

CENTRO UNIVERSITÁRIO UNINOVAFAPÍ
BACHARELADO EM DIREITO

ISRAEL DOURADO DE BARROS
JOSÉ LUCAS OLIVEIRAARRUDA

CRIMES CIBERNÉTICOS: análise evolutiva na perspectiva da legislação penal brasileira

TERESINA
2023

ISRAEL DOURADO DE BARROS
JOSÉ LUCAS OLIVEIRAARRUDA

CRIMES CIBERNÉTICOS: análise evolutiva na perspectiva da legislação penal brasileira

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAPI, como requisito
parcial para obtenção do grau de Bacharelado
em Direito.

Orientadora: Professora Doutora Diná da
Rocha Loures Ferraz

TERESINA

2023

FICHA CATALOGRÁFICA

B277c

Barros, Israel Dourado de.

Crimes cibernéticos: análise evolutiva na perspectiva da legislação penal brasileira / Israel Dourado de Barros, José Lucas Oliveira Arruda. – Teresina: Uninovafapi, 2023.

Orientador: Prof^a. Dr^a. Diná da Rocha Loures Ferraz. Centro Universitário UNINOVAFAPI, 2023.

22 p.; 23cm

Monografia (Graduação em Direito) – Centro Universitário UNINOVAFAPI, Teresina, 2023.

1. Crimes. 2. Crimes cibernéticos. 3. Lei. 4. Código penal. 5. Artigo. 6. Legislação. I. Título. II. Lira, Gillian Santana Mendes.

CDD 336.29

Catálogo na publicação
Francisco Renato Sampaio da Silva – CRB/1028

ISRAEL DOURADO DE BARROS
JOSÉ LUCAS OLIVEIRAARRUDA

CRIMES CIBERNÉTICOS: análise evolutiva na perspectiva da legislação penal brasileira

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAPI, como requisito
parcial para obtenção do grau de Bacharel em
Direito.

Data de aprovação ____/____/____

BANCA EXAMINADORA

Profª Dra. Diná da Rocha Loures Ferraz
Centro Universitário - UNINOVAFAPI
(Orientadora)

Prof.ª titulação
Centro Universitário - UNINOVAFAPI
(1º Examinador)

Prof.ª titulação
Centro Universitário - UNINOVAFAPI
(2º Examinador)

AGRADECIMENTOS

Eu, José Lucas, dedico este trabalho à memória do meu falecido avô, José Edson Arruda, que sempre me inspirou e contribuiu para minha perseverança ao longo de todo o desenvolvimento desse trabalho e também aos meus avós maternos, João Batista de Oliveira e Chislane Brito de Oliveira, por todo o apoio, amor e exemplo de vida, sempre me mostrando que dias melhores podem acontecer. Grato ao meu pai, José Edson Arruda Filho, e a minha mãe, Lyssia Brito de Oliveira Arruda, por sempre acreditarem na minha capacidade para superar as adversidades que enfrentei. E, por fim, agradeço a minha irmã, Maria Eduarda Oliveira Arruda, que contribuiu para minha formação acadêmica e para o meu desenvolvimento intelectual.

Eu, Israel Dourado, agradeço primeiramente a Deus, e a minha família, os meus pais, irmãos e minha namorada, que se fazem sempre presentes na minha vida social e acadêmica, me apoiando e fortalecendo cada dia mais. Essas pessoas demonstram sempre a importância de se valorizar o essencial do ser humano (humildade, simplicidade e honestidade), superando as adversidades e trilhando uma trajetória de conquistas. Mesmo com obstáculos, os méritos almejamos podem ser conquistados.

