CENTRO UNIVERSITÁRIO DE BELO HORIZONTE
BARCHARELADO EM DIREITO

A TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS:
Uma análise da adequação das leis existentes para lidar com os desafios e especificidades dos crimes cometidos no ambiente digital

Luiz Fernando Costa

Belo Horizonte
2023

Luiz Fernando Costa

A TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS:

Uma análise da adequação das leis existentes para lidar com os desafios e especificidades dos crimes cometidos no ambiente digital

Artigo científico apresentado ao Centro Universitário de Belo Horizonte, como requisito de cumprimento do componente curricular obrigatório: Trabalho de Conclusão de Curso.

Belo Horizonte

2023

A TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS

THE TYPIFICATION OF CYBER CRIMES

Resumo

Este artigo aborda a tipificação de crimes cibernéticos no âmbito jurídico, analisando como as leis atuais enfrentam os desafios do ambiente digital.

A pesquisa avalia a eficácia dessas leis na repressão e punição de crimes cibernéticos.

A abordagem inclui uma revisão detalhada da legislação sobre crimes cibernéticos e uma análise crítica de suas possíveis lacunas e pontos de menor eficácia, ilustradas por estudos de caso que destacam obstáculos enfrentados pelas especificidades das condutas realizadas no ambiente digital.

Os resultados indicam deficiências significativas na punição e prevenção eficazes, sugerindo o debate para reformas legislativas contínuas devido às complexidades do ambiente digital, como anonimato, jurisdições e evolução das técnicas de fraude.

Descobertas apontam para a necessidade de reformas ágeis e adaptáveis às novas ameaças, proporcionando um arcabouço legal robusto para combater crimes cibernéticos.

A conclusão destaca os desafios das reformas legais, sublinhando a importância de manter equilíbrio entre proteção dos direitos individuais e segurança cibernética.

Este estudo contribui para discussões sobre reformas legislativas e diretrizes eficazes na prevenção dos crimes cibernéticos, reconhecendo a necessidade de equilíbrio entre direitos individuais e segurança cibernética.

Palavras-chave: Crimes cibernéticos. Eficácia. Legislação. Reformas legislativas. Segurança cibernética.

Abstract

This article addresses the classification of cybercrimes in the legal sphere, examining how current laws face the challenges of the digital environment.

The research assesses the effectiveness of these laws in suppressing and punishing cybercrimes.

The approach includes a detailed review of legislation on cybercrimes and a critical analysis of possible gaps and less effective points, illustrated by case studies highlighting obstacles faced by the specificities of conduct in the digital environment.
The results indicate significant deficiencies in effective punishment and prevention, suggesting a debate for ongoing legislative reforms due to the complexities of the digital environment, such as anonymity, jurisdictions, and the evolution of fraud techniques.
Findings point to the need for agile and adaptable reforms to address new threats, providing a robust legal framework to combat cybercrimes.
The conclusion highlights the challenges of legal reforms, emphasizing the importance of maintaining a balance between protecting individual rights and cybersecurity.
This study contributes to discussions on legislative reforms and effective guidelines in preventing cybercrimes, recognizing the need for a balance between individual rights and cybersecurity.

Key-words: Cybercrimes. Effectiveness. Legislation. Legislative reforms. Cybersecurity.

SUMÁRIO

1 INTRODUÇÃO 3

2 CRIMES CIBERNÉTICOS NO DIREITO PENAL BRASILEIRO: UMA REVISÃO ABRANGENTE 4

2.1 O conceito de crime cibernético 5

2.2 Estelionato e crimes conexos 6

2.2.1 Crimes contra a honra 6

3 LEIS PENAIS E CRIMES CIBERNÉTICOS: ANÁLISE NO CONTEXTO BRASILEIRO 7

3.1 Código Penal Brasileiro e os desafios da adaptação à era digital 8

3.2 A Lei Carolina Dieckmann: (in)eficácia e modificações 10

3.3 Lei Geral de Proteção de Dados e a busca por segurança digital 12

3.4 Lei 14.132/2021 e o *cyberstalking* 14

4 CONSIDERAÇÕES FINAIS 17

REFERÊNCIAS 19

1 INTRODUÇÃO

Os crimes cibernéticos estão se tornando um grande desafio para as ciências jurídicas no mundo moderno, marcado pelo rápido avanço das tecnologias da informação. O objetivo deste artigo é realizar uma análise completa da tipificação dos crimes de fraude cibernética usando as leis penais em vigor. O estudo começa com uma breve explicação do contexto do problema de pesquisa, o que facilita a compreensão da situação.

A revolução tecnológica da última década causou mudanças significativas nas interações humanas, na economia e na sociedade em geral. O surgimento da internet e outras tecnologias digitais abriu caminho para um novo paradigma na comunicação e na interconexão mundial. No entanto, o ambiente digital em constante expansão levou à proliferação dos crimes virtuais. Neste contexto, os delitos convencionais se mudaram para o mundo virtual, colocando o sistema jurídico em situações inéditas. O Brasil está entre os países mais afetados pelos crimes cibernéticos. Pesquisa estatística apontou que cerca de 42 milhões de brasileiros são afetados pelos crimes cibernéticos. (DINO, 2017, online).

