# VULNERABILIDADE SOCIAL FRENTE A TECNOLOGIA VIRTUAL UMA ANÁLISE COMPARATIVA ENTRE A NETZDG E A SOLUÇÃO BRASILEIRA

Márcia Silva Lima[1]
Mônica Moreira de Jesus Amaro[2]
Cristiane Ingrid de Souza Bonfim[3]

## RESUMO

Esta pesquisa apresenta o cenário crítico da vulnerabilidade social frente a crimes cibernéticos no Brasil, trazendo uma análise sucinta sobre situação do poder público no combate a esses crimes. Nesses últimos dez anos, podemos nitidamente notar como o avanço da tecnologia no mundo trouxe a sociedade meios de ferramentas de trabalhos tecnológicos como: redes sociais, aplicativos bancários, vendas on-line e outras utilidades apenas ao alcance de um `click". No caso do Brasil, sendo o país da América Latina que mais se utiliza as redes sociais, este artigo mostra pesquisas feitas em como essa modernidade também veio acompanhada de problemas sociais e econômicos frente a uma sociedade vulneráveis a crimes cibernéticos e a dificuldade da aplicação das leis brasileiras no combate a esses crimes. Mostra também, a necessidade de uma educação digital e um comparativo da Lei *NetzDG* alemã com a regulação brasileira. Mesmo com a mudança nas leis trazendo o aumento de pena para quem comete estelionato digital, ainda assim não há uma notória mudança no comportamento desses indivíduos. Tecnicamente, ainda há uma falta de melhoria para um processo investigativo mais eficiente contra essas quadrilhas. Mesmo assim, é consenso que apenas punir o crime não resolve quando há uma extrema necessidade de uma educação digital mais abrangente. Mesmo com a Lei Geral de Proteção de Dados – LGPD, sequer houve uma diminuição desses crimes, conforme consta dados nesses últimos dois anos. Contudo, o presente artigo traz uma demonstração do cenário atual dos crimes praticados nas plataformas digitais.

**PALAVRAS – CHAVES:** Tecnologia Virtual; Crimes Cibernéticos; Responsabilização dos Provedores

## INTRODUÇÃO:

O presente artigo aborda acerca dos crimes cibernéticos com a mesma finalidade de estelionato tipificado no artigo 171 do Código Penal Brasileiro de 1940. A perspectiva da presente pesquisa está relacionada aos ataques nas redes de internet com resultado de extorsão.

Traz também dados da intensificação desses crimes no Brasil, um comparativo da *NetzDG* alemã e a regulação brasileira no combate a esses crimes virtuais, a vulnerabilidade social frente a esses ataques, as discursões acerca das punições em leis mais rigorosas e a responsabilização dos provedores de rede e como pode ser aplicada uma educação digital para prevenção desses golpes na *internet*.

O objetivo principal da presente pesquisa é analisar o crime de estelionato virtual no

[1]Graduanda em Direito pela Faculdade Evangélica Raízes, Anápolis, Goiás marciasilva9197@gmail.com.
[2]Graduanda em Direito pela Faculdade Evangélica Raízes, Anápolis, Goiás mônicadeamaro@gmail.com.
[3]Especialista em Direito Penal e Processo Penal, Mestrado (Universidade Evangélica de Goiás - EVANGÉLICA), professora, Faculdade Evangélica Raízes, Anápolis, Goiás, cristiane.bonfim@docente.faculdaderaizes.edu.br.

âmbito das plataformas digitais como: redes sociais, sites e e-mail. Traz também de forma sucinta a forma de como esses crimes são desenvolvidos por agentes comuns e, as consequências desses crimes na vida cotidiana do brasileiro. A metodologia adotada neste estudo, foi verificada com base em artigos, doutrina, legislação, todos temas envolvidos na área cibernética para trazer uma maior visão clara da situação atual do Brasil no âmbito dos acontecimentos de crimes virtuais.

Para melhor compreensão, o estudo está organizado em três seções principais, contendo: noções gerais acerca da internet e sua utilização, crimes digitais, uma análise dos crimes digitais e, responsabilização dos provedores com uma análise do Brasil e a *NetzDG* Alemã, uma análise sucinta da lei que alterou dispositivos do Código Penal Brasileiro (1940) com aumento de penas mais severas com o intuito de dificultar invasões de dispositivos eletrônicos, evitando fraudes e outros delitos cometidos em ambiente digital, prevendo agravantes quando esses crimes forem cometidos com uso da *internet*.

Os fundamentos legais a luz da Lei Geral de Proteção de Dados – LGPD, para que o usuário da *internet* tenha segurança quando se tratar da inviolabilidade dos seus dados pessoais e da dignidade humana. Também, este presente artigo traz uma visão no saber autores em diversos artigos e *sites* publicados e de jurista como Cunha, e outros autores como: Truzzi (2021, p. 221), Muller (2021, p. 103) e Doneda (2013, p. 44).

## 1. CRIMES CIBERNÉTICOS NO BRASIL E, RESPONSABILIZAÇÃO NORMATIVA NO SISTEMA BRASILEIRO DOS PROVEDORES DE REDES SOCIAIS PELO CONTEÚDO PUBLICADO.

Inicialmente cumpre salientar que a *internet* e o avanço da tecnologia no mundo trouxeram a sociedade, não importando a classe social, uma forma globalizada de interação, marketing digital, publicidades, meios de ferramentas de trabalhos tecnológicos cada vez mais modernos e acessíveis em diversas árias comerciais, como por exemplo: redes sociais, aplicativos bancários, vendas *on-line* com inúmeras formas de compras virtuais.

