vez mais digital. A fuga de dados pessoais pode levar a vários tipos de abuso, incluindo extorsão e roubo de identidade.

> As deepfakes fazem parte dos crimes de phishing, uma técnica que usa fraude, truque ou engano para **manipular as pessoas e obter informações confidenciais.**
> A técnica foi disseminada principalmente durante o período eleitoral de 2022. Por meio da inteligência virtual é possível produzir vídeos realistas em que indivíduos aparecem fazendo ou falando coisas que nunca fizeram ou disseram.
> Com isso, os golpistas podem manipular vídeos e disparar conteúdos distorcidos. Especialistas alertam para a importância de saber identificar essa prática a fim de evitar cair em crimes cibernéticos (Miranda, 2023)

C. Crimes contra a honra: Os crimes cibernéticos também se enquadram na área da difamação e do insulto. A difusão de informações difamatórias ou ofensivas na Internet pode prejudicar a reputação e a dignidade das vítimas, originando processos judiciais e conflitos interpessoais.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (Brasil, 1988).

A honra é inviolável, construída durante toda a vida, protegida pela Constituição Federal e tem consideração íntima própria.

> Já a doutrina costuma conceituar honra sobre vários aspectos. A princípio, distingue-se a objetiva da subjetiva.
> a) Honra objetiva: diz respeito à opinião de terceiros aos atributos físicos, intelectuais, morais de alguém. O sujeito acredita que goza no seu meio social, ou seja, é aquela que se refere a conceituação do indivíduo perante a sociedade. (apud Capez, 2014).
> b) Honra subjetiva: refere-se à opinião do sujeito a respeito de se mesmo, ou seja, de seus atributos físicos, intelectuais e morais, em suma, diz com sua autoestima. Não importa a opinião de terceiros. (apud Capez, 2014; Martins, 2020)

A calúnia é um crime contra a honra, considerado o mais grave, onde ocorre a descrição de um acontecimento, imputado a uma vítima, que além de falso, é definido como crime. Localiza-se no artigo 138 do Código Penal:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa. § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga. § 2º - É punível a calúnia contra os mortos. Exceção da verdade § 3º - Admite-se a prova da verdade, salvo: I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível; II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141; III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível (Brasil, 1940).

A difamação, de menor gravidade do que a calúnia, porém consta no Código Penal, são os fatos considerados ofensivos a reputação da vítima, artigo 139 do Código Penal:

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa. Exceção da verdade Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções. (Brasil, 1940).

E por fim a injúria, de acordo com Martins (2020), *é considerada a menos grave de todas as infrações que visam proteger a honra, entretanto, não existe imputação de fato, mas, sim, atributos morais, intelectuais e físicos à pessoa do agente.*

> Art. 140 - Injuriar alguém, ofendendo- lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa. § 1º - O juiz pode deixar de aplicar a pena: I - quando o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria. § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência. § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: Pena - reclusão de um a três anos e multa (Brasil, 1940).

Analisando o artigo acima citado do Código Penal, podemos observar que podem ocorrer 3 tipos de injúria, sendo elas, a injúria simples citada no início do artigo, a injuria real, consignada no inciso 2º e a injúria preconceituosa tipificada no inciso 3º deste mesmo artigo. Todas as formas de injurias atacam a honra, porém a real e a preconceituosa, ferem a dignidade e utilizam elementos diretamente ligados a condição da pessoa, se tornando mais sérias.

D. Crimes cibernéticos complexos: Além dos crimes mais comuns, o Brasil enfrenta desafios relacionados a crimes cibernéticos complexos, como ataques cibernéticos contra infraestrutura crítica, espionagem cibernética e atividades de grupos criminosos organizados no ambiente digital.

O crime cibernético é uma ameaça crescente no Brasil com consequências que afetam indivíduos, empresas e a segurança nacional. Embora esforços significativos tenham sido feitos para combater esses crimes, a constante evolução da tecnologia e das táticas criminosas exige uma abordagem abrangente e adaptativa para garantir a segurança no ambiente digital do Brasil.

> Sob essa óptica, os crimes cibernéticos cobrem uma ampla gama de atividades, todas geralmente realizadas através de uma conexão de rede. Entre as técnicas mais

> comumente usadas pelos criminosos para a prática dos crimes informáticos propriamente ditos, destacam-se o uso de softwares maliciosos e técnicas de engenharia social para obter informações confidenciais. Além disso, algumas ações ilegais frequentes incluem o acesso não autorizado, a sabotagem, a interceptação de comunicações, fraudes eletrônicas, a disseminação de vírus e malware, difamação e calúnia, e a pornografia infantil.[...] Nessa mesma linha, as fraudes eletrônicas, no qual buscam obter ganhos financeiros ilegítimos através de técnicas de engenharia social, como phishing e spoofing, por meio de envio de mensagens falsas que se passam por comunicações autênticas de empresas conhecidas, como bancos ou lojas online (Vieira, 2023).

Assim como os crimes cibernéticos utilizam de táticas cada vez mais sutis para obterem informações e acesso a dados de maneira ilegal, porém de forma confidencial, tem aqueles que se utilizam de falsas mensagens, se passando por empresas autênticas, conhecidas, acima de quaisquer suspeitas, porém depois que o acesso é realizado, ou as transações são concluídas, os dados são roubados, o vírus instalado, o pagamento realizado a página desaparece, enfim, o inúmeras situações onde pode vir a perceber o erro, porém não há como rastrear ou recuperar o prejuízo.

> Por fim, a pornografia infantil, um crime de extrema gravidade, envolve a produção, distribuição, veiculação ou armazenamento de material pornográfico contendo menores de idade, sendo este delito previsto no Estatuto da Criança e do Adolescente e sujeito a penalidades severas. Sob essa informação, os dados da SaferNet Brasil mostram que, em 2018, o Brasil registrou um total de 133.732 queixas de delitos virtuais, 110% a mais em relação ao ano anterior. O principal crime denunciado foi a pornografia infantil. Segundo a organização, nos últimos 14 anos, mais de 4,1 milhões de denúncias anônimas foram contabilizadas contra 790 mil endereços eletrônicos por divulgarem conteúdo inapropriado na internet. Além desses dados, o jornal New York Times informou, em 2019, que empresas de tecnologia registraram mais de 45 milhões de fotos e vídeos online de crianças vítimas de abuso sexual. O número é mais que o dobro do registrado no ano anterior (Vieira, 2023).