A focalização deste estudo recai sobre um problema de relevância inegável: a capacidade das leis penais atuais em lidar com eficácia com a complexidade dos crimes de fraude cibernética. O problema em questão é claramente identificado e delimitado. Concentramo-nos na abordagem teórica e metodológica de aspectos específicos e elementos do problema, enquanto consideramos um período específico.

Esta pesquisa tem um objetivo claro: avaliar a eficácia das disposições legais atuais para lidar com os desafios impostos pela fraude cibernética. Além disso, buscamos entender como as leis relacionadas a esse tipo de crime se adaptam ao cenário digital em rápido desenvolvimento. Ao realizar uma investigação abrangente, esperamos fornecer informações que ajudem a contribuir com o debate de reformas legais sensatas e políticas eficazes.

A relevância deste estudo é multifacetada. Do ponto de vista técnico, ele aborda a necessidade urgente de adaptação das estruturas legais às demandas da era digital. Socialmente, reconhece a importância de proteger indivíduos e instituições contra os impactos prejudiciais dos crimes cibernéticos. No âmbito acadêmico, enriquece o debate acadêmico sobre o panorama jurídico em constante evolução. Política e legalmente, esta pesquisa busca contribuir com reflexões e fundamentos necessários

para possíveis alterações legais essenciais, a fim de combater efetivamente a fraude cibernética.

Neste contexto, identificamos a lacuna de pesquisa: a potencial necessidade de ajustes nas leis penais para acompanhar as ameaças digitais em constante mutação. A hipótese central que norteia este estudo é que as leis penais atuais podem não ser completamente adequadas para abordar os desafios específicos dos crimes cibernéticos. Essa hipótese será avaliada com base na revisão da literatura existente, mantendo-se atualizada, e levando em consideração os limites cognitivos das teorias pertinentes.

Para realizar este artigo científico, será utilizada uma abordagem que combina pesquisa bibliográfica e análise crítica da legislação em vigor. A revisão da literatura se concentrará em autores pertinentes no campo das ciências jurídicas, selecionando fontes com base em pertinência e atualidade. O tema será abordado por meio de uma análise crítica da legislação, que avaliará a eficácia das leis penais atuais em vários contextos jurídicos.

O objetivo deste estudo é fornecer uma análise abrangente das questões legais relacionadas à fraude cibernética. Ele contextualiza o problema, define os objetivos e a metodologia da pesquisa, destaca a importância da pesquisa e sugere uma hipótese para que seja discutida, considerando a importância da adaptação ao mundo digital contemporâneo. A estrutura do artigo a seguir seguirá essa introdução e abordará cada um desses tópicos com mais profundidade.

2 CRIMES CIBERNÉTICOS NO DIREITO PENAL BRASILEIRO: UMA REVISÃO ABRANGENTE

Uma nova categoria de crimes conhecida como crimes cibernéticos surgiu como resultado da crescente interconexão criada pela tecnologia digital. Esses crimes são tipificados e regulamentados pelo Direito Penal brasileiro. Nesta seção, examinaremos as principais características desses crimes à luz da legislação brasileira, identificando suas categorias e destacando exemplos pertinentes para demonstrar suas complexidades e consequências no contexto nacional.

A legislação penal atual, em um contexto de rápidas mudanças sociais e avanços tecnológicos, frequentemente apresenta falhas que são preenchidas por interpretações análogas, as quais divergem da intenção original do legislador na

norma. No entanto, tanto o Código Penal, em seu artigo 1°, quanto a Constituição Federal, no artigo 5°, inciso XXXIX, estabelecem a impossibilidade de se recorrer a interpretações análogas que seriam "*in malam partem*," o que não é permitido pelo princípio da legalidade. Tal princípio proíbe a utilização de analogia no Direito Penal em situações que possam prejudicar o agente da conduta, como leciona Guilherme de Souza Nucci:

> [...] se noutros campos do Direito a analogia é perfeitamente aplicável, no cenário do Direito Penal ela precisa ser cuidadosamente avaliada, sob pena de ferir o princípio constitucional da legalidade (não há crime sem lei que o defina; não há pena sem lei que a comine). Nesse caso, não se admite a analogia in malam partem, isto é, para prejudicar o réu. (NUCCI, 2017, p.36).

Portanto, a aplicação da analogia só é admissível quando beneficia a pessoa a quem a prática do ato ilícito é atribuída, o que, de fato, impõe restrições à aplicação das leis diante de inúmeras lacunas, deixando a penalização desses atos sujeita a desafios.

2.1 O conceito de crime cibernético

Doutrinariamente, inexiste consenso acerca do conceito de crime cibernético. A complexidade e a dinâmica desse campo específico da criminalidade digital desafiam a criação de uma nomenclatura única e consolidada. Diversos termos têm sido utilizados para descrever atividades ilícitas que envolvem o uso de dispositivos informáticos, a manipulação de redes de transmissão de dados e a lesão a bens jurídicos, entre outros aspectos relevantes. Nesse contexto, é fundamental explorar as nuances dessa discussão para compreender a variedade de perspectivas e abordagens adotadas pelos estudiosos do tema.