RESUMO

O presente trabalho faz uma análise de conteúdos bibliográficos acerca do surgimento dos crimes cibernéticos e os seus conceitos, em decorrência dos avanços tecnológicos, da globalização e da facilidade ao acesso à internet. Busca também fazer uma análise evolutiva dos crimes abordados nesse trabalho, como estelionato, furto, stalking, estelionato afetivo, na legislação penal brasileira para entender a tipicidade das condutas que prejudicam um bem jurídico assegurado e fundamental dos indivíduos. Um marco importante na legislação brasileira, foi a criação da Lei nº 12.737/2012, conhecida como a Lei Carolina Dieckmann, que criminaliza a invasão de privacidade aos dispositivos e sistemas informáticos. Subsequentemente, veio a promulgação da Lei nº 12.965/2014, o Marco Civil da internet, impondo as devidas responsabilidades e questões de privacidade dos usuários. Dessa forma, o principal objetivo desse estudo é demonstrar a necessidade e a importância de preencher as lacunas ainda existentes quanto à forma e os responsáveis pelos atos ilícitos, nos mecanismos normativos, e de se fazer fácil entendimento no domínio das ferramentas dos meios informáticos, mostrando os riscos e limites de algumas facilidades, oriundas de ilicitude, buscando sempre uma forma de se utilizar da vulnerabilidade dos usuários, para obter uma vantagem indevida.

Palavras- chaves: Crimes; Crimes Cibernéticos; Lei; Código Penal; Artigo; Legislação.

ABSTRACT

The present work carried out a study, through bibliographic contents, about the emergence of cybercrimes and their concepts, as a result of technological advances, globalization and ease of access to the internet. It also seeks an evolutionary analysis of the crimes covered in this work, such as: embezzlement, theft, stalking, affective embezzlement, in Brazilian criminal legislation to understand the typicality of conduct that harms an assured and fundamental legal asset of individuals. An important milestone in Brazilian legislation was the creation of Law No. 12,737/2012, known as the Carolina Dieckmann Law, criminalizing the invasion of privacy of computer devices and systems. Subsequently, Law No. 12,965/2014, the Internet Civil Rights Framework, was enacted, imposing due responsibilities and privacy issues on users. Thus, the main objective of this study is to demonstrate the need and importance of filling the gaps that still exist, regarding the form and those responsible for illicit acts, normative mechanisms and making it easy to understand the mastery of computer tools, showing the risks and limits of some facilities, arising from illegality, always looking for a way to use the users' vulnerability, to obtain an undue advantage.

Keywords: Crimes; Cyber Crimes; Law; Penal Code; Article; Legislation.

1 INTRODUÇÃO

O presente artigo tem por desígnio abordar a importância em torno da relação positiva quanto aos crimes cibernéticos ligados à legislação brasileira de acordo com o Código Penal. Objetiva também abordar crimes qualificados, como violação de dispositivo informático, furtos e estelionatos cometidos pela internet ou por meio de dispositivos eletrônicos, bem como a perspectiva por meio da sua análise evolutiva, trazidas pela avanço tecnológico, com sua eficiência em pontos positivos e negativos.

Inicialmente, é necessário entender que o conceito de dados pessoais diz respeito, na verdade, às informações pessoais relacionadas às pessoas para que sejam identificadas ou identificáveis, como por exemplo, registro geral, endereço, localização, exame médico ou endereço de *internet protocol* (IP) e Cadastro de Pessoas Físicas. Denominadas pelo artigo 7º da Lei Geral de Proteção de Dados (LGPD), *in verbis*:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. (BRASIL, 2018, N. P)

O referido artigo explica que os dados pessoais só podem ser acessados por profissionais qualificados nos quais são conceituados pelo legislador que tiveram essa diferenciação, pois são dotados de um alto potencial de dano e discriminação, dados de saúde, filiação sindical ou partidária e dados biométricos.

Assim a LGPD conceitua o papel do controlador e do operador: o primeiro se trata de pessoa física ou jurídica responsável por tomar as decisões e definir a finalidade de tratamento de dados pessoais, o segundo se trata do subordinado do controlador, podendo ser uma pessoa de direito público ou privado.