Os crimes contra a honra, contra o pudor, a violência sexual, pedofilia, em se tratando do envolvimento com menores de idade, apesar da penalidade severa não tem intimidado os perversos que se deleitam com esse tipo de criminalidade e o número de vítimas, conforme a citação, tem crescido anualmente.

No entanto, a sensibilização do público para a segurança digital ainda é uma área que requer atenção. A Cyber educação é essencial para que os cidadãos protejam as suas informações pessoais e reconheçam os perigos da Internet.

Educar para acessar, educar para postar, educar para navegar e cobrar mais agilidade das autoridades competentes em agilizar os processos de investigação e punição dos autores, pois não se trata somente de pessoas que praticam, mais também daquelas que pagam para assistir as imagens divulgadas.

1.1 Proteção Legal das atividades nas redes cibernéticas e as questões legais no Brasil

Com o advento da criação da internet, que a princípio foi para uso militar e depois passou a ser utilizada nas universidades americanas e institutos de pesquisas, somente a partir da década de 1990 se deu início à exploração mercadológica e depois chegou ao que conhecemos hoje, ao sistema de páginas de rede.

A internet se tornou de uso essencial na sociedade em todas as áreas: saúde, educação, governo, economia, transporte, todas as relações sociais, comerciais, culturais, pessoal e segurança logo os criminosos viram um local potencial para agir e violar direitos e o *cibercrime* tornou-se um fenômeno mundial.

Foi necessário criar normas de segurança, uma legislação de política comum, onde se originou a Convenção de Budapeste, criada no início de 2000, pelo Conselho Europeu na Hungria, por 05 países inicialmente, promulgada apenas em 2004, agora já se agregando 20 países.

Possuindo 48 artigos, a Convenção de Budapeste (2001) tem como destaque:

> 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 (Vieira, 2023)

E ainda ressalta:

> Os crimes previstos pela Convenção de Budapeste são acometidos de forma dolosa para que seja imputada a responsabilidade criminal, sendo que, em casos específicos, é exigido uma intenção e soma específica, como estabelecido no Art. 8º: Fraude relacionada com computadores.
> O Capítulo ao qual refere-se o Direito Penal Substantivo – Arts 2º ao 13 – define 9(nove) crimes agrupados em 4(quatro) categorias distintas, seguidos pela responsabilidade acessória e respectivas sanções (Vieira, 2023).

São considerados crimes cibernéticos, de acordo com esse Tratado, para que sejam classificadas as infrações penais:

> Acesso ilícito (Art. 2º): da prática intencional de acesso ilícito a um sistema informático ou parte dele; b) Intercepção ilícita (Art. 3º): da prática intencional a interceptação não autorizada; c) Dano provocado nos dados (Art. 4º): da prática intencional à danificação, a exclusão de dados, a deterioração, a alteração ou supressão não autorizada de dados; d) Sabotagem informática. (Art. 5º): da prática intencional, a perturbação grave e não autorização quando do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados; e) Utilização indevida do dispositivo (Art. 6º): da prática intencional e ilícita, a saber: produção, venda, aquisição para efeitos de utilização, importação, distribuição e suas outras formas e estar em possa de material criminoso; f) Falsificação informática.

Muito importante ressaltar que os acessos, práticas e intercepções ilícitas, intencionais, não autorizadas, uso abusivo de dispositivos, interferência de dados, interferência de sistemas, causam danos e estes precisam ser classificados como infrações penais, algo que até o momento não estava explicitamente dessa forma.

Continuando, a Convenção de Budapeste ainda classificou:

> (Art. 7º): da prática intencional e ilícita, a introdução, a alteração, a exclusão ou a supressão de dados dos quais não resultem em autenticidade; g) Burla informática (Art. 8º): da prática intencional e ilícita, prejuízo patrimonial causado a outrem por meio de qualquer introdução, alteração, exclusão ou supressão de dados, bem como, qualquer interferência nas funções de um sistema informático com a intenção de benefício econômico; h) Infrações relacionadas com pornografia infantil (Art. 9º): quando da prática de forma intencional e ilegítima por meio de um sistema informático: produção, oferta, disponibilização, difusão, posse e deverá abranger a todos os menores de 18(dezoito) anos de idade; e i) Infrações relacionadas a violação de direitos autorais e conexos (Art. 10º).

As intenções fraudulentas, produzindo dados não autênticos, intenção ilegítima ou similar, da alteração, da eliminação ou da supressão de dados informáticos e as infrações relacionadas à pornografia infantil, violações do direito de autor e conexos, se seguiram também, pois a necessidade de regulamentação específica era necessária para o meio digital.

O ambiente cibernético brasileiro é governado por uma série de leis e regulamentos que visam estabelecer um quadro jurídico sólido para proteger os direitos dos usuários da internet e regular as atividades online, porém não era ainda, em 2021, um Estado membro do Tratado de Budapeste, mais as leis que se seguiram estão alinhadas com este. Até 2012 não havia legislação específica para os crimes cibernéticos.

Vieira (2023) observa que:

> O primeiro foi o Projeto de Lei nº 84/99, proposto pelo deputado Luiz Piauhylino, também conhecido como Lei dos Crimes Digitais, visando tipificar como crime ações como invasão e modificação de conteúdo de sites, roubo de senhas, criação e disseminação de vírus, dentre outros. Em seguida, o senador Luiz Estevão apresentou o Projeto de Lei do Senado n.º 151/00, propondo a obrigatoriedade da guarda dos registros de conexão dos usuários da internet, uma medida que visava aumentar o controle sobre as atividades online e facilitar a investigação de crimes cibernéticos. A Lei dos Crimes Digitais foi aprovada na Câmara em 2003 e, em 2008, passou por modificações no Senado, retornando à casa de origem para avaliação das alterações propostas.

Com os prejuízos e transtornos causados pelos crimes digitais é que surge a necessidade de uma legislação específica para esta área, pois se trata de um ambiente diferente onde somente com o controle sobre as atividades existe a possibilidade de uma investigação, porém para isso se faz necessário uma legislação e suporte suficiente para que possa ser realizado.

1.2 Legislação penal e crimes cibernéticos

A Internet se tornou o meio de maior comunicação, trabalho, estudo e interação social, entre outras atividades elencadas. Também muitas demandas se agregaram a ela e as redes sociais são os ambientes mais procurados tanto por internautas que buscam se socializar, empresas que querem realizar pesquisas, e refúgio de criminosos para elaborarem suas práticas.