Corroborando com esse entendimento, “não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos.” (DA SILVA, 2015, p.39)

De forma sucinta, crimes cibernéticos podem ser definidos como atividades ilegais realizadas por meio do uso de dispositivos informáticos, independentemente de estar conectados à internet. Esses crimes também incluem ações criminosas dirigidas contra equipamentos tecnológicos, sistemas de informação ou bases de

dados. Essas ações criminosas exploram as falhas do mundo digital, como fraudes e invasões até a disseminação de códigos maliciosos. O núcleo dos crimes cibernéticos reside na violação das regras e padrões que regulam o uso ético e legal da tecnologia. Isso coloca a legislação penal moderna em constante desafio.

2.2 Estelionato e crimes conexos

O estelionato, previsto no artigo 171 do Código Penal Brasileiro, é um crime que envolve o uso de artifícios para enganar alguém e obter vantagens indevidas. A fraude cibernética muitas vezes se enquadra nessa categoria, incluindo casos de phishing e golpes online, mantendo a vítima em erro com o objetivo de obter vantagem. Assim define Assunção (2021):

> Tratando-se do crime de estelionato no ambiente da internet, o sujeito ativo mantém a vítima em erro, sob a finalidade de obter vantagem ilícita para si próprio. Também considera-se crime cibernético exaltar ou elogiar criminoso ou ato criminoso de maneira pública, caracterizando crime de apologia de crime ou de criminoso. (ASSUNÇÃO, 2021, p.8)

Nesse sentido, destaca-se a dinâmica específica desse delito digital. No estelionato online, o sujeito ativo busca manter a vítima em erro com o objetivo de obter vantagem ilícita para si próprio. Essa definição ressalta a continuidade do princípio fundamental do estelionato, que envolve enganar e ludibriar outra parte para alcançar vantagem indevida.

Ao tratar do estelionato no ambiente virtual, é crucial considerar as particularidades desse cenário, onde os meios digitais oferecem novas oportunidades para a prática desse crime. A agilidade e a globalidade da internet proporcionam um campo fértil para ações fraudulentas, exigindo uma adaptação constante das leis e dos mecanismos de combate.

Outros delitos de violações de patrimônio, como a obtenção não autorizada de dados pessoais como informações bancárias, ou o desvio de recursos financeiros, são frequentemente associadas a crimes cibernéticos. Alguns artigos do Código Penal Brasileiro abordam essas infrações, como o 155, § 4º, II, que trata do furto mediante fraude.

2.2.1 Crimes contra a honra

Com relação aos crimes contra a honra, observa-se uma preocupante escalada desse tipo de conduta criminosa nos últimos anos, uma vez que cada vez mais surgiram ferramentas de mídia e redes sociais que, se por um lado, facilitaram a comunicação entre pessoas do mundo todo, também facilitaram o cometimento de crimes dessa natureza por trás das telas dos smartphones, computadores e outros dispositivos que disponibilizam o acesso à rede.

> Outra modalidade de delito tipificado no código incriminador que se adequa aos chamados crimes cibernéticos impróprios, diz respeito aos crimes que tem por objetivo tutelar o bem jurídico honra. Calúnia, difamação e injúria, crimes contra a honra elencados respectivamente nos artigos 138, 139 e 140 do Código Penal, são infrações que ganharam maior amplitude, através da utilização de ferramentas informáticas como as mídias sociais, blogs, sites, aplicativos de comunicação, dentre outros, que facilitam e dinamizam o cometimento desses ilícitos. (MATSUYAMA E LIMA, 2017, p.7).

Nessa seara, Matsuyama e Lima (2017) destacam a evolução e a ampliação dos crimes contra a honra, especialmente os previstos nos artigos 138, 139 e 140 do Código Penal. A mudança nas dinâmicas sociais, impulsionada pelo advento da internet e das mídias sociais, trouxe uma nova dimensão para esses delitos. A utilização de plataformas digitais como mídias sociais, blogs, sites e aplicativos de comunicação proporcionou uma maior amplitude e eficiência na prática dessas infrações. O alcance potencialmente ilimitado dessas ferramentas e sua capacidade de facilitar a propagação rápida de informações contribuem para a dinamização e intensificação dos crimes contra a honra.

3 LEIS PENAIS E CRIMES CIBERNÉTICOS: ANÁLISE NO CONTEXTO BRASILEIRO

A análise dos crimes de fraude cibernética no Brasil requer uma compreensão aprofundada das leis penais brasileiras e de como essas leis se aplicam aos crimes virtuais. Serão examinadas importantes leis penais brasileiras relacionadas a crimes cibernéticos, destacando sua estrutura e o quão eficazes são para o combate à crimes digitais.

No Brasil, o sistema legislativo adota o princípio da reserva legal, respaldado pela Constituição da República e pelo Código Penal. Observa-se, então, a existência

da exclusividade da lei para a criação e definição de crimes e contravenções penais, assim como a cominação de suas respectivas penas.

> Não há crime, sem lei anterior que o defina. Especialmente quando tratamos de tecnologia da informação, a técnica para criar leis deve ser outra. Isto porque o legislador deve ter o cuidado para que não conceba uma ordenação jurídica natimorta, que ingressa no arcabouço legislativo de modo ultrapassado. (JESUS E MILAGRE, 2016, p.13).