A LGPD, consecutivamente aos longos dos anos, tenta resolver as problemáticas dos crimes virtuais. A primeira delas que vale ressaltar é como que o avanço tecnológico prejudica a intimidade do cidadão que recorre aos meios jurídicos para proteger sua identidade, uma vez que é seu direito não ser exposto da forma que as empresas bem querem ou entenderem. A segunda problemática, uma das mais importantes desse artigo, é o surgimento da espionagem, pois a sociedade moderna não está totalmente preparada para se proteger dessa ameaça de hackers, um perigo tanto para os cidadãos quanto para o próprio governo.

Pensando em um futuro próximo, o primeiro passo foi tomado pela Organização das Nações Unidas (ONU) 1948. Em uma sociedade pós-guerra, surge a Declaração dos Direitos Humanos, trazendo consigo direitos a serem inalienáveis e intransferíveis, como por exemplo, o direito à proteção da vida privada e à intimidade, visto que os governos tiranos da Alemanha nazista e da Itália fascista, utilizavam de listas de dados governamentais de cidadãos para retirar uma série de características únicas a fim de controlar os meios de informação da população. Conforme o artigo 3º da Declaração dos Direitos Humanos: “Todo indivíduo tem direito à vida, à liberdade e à segurança pessoal.” (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948, N.P)

Além de outros pioneiros, que deram os primeiros passos para a conquista de direitos, como as primeiras leis europeias, manifestações da Organização e Cooperação e Desenvolvimento Econômico (OCDE), as primeiras diretrizes da União Europeia, que se tornaria o berço das regulamentações e legislações de privacidade, a *General Data Protection Regulation* (GDPR), que era um regulamento de proteção de dados europeus, vinculado e aplicável a todos os países membros do espaço europeu, com sua função única de exportação de dados para fora da União Europeia, estabelecendo assim seu próprio regulamento de privacidade. Com base no entendimento de Tarcísio (2022) e Ruth (2022), no livro Lei Geral de Proteção de Dados Pessoais:

O GDPR teve sua eficácia plena (vigência) em 25 de maio de 2018, após 24 meses de sua publicação (*vacatio legis*), fruto de um longo processo de negociações e emendas que tomou quatro anos até culminar no texto final para aprovação do regulamento, trazendo à tona importantes discussões e preocupações à Europa e a todos os países que, de alguma forma, com ela se relacionam, não só devido à relevante unificação da legislação de proteção de dados europeia, como também pelas rigorosas sanções que ali estão previstas. A finalidade primordial do GDPR foi a de harmonizar as leis de privacidade de dados em todos os Estados-Membros da União Europeia. (TEIXEIRA; GUERREIRO, 2022, p.9)

Nos tempos atuais, não há uma disparidade em relação às causas da falta de privacidade na sociedade. Os avanços tecnológicos dos meios de comunicação acabou trazendo atenção à influência e o aprimoramento das tecnologias fez com que se despertasse, dentro de cada indivíduo, uma certa curiosidade em conteúdo e dados alheios. Com isso, surge a necessidade de como devemos protegê-los, mesmo os sujeitos sendo expostos e privados em redes de uso mundial, mas cabe aqui a seguinte indagação: até onde podemos relacionar ou impor um limite, com o respeito ao direito de privacidade?

O crescimento desenfreado, as grandes transformações e os consecutivos avanços tecnológicos interligam e globalizam a sociedade contemporânea de forma que trouxe pontos positivos, como a criação da sociedade da informação, um coletivo de indivíduos conectados entre si e uma facilidade maior de obter informações e os negativos, como a desigualdade econômica e a uniformidade cultural.

No entanto, uma rede aberta e com uma facilidade de acesso e domínio por todos, acaba se tornando um meio perigoso e se torna um local de condutas ilícitas pelos usuários. Com isso, surge a necessidade de se impor limites, pois a forma de disseminação da violação do direito de proteção à vida privada, ou seja, a privacidade, afronta um direito líquido e certo, sendo assim, a temática está em debate no âmbito jurídico.