Crimes contra a honra, difamação, racismo, conteúdo ofensivo, crimes contra a imagem, contra a intimidade, tem seus efeitos potencializados e, de acordo com a intenção daquele que quer praticar o ato criminoso, a velocidade da transmissão atinge milhares de visualizações, causando consequências inimagináveis.

Crianças e adolescentes, grandes usuários de redes sociais, internautas ativos, em seus jogos online, se comunicam com diversas pessoas, e muitas vezes nem mesmo sabem com quem realmente estão falando.

O Estatuto da Criança e do Adolescente sofreu uma alteração em 2008, justamente para tentar controlar essa situação, foi a publicação da Lei Nº 11.829, de 25 de novembro de 2008, que altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.

> Art. 1º Os arts. 240 e 241 da Lei nº 8.069, de 13 de julho de 1990, passam a vigorar com a seguinte redação:
> "Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: [...]
> "Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:[...]
> "Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: [...]

Como bem foi pontuado nos artigos, "qualquer meio" de produção ou reprodução, pois quando se pensa em equipamento midiático, há diversas formas de realizar tal registro. Antigamente eram as fotos reveladas, depois as filmadoras, vídeo cassete, DVD, *pendrive,* então as redes sociais, MSN, Orkut, Facebook, Messenger, Skype, Instagram, e a Internet invisível: "Deep Web" e "Dark Web".

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:[...]
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:[...]
> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:[...]
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais."[...] (Brasil, 2018)

Todos os meios de captação de informação, produção ou disseminação desse tipo de informação, assim como aliciar ou assediar crianças através deles para a prática de ato libidinoso foi classificado como crime.

Percebe-se então que a internet se tornou o local preferido para os atos de perversão devido às facilidades que contribuem para a disseminação de conteúdos de cunho pornográfico, assim como interagir com as pessoas e manipular, sendo possível obter o conteúdo requerido da própria pessoa, dentro de sua casa, com um clique apenas, através do compartilhamento e arquivos, nas redes sociais ou aplicativos de mensagens, entre outros.

Ainda ocorreram situações conflitantes até a publicação em 2012, a Lei nº 12.737, chamada de "Lei Carolina Dieckmann", que diz respeito aos crimes praticados nas redes cibernéticas, a legislação penal brasileira, onde aborda crimes relacionados à invasão de dispositivos e vazamento não autorizado de conteúdo privado, o que é relevante para casos de invasão de privacidade e disseminação não autorizada de fotos e vídeos íntimos.

Houve alteração nos artigos 154-A e 154-B do Código Penal Brasileiro, através da Lei 12.737, como segue:

> Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> Invasão de dispositivo informático
> 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:
> [...]
> 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.

Além disso, os crimes de injúria, difamação e calúnia – crimes contra a honra, que podem ocorrer nas redes cibernéticas, são regidos pelo Código Penal Brasileiro. A jurisprudência brasileira tem se adaptado para abordar casos de crimes digitais, como a difamação *online*, aplicando as leis de maneira apropriada para o ambiente virtual.

> "'Crimes contra a honra praticados pela internet são formais, consumando-se no momento da disponibilização do conteúdo ofensivo no espaço virtual, por força da imediata potencialidade de visualização por terceiros' (CC 173.458/SC, Rel. Ministro João Otávio de Noronha, Terceira Seção, DJe 27/11/2020)." *apud* Martins, 2023

Com o avanço em potencial dos crimes cibernéticos, a Lei Carolina Dieckmann foi um grande avanço na modernização da legislação brasileira, porém ainda com grandes desafios pois os criminosos se atualizam rapidamente, mudando estratégias e evolui do junto com a tecnologia.

1.3 Responsabilidade dos provedores

Em 2014 foi promulgada a Lei nº 12.965, também conhecida como o Marco Civil da Internet, é uma legislação de grande importância no Brasil. Ela foi promulgada com o propósito de estabelecer princípios, garantias, direitos e deveres para o uso da internet no país. O Marco Civil da Internet é um conjunto de normas mais sólidas para as atividades nas redes cibernéticas brasileiras, como uma Constituição da Internet.

Uma das características mais marcantes do Marco Civil da Internet é a proteção da neutralidade da rede. Esse princípio assegura que todos os dados transmitidos na internet sejam tratados de forma igualitária pelos provedores de internet, sem discriminação por conteúdo, origem, destino ou serviço. Isso garante que os usuários tenham acesso livre e imparcial à informação e à inovação online.

Sobre a proteção dos registros, dados pessoais e às comunicações privadas, a Lei diz:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. (Brasil, 2014)

Fazer um trabalho de conscientização sobre a forma segura de navegação e utilização das redes é muito importante, porém os provedores também necessitam ser regulamentados e disporem de normas para registro e guarda dos dados. A responsabilidade sobre a preservação da honra está sob a guarda do provedor e este precisa adotar medidas específicas de segurança e sigilo.

> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. (Brasil, 2014)

Além da neutralidade da rede, o Marco Civil da Internet aborda a responsabilidade dos provedores de serviços online:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput,** observado o disposto nos §§ 3º e 4º do art. 13.

> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Ele estabelece que os provedores não são responsáveis pelo conteúdo gerado por terceiros, a menos que descumpram ordens judiciais específicas para a remoção de conteúdo ilegal. Isso visa a equilibrar a proteção da liberdade de expressão com a necessidade de combater conteúdo ilegal, como discurso de ódio, pornografia infantil e a disseminação de informações difamatórias e injuriosas nas redes cibernéticas.

Um ataque cibernético a um servidor de internet, os chamados de hackers, termo usado para definir uma pessoa com alto conhecimento para cometer um crime cibernético com profundo conhecimento de informática, estes roubam dados sigilosos ou a identidade do titular dos dados para domínio daquele servidor, porém muitas podem ser suas motivações, desde financeiras como demonstração de poder ou ideológica, entre outras.

1.4 Lei Geral de Proteção de Dados (LGPD - LEI Nº 13.709/2018)

Outra legislação crucial para as atividades nas redes cibernéticas no Brasil é a Lei Geral de Proteção de Dados (LGPD). Promulgada em 2018, a LGPD estabelece diretrizes rigorosas para a coleta, processamento e armazenamento de dados pessoais, visando proteger a privacidade dos indivíduos. Ela se aplica a todas as entidades que lidam com dados pessoais, incluindo empresas que operam online. A LGPD é particularmente relevante para a proteção de informações pessoais nas redes sociais, serviços online e transações comerciais realizadas na internet.