Apenas ao alcance de um *"click"*, temos um mundo digital ao nosso alcance. Com todo esse mundo a explorar, desperta uma análise profunda de como o usuário pode estar resguardado contra diversas formas de crimes cibernéticos cada vez mais eficazes em suas ações altamente treinados para cometer o crime virtual convencendo a vítima por uma oferta tentadora. Isso mostra o quão necessário é uma educação digital no combate a esses tipos de crimes.

No caso do Brasil, sendo o país da América Latina que mais se utiliza as redes sociais,

segunda um levantamento feito pela *Comscore* (empresa de análise de internet dos Estados Unidos), publicado pela revista Forbes Tech, mostra que o Brasil é o primeiro da América Latina em acesso as plataformas, o equivalente a 131,5 milhões de pessoas, atrás da Índia e Indonésia, e à frente dos Estados Unidos, México e Argentina. (Pacete, 2023, *on-line*).

Os benefícios advindos do avanço tecnológico vão muito além da interação social, com o avanço tecnológico cresceu-se também os crimes nesse ambiente, os chamados "crimes cibernéticos". Como as políticas de prevenção tem atuado no combate a esses crimes?

A aplicabilidade da Lei trouxe resultados eficazes nesse combate? Mesmo com mudanças nas Leis de combates a esses crimes, ainda assim, será necessário criar mecanismos que automaticamente crie um sistema de alerta no ato do crime? Uma política de educação digital pode ser uma forte aliada a prevenção desses crimes frente a uma sociedade tão vulnerável? Na opinião de Muller, ela diz o seguinte:

> O acesso massificado e o compartilhamento irresponsável de dados nas redes sociais gera a criação de um ambiente de falta de conhecimento e de desinformação, no qual não recebe dados originalmente de suas fontes, nem ao menos, de forma verídica. (Muller, 2021, p. 103).

Esse fenômeno massificante do uso das redes sociais no Brasil, gera grande preocupação nas questões de segurança digital, permitindo cada vez mais o acesso descontrolado na *internet*, com isso, a privacidade seja ela civil ou jurídica ficam à mercê de criminosos com uma vasta quantidade de informações, facilitando seus atos inescrupulosos.

A *internet* é utilizada de inúmeras formas, no mercado financeiro segmentado por sua natureza complexa, seja física ou *on-line*, no âmbito educacional, operações bancárias, entretenimento, solicitação de serviços e muitas outras coisas mais. Com isso, as informações de dados pessoais são desenfreadamente compartilhadas para o acesso a esses tipos de serviços.

Com a utilização desses meios os dados pessoais de uma pessoa ficam vulneráveis à ação de criminosos cibernéticos que usam de sua conduta ardilosa para enganar alguém, e assim, conseguir o que se pretende de forma fácil e precisa, a exemplo disso, vale destacar que um dos maiores crimes praticados na internet no brasil é o de estelionato virtual, é uma ação criminosa e, esse meio fraudulento induz a vítima a erro para conseguir vantagem ilícita.

O Código Penal Brasileiro (1940) em seu artigo 171, traz o seguinte: "Obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém a erro, mediante artifício ardil, ou qualquer outro meio fraudulento". Contudo, em muitos casos, essas ações são sutilmente infiltradas sem o mínimo de percepção por parte de uma vítima até mesmo provida de conhecimento.

Em algum momento e lugar um cidadão brasileiro teve um contato de uma pessoa se passando por um familiar, ou teve seu *whatsapp* "clonado", suas redes sociais e cartões bancários clonados, recebeu uma oferta tentadora por aquele produto desejado, ou até mesmo recebeu um "boleto falso".

Habitualmente, uma parte significativa das fraudes eletrônicas ocorrem como forma de "iscas" fazendo vítimas com muita facilidade. No dizer de Gisele Truzzi, fala que:

> Esse tipo de "isca" ´é comumente chamado de "*phishing scam*": uma tentativa dos criminosos em induzir as potenciais vítimas a fornecerem informações pessoais ou clicarem em determinado link. Se a vítima acabar fornecendo a informação desejada (exemplo: um código enviado via SMS) [...]. (Truzzi, 2021, p. 221).

Esses criminosos utilizam técnicas muito eficazes para cometerem os crimes virtuais, eles usam nomes e imagens idênticas as originais e sites semelhantes. Necessita-se de uma análise profunda e estar sempre atento ao que é solicitado pelo serviço a ser prestado, é uma forma de evitar essas fraudes e verificar se está dentro da norma de acordo com a política de privacidade e verificações de segurança da empresa, fazer um comparativo com as avaliações feitas por clientes anteriores.

Para Cavalcante (2021, *on-line*), a atuação do agente quando obtém a vantagem ilícita por meio de informações que ele obteve da própria vítima ou de um terceiro que foram induzidos em erro, se traduz pela sutileza da conduta criminosa do agente, ressalta que a maneira como aborda a vítima por meio de um dispositivo eletrônico, parece ser mais eficaz quanto ao fato de estar em ambiente remoto, mas ao mesmo tempo, ao alcança de suas mãos.

> O grande diferencial aqui é que a atuação do agente foi por meio eletrônico, ou seja, a vítima ou o terceiro foram induzidos a erro por meio de: redes sociais (ex: Facebook, Instagram), contatos telefônicos (ex: simulando que se trata de ligação da operadora de cartão de crédito), envio de correio eletrônico fraudulento (ex: e-mail que imita correspondência da loja, banco etc.), ou qualquer outro meio fraudulento análogo. (Cavalcante, 2021, *on-line*).