Em uma compreensão mais simples, para os operadores do direito que trabalham nesse ramo, tendo como vista que os dados pessoais protegidos por leis e pelo Código Penal e Processual Penal, resguarda seus direitos e puni aqueles que ferem para adquirir vantagem ilícita sobre o alvo, caso não sejam protegidos podem gerar catástrofes e danos irreparáveis. Pois o uso indevido destas informações pode causar golpes em seu nome, fraudes, criminosos podem afetar o perfil do crédito dos consumidores ou trazer prejuízos financeiros às vítimas.

Então, como atualmente os dados são um catalizador econômico tão grande que é preciso ter um contrapeso que são as regulações de proteção. Estas regulações são na verdade medidas em que a Polícia Federal criou a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC), para combater estes crimes esta unidade tem como objetivo proteger as pessoas das consequências dos crimes informáticos ao próprio proprietário nas quais os criminosos não comecem a utilizar as informações pessoais de forma indiscriminada e que a população tenha meios de como se proteger dessas injustiças. Por essa razão, no entendimento do doutrinador Eduardo Tomasevicius Filho (2021) no seu livro “Lei Geral de Proteção de Dados Brasileira”:

Dados pessoais sempre foram essenciais tanto para o setor privado como público. No primeiro caso, o acesso a informações sobre concorrentes, fornecedores, clientela, hábitos e preferências dos consumidores podem sacramentar o sucesso ou fracasso de qualquer empreendimento; já no setor público, a organização, planejamento e execução de serviços e políticas públicas, cobrança de tributos, repressão criminal e, de modo mais específico, ações de inteligência e contrainteligência reclamam o manejo de volume considerável de dados, sem os quais a Administração Pública ficaria completamente desarticulada. (FILHO, 2021, p. 97)

No segundo tópico do presente artigo o conceito de crimes cibernéticos é, na verdade, uma consequência do avanço tecnológico da sociedade e é praticável por qualquer meio de comunicação, sendo muito pouco debatido ainda no Brasil e causando prejuízo a milhares de

Brasileiros, pois traz crimes horríveis, como estelionato e o estelionato afetivo, apologia ao crime, nazismo, xenofobia, entre outros.

O entendimento no Código Penal acerca dos crimes cibernéticos aborda toda uma linha de raciocínio clara e objetiva sobre os crimes informáticos e suas consequências para quem os comete. À vista disso, a codificação penal aduz que as atitudes dos criminosos são horripilantes, ferindo direitos de todos os seres humanos, infringindo a privacidade, respeito, os bons costumes e uma vida social saudável.

A temática das modificações da legislação penal explica que ao longo de toda uma análise evolutiva dos crimes cibernéticos obteve-se muitas alterações e novidades em suas legislações, como por exemplo, o crime de stalking, trazido pelo entendimento da Lei Federal 14.132/ 2021, o novo entendimento do estelionato afetivo que fere os direitos intrínsecos de todo ser humano e, por fim, o crime de furto, em que o hacker pode acabar invadindo dados pessoais para efetuar mais golpes.

Nesse destarte, o objetivo desse estudo está intimamente ligado à evolução da sociedade e dos ordenamentos jurídicos, em compasso com o avanço dos crimes cibernéticos, surgindo a necessidade de estudarmos e aprimorarmos os conhecimentos para assim contribuir com o combate à violação de direitos dos indivíduos. e para trazer mais profissionais qualificados nesta área que ainda está em desenvolvimento no Brasil, assim, para ressaltar a importância deste artigo para os novos operadores do direito que se interessem neste novo ramo do direito.

2 CRIMES CIBERNÉTICOS

Para que seja possível compreender o conceito do que vem a ser crimes cibernéticos, é de suma importância entender a sua origem. Segundo o entendimento de Eric Hobsbawm (1995), em seu livro “A era dos extremos”, o autor realiza uma análise a respeito do século XX, chamando-o de “breve”, pois ocorrem inúmeras mudanças na sociedade em um curto período de tempo. Assim, em meados da década de 50, a “globalização” não tinha a dimensão que possui atualmente, os meios de comunicação e informação eram menos dinâmicos, sendo utilizados instrumentos como cartas, fax, telefones de fio, dentre outros.