Segundo Vieira, 2023:

> Assim, mostra-se como uma legislação inovadora no Brasil, estabelecendo princípios e conceitos direcionadores para um uso seguro de dados. Esta lei tem como objetivo equilibrar a proteção eficaz dos direitos dos titulares desses dados e, simultaneamente, permitir o processamento de dados pessoais e sensíveis para propósitos específicos, incluindo a pesquisa científica. A LGPD introduziu pela primeira vez no sistema jurídico brasileiro um conjunto de normas e princípios voltados para a regulação do tratamento de dados pessoais em todas as atividades diárias dos cidadãos, abrangendo vários setores.

Todas as atividades realizadas na internet estão gerando e compartilhando uma imensa quantidade de dados, o tempo todo, e este precisam ser preservados, privativos, e estarem seguros.

> O artigo 3º da LGPD estabelece que a lei será aplicada independentemente do meio, do país da sede ou de onde os dados estão localizados. No entanto, existem exceções à aplicação desta lei, como no caso do tratamento de dados por indivíduos para fins exclusivamente privados, uso para finalidades jornalísticas, artísticas ou acadêmicas, ou para segurança pública, defesa nacional e investigação criminal, entre outros. A LGPD também define termos-chave como "dados pessoais" e "dados sensíveis". Estes últimos são particularmente importantes para a privacidade, pois uma violação pode resultar em consequências graves. Uma maior proteção é concedida a esses dados, que estão intrinsecamente ligados à liberdade e à dignidade do indivíduo (Vieira, 2023)

Atualmente o Brasil possui uma estrutura legal robusta para proteger os direitos e regulamentar as atividades nas redes cibernéticas, abordando questões como neutralidade da rede, privacidade de dados e punição de crimes digitais.

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia cita:

> (27) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, das consequências e das garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção especial deverá aplicar-se, nomeadamente, à criação de perfis de personalidade; à recolha de dados pessoais relativos às crianças aquando da utilização de serviços disponibilizados diretamente a um menor nos sítios Web das instituições e dos órgãos da União, tais como os serviços de comunicação interpessoal ou de venda de bilhetes em linha; e ao tratamento de dados pessoais com base no consentimento (Estrasburgo, 2018).

Essas leis desempenham um papel fundamental na garantia de um ambiente online seguro e ético, bem como na proteção dos direitos dos cidadãos brasileiros no mundo digital em constante evolução, em consonância com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, porém ainda é se faz necessário uma implementação mais efetiva.

2. PERSPECTIVAS DE MELHORIA DO SISTEMA DE PUNIÇÃO AOS CRIMES PRATICADOS NAS REDES

No contexto em constante evolução das redes cibernéticas, é essencial avaliar e melhorar constantemente o sistema de sanções para crimes cometidos *online*. A atualização da legislação penal é um passo essencial para enfrentar os desafios colocados pelo *cybercrime*. A legislação deve refletir a dinâmica do ambiente em linha e abordar questões emergentes, como o aumento do *cyberbullying*, a propagação de conteúdos difamatórios nas redes sociais e os crimes de ódio na Internet. A clareza e a abrangência da lei são essenciais para garantir que os criminosos digitais sejam devidamente responsabilizados pelas suas ações.

> A lei sancionada em 2012 previa o prazo de 120 dias para entrar em vigor. Portanto, desde março de 2023 existe no país uma lei que criminaliza a invasão de celulares, computadores ou sistemas informáticos para obter, adulterar ou destruir dados a fim de obter vantagem ilícita, que também pode ser o objetivo da invasão dos dispositivos informáticos para instalar vulnerabilidades. As penas previstas na Lei Carolina Dieckmann para o crime tiveram um aumento significativo em 2021, quando entrou em vigor outra legislação sobre o tema a partir de projeto do senador Izalci Lucas, do PSDB do Distrito Federal (Araújo, 2023)

A revisão legislativa deverá começou a considerar a harmonização com tratados e acordos internacionais relacionados com a segurança e a criminalidade cibernética. Isto é crucial porque muitos crimes cibernéticos têm uma dimensão transnacional e requerem cooperação internacional para uma investigação e punição eficazes.

Em 12 de abril de 2023 foi publicado o Decreto nº 11.491 que promulga a Convenção sobre o Crime Cibernético firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001, com o seguinte texto:

> **O VICE-PRESIDENTE DA REPÚBLICA**, no exercício do cargo de Presidente da República, no uso da atribuição que lhe confere o art. 84, **caput**, inciso IV, da Constituição, e
> Considerando que a República Federativa do Brasil firmou a Convenção sobre o Crime Cibernético, em Budapeste, em 23 de novembro de 2001;
> Considerando que o Congresso Nacional aprovou a Convenção por meio do Decreto Legislativo nº 37, de 16 de dezembro de 2021; e
> Considerando que o Governo brasileiro depositou, junto ao Secretário-Geral do Conselho da Europa, em 30 de novembro de 2022, o instrumento de ratificação à Convenção e que esta entrou em vigor para a República Federativa do Brasil, no plano jurídico externo, em 1º de março de 2023; [...]
> Art. 1º Fica promulgada a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001, anexa a este Decreto.
> Art. 2º São sujeitos à aprovação do Congresso Nacional atos que possam resultar em revisão da Convenção e ajustes complementares que acarretem encargos ou compromissos gravosos ao patrimônio nacional, nos termos do inciso I do **caput** do art. 49 da Constituição. (Brasil, 2023)

Com este decreto de adesão à Convenção de Budapeste, também já alinhada com os objetivos da Lei n.º 12.965/2014 nomeada como Marco Civil da Internet, o país tem em suas mãos condições de realizar abordagens mais rápidas aos crimes virtuais assim como realizar punições, visando inibir o avanço de atos criminosos e elucidar os já cometidos com maior rapidez.

O Brasil se tornando signatário de acordos de cooperação internacional facilita a comunicação entre outros países que enfrentam situações semelhantes.