É pertinente, então, uma reflexão acerca da dinâmica da legislação em relação à tecnologia da informação. Ao afirmar que "não há crime sem lei anterior que o defina", Jesus e Milagre (2016) ressaltam a importância da clareza e especificidade das normas legais, particularmente em um cenário tão dinâmico quanto a tecnologia da informação.

A tipificação dos crimes cibernéticos está fundamentada no Código Penal Brasileiro, bem como em legislações complementares. É essencial analisar como essas leis abordam as condutas específicas relacionadas à fraude cibernética e como os tipos penais estão definidos. Dentre as leis e regulamentações relevantes, destaca-se o Código Penal, que contém disposições relacionadas a crimes cibernéticos, como estelionato, furto mediante fraude e difamação (além de outros crimes contra a honra), a Lei Nº 12.737/2012 (Lei Carolina Dieckmann) que estabeleceu penalidades específicas para invasão de dispositivos informáticos e obtenção não autorizada de dados, a Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados) que regulamenta o tratamento de dados pessoais e prevê sanções administrativas em casos de vazamento de dados pessoais, o que está diretamente relacionado a crimes cibernéticos e a Lei Nº 14.132/2021, que trouxe a previsão legal dos crimes de *stalking* e *cyberstalking*, em um importante movimento contra práticas criminosas que cada vez mais são frequentes, tanto no meio físico quanto no ambiente virtual.

3.1 Código Penal Brasileiro e os desafios da adaptação à era digital

O Código Penal Brasileiro, promulgado em 1940, é um pilar fundamental do sistema jurídico nacional. No entanto, ao enfrentar os desafios trazidos pelos crimes cibernéticos, que ocorrem à medida que a tecnologia avança e, consequentemente, dá margem para que novas ações criminosas sejam tomadas no ambiente virtual,

torna-se pertinente a discussão acerca de atualização na legislação, para que possa melhor se adequar ao avanço tecnológico e novas formas de condutas criminosas.

Segundo o ministro do Superior Tribunal de Justiça, Rogerio Schietti, o Direito não está totalmente preparado para enfrentar desafios do desenvolvimento cibernético e à criminalidade digital, como visto em Galli (2017):

> [...] a tecnologia de troca de dados proporcionada pela internet tem características que “atraem” a prática de crimes, como o anonimato, dificuldades de rastreamento, abrangência potencialmente ilimitada de vítimas, eficiência e rapidez na troca de informações, inexistência de fronteiras e debilidade dos meios de tutela penal. (GALLI, 2017, online)

Schietti aborda de maneira perspicaz as características peculiares da tecnologia de troca de dados pela internet, destacando como essas características podem incentivar a prática de crimes. A análise do Ministro ressalta vários aspectos cruciais que tornam o ambiente digital propício para atividades ilícitas. A menção ao anonimato destaca a facilidade com que os criminosos podem ocultar sua identidade online, dificultando as investigações e tornando o rastreamento uma tarefa desafiadora. A abrangência potencialmente ilimitada de vítimas evidencia a escala global dos crimes cibernéticos, onde um ataque pode afetar múltiplos indivíduos, organizações ou até mesmo países.

A rapidez e eficiência da troca de informações na internet são apontadas como um fator favorável para os criminosos, pois permitem a propagação instantânea de dados maliciosos. A menção à inexistência de fronteiras destaca a natureza transnacional dos crimes cibernéticos, muitas vezes ultrapassando as jurisdições tradicionais.

Além disso, a referência à debilidade dos meios de tutela penal indica um desafio enfrentado pelas autoridades legais na proteção contra crimes online, revelando a importância de se debater a necessidade de instrumentos legais mais robustos e adaptados ao ambiente digital.

A aplicação de alguns tipos penais tradicionais, como estelionato e furto mediante fraude, demanda interpretações elásticas para abarcar as nuances dos crimes virtuais. A adaptação do Código Penal à dinâmica do mundo digital é vital para assegurar uma resposta jurídica eficaz e proporcional à natureza dessas práticas. A constante evolução das técnicas virtuais exige uma revisão contínua, garantindo que a legislação esteja alinhada com os desafios emergentes.

3.2 A Lei Carolina Dieckmann: (in)eficácia e modificações

A Lei Nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi criada em resposta a um caso de repercussão nacional envolvendo o vazamento de fotos íntimas da atriz Carolina Dieckmann na internet. Sancionada em dezembro de 2012, a legislação teve como objetivo principal criminalizar condutas relacionadas a crimes cibernéticos, em particular, a invasão de dispositivos informáticos e a obtenção não autorizada de dados.

Essa lei foi criada principalmente para preencher lacunas na legislação brasileira sobre delitos cometidos no ambiente digital. O estabelecimento de mecanismos legais que coibissem e punissem práticas danosas nesse contexto foi necessário porque, antes de sua promulgação, o ordenamento jurídico carecia de dispositivos específicos para lidar com as crescentes ameaças cibernéticas.

A referida lei trouxe ao Código Penal brasileiro o acréscimo dos arts. 154-A e 154-B, cuja transcrição original era:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa [...]
>
> 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 artigos 266 e 298 do mesmo diploma penalista foram modificados pela mencionada lei, que consideram as ações realizadas com tais dispositivos, crimes cibernéticos.