Logo é possível compreender que o avanço tecnológico acompanhou o desenvolvimento social, onde esses instrumentos, que foram desenvolvidos com o intuito de facilitar a vida do ser humano, cada vez mais podem ser observados dentro do cotidiano.

Consequentemente, veio a necessidade de uma legislação que tivesse como objetivo regular as relações digitais.

Com essa nova dinâmica nos espaços digitais, veio as transformações. Não somente no meio tecnológico, mas sim nas mudanças de conceitos, métodos de trabalho e estrutura das sociedades e nas relações sociais. Dessa forma, a consequência do surgimento da Internet ocasionou no aparecimento de novos crimes que antes não existiam. Podemos conceituar os crimes cibernéticos, segundo o doutrinador Marcelo Xavier de Freira Crespo (2011), em sua obra “Crimes digitais”, assim:

Concretamente, os crimes digitais importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e discriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros. (CRESPO, 2011, p. 20)

À luz da doutrina pode-se notar que os crimes por meio da informática estão e são limitados ao uso dos computadores, ou seja, uma rede de dados que facilite o acesso e domínio de uma maioria de usuários. Ainda sobre o conceito e à luz da doutrina, o autor Emerson Wendt Higor Vinicius Nogueira Jorge (2013) aduz que:

Nos moldes do que foi anteriormente comentado, decidimos utilizar o termo “crimes cibernéticos” para definir os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral). Além dessa questão, apenas para fins didáticos, apresentamos uma classificação para as denominadas “condutas indevidas praticadas por computadores” (JORGE, 2013, pág. 18)

Podemos destacar, portanto, que os conceitos de crimes cibernéticos são de alta extensão e amplitude, mas é algo restritivo pelo uso dos meios de comunicações e base de dados. Como consequência dessa restrição, se torna algo bem mais preocupante e urge a urgência de ser debatido.

Nesse mesmo contexto, devido ao avanço e à facilidade do acesso à internet, ações criminosas se tornaram mais complexos e comuns, como por exemplo: o surgimentos dos hackers (clonagem de dados pessoais e bancários), pirataria de programas e filmes, apologia ao nazismo, xenofobia e pornografia infantil, sendo este último um dos crimes que mais cresce e traz consigo uma preocupação enorme.

Atualmente esses crimes passaram a ser mais frequentes e muitas das vezes se tornarem mais complexos em suas formas de atuações, necessitando de um estudo aprofundado,

diário e de métodos coercitivos como: criação de novas leis, tornando-as mais brandas, debates, palestras inclusivas do uso e risco. Pode-se citar alguns desses crimes, como: estelionato (tanto de pessoa física ou jurídica), racismo, homofobia, apologia ao nazismo, xenofobia e tantos outros crimes.

Com o surgimento de críticas à inexistência de uma legislação, uma lei que acompanhasse o progresso da sociedade, houve a necessidade da criação de uma norma, com o objetivo de regular e disciplinar os indivíduos. Sendo assim, surgiu a Lei nº 12.737/2012, conhecida popularmente como “Lei Carolina Dieckmann”. Esse instrumento normativo veio para complementar a defesa de direitos já garantidos e constitucionalmente fundamentais, são eles: direito à intimidade, à vida privada, à honra e à imagem das pessoas. Eles podem ser encontrados no Artigo 5º, inc. X:

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 à indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 2012, N.P).