Citando o Preâmbulo da Convenção de Budapeste (2021):

> Considerando que o objetivo do Conselho da Europa é alcançar uma maior unidade entre seus membros;
> Reconhecendo a importância de fomentar a cooperação com as outras Partes desta Convenção;
> Convencidos da necessidade de buscar prioritariamente uma política criminal comum destinada à proteção da sociedade contra o crime cibernético, nomeadamente pela adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas;
> Conscientes das profundas mudanças desencadeadas pela digitalização, interconexão e contínua globalização das redes informáticas;
> Preocupados com os riscos de as redes informáticas e as informações eletrônicas também poderem ser utilizadas para a prática de crimes e de as provas dessas infrações poderem ser armazenadas e transferidas por meio dessas redes; (Convenção de Budapeste, 2021)

É importante observar o que foi considerado, pois a busca para uma política comum de proteção contra o crime cibernético estava sendo proposta nesta convenção visando à globalização das redes, uma vez que a legislação não está acompanhando essa movimentação. Com o reconhecimento de ter um tratado de parcerias onde os países que a estes aderissem pudessem compartilhar da mesma legislação, prevenção, troca de informação, disponibilidade de dados, facilitaria as condutas de penalização dos criminosos.

E ainda:

> Reconhecendo a necessidade de cooperação entre os Estados e a indústria no combate aos crimes eletrônicos e a necessidade de proteger interesses legítimos no uso e desenvolvimento da tecnologia da informação;
> Acreditando que um combate eficiente aos crimes cibernéticos exige uma cooperação internacional em assuntos penais mais intensa, rápida e eficaz;
> Convencidos de que a presente Convenção é necessária para impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como para impedir o abuso de tais sistemas, redes e dados, ao prever a criminalização de tais condutas, tal como se encontram descritas nesta Convenção, e ao prever a criação de competências suficientes para combater efetivamente tais crimes, facilitando a descoberta, a investigação e o julgamento dessas infrações penais em instâncias domésticas e internacionais, e ao estabelecer mecanismos para uma cooperação internacional rápida e confiável; (Convenção de Budapeste, 2021)

Um aspecto muito importante é a prevenção de competências para o combate efetivo que facilita a descoberta, investigação e julgamento das infrações penas nas instanciais, porém é necessária a cooperação proposta por esse tratado que torna rápida e confiável por ter acesso aos mesmos ideais uma vez que asseguram os mesmos interesses. Essa globalização das legislações sobre as redes, os dados, as linhas do crime, facilitam a prevenção e a punição, pois não terão já direito de livre acesso entre os países signatários.

> Atentos para a necessidade de assegurar o devido equilíbrio entre os interesses dos órgãos de persecução criminal e o respeito aos direitos humanos fundamentais, tal como previstos na Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais, de 1950, no Pacto das Nações Unidas sobre Direitos Civis e Políticos, de 1966, bem como em outros tratados internacionais sobre direitos humanos que reafirmem o direito universal à liberdade de consciência, sem interferência de qualquer espécie, bem como o direito à liberdade de expressão, que inclui a liberdade de buscar, receber e compartilhar informações e ideias de qualquer espécie, independentemente de limites, e os direitos à intimidade e à privacidade; (Convenção de Budapeste, 2021)

Um aspecto crítico da melhoria do sistema penal é investir em capacidades de investigação cibernética. As autoridades devem ter recursos financeiros, tecnológicos e humanos para rastrear, identificar e deter criminosos digitais. Isto inclui a formação de especialistas em investigação cibernética e a aquisição de tecnologia avançada para análise forense digital.

A cooperação entre diferentes agências governamentais, como a polícia, o Departamento da Administração Pública e o sistema judicial, é fundamental para o sucesso das investigações. Além disso, a cooperação internacional é essencial para combater o crime cibernético que transcende as fronteiras nacionais. As parcerias com outras nações, agências de aplicação da lei e organizações internacionais são essenciais para investigações eficazes.

> Conforme determina a lei 12.735/12 os órgãos da polícia judiciária devem criar setores especializados no combate a crimes virtuais. Somente, alguns estados brasileiros já possuem tais setores, que tem uma delegacia especializada para verificar a ocorrência desses delitos. (OTSU, 2023)

A sensibilização do público desempenha um papel fundamental na prevenção do cibercrime e na promoção de um ambiente online mais seguro. As campanhas de *Cyber* educação devem ser amplamente divulgadas para informar os cidadãos sobre os riscos online, como identificar ameaças e como denunciar atividades criminosas.

> A educação digital desempenha um papel essencial na prevenção de crime virtual, capacitando as pessoas a compreender os riscos inerentes ao ambiente online e adotar práticas seguras.
> Através da conscientização sobre as diversas ameaças cibernéticas, como phishing, malware e fraudes online, as pessoas podem desenvolver a capacidade de reconhecer sinais de alerta, como e-mails suspeitos, atividades não reconhecidas em suas contas e comportamento anormal de dispositivos.
> A educação digital também promove a adoção de medidas de segurança essenciais, como a criação de senhas fortes e únicas para contas online, bem como a ativação da autenticação de dois fatores sempre que possível, tornando a invasão de contas por parte de criminosos mais difícil (Advocacia, 2023)

As escolas desempenham um papel fundamental na educação dos jovens sobre a segurança digital, ensinando competências de navegação segura na Internet e incentivando um comportamento online responsável.

A cooperação entre os setores público e privado é essencial para melhorar o sistema de punição do crime cibernético. As empresas de tecnologia desempenham um papel importante na identificação e remoção de conteúdos ilegais, bem como na proteção dos dados dos utilizadores. As parcerias estratégicas com o governo podem facilitar a partilha de informações, acelerar a resposta a incidentes de segurança e permitir uma ação coordenada contra os criminosos *online.*

Em suma, a melhoria do sistema de condenação para crimes cibernéticos requer uma abordagem abrangente que inclua a atualização das leis, o investimento em investigações cibernéticas, a sensibilização do público, as parcerias público-privadas, a integração de tecnologias avançadas e o tratamento adequado dos delinquentes juvenis. Somente por meio de esforços coordenados em múltiplas frentes será possível enfrentar os desafios em constante evolução do mundo digital e garantir um ambiente online seguro e ético para todos os cidadãos brasileiros.

3. IMPACTO NAS ESCOLAS E IMPLICAÇÕES PSICOLÓGICAS

Os crimes cibernéticos têm se infiltrado em diversas esferas da sociedade brasileira, inclusive no ambiente escolar, onde o impacto é particularmente preocupante. As escolas, que historicamente deveriam ser espaços seguros para a aprendizagem e o desenvolvimento pessoal dos alunos, tornaram-se agora ambientes vulneráveis ao *cyberbullying* e outras formas de cibercrime. Além disso, as consequências psicológicas destas experiências são profundas e muitas vezes ignoradas.