Entretanto, como qualquer legislação, a Lei Carolina Dieckmann trouxe desafios e fragilidades. Diversas críticas, então, surgiram, sendo as principais acerca da punição estabelecida, considerada branda para o avançar da tecnologia e o contexto atual, já que em um ambiente virtual cada vez mais integrado aos aspectos de vida pessoais da sociedade, condutas criminosas cometidas nesse âmbito se tornam cada vez mais graves e causam danos cada vez maiores às vítimas.

Também foi alvo de ferrenhas críticas o fato de a redação legislativa apenas prever a conduta criminosa “mediante violação indevida de mecanismo de segurança”. Tal previsão foi considerada inadequada, já que nem sempre as condutas criminosas se dão mediante a referida violação.

Em 2021, foi então promulgada a Lei 14.155/2021, que veio a alterar a Lei Carolina Dieckmann trazendo alterações aos pontos acima destacados, com penas mais rígidas para os infratores e retirando o requisito de ser a conduta “mediante violação indevida de mecanismo de segurança”, entre outras alterações.

> Art. 154-A – Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

Todavia, uma crítica relevante que permanece até os dias atuais é relacionada ao núcleo do tipo penal. A observação de que o verbo "invadir" não reflete de maneira adequada uma conduta informática. O termo utilizado pelo legislador remete a uma conduta dotada de violência ou ameaça, o que é pouco comum em crimes cometidos no ambiente virtual. Na maioria das vezes, o hacker se vale de alguma falha de segurança ou até mesmo da anuência da vítima para consolidar a conduta criminosa, como visto em Castro (2012).

> Ou seja, em nenhum de acesso remoto se pode dizer que o agente mal-intencionado agiu de modo violento para obter os dados do usuário. O que houve foi o emprego de ardil. Para resumir o que se sucede nesses casos, acaba sendo o próprio usuário a permitir que seus dados sejam acessados. Desta maneira, embora cotidianamente se noticiem invasões de determinado servidor e ou empresa por hackers que invadiram seus sistemas e acessaram informações indevidamente, o que se deve ter em mente é que isso só foi possível porque o próprio usuário assim o permitiu, ainda que por desconhecimento sobre o funcionamento do sistema computacional e por isso mesmo foi vítima de um ardil. (CASTRO, 2012, online)

No trecho, o professor e advogado Luiz Augusto Sartori de Castro traz uma perspectiva crítica e esclarecedora sobre o termo "invadir" no contexto da Lei Carolina Dieckmann, destacando a ausência de violência física ou acesso remoto violento por parte do agente mal-intencionado, ressaltando que, na maioria dos casos, o que ocorre é a utilização de ardil. Essa observação é crucial para compreender a natureza das ações cibernéticas, nas quais o usuário muitas vezes inadvertidamente permite o acesso aos seus dados.

A ênfase na participação involuntária do próprio usuário, que finalmente permite o acesso a seus dados por meio de artifícios, destaca a importância da conscientização e da educação digital. A necessidade de medidas preventivas, como a promoção da cibersegurança e a conscientização sobre práticas seguras de uso de dispositivos digitais, é reforçada pela menção de que a intrusão é possível devido ao desconhecimento do usuário sobre como funciona um sistema computacional.

Essa perspectiva ressalta a complexidade das interações cibernéticas e a necessidade de abordagens legislativas que tenham em conta não apenas atividades criminosas, mas também a conscientização para mitigar vulnerabilidades e prevenir práticas prejudiciais no ambiente digital.

3.3 Lei Geral de Proteção de Dados e a busca por segurança digital

A Lei Geral de Proteção de Dados (Lei Nº 13.709/2018), emergiu como resposta legislativa à crescente preocupação com a privacidade e segurança dos dados pessoais no ambiente digital. A lei enfatiza a proteção de dados pessoais, dando aos titulares mais controle sobre suas informações.

Acerca da definição do termo dados pessoais, a própria Lei Geral de Proteção de Dados traz em seu artigo 5º, inciso I, a definição, *in verbis*: “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;”. Isso quer dizer, que, em outras palavras, na definição trazida pelo dispositivo legal, dado pessoal é aquele que permite identificar uma pessoa, seja essa identificação de forma direta ou indireta.

Diante disso, a proteção aos dados pessoais proteção não apenas protege as pessoas (seja pessoa natural ou pessoa jurídica) contra o uso indevido de suas informações, mas também torna o local mais seguro, buscando dificultar com que os cibercriminosos obtenham dados sensíveis explorando vulnerabilidades.

Para o descumprimento de suas disposições, a legislação impõe penalidades severas. As consequências incluem advertências, multas que podem chegar a valores expressivos e a possibilidade de proibição do tratamento de dados. Em seu artigo 52, a Lei Geral de Proteção de Dados elenca as sanções administrativas previstas, e essas punições funcionam como um forte dissuasor, forçando as empresas a adotar medidas rígidas de segurança cibernética. Dessa forma, a Lei Geral de Proteção de Dados ajuda na prevenção de vazamentos de dados estabelecendo rigorosos

requisitos de segurança. Empresas devem adotar práticas avançadas de cibersegurança para evitar o acesso não autorizado e proteger dados sensíveis de ataques cibernéticos.