A Lei Carolina Dieckmann pode ser comparada à Teoria Tridimensional do Direito, de Miguel Reale, pois o seu surgimento se deu com a necessidade de preencher uma lacuna normativa de um direito que estava sendo ferido. Partindo do pressuposto de que essa teoria idealizava que para sua concretização e aplicação, baseava-se em três aspectos. O primeiro é o fato jurídico, o segundo o valor e o terceiro a norma propriamente dita. Consequentemente a existência do fato fez com que a norma propriamente dita fosse criada em conjunto com um ordenamento de maior relevância social em prol da defesa de um direito líquido e certo (JUNIOR, 2018).

Contudo, após iniciar o estudo sobre os crimes cibernéticos, juntamente com o entendimento de seus diversos conceitos e especificações, é possível notar que esse assunto é de suma importância para a era contemporânea. Isso se explica por conta do forte domínio dos usuários das redes sociais, onde muitas vezes estão expostos a riscos e perigos com a exposição de dados e informações pessoais. Em muitos casos, o vazamento dessas informações pode ser usados a favor da criminalidade, o que acarreta em prejuízos irreparáveis para as vítimas.

3 CÓDIGO PENAL SOBRE CRIMES CIBERNÉTICOS

Ainda não existe um entendimento certo e objetivo sobre o conceito de crimes

cibernéticos por parte dos doutrinadores que estudam essa temática, pois com o processo de globalização e com o acesso à informação cada vez mais dinâmico, pode-se entender que a internet está sempre em uma constante mudança. Nesse sentido, a doutrinadora Patrícia Santos da Silva (2015), faz o seguinte comentário sobre as redes sociais ou plataformas on-line:

[...] que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (SILVA, 2015, p. 39)

Vale ressaltar que o Código Penal de 1940 tem tipificações penais a punir as ilicitudes praticadas com o uso da tecnologia. Pensando-se em delitos digitais como aqueles em que apenas o *modus operandi* é a tecnologia moderna, o Código já é capaz de punir vários tipos de delitos, desde os crimes contra a honra, crimes patrimoniais, contra a pessoa, de disputa mercantil desleal, por exemplo.

As redes sociais e outros meios de plataformas on-line vieram com uma premissa de melhorar as comunicações entre os indivíduos para que seja uma forma mais rápida e prática e também fonte de conhecimento para aqueles que desejam aprender ou até mesmo uma fonte de renda. Porém, acaba se tornando um ambiente tóxico, obscuro e de intimidação, já que os usuários que não respeitam as regras e diretrizes de cada plataforma podem cometer crimes cibernéticos (SILVA, 2015).

Assim sendo, a legislação penal tem como propósito advertir e proibir as atitudes de criminosos que cometem crimes tipificados, anticonstitucionais e que agredem grupos sociais que não possuem voz na sociedade. Tais crimes, leis e normas jurídicas são criadas com o intuito de serem mais rígidas, com o objetivo de proteção aos cidadãos e de um sistema judiciário com penas justas e certas para os flagícios. Com isso, é possível classificar as condutas que são incrimináveis tendo em vista o Código Penal e o livro de “Crimes Digitais” de Marcelo Xavier de Freitas Crespo (2011), que explica:

Embora se diga que classificações não são corretas ou equivocadas, mas úteis ou inúteis, cumpre classificarmos os crimes digitais, pois a partir disso é que se fará exposição sobre condutas específicas. Mas, antes de qualquer coisa, é preciso delinear algumas ideias sobre as classificações apresentadas pela doutrina.” [...]

Sieber, notadamente um dos maiores estudiosos do tema, em parecer sobre crimes relacionados com o computador, elaborado especialmente para a Comissão Europeia e já atualizando ideias suas passadas, classificou os ilícitos da seguinte forma:

- a) Violações à privacidade
- b) Crimes econômicos
 - a. Hacking
 - b. Espionagem
 - c. “Piratarias” em geral (cópias não autorizadas)
 - d. Sabotagem e extorsão

- e. Fraude
- f. Crime organizado
- g. Guerra “eletrônica”. (Crespo, 2011, p.24)