Em 2020 a OMS – Organização Mundial de Saúde, declarou a Pandemia do Corona vírus - Covid19, doença até então desconhecida, que se iniciou na China, onde até aquele momento não se sabia ao certo o modo de transmissão, prevenção e não se tinha medicamentos para cura. O país parou praticamente por alguns meses e o ensino passou a ser remoto em alguns lugares, com material impresso, depois aulas totalmente *online*.

Para alguns alunos foi muito complicado não ter o convívio social e para professores não foi diferente, pois todos tiveram que se adaptar a um novo perfil, até então utilizado pelo ambiente do Ensino à Distância, com aulas gravadas, ou transmitidas vias plataformas educacionais, *classroom,* elaborar materiais para disponibilizar nas escolas para os que não tinham acessos online, se desdobrarem em atendimentos via WhatsApp.

> Com esse novo perfil de trabalho, os colaboradores se esforçam cada vez mais, assumindo responsabilidades, trabalhando horas incansáveis, sempre à procura de um reconhecimento profissional. A pressão psicológica é, na atualidade, uma das maiores causas de stress e transtornos comportamentais nas organizações, que incluem indústrias, comércio, prestação de serviços, área da saúde e, também, da educação. (Jorge *et al.,* 2021, p. 182)

O ambiente escolar passou a ser um ambiente mais vulnerável com o advento das redes sociais e da comunicação online, que tornou mais fácil a ligação entre os alunos, mas também abriu caminho para abusos e comportamentos prejudiciais. No ambiente escolar comum o bullying é largamente praticado, porém o *cyberbullying* ultrapassa barreiras, que pode incluir ameaças, calúnias, insultos e humilhação pública, não conhece fronteiras físicas. Invade a vida dos estudantes, infiltra-se nos seus dispositivos pessoais e monitoriza-os em todo o lado, 24 horas por dia, 7 dias por semana.

São ações do *cyberbullying:*

> "Hater: palavra que significa aquele que odeia. São pessoas que disseminam o ódio no ambiente virtual, atacam outras pessoas com ofensas e humilhações, de forma sistemática.
> Sexting: palavra originada a partir das palavras sex (sexo) e texting (ato de trocar mensagens de texto ou conversar por plataformas virtuais). O sexting consiste na troca de mensagens de cunho sexual, podendo ou não conter imagens de nudez das pessoas envolvidas. Quando há essa troca de imagens, o sexting pode tornar-se perigoso, pois pode ser divulgado por aquele que recebeu as imagens, ou hackers podem invadir os aparelhos e divulgarem o conteúdo. A divulgação das imagens, que rapidamente viralizam na rede, pode levar a vítima a sofrer com o cyberbullying.
> Revenge porn: essa expressão significa, literalmente, vingança pornográfica. Ele diz respeito ao ato de divulgar imagens eróticas e de nudez de uma pessoa que as enviou à outra confiando em sua índole, mas que as divulga como forma de vingança e punição." Porfírio (2023)

As consequências psicológicas do *cyberbullying* são perturbadoras. As vítimas muitas vezes experimentam ansiedade, depressão e estresse relacionados ao medo de serem agredidas novamente. O isolamento social é comum, pois muitas vítimas se afastam dos amigos e das atividades sociais para evitar maior exposição ao abuso online. Em casos extremos, o *cyberbullying* pode até levar a pensamentos suicidas.

O estudante pode manifestar sintomas na área da comunicação, aprendizagem, interação social, higiene pessoal, que pode expressar que algo está acontecendo que está bloqueando. Quando a escola chama a família e comunica que a criança não está conseguindo aprender, ou se relacionar, esta mãe chega com esse sintoma: “meu filho não quer mais estudar, não fala com a gente, está diferente”.

Porém, esse “não aprende”, “diferente” pode estar relacionado à fixação deste sujeito que o está impedindo de crescer que pode ser um desejo da criança, de se libertar.

Muitas vezes, a criança com dificuldade de aprendizagem acaba sofrendo o *Bullying*, este por sua vez, se entende como todas as formas de atitudes agressivas, intencionais e repetidas, que ocorre sem motivação evidente, executada dentro de uma reação desigual de poder. No entanto esses atos repetidos e o desequilíbrio de poder são características essenciais para intimidação da vítima. O mais comum, entretanto, é pensar que há apenas dois envolvidos: a vítima e o agressor, no entanto, existe um alerta para uma terceira pessoa fundamental neste processo: o espectador, ele é quem dá a continuidade do conflito (Silva, 2010).

E necessário que os pais ou profissionais da escola atentem a esses sinais de acordo com Ana Beatriz Barbosa Silva:

> [...] na escola geralmente no recreio, encontram-se isoladas do grupo ou perto de algum adulto que possa protegê-las, na sala de aula apresenta postura retraída mostrando-se comumente tristes, deprimidas ou aflitas, demonstra muita dispersão, tem faltas frequentes; nos jogos ou atividades em grupos são sempre as últimas a serem escolhidas; aos poucos vão se desinteressando das atividades a das tarefas escolares e em casos mais dramáticos apresentam hematomas, arranhões, cortes, roupas danificadas ou rasgadas sem uma natural explanação (Silva; 2010, p. 48)

Essa luta em liberar o reprimido, gera uma angústia, um sofrimento individual muitas vezes travado em silêncio e manifesto diariamente.

O inconsciente abriga elementos que não estão acessíveis à consciência, que por ela foi censurado, reprimido ou excluído, porém não estão esquecidos e afetam a consciência quando são liberados, mostrando que nada perderam de sua força emocional.

> "Aprendemos pela experiência que os processos mentais inconscientes são em si mesmos intemporais. Isto significa em primeiro lugar que não são ordenados temporalmente, que o tempo de modo algum os altera, e que a ideia de tempo não lhes pode ser aplicada" (Freud, 1925-1926, p. 39)

Sendo o conteúdo inconsciente independentes do tempo que pode ser alterado ou medido, estes acabam sendo os principais determinantes da personalidade, as fontes da energia psíquica, as pulsões e os instintos.

Como a mente não se reduz somente à memória, mas ocorre toda uma atividade consciente onde um dos resultados da censura é a produção de material para o inconsciente, e este se manifesta

através de sintomas, sonhos, assim como as resistências, passando a não ser acessível pelo consciente.

A ação dos fármacos utilizados para quadros de ansiedade, prejudicam o funcionamento do sistema de inibição, fazendo com que a pessoa consiga desempenhar suas funções diminuindo o nível exagerado de vigilância, porém não solucionam a real situação.