Todavia, ainda assim há registros de casos de vazamento de dados. No Brasil, o caso Cyrela foi conhecido como o primeiro a ter uma empresa condenada sob a ótica da Lei Geral de Proteção de Dados, como vemos em Demartini (2020):

> O caso envolve um cliente que comprou um apartamento em novembro de 2018 e, na sequência, passou a receber ligações indesejadas de instituições financeiras e empresas de decoração oferecendo serviços associados à aquisição do imóvel. Na visão da juíza Tonia Yuka Koroku, da 13ª Vara Cível de São Paulo, a Cyrela não apenas infringiu normas da LGPD como também direitos previstos no Código de Defesa do Consumidor e da própria Constituição. (DEMARTINI, 2020, online)

O caso exemplifica as implicações legais e éticas de vazamentos de dados, sinalizando para as empresas a necessidade urgente de implementar medidas robustas de segurança e transparência. O episódio ressalta a importância de uma abordagem cuidadosa na gestão de dados pessoais, não apenas para evitar implicações legais, mas também para preservar a confiança do consumidor e a reputação da empresa no mercado. Esse tipo de incidente destaca a relevância crescente da proteção de dados em um cenário onde a privacidade dos indivíduos é cada vez mais valorizada e regulamentada.

Todavia, apesar de haver grande apelo nos tribunais pela incidência da Lei Geral de Proteção de Dados em diversos casos, a ocorrência de punições de natureza indenizatória não é o que se verifica em maioria, via de regra. Um levantamento feito sobre o ano de 2021 evidencia que, de 465 decisões relacionadas à Lei Geral de Proteção de Dados, expressivos 77% delas não resultaram em condenação (PAIVA, 2022).

Esse cenário pode indicar diferentes interpretações judiciais, complexidades na aplicação da lei ou, em alguns casos, a necessidade de ajustes nas estratégias de ação. Além disso, é importante lembrar que a Lei Geral de Proteção de Dados é uma legislação relativamente nova. O grande número de decisões que não resultaram em condenações pode ser uma indicação de que as empresas e organizações estão na fase inicial de adaptação às novas exigências. As decisões judiciais podem mudar conforme a maturidade das práticas de proteção de dados avança. Isso nos dá uma

compreensão mais profunda da interpretação e aplicação da Lei Geral de Proteção de Dados.

Conclui-se então que é necessário observar a complexidade e a dinâmica do cenário jurídico em torno da Lei Geral de Proteção de Dados. À medida que mais casos são julgados, será fundamental o entendimento jurisprudencial, contribuindo para a consolidação de parâmetros consistentes no tratamento das questões relacionadas à proteção de dados no Brasil.

3.4 Lei 14.132/2021 e o *cyberstalking*

É notável que a legislação brasileira vem evoluindo à medida que surgem as necessidades de adaptações aos novos meios de interações humanas que a tecnologia proporciona.

As redes sociais ganharam extrema popularidade na última década, fazendo com que as relações entre pessoas fossem encurtadas. O contato nunca foi tão fácil e simplificado, tornando possível interações entre pessoas de praticamente quaisquer lugares e, principalmente, a possibilidade de acompanhar a rotina de outras pessoas. Nesse sentido, merece destaque a Lei 14.132/2021, que tipificou uma das mais importantes condutas criminosas que existem nas redes: o *cyberstalking*.

Antes de nos debruçarmos sobre o *cyberstalking* e seu conceito, é necessário compreender ao conceito da mesma conduta, porém no meio físico, denominada como *stalking*.

Stalking é um termo da língua inglesa derivada do verbo *to stalk*, que pode ser interpretado como perseguir, vigiar, espionar. A motivação da prática pode ser dar por diversas razões, sendo uma das mais comuns entre elas, a título exemplar, o epílogo de um relacionamento amoroso, onde uma das partes envolvidas não se conforma com a decisão de outra e viola sua integridade, a princípio, psicológica, normalmente de maneira repetitiva e incessante, podendo escalar para situação mais grave como atentar à integridade física ou até mesmo à vida. Segundo a psicóloga e criminóloga italiana Alessia Micoli:

> [...] o *stalking* é uma forma de agressão psicológica e física direta, que visa sobrepujar a vontade da vítima, destruir sua moral e sua capacidade de resistência por meio de um gotejamento incessante, em um contexto de crescente perseguição, insistente como os pingos que, com o passar do tempo, escavam a pedra. O stalker persegue, ameaça, maltrata a vítima,

> fazendo com que nasça nesta um estado de ansiedade e medo que pode chegar a comprometer o desenvolvimento normal do seu cotidiano. (2012 apud AMIKY, 2014, p. 12-13)

Portanto, destaca-se de maneira eloquente a complexidade e a gravidade do fenômeno do *stalking*, transcendendo a mera definição de perseguição. Ao descrever o comportamento do agressor como um "gotejamento incessante," a metáfora adotada ilustra vividamente a persistência e a insidiosidade desse tipo de violência. O impacto não se limita apenas à esfera psicológica da vítima; há uma clara intenção de minar sua resistência e moral.