Embora tudo pareça ser simples para a vítima, sabemos que para o criminoso tem todo um processo e esquematização, a abordagem não ataca apenas um, mas um complexo de contatos digitais atacados por *hackers* que burlam sistemas de formas hábeis para tentativas de cometimentos desses crimes na *internet*.

A intensificação dos crimes cibernéticos no brasil se caracteriza pelo acesso que o indivíduo tem de obter informações de dados cadastrais das vítimas, é bem verdade que há uma certa dificuldade desses criminosos serem descobertos pelas autoridades sem que possam ter suas identidades reconhecidas.

Segundo um artigo publicado (Dino noticia, 2023, *on-line*) e de acordo com um estudo realizado pelo laboratório de inteligência e ameaças, *Fort Guard Labs*, e publicado pela CNN, somente no primeiro semestre de 2022, o país sofreu cerca de 31,5 bilhões de tentativas de ataques Cibernéticos, representando um aumento de 94% em relação aos 16,2 bilhões do ano anterior. Mesmo com o advindo da Lei 13.709/2018, que trouxe requisitos para o tratamento de dados pessoais, ainda assim, não foi suficiente o bastante para a responsabilização tanto dos criminosos como para os que regulam os fornecedores e provedores.

Nessa análise ampla da *internet* no brasil, com meios que regulam, também traz uma inspiração da Lei brasileira com a controversa Lei alemã a *NetzDG* (que será abordada com mais complexidade na segunda fase deste presente artigo), essa Lei, inspirou o Brasil nos combates aos crimes virtuais. Vejamos essa análise crítica na opinião de Mariana Schreiber:

> As plataformas são muito relutantes em conceder aos pesquisadores o acesso necessário para realizar pesquisas", afirma ao defender o acesso direto a dados e algoritmos por meio de APIs (as instruções e padrões de programação para acesso a um aplicativo). (Schreiber, 2020, *on-line*).

A lei alemã inspira o Brasil a tomar medidas mais rígidas em relação ao combate aos crimes virtuais e de maneira geral as responsáveis pelos provedores de acesso à rede. Ainda se tem muitas críticas em relação a essas tomadas de decisões, levando em consideração que tais penas aplicadas ainda não estão sendo suficientes para o combate aos crimes de estelionato virtual no país.

O Brasil, é um país em que há democracia de conteúdo publicados na *internet* e uso literalmente livre para o nicho variado do comercio digital tornando o Brasil totalmente moderno nessa questão. Posteriormente, abordar-se-á sobre o impacto da Lei Geral de Proteção de Dados e a aplicação da Lei 14.155/21 na alteração do artigo 171, do Código Penal Brasileiro (1940), visando o aumento de pena para o combate de crimes cibernéticos.

## 2. A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS, A DEFINIÇÃO DA LEI 14.155/21 E A TIPICIDADE CRIMINAL

A crescente dependência das tecnologias digitais nas últimas décadas transformou radicalmente a maneira como as pessoas interagem, consomem e trabalham. No entanto, esse avanço também abriu espaço para novas formas de criminalidade, exigindo respostas mais eficazes do ordenamento jurídico. Foi nesse contexto que surgiu a Lei nº 14.155, de 27 de maio de 2021, como um marco relevante no combate aos crimes cibernéticos no Brasil.

Essa lei alterou dispositivos do Código Penal Brasileiro (1940) para tornar mais severas as punições relacionadas a invasões de dispositivos eletrônicos, fraudes eletrônicas e outros delitos cometidos em ambiente digital.

Um dos pontos centrais da nova legislação foi a reformulação do artigo 171, do Código Penal, referente ao estelionato, prevendo aumento de pena quando esses crimes forem cometidos por meio eletrônico ou com uso da *internet*.

A mudança representa um reconhecimento formal de que o meio digital não é apenas um novo cenário de interação social, mas também um novo campo de vulnerabilidades, muitas vezes exploradas por criminosos com alto grau de sofisticação técnica.

Além disso, a Lei 14.155/2021 também estabelece penas mais rigorosas quando os crimes têm como vítimas pessoas idosas ou vulneráveis, o que reflete uma preocupação social com aqueles que, muitas vezes, são os alvos preferenciais de golpes virtuais.

Com isso, busca-se não apenas punir de forma mais proporcional esses atos ilícitos, mas também funcionar como um instrumento de prevenção. Vejamos as seguintes mudanças segundo Cavalcante (2021, *on-line*), em relação as três alterações realizadas no art. 171, que trata sobre estelionato:

> As alterações no crime de estelionato inseriram o § 2º-A, prevendo a qualificadora do estelionato mediante fraude eletrônica, acrescentou o § 2º-B, com uma causa de aumento de pena relacionada com o § 2º-A, modificou a redação da causa de aumento de pena do § 4º. Art. 171 (...): § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Cavalcante 2021, *on-line*).

Contudo, ainda que represente um avanço legislativo importante, é preciso reconhecer que a eficácia da lei depende diretamente da capacidade do Estado em investigar e processar esse tipo de crime. A complexidade técnica envolvida nos delitos cibernéticos exige uma atualização constante dos meios de investigação e do preparo das forças de segurança, o que nem sempre acompanha o ritmo das mudanças tecnológicas.