> Entender que o córtex pré-frontal é importante para a autorregulação comportamental e que ele se desenvolve gradualmente pode explicar por que, por exemplo, as crianças têm dificuldade de: (a) interromper uma atividade e passar para outra atividade; (b) planejar com antecedência, (c) fazer mais de uma tarefa ao mesmo tempo, (d) concentrar-se por longos períodos de tempo, e (e) renunciar a recompensas imediatas. Os resultados de pesquisas sobre a neurociência cognitiva do desenvolvimento sugerem que esses comportamentos são uma parte normal do crescimento e, até certo ponto, sua origem está relacionada à forma de funcionamento do cérebro nessa etapa da vida (Kanapp, 2013, p. 1)

Para que o processo de aprendizagem ocorra de forma satisfatória se faz necessário o bom desempenho das funções cerebrais e do desenvolvimento psíquico pois o este processo envolve simbolizações, sentimentos e emoções que podem ser bloqueadas através de inibições e conflitos, pois estes são atemporais e produzem sofrimento psíquico.

No passado, as escolas podem ter oferecido algum nível de proteção contra o bullying tradicional porque as vítimas podiam encontrar refúgio em casa ou noutros locais longe dos agressores. No entanto, o *cyberbullying* desafia esta noção de santuário, uma vez que segue as vítimas até as suas casas através de dispositivos eletrônicos. Isso cria um ambiente de perseguição virtual do qual é difícil escapar.

Os invasores no ambiente digital geralmente têm uma vantagem significativa. Eles podem coletar informações pessoais e emocionais sobre suas vítimas por meio de postagens nas redes sociais e interações online. Esta informação é então usada para atacar danos emocionais, tornando os ataques mais prejudiciais e mais difíceis de combater.

O Governo do Estado do Paraná, em 2023, encaminhou às escolas o Guia De Orientações - Às Equipes Diretivas E Pedagógicas Dos Protocolos De Situações De Violência Intra E Extraescola. Este guia foi elaborado para orientar em todas as situações de violências contra crianças e adolescentes, carregam especificidades, urgências e emergências, sendo necessária ação rápida para minimizar os danos e proteger os envolvidos. Tem como alvo garantir que todos na escola saibam o que fazer para identificar, agir, encaminhar e notificar às situações de violência, cuidando para não expor e revitimizar as (os) estudantes, através da Revelação Espontânea.

> A revelação espontânea acontece quando a criança ou adolescente escolhe um(uma) profissional, pode ser qualquer pessoa do ambiente escolar, e revela que foi vítima ou testemunha de violência. Essa pessoa deve acolher, credibilizar o relato, respeitar. O papel do(da) profissional na revelação espontânea é acolher, não precisa fazer perguntas, não precisa entender, não precisa buscar provas. Evitar demonstrar reações que possam constranger, impressionar ou sugestionar, ouvir sem julgamento de valor ou questionamentos. O(a) profissional que foi escolhido(a)à é porque despertou confiança na criança ou no adolescente. O que se deve fazer é apenas ouvir o relato, no final agradecer a confiança, dizer que vai buscar ajuda e que ele(ela) foi muito corajoso(a) em revelar a situação (Paraná, 2023)

É essencial que as escolas, os educadores e os pais estejam conscientes das consequências do cibercrime, especialmente do *cyberbullying*, na vida dos alunos. A promoção de uma cultura de segurança digital e a educação sobre competências emocionais são essenciais para ajudar os jovens a enfrentar este desafio. As políticas escolares devem ser atualizadas para abordar eficazmente o *cyberbullying*, concentrando-se não apenas nas consequências para os agressores, mas também no apoio às vítimas.

CONSIDERAÇÕES FINAIS

A Internet, desde a sua criação, vem sendo aprimorada e propiciando mudanças em todas as áreas, seja ela profissional, educacional, social, organizacional, saúde, cultural, relacionamentos, comércio, enfim, assim como tem espaço para todos inovarem, as mentes criminosas também investiram nessa área, viram um potencial muito grande para agir rapidamente e os crimes cibernéticos, que no início não tinham nenhuma regulamentação, estavam à mercê de seus algozes.

Percebe-se que a liberdade na rede social e a velocidade da comunicação, facilitam os crimes praticados, uma vez que as exposições em demasia dão margem para os criminosos cibernéticos escolherem suas vítimas e as perseguirem, logo os crimes contra a honra são os mais práticos e devido a essa premissa foram discorridos com maior ênfase nesse material que procurou demonstrar como afeta os usuários de toda a rede.

A necessidade de uma legislação específica para os crimes cibernéticos é crescente assim como colocar em prática. Grandes conquistas já foram realizadas como a Lei nº 12.737/2012, "Lei Carolina Dieckmann", a Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD). a Lei nº 12.965/2014, também conhecida como o Marco Civil da Internet, e o Decreto nº 11.491/2023 que promulga a Convenção sobre o Crime Cibernético firmada pela República Federativa do Brasil, em Budapeste (2021). Muito ainda há que se pôr em ação, realizar as mudanças propostas nestas leis para efetivação de uma real proteção e punição dos crimes cibernéticos.

REFERÊNCIAS

ADVOCACIA, Galvão & Silva. **Crime Virtual:** Compreendendo os Delitos e Protegendo-se no Ambiente Digital**:** como a educação digital pode ajudar na prevenção de crimes virtuais?. Como a educação digital pode ajudar na prevenção de crimes virtuais?. [S. l.]: Galvão e Silva, 2023. Disponível em: https://www.galvaoesilva.com/crime-virtual/. Acesso em: 07 nov. 2023.

ARAÚJO, Janaína. **Os dez anos de vigência da lei carolina dieckmann:** a primeira a punir crimes cibernéticos. Brasilia: Senado Federal, 2023. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmannaprimeiraapunircrimescibernetico s#:~:text=Discuss%C3%B5es%20e%20vota%C3%A7%C3%A3o%20da%20primeira,era%20fonte%20de%20preju%C3%ADzos%20financeiros.&text=A%20INVAS%C3%83O%20DE%20COMPUTADORES%20OU,ANOS%20DE%20RECLUS%C3%83O%20E%20MULTA. Acesso em: 07 nov. 2023.

BRASIL. (org.). **Estatuto da Criança e do Adolescente**: lei no 8.069, de 13 de julho de 1990. Lei no 8.069, de 13 de julho de 1990. 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 06 nov. 2023.