A analogia com os "pingos que escavam a pedra" evoca a imagem de um processo gradual, mas implacável, sugerindo que, ao longo do tempo, o *stalking* pode corroer a integridade emocional da vítima. A abordagem holística da agressão, incorporando aspectos físicos e psicológicos, destaca a necessidade de uma compreensão mais aprofundada desse fenômeno, não apenas como uma forma de perseguição, mas como uma estratégia de agressão multifacetada.

A partir disso, surge então o conceito de *cyberstalking*, trazendo uma adaptação da conduta anteriormente conhecida para o mundo virtual. No *cyberstalking*, o agente utiliza dos meios virtuais para perturbar a vítima de forma indesejável. Segundo Brito (2013):

> [...] a exemplo do que ocorreu com o bullying, o *stalking* ganhou uma ferramenta que facilitou o serviço do perseguidor (stalker), e potencializou os danos causados às vítimas. Emails, tweets, visitas de perfil e até as famosas “cutucadas” podem servir de exemplos de novos meios de execução proporcionados pelo uso da internet, passando com isso a denominar-se *Cyberstalking*. (BRITO, 2013, p. 84)

Portanto, para se caracterizar o *stalking virtual*, é imprescindível que a conduta seja por meios digitais como redes sociais, e-mails etc. No mesmo sentido, corrobora Crespo (2022):

> O *cyberstalking* é, portanto, o uso da tecnologia para perseguir alguém e se diferencia da perseguição “offline” (ou mero *stalking*) justamente no que tange o modus operandi, que engloba o uso de equipamentos tecnológicos e o ambiente digital. Além disso, o *stalking* e o *cyberstalking* podem se mesclar, havendo as duas formas concomitantemente. O stalker –indivíduo que pratica a perseguição – mostra-se onipresente na vida da sua vítima, dando demonstrações de que exerce controle sobre ela, muitas vezes não se limitando a persegui-la, mas também proferindo ameaças e buscando ofendê-la ou humilhá-la perante outras pessoas. Curiosamente o *cyberstalking* é cometido, muitas vezes, não por absolutos desconhecidos, mas por pessoas

> conhecidas, não raro por ex-parceiros como namorados, ex-cônjuge, etc. (CRESPO, 2022, online)

Outro fator crucial para a caracterização do *cyberstalking* é a violação da privacidade da vítima sem sua autorização, ou seja, a perseguição de forma indevida e contra a vontade da vítima.

Nesse sentido, em 2021 a Lei 14.132 veio a alterar o Código Penal brasileiro trazendo a tipificação da conduta de *stalking*, assim como o *cyberstalking*, com a seguinte redação:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

Observando ao disposto na legislação, destacam-se alguns pontos importantes que corroboram com o conceito de ambos os crimes. Ao empregar o termo “reiteradamente”, o legislador foca em deixar claro que a essência da conduta de *stalking* (ou, qual seja, *cyberstalking*), é fundamental que haja repetição na ação. Logo, a prática isolada não caracteriza a conduta criminosa, sendo exigido o fator habitualidade no comportamento do agente.

Outro importante ponto a ser contemplado no dispositivo legal é aquele que faz com que a tipificação da conduta seja abrangente e alcance o ambiente virtual. Ao utilizar a expressão “por qualquer meio”, o legislador estende o tipo penal da perseguição aos meios digitais e não apenas aos meios presenciais, abarcando o *cyberstalking*.

A Lei Nº 14.132/2021 pode ser compreendida como um avanço importante, reconhecendo a natureza multifacetada do crime de *stalking*, inclusive no ambiente digital. A criação de mecanismos que acompanhem a rápida evolução das formas de *stalking* é essencial para garantir que a legislação cumpra sua função de proteger as vítimas de perseguição, independentemente do meio utilizado pelos agressores.

Dessa forma, entendemos que as reformas legislativas buscando a adaptação do cenário jurídico sempre serão bem-vindas, já que à medida que crescem e surgem a possibilidade de novos tipos de práticas criminosas, o Direito, como instrumento de promover justiça e defesa dos interesses coletivos, deve estar preparado.

Contudo, “o legislador deve ter o cuidado para que não conceba uma ordenação jurídica natimorta, que ingressa no arcabouço legislativo de modo ultrapassado.” (JESUS E MILAGRE, 2016, p.13)

A ênfase na necessidade de uma abordagem diferenciada na criação de leis para a tecnologia da informação destaca a complexidade desse campo e a importância de uma legislação que seja adaptável e relevante ao contexto contemporâneo. A expressão "ordenação jurídica natimorta" enfatiza a possibilidade de leis que, ao não acompanharem o ritmo das mudanças tecnológicas, tornam-se obsoletas desde o momento de sua concepção.

É de extrema importância entender que o legislador deve agir com cautela para evitar a criação de leis que se tornem rapidamente ultrapassadas, incapazes de lidar com os avanços contínuos na tecnologia. Essa visão destaca a necessidade de uma abordagem proativa na elaboração de legislação relacionada à tecnologia da informação, buscando antecipar futuros desenvolvimentos e garantir que as leis permaneçam relevantes ao longo do tempo. Essa reflexão é crucial para assegurar a eficácia e a durabilidade das normas jurídicas em um ambiente tão dinâmico e inovador como o da tecnologia da informação.