Vejamos as modificações da redação que a Lei alterou mediante uma tabela publicada por (Cunha, 2021, *on-line*).

| **Redação anterior** | **Redação dada pela Lei 14.155/21** |
|---|---|
| Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:<br>Pena – reclusão, de um a cinco anos, e multa, de | Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: |

| | |
|---|---|
| quinhentos mil réis a dez contos de réis. | Pena – reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. |
| | § 2º-A – A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. |
| | § 2º-B – A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. |
| § 3º – A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência. | § 3º – A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência. |

fonte: Cunha, 2021, *on-line*.

Assim, embora a Lei 14.155/2021 seja um passo necessário, ela por si só não resolve os desafios impostos pelos crimes digitais, sendo parte de um processo mais amplo de adaptação do sistema jurídico à realidade virtual que nos cerca.

Nas últimas décadas, o Brasil vivenciou um aumento significativo nos crimes cibernéticos, impulsionado pela ampliação do acesso à internet e pela sofisticação das técnicas utilizadas por agentes mal-intencionados. Ataques virtuais, como invasões de sistemas, roubos de dados pessoais e financeiros, disseminação de *malware* e fraudes eletrônicas, passaram a integrar o cotidiano das ameaças enfrentadas tanto por indivíduos e por empresas.

Em resposta a esse cenário, o Estado brasileiro tem desenvolvido e aprimorado um arcabouço normativo voltado à proteção do ambiente digital e à repressão das condutas ilícitas praticadas por meio eletrônico. A construção da legislação brasileira sobre crimes informáticos teve início com a promulgação da Lei nº 9.610/1998, que dispõe sobre os direitos autorais, atualizando a antiga legislação de propriedade intelectual. Embora não trate diretamente de delitos cibernéticos, essa norma passou a ser invocada em casos de reprodução não autorizada de conteúdo protegido em ambientes digitais.

Nesse contexto, surgiu o chamado Projeto de Lei Azeredo (PL 84/1999), que pretendia estabelecer um marco legal mais rígido para crimes de informática, mas acabou sendo duramente criticado por movimentos civis e acadêmicos por representar, segundo seus opositores, um risco à liberdade de expressão e ao uso livre da internet.

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

A LGPD estabelece fundamentos legais para o tratamento de dados pessoais, que incluem o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, à inviolabilidade da intimidade e à dignidade humana. Ela se aplica a qualquer operação de tratamento realizada no território nacional ou que tenha por objetivo a oferta de bens e serviços a indivíduos localizados no Brasil, independentemente do local da sede do agente de tratamento.

De acordo com a lei, os dados pessoais são quaisquer informações relacionadas a uma pessoa natural identificada ou identificável, enquanto os dados pessoais sensíveis são aqueles que revelam, dados genéticos ou biométricos.

A lei também cria a figura da Autoridade Nacional de Proteção de Dados (ANPD), responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Entre suas competências estão a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e a aplicação de sanções administrativas.

O não cumprimento da LGPD pode gerar sanções administrativas como advertências, multas de até 2% do faturamento da empresa (limitadas a R$ 50 milhões por infração), publicização da infração, bloqueio e até eliminação dos dados pessoais tratados de forma irregular. O avanço das tecnologias digitais transformou profundamente a maneira como os indivíduos se relacionam, trabalham, estudam e se informam.

Diversas empresas já foram multadas no Brasil por violarem a Lei Geral de Proteção de Dados (LGPD). A Cyrela foi a primeira condenada judicialmente por uso indevido de dados pessoais. A ANPD (Autoridade Nacional de proteção de dados) aplicou multa à *Telekall Infoservice* por comercializar dados de eleitores, (São Paulo: Nowcy, 2020).

O Banco Safra e outras instituições financeiras foram penalizadas por assédio a aposentados com base em dados obtidos ilegalmente. As sanções mostram o avanço na fiscalização e a necessidade de conformidade com a LGPD, (Brasilia: ANPD, 2023).

Contudo, esse mesmo ambiente virtual que facilita o cotidiano também se tornou palco de novas formas de violência e criminalidade. Os crimes cibernéticos, praticados com o uso de dispositivos eletrônicos e redes de *internet*, têm provocado impactos sociais significativos, tanto no nível individual quanto coletivo.

De acordo com Doneda (2013, p. 44), “a crescente digitalização das relações sociais

implica a ampliação dos riscos de exposição de dados, violação de privacidade e surgimento de novos danos morais". Em outras palavras, os crimes cometidos no ambiente digital não são meramente técnicos; eles têm reflexos reais na vida das vítimas.

A divulgação indevida de imagens íntimas, os ataques de ódio em redes sociais, os golpes financeiros e o roubo de identidade digital são exemplos de condutas que geram sofrimento psicológico, exclusão social e desestruturação emocional.

Além do impacto direto nas vítimas, a criminalidade digital afeta a confiança da sociedade nas plataformas digitais. Segundo Reisdorfer (2020, p. 212), "o medo de sofrer ataques virtuais tem levado muitas pessoas a se afastarem do convívio digital, restringindo sua participação no espaço público *on-line*". Isso compromete o pleno exercício da cidadania digital, dificultando o acesso à informação, à educação remota, ao trabalho digitalizado e aos serviços públicos eletrônicos.

O ambiente cibernético ainda apresenta peculiaridades que dificultam a responsabilização dos autores. A facilidade de anonimato, o uso de criptografia, redes privadas e o alcance transnacional das ações criminosas são entraves para a investigação e punição efetiva dos responsáveis. Como aponta Castells (2003, p. 145), "a lógica das redes de informação subverte as fronteiras tradicionais do Estado, impondo um desafio jurídico sem precedentes".