BRASIL. **Decreto Lei nº 12.737: lei de crimes cibernéticos.** Brasília: Planalto, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/ato20112014/2012/lei/l12737.htm. Acesso em: 05 out. 2017.

BRASIL. **Decreto-lei 2.848 de 7 de dezembro de 1940**. Brasília: Planalto, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 05 nov. 2023

BRASIL. **Constituição (1988). Constituição da República Federativa Do Brasil**. Brasília: Constituição, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituição/constituicaocompilado.htm. Acesso em: 05 nov. 2023.

BRASIL. **Convenção sobre o Crime Cibernético**: decreto nº 11.491, de 12 de abril de 2023. decreto nº 11.491, de 12 de abril de 2023. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 07 nov. 2023.

CONVENÇÃO DE BUDAPESTE. **Convenção sobre o Cibercrime.** [S. l.]: Convenção sobre o Cibercrime. 2001. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci-en/rules-and-legislation/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 05 nov. 2023.

DMITRY BESTUZHEV (Brasil). Diretor da Equipe Global de Pesquisa e Análise (Great) da Kaspersky Para A América Latina. (org.). **Kaspersky divulga seus prognósticos de segurança de 2022 para a América Latina**. [S. l.]: Kaspersky, 2021. Disponível em: https://www.kaspersky.com.br/about/press-releases/2021_kaspersky-divulga-seus-prognosticos-de-seguranca-de-2022-para-a-america-latina. Acesso em: 05 nov. 2023.

ESTRASBURGO. PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho**: regulamento geral de proteção de dados (gdpr) da união europeia. Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. [S. l.]: Estrasburgo, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1552577087456&uri=CELEX:32018R1725. Acesso em: 07 nov. 2023.

FREUD, Sigmund. **Além do princípio do prazer, psicologia de grupo e outros trabalhos:** Volume XVIII. Viena: Ed brasileira: Imago, 1925/1926. (Coleção Obras Psicológicas Completas de Sigmund Freud).

INTERNATIONAL IT (São Paulo). **Anuário de Segurança Pública 2023:** Crimes Digitais Aumentam 65,2%**.** São Paulo: International IT, 2023. Disponível em: https://www.internationalit.com/post/anu%C3%A1rio-de-seguran%C3%A7a-p%C3%BAblica-2023-crimes-digitais-aumentam-65-2. Acesso em: 05 nov. 2023.

JORGE, Elisangela Emilia et al. **Saúde mental no século xxi indivíduo e coletivo pandemico: níveis de ansiedade em docentes perante a pandemia de orthocoronavirinae (covid-19).** Guarujá São Paulo: Científica Digital, 2021. 280 p. (S 255). Disponível em: https://downloads.editoracientifica.org/books/978-65-87196-90-9.pdf. Acesso em 05 nov. 2023.

KNAPP, K.; MORTON, J. B. Desenvolvimento do Cérebro e Funcionamento Executivo. *In:* TREMBLAY, R. E.; BOIVIN, M.; PETERS R. D. E. V.; MORTON, J. B. **Enciclopédia sobre o Desenvolvimento na Primeira Infância** [on-line]. http://www.enciclopedia-crianca.com/funcoes-executivas/segundo-especialistas/desenvolvimento-do-cerebro-e-funcionamento-executivo. Acesso em 05 nov. 2023.

MAPUTO. Intic. Instituto Nacional de Tecnologias de Informação e Comunicação (org.). **FBI prevê maior proliferação de crimes cibernéticos para 2023**. [*S. l.: s. n.*], 2023. Disponível em: https://www.intic.gov.mz/fbi-preve-maior-proliferacao-de-crimes-ciberneticos-para-2023/. Acesso em: 05 nov. 2023.

MARTINS, Patrícia. Crimes Cibernéticos e a correlação ao Crime Contra Honra. **Jusbrasil**, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-e-a-correlacao-ao-crime-contra-honra/782377147. Acesso em: 05 nov. 2023.

MIRANDA, Leandro. **5 crimes virtuais para as empresas tomarem cuidado em 2023**. São Paulo: Portal Urbinar, 2023. Disponível em: https://portalturbinar.com.br/crimes-virtuais-2023. Acesso em: 05 nov. 2023.

MONEYLAB (Brasil). Brasil aparece em 2º em ranking de ataques cibernéticos. **Infomoney,** 2023. Disponível em: https://www.infomoney.com.br/negocios/brasil-aparece-em-2o-em-ranking-de-ataques-ciberneticos-como-se-proteger/. Acesso em: 05 nov. 2023.

NASCIMENTO, Talles Leandro Ramos. Crimes Cibernéticos **Conteudo Juridico**, Brasilia-DF: 17 dez 2018. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 06 nov. 2023.

OTSU, Denise Pereira. **crimes cibernéticos e os limites da liberdade de expressão nas redes**. [*S. l.: s. n.*], 2023. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/35166/1/CRIMES%20CIBERNE%CC%81TICOS%20%281%29.pdf. Acesso em: 07 nov. 2023.

PORFÍRIO, Francisco. Cyberbullying": o cyberbullying pode ser pior que o bullying no ambiente escolar, pois a vítima não pode fugir dele. **Brasil Escola**, 2023. Disponível em: https://brasilescola.uol.com.br/sociologia/cyberbullying.htm. Acesso em: 05 nov. 2023.

PWC BRASIL (Brasil). **Pesquisa Global sobre Fraudes e Crimes Econômicos 2022**: protegendo o perímetro: o aumento da fraude externa. Protegendo o perímetro: o aumento da fraude externa. [S. l.]: PWC BRASIL, 2022. Disponível em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2022/pesquisa-global-sobre-fraudes-e-crimes-economicos-2022.html. Acesso em: 05 nov. 2023.

SILVA, Ana Beatriz B. **Bullying:** mentes perigosas nas escolas. Rio de Janeiro: Editora Objetiva Ltda, 2010.

VIEIRA, Maria Eduarda Pereira. **A adesão do brasil a convenção de budapeste e a correção das deficiências legislativas quanto aos crimes cibernéticos**. [*S. l.: s. n.*], 2023. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/248821/A%20ADES%C3%83O%20DO%20BRASIL%20A%20CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE%20E%20A%20CORRE%C3%87%C3%83O%20DAS%20DEFICI%C3%8ANCIAS%20LEGISLATIVAS.%20Vers%C3%A3o%20final%20-%20Documentos%20Google%20%281%29.pdf?sequence=1&isAllowed=y. Acesso em: 05 nov. 2023.