4 CONSIDERAÇÕES FINAIS

Após uma revisão abrangente sobre crimes cibernéticos no Direito Penal brasileiro, abordando conceitos, estelionato e crimes conexos, bem como crimes contra a honra, foi possível explorar a complexidade desse cenário jurídico em constante evolução. A análise das leis penais brasileiras, como o Código Penal, a Lei Carolina Dieckmann, a Lei Geral de Proteção de Dados e a Lei 14.132/2021, revelou desafios na adaptação à era digital e na eficácia das legislações para lidar com crimes cibernéticos.

O Código Penal Brasileiro, embora tenha sido desenvolvido para uma realidade analógica, pode enfrentar dificuldades na abordagem dos crimes digitais, revelando a necessidade de adaptações e potenciais reformas. A Lei Carolina Dieckmann, surgida em resposta a um caso midiático, apresentou modificações, mas foi alvo de críticas e ainda suscita questionamentos quanto à sua eficácia. A Lei Geral de Proteção de Dados trouxe avanços na proteção de dados, mas desafios persistentes permanecem com relação à sua aplicabilidade e punições, como verificamos em dados estatísticos.

A Lei 14.132/2021, focando nos crimes de *stalking* e *cyberstalking*, trouxe uma abordagem específica, sendo considerada um ponto positivo, mas concluímos que as reformas legislativas devem ser feitas com cautela, já que a evolução tecnológica acontece de forma extremamente rápida, trazendo desafios na adequação das leis ao contexto de determinado momento. No geral, percebe-se a urgência de atualizações legislativas para enfrentar as constantes evoluções do ambiente digital.

Conclui-se que, embora haja esforços legislativos, a complexidade dos crimes cibernéticos exige uma abordagem dinâmica e adaptável. Recomenda-se uma contínua revisão das leis existentes, considerando a rápida evolução das tecnologias e a diversidade de ameaças digitais. Sugere-se, ainda, a promoção de debates e pesquisas interdisciplinares para aprimorar a compreensão e enfrentamento dos desafios jurídicos na era digital.

REFERÊNCIAS

AMIKY, Luciana Gerbovic. **Stalking**. 2014. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica de São Paulo, São Paulo. 2014. Disponível em: https://tede2.pucsp.br/bitstream/handle/6555/1/Luciana%20Gerbovic%20Amiky.pdf. Acesso em: 04, novembro de 2023.

ASSUNÇÃO, Mayume da Silva. **A tipicidade dos crimes cibernéticos no direito penal brasileiro: Um estudo sobre o impacto da Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos**. Guanambi-BA. 2021.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. [S. l.], 1 jan. 1942.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. [S. l.], 30 mar. 2013.

BRASIL. Lei Nº 13.709/2018, de 14 agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. [S. l.], 18 set. 2020

BRASIL. Lei nº 14.132, de 31 de março de 2021. **Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais)**. [S. l.], 31 mar. 2021.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato**. [S. l.], 27 maio 2021.

BRITO, A. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

SARTORI DE CASTRO, Luiz Augusto. **"Lei Carolina Dieckmann seria a salvação da internet?**. Migalhas. Brasil, 2012. Disponível em: https://www.migalhas.com.br/depeso/167980/lei-carolina-dieckmann--seria-a-salvacao-da-internet. Acesso em 31, outubro de 2023.

CRESPO, Marcelo. **Algumas reflexões sobre o cyberstalking**. Disponível em: https://canalcienciascriminais.com.br/algumas-reflexoes-sobre-o-cyberstalking/. Acesso em: 14, novembro de 2023.

DAMARTINI, Felipe**. Cyrela é a 1ª empresa condenada por descumprir a LGPD e deve pagar R$ 10 mil**. Brasil, 2020. Disponível em: https://canaltech.com.br/juridico/cyrela-e-a-1a-empresa-condenada-por-descumprir-a-lgpd-e-deve-pagar-r-10-mil-172465/. Acesso em 06, novembro de 2023.

DA SILVA, Patrícia Santos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

DINO. **Crimes virtuais afetam 42 milhões de brasileiros**. Jornal Estadão. São Paulo/SP, 2017. Disponível em: https://www.estadao.com.br/foradeultimas/crimes-virtuais-afetam-42-milhoes-de-brasileiros. Acesso em 17, outubro de 2023.

GALLI, Marcelo. **Direito não está preparado para enfrentar criminalidade digital, diz Rogerio Schietti**. Conjur. Brasil, 2017. Disponível em: https://www.conjur.com.br/2017-mai-26/direito-nao-preparado-enfrentar-crime-digital-schietti/. Acesso em 26, outubro de 2023.

JESUS, Damásio de, e MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. **Crimes cibernéticos: atipicidade dos delitos**. 2017.

NUCCI, Guilherme de Souza. **Código penal comentado**. 14. ed. Rio de Janeiro: Forense, 2017.

PAIVA, Letícia. **LGPD: 77% das decisões que citam lei não resultaram em condenação em 2021**. São Paulo, 2022. Disponível em: https://www.jota.info/justica/lgpd-condenacao-77-das-decisoes-nao-27012022. Acesso em 08, novembro de 2023.