Outro aspecto relevante é o agravamento da vulnerabilidade de certos grupos sociais. Mulheres, crianças, adolescentes, idosos e pessoas LGBTQIAPN+ estão entre os principais alvos de violência cibernética, como *cyberbullying*, perseguição virtual, chantagens e discriminação. Isso evidencia que o impacto social dos crimes cibernéticos não se restringe ao indivíduo, mas revela dinâmicas estruturais de opressão e desigualdade que se reproduzem na esfera digital.

Do ponto de vista econômico, os crimes virtuais também causam prejuízos expressivos. Relatórios da Interpol e da *McAfee* apontam que os danos financeiros globais causados por crimes cibernéticos já ultrapassam trilhões de dólares anuais. Empresas sofrem com vazamentos de dados, ataques de *ransomware* e fraudes, o que afeta sua imagem institucional, credibilidade no mercado e estabilidade operacional.

Diante dessa realidade, torna-se indispensável uma atuação integrada entre Estado, sociedade civil e setor privado para conter os efeitos sociais dessa modalidade de crime. É necessário investir em políticas públicas voltadas à segurança digital, fomentar a educação midiática e digital nas escolas, fortalecer os mecanismos de denúncia e ampliar o acesso à justiça para as vítimas. Como ressalta Doneda (2019, p. 92), "a proteção da dignidade humana na sociedade da informação passa pelo reconhecimento do direito à segurança e à privacidade no ambiente digital". Portanto, o impacto social dos crimes cibernéticos é complexo e multifacetado.

Ele exige não apenas respostas punitivas, mas também preventivas, pedagógicas e reparatórias, com foco na proteção dos direitos fundamentais e na construção de um ambiente digital ético, seguro e acessível a todos. Assim também analisar o processo de investigação e as dificuldades de identificar o indivíduo a seguir.

## 3. CRIMES DIGITAIS: O PROCESSO DE INVESTIGAÇÃO E AS DIFICULDADE DE IDENTIFICAR O INDIVÍDUO.

As autoridades responsáveis pela justiça penal têm necessidade de novas habilidades técnicas e legais na investigação, impulsionadas pelo crescimento dos crimes virtuais. Diferente dos crimes comuns, os crimes cometidos *on-line* não deixam rastros físicos, o que faz da identificação do crime um dos maiores entraves para a punição penal.

A complicação aumenta porque, quase sempre, o criminoso é de longa data, anonimamente é protegido por várias camadas de criptografia e disfarces digitais. Contudo, o estelionato virtual no Brasil tem apresentado crescimento significativo nos últimos anos.

De acordo com o Anuário Brasileiro de Segurança Pública de 2024, houve um aumento de 13,6% nos casos de estelionato virtual entre 2022 e 2023. Além disso, uma pesquisa do Instituto DataSenado revelou que 24% da população brasileira com mais de 16 anos foi vítima de golpes virtuais nos últimos 12 meses, totalizando mais de 40 milhões de pessoas.

Esse cenário reflete a crescente migração de crimes do ambiente físico para o virtual, impulsionada pela popularização de tecnologias como o Pix e o aumento do uso de dispositivos móveis. Os criminosos tiram proveito de redes privadas virtuais (VPNs), servidores *proxy*, contas falsas e do navegador Tor, que dão acesso à *deep web e à dark web*, ou que dificultam a descoberta do IP original.

Para Moraes (2020, p. 214), “a sensação de que ninguém está vendo, criada pelo anonimato digital, estimula ações criminosas que dificilmente aconteceriam no mundo real, já que a chance de ser responsabilizado é maior”. Além disso, diversas infrações virtuais cruzam fronteiras, o que coloca as investigações em um cenário de jurisdição internacional.

Um mesmo crime pode ter vítimas em um país, servidores em outro e crimes em um terceiro, o que exige cooperação jurídica internacional. Segundo Silva (2019, p. 102), “a falta de um tratado internacional amplo e eficaz para crimes na internet causa problemas na coleta de provas e na concretização da justiça”.

Outro ponto fraco é a natureza instável das experiências digitais. Registros (logs), *e-mails*

e rastros de navegação são rápidos e podem ser apagados facilmente. Isso exige que as autoridades ajam e tenham conhecimento técnico sobre como coletar e guardar testes eletrônicos rapidamente. Como Sousa (2018, p. 167) destaca, “o tempo é crucial em crimes digitais: se demorar para tomar medidas, as provas podem ser perdidas para sempre”.

No Brasil, o Marco Civil da Internet (Lei nº 12. 965/2014) ajudou bastante ao criar regras sobre como salvar e liberar dados de conexão e acesso a aplicativos, dando segurança jurídica aos processos de investigação. No entanto, o acesso a esses dados depende de ordem judicial, o que, apesar de garantir a privacidade, pode atrasar as investigações, principalmente em casos urgentes. Ainda assim, muitas delegacias não têm o que precisam para lidar com crimes virtuais. A falta de equipamentos, pessoais especializados e bancos de dados integrados ainda é comum, especialmente fora das grandes cidades. A falta de delegacias que só cuidam de crimes virtuais prejudica a uniformidade e a qualidade das investigações.

Para que as apurações tragam resultados reais, é essencial turbinar a perícia de delegados, peritos e outros peritos do direito. Urge também estreitar a colaboração entre nações e autoridades, abrindo vias rápidas e eficazes para a troca de informações e dados. Como frisa Greco (2021, p. 318), “combater o crime digital requer um novo jeito de investigar, que una inteligência, tecnologia e parceria entre instituições. "

Assim, a saga para achar os criminosos em crimes virtuais tem mil rostos, com lanças técnicas, jurídicas e da máquina pública. Vencer esse desafio pede que o governo, empresas e entidades de fora joguem juntas, com leis que casem com o mundo digital. Existem diversos atores no enfrentamento dos crimes cibernéticos por exemplo delegados, juízes, policiais, contudo, a atuação do Ministério Público, destaca-se enquanto fiscal da lei, é o que vemos a seguir.

## 3.1. A Atuação do Ministério Público nos Crimes Virtuais.

Os promotores públicos são uma pedra angular do sistema de justiça brasileiro, desempenhando um papel fundamental tanto na prevenção quanto na repressão de atividades criminosas, principalmente no domínio digital. Dada a crescente complexidade dos delitos virtuais e seu amplo impacto na sociedade, é fundamental reforçar a atuação do Ministério Público no combate aos crimes cibernéticos.

Esses esforços, já essenciais em outras áreas, estão assumindo nova importância em decorrência dos problemas impostos pela tecnologia. Conforme previsto na Constituição Federal de 1988, o Ministério Público tem como atribuição institucional a ação penal pública privativamente, zelando pela observância das normas legais e pela defesa dos direitos coletivos e

individuais (BRASIL, 1988, art. 129, I e III). Em relação aos crimes virtuais, isso envolve iniciar processos criminais, supervisionar investigações, analisar inquéritos e proteger os direitos fundamentais das vítimas, que muitas vezes enfrentam degradação pública, golpes, violações de privacidade e tentativas de extorsão.

Para combater crimes cibernéticos de forma eficaz, os promotores públicos precisam de conhecimento técnico, aprendizado contínuo e colaboração com agências policiais especializadas. Greco (2021, pág. 326) destaca que “a complexidade dos crimes virtuais exige do Ministério Público uma atuação estratégica e não apenas reativa, pautada em inteligência e análise de dados digitais."

Nos últimos anos, vários gabinetes de promotores públicos estaduais e o Ministério Público Federal começaram a criar unidades especializadas em crimes cibernéticos, com promotores treinados para lidar com crimes como violações de dados, abuso sexual infantil *on-line*, difamação em mídias sociais e fraude bancária eletrônica. Essa especialização é realmente importante para que o parquet faça bem o seu trabalho, principalmente considerando a rapidez com que esses crimes acontecem e o quão instáveis as evidências digitais podem ser.

Além da punição, os promotores públicos também desempenham um papel significativo na educação e prevenção digital. Diferentes campanhas educacionais foram lançadas para conscientizar o público sobre segurança *online*, crimes de ódio e uso indevido de dados pessoais. Os promotores públicos também têm trabalhado ativamente para firmar Acordos de Ajustamento de Conduta (TACs) junto a plataformas e empresas de tecnologia, buscando compromissos dedicados a aprimorar a segurança digital e garantir a proteção dos consumidores.

Quando se trata de colaboração global, o Ministério Público do Brasil também se envolve em redes cooperativas para combater crimes transfronteiriços, especialmente aqueles que envolvem pornografia infantil, tráfico de dados e golpes internacionais. Como Silva e Cruz observaram em (2019, p. 213), "a natureza interconectada dos crimes digitais significa que o Ministério Público não deve apenas estar presente durante as investigações, mas deve realmente assumir a liderança na conexão com órgãos internacionais e de tecnologia."

Portanto, fica claro que o trabalho do Ministério Público em crimes cibernéticos não se resume apenas a apresentar acusações em tribunal; significa também coordenar diferentes instituições, fazer parte de políticas públicas, defender direitos básicos e adotar uma abordagem estratégica e proativa no mundo digital.

Em Goiás, o Ministério Público, por meio do *Cyber Gaeco*, investigou e denunciou quatro integrantes de uma organização criminosa especializada em crimes cibernéticos, incluindo estelionato virtual sedeada em São Paulo. Durante a investigação apurou-se que o os integrantes

da quadrilha tinham diferentes meios para fornecer laranjas a outros criminosos e enganar vítimas de vários Estados da Federação.

Os criminosos utilizavam perfis falsos em aplicativos de mensagens para aplicar golpes financeiros. As penas aplicadas somaram mais de 65 anos de prisão. O caso foi julgado pelo Tribunal de Justiça do Estado de Goiás, com base no artigo 171, § 2º-A, do Código Penal.

Dado o aumento dos crimes cibernéticos, é essencial fortalecer a agência estruturalmente, garantindo que haja mais promotores especializados, acesso a ferramentas digitais de investigação e maneiras de compartilhar informações rapidamente conforme elas acontecem. Lutar contra os delitos *online* não pode ser apenas tarefa do Judiciário e das forças de segurança. É um problema que pede a criação e a aplicação de políticas públicas que sejam completas, preventivas e educativas, envolvendo a proteção da comunidade digital. Dada a enorme expansão dos crimes na *internet*, o governo tem que fazer mais do que apenas reprimir: é crucial planejar, organizar e investir em ações que construam um espaço virtual que seja seguro, acessível e responsável.

Políticas públicas para a segurança digital são cruciais para organizar as instituições, definir o que é mais importante, distribuir os recursos e mobilizar a sociedade. Segundo Pinho e Silva (2021, p. 88), "o governo no mundo *on-line* deve juntar a repressão bem feita com políticas de educação digital, acesso à tecnologia e proteção de grupos mais frágeis, como crianças, idosos e mulheres". Essa maneira de encarar o problema é essencial para garantir que não apenas a queda na criminalidade, mas também a aplicação verdadeira dos direitos mais básicos no ambiente virtual.

No Brasil, algumas ações recentes mostram que estamos avançando nesse sentido. O Governo Federal, com a Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada em 2020, sugeriu caminhos para a proteção do espaço cibernético do país, desde a segurança das informações nos órgãos públicos até as campanhas para conscientizar a população. A política planeja ações em conjunto entre o Executivo, o Legislativo, o Judiciário, as empresas e as universidades, confirmando que os problemas relacionados aos crimes cibernéticos afetam todos (BRASIL, 2020).

Entretanto, nos estados e municípios, percebe se uma grande diferença na aplicação de políticas públicas para a segurança na *internet*. Em muitos lugares, ainda faltam delegacias especializadas e programas nas escolas que ensinam como usar a *internet* com segurança. A falta de uma política pública que todo o país contribui para que as vítimas se sintam sem justiça e proteção.

Um ponto importante é a necessidade de ensinar sobre o mundo digital desde cedo nas

escolas. Incluir temas como cidadania digital, uso consciente das redes, combate às notícias falsas e segurança *on-line* pode diminuir bastante os crimes e os perigos na *internet*. Como diz Doneda (2019, p. 92), “ensinar o usuário a pensar é uma das maneiras mais eficazes de evitar crimes virtuais, pois dá poder ao cidadão e aumenta sua proteção”.

Outro foco importante deve ser impulsionar a governança de dados em todas as agências governamentais. Infelizmente, violações de dados em instituições públicas se tornaram algo comum e alimentam golpes digitais, além de colocar a privacidade dos cidadãos em sério risco. A Lei Geral de Proteção de Dados Pessoais (Lei nº. 13.709/2018) é um grande avanço sem dúvida, mas colocá-lo em prática ainda exige conectar estratégias governamentais com iniciativas de conscientização.

Portanto, combater o crime cibernético precisa ser visto como uma tarefa de todos. O governo, em particular, precisa liderar o caminho criando políticas fortes baseadas em pesquisas sólidas, envolvendo diferentes agências trabalhando juntas e trazendo o público para a discussão. A segurança digital precisa de investimento, novas ideias e um compromisso moral para construir uma cultura de segurança e responsabilidade ao usar essas tecnologias.

## CONCLUSÃO

A pesquisa realizada possibilitou uma compreensão profunda e fundamentada dos impactos sociais gerados pelos delitos cibernéticos, evidenciando que tais atividades não apenas infringem normas legais, mas também enfraquecem laços sociais, desorganizam relações interpessoais e criam uma sensação de insegurança coletiva no espaço digital. A intensificação da digitalização na vida diária expõe às pessoas ameaças antes inexistentes, ampliando as repercussões de cada transgressão e tornando essas consequências crimes ainda mais complexos, silenciosos e, muitas vezes, irreversíveis.

A investigação relatou esses crimes declarados, desafios técnicos e jurídicos que dificultam a responsabilização dos infratores. O anonimato fornecido pelas tecnologias, a efemeridade das provas e a falta de cooperação internacional eficaz são elementos que prejudicam a efetividade da ação penal. A lentidão e a insuficiência de recursos nas delegacias agravaram o quadro, ressaltando a importância de um aparelho estatal que seja especializado e atualizado. Nesse contexto, destaca-se a importância do Ministério Público como agente fundamental na atuação contra os crimes cibernéticos. Sua atuação deve ser cada vez mais estratégica, colaborativa e em consonância com as novas realidades digitais.

A presença de promotoras especializadas e de iniciativas externas à educação digital e à

proteção de dados indica um progresso institucional necessário, embora ainda desigual entre as diferentes esferas federativas.

Finalmente, observamos que um enfrentamento eficaz desse tipo de criminalidade depende da coordenação das políticas públicas integradas, que transcendem a repressão e incluem a educação, a inclusão digital e a proteção de populações vulneráveis. A realização de programas nacionais, como a Estratégia de Segurança Cibernética, e a supervisão da Lei Geral de Proteção de Dados são passos relevantes, mas ainda são insuficientes ante a rápida evolução dos crimes virtuais.

Conclui-se, portanto, que a luta contra os crimes cibernéticos exige uma abordagem abrangente, envolvendo o sistema judiciário, os criadores de políticas públicas, a sociedade civil e o setor empresarial. Mais do que apenas penalizar, é necessário prevenir, proteger e educar, fomentando uma cultura de segurança digital que respeite a dignidade humana, promova direitos fundamentais e construa um ambiente virtual que seja mais ético, justo e seguro para todos.

## SOCIAL VULNERABILITY TO VIRTUAL TECHNOLOGY A COMPARATIVE ANALYSIS BETWEEN NETZDG AND THE BRAZILIAN SOLUTION


## ABSTRACT

This research presents the critical scenario of social vulnerability in the face of cybercrimes in Brazil, providing a brief analysis of the critical situation of the government in combating these crimes. In the last 10 years, we can clearly see how the advancement of technology in the world has brought society. It provides technological work tools such as social networks, banking applications, online sales and other utilities just a click away. In the case of Brazil, being the Latin American country that uses social networks the most, this article shows research done on how this modernity has also come with social and economic problems in the face of a society vulnerable to cybercrimes and the difficulty of applying Brazilian laws to combat these crimes. It also shows the need for digital education and a comparison of the German NetzDG Law with Brazilian regulations. Even with the change in the law bringing increased penalties for those who commit digital fraud, there has still not been a notable change in the behavior of these individuals. Technically, there is still a lack of improvement for a more efficient investigative process against these gangs. Even so, it is a consensus that simply punishing the crime does not solve the problem when there is an extreme need for more comprehensive digital education. Even with the General Data Protection Law - LGPD, there has not even been a decrease in these crimes, according to data from the last two years. However, this article provides a demonstration of the current scenario of crimes committed on digital platforms.


**KEYWORDS:** Virtual Technology; Cybercrimes; Responsibility of Providers

## REFERÊNCIAS

BRASIL. D**ecreto nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, sobre contratação no comércio eletrônico. Diário Oficial da União, Brasília, DF, 15 mar. 2013.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal e o Código de Processo Penal para dispor sobre crimes cibernéticos. Diário Oficial da União, Brasília, DF, 28 maio 2021.

BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998.** Regula os direitos autorais e dá outras providências. Diário Oficial da União, Brasília, DF, 20 fev. 1998.

BRASIL, **Vade Mecum**, Saraiva. Obra coletiva com a colaboração de Lívia Céspedes e Fabiana Dias da Rocha. Editorial de Legislação do Selo Saraiva Jur. 29ª ed. São Paulo: Saraiva, 2020. 400 p. (Legislação Brasileira).

CASTELLS, M. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Rio de Janeiro: Jorge Zahar, 2003.

CAVALCANTE, Márcio André Lopes. **Lei 14.155/2021: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato**. Publicado 29/05/2021. <https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html>. Acesso em: 02/05/2025, as 13:40.

CRESPO, R. C. **Criminalidade na era digital: aspectos penais e processuais**. São Paulo: Atlas, 2011.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP**. Publicado: 28/05/2021. <https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/>. Acesso em: 02/05/2025, as 17H.

DINO. **Brasil vive aumento no número de crimes cibernético.** Por Dino, 01/08/2023. <https://valor.globo.com/patrocinado/dino/noticia/2023/08/01/brasil-vive-aumento-no-numero-de-crimes-ciberneticos.ghtml>. Acesso em: 11/12/2024.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2013.

DONEDA, D. **O direito à prote0ção de dados pessoais**. São Paulo: Atlas, 2019.

FERREIRA, A. D. **Manual de direito penal e crimes de informática.** São Paulo: Revista dos Tribunais, 2001.

FERREIRA, A. D. **Manual de direito penal e crimes de informática.** São Paulo: Revista dos Tribunais, 2001.

GRECO, R. **Curso de direito penal**: **parte especial**. Volume III. 18. ed. Rio de Janeiro: Impetus, 2021.

JORGE, H. V. N.; WENDT, E. **Investigação criminal de crimes cibernéticos.** São Paulo: Saraiva, 2012.

MORAES, A. C. **Crimes cibernéticos e investigação criminal**. São Paulo: RT, 2020.

MULLER, Leticia Sabbadine. **Manual de Educação digital, cibercidadania e prevenção de crimes cibernéticos: Noções de Compliance na Educação Digital.** São Paulo - SP: Editora JusPODIVM, 2021.

PACETE, Luiz Gustavo. **Brasil é o terceiro maior consumidor de redes sociais em todo o mundo.** <https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>. Acesso em: 08/12/2024.

PINHO, J. A. G.; SILVA, M. P. **Políticas públicas de segurança digital no Brasil**. Brasília: Enap, 2021.

REISDORFER, D. M. **Cidadania digital e segurança da informação**. In: SOUSA JUNIOR, J. A. et al. (org.). Direito e internet: desafios contemporâneos. São Paulo: Revista dos Tribunais, 2020. p. 209–225.

SCHREIBER, Mariana - @marischreiber. **A controversa lei alemã que inspira projeto de lei das Fake News.** Da BBC News Brasil em Brasília. 26 agosto 2020. <https://www.bbc.com/portuguese/brasil-53914408>. Acesso em: 11/12/2024.

SILVA, D. J. **Cooperação internacional no combate aos crimes cibernético**s. São Paulo: Saraiva, 2019.

SOUSA, F. H. **Provas digitais no processo penal: desafios e perspectivas.** Belo Horizonte: D'Plácido, 2018.

TEIXEIRA, M. F. **Crimes cibernéticos: prevenção, repressão e cooperação jurídica internacional.** Curitiba: Juruá, 2014.

TRUZZI, Gisele. **Manual de Educação digital, cibercidadania e prevenção de crimes cibernéticos: Fraudes e Crimes Eletrônicos: Como se Proteger e Combater.** São Paulo - SP: Editora JusPODIVM, 2021.

VIANA, T.; MACHADO, F. **Crimes informáticos e proteção penal**. Belo Horizonte: Fórum, 2013.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Brasília: Câmara dos Deputados, 1999. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: [Acesso em: 04 de junho de 2025].

Brasília: **ANPD**, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd>. Acesso em: 23 maio 2025.

NOWCY. **Cyrela é a 1ª empresa a violar a LGPD e ser condenada.** São Paulo: Nowcy, 2020. Disponível em: <https://nowcy.com.br/cyrela-e-a-1a-empresa-a-violar-a-lgpd-e-ser-condenada/>. Acesso em: 23 maio 2025.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Art. 129, incisos I e III.