Ressaltando um conceito utilizado por autores renomados, como Jesus e Milagre (2016), o texto “Manual de crimes informáticos” trata sobre crimes virtuais que podem ser cometidos e que são interpretados na Legislação vigente, sendo eles:

- a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si, para esses delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
- b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para esses delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum tipo penal;
- c) crimes informáticos mistos: são crimes complexos em que, além de proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre à existência de dois tipos penais distintos, cada qual protege um bem jurídico;
- d) crime informático mediato ou indireto: trata-se delito informático praticado para a ocorrência de um delito não informático consumando ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto). (JESUS; MILARE, 2016, p. 49)

No final do século XX, com o aumento da popularização dos computadores, a Lei nº. 9.983/2000 do Código Penal brasileiro adquiriu algumas tipificações do sistema informático/digital que visam a ilicitude criminal dessas condutas, sendo esses, os Arts.313-A e o 313-B do CP:

Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000) Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)

Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000) Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000) (BRASIL, 2000, N.P)

Contudo, houve a criação de uma lei que foi sancionada no dia 30 de novembro de 2012, com o objetivo de ser a primeira lei específica de crime cibernético no sistema judiciário brasileiro, a Lei nº 12.737/2012, Lei Carolina Dieckmann.

Após a divulgação de imagens íntimas, 36 fotos roubadas, a atriz Carolina Dieckmann sofreu uma tentativa de extorsão dos criminosos para que sua intimidade não fosse divulgada. O fato comoveu todo o país e pressionou as autoridades em relação à gravidade do problema.

O acontecimento trouxe à tona uma realidade comum aos usuários de redes sociais, mas que até então era raramente debatido pelas autoridades brasileiras. Com esse terrível feito, a Lei buscou um novo entendimento perante o artigo 154- A, no Código Penal, *in verbis*:

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- reclusão, de 1(um) a 4 (quatro) anos, e multa. (BRASIL, 1940, N.P)

Com base na interpretação do legislador, a prática certa desse delito sempre vai ser a intuição de invadir, recolher informações pessoais alheias, tirar proveito disso e extorquir da forma que bem entender.

Por essa mesma razão, a prática delituosa acompanhada pela evolução da tecnologia sempre estará em constante mudança e evolução, pois o legislador sempre terá que encontrar soluções para a proteção da população e impor sanções mais rígidas e restritivas aos hackers que cometem tais delitos.

Para completar ainda mais a ênfase da dificuldade do Código penal, legislações e leis no sistema judiciário brasileiro, há uma grande disparidade pelo fato de o Brasil ainda estar longe de realmente ser eficiente no combate contra hackers em comparação a outros países, que já são exemplos de combate contra os crimes virtuais, pois têm mecanismos de defesa no software, proteção ou regulação de internet para crianças.

4 AS MODIFICAÇÕES NA LEGISLAÇÃO PENAL E PROCESSUAL PENAL NO BRASIL DAS PENAS DOS CRIMES VIRTUAIS

4.1 ESTELIONATO

A nova lei 14.155/2021 trouxe novas modificações a respeito do agravamento da pena para o crime de invasão de dispositivo informático previsto no artigo 154-A, do CP, já mencionado anteriormente, que se trata em proteger ainda mais as vítimas e ter um efeito com maior ferocidade em punir os hackers, para que esses infratores não obtenham o aparelho digital da vítima, com o fim de obter informações alheias, corromper, destruir dados ou apagar sem autorização do usuário do dispositivo.

Com essa nova lei vigente, veio os agravos para reforçar a pena desse delito de estelionato. Com a meta de combater o dano causado por esses criminosos acovardados, que de tal forma, foi criado uma qualificadora do crime de estelionato, conforme estabelece o Código Penal brasileiro:

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:

§ 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 terceiros

induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

(Incluído pela Lei nº 14.155, de 2021)

§ 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. (Incluído pela Lei nº 14.155, de 2021) (BRASIL, 1940, N.P).

A fraude pode ser cometida por meio da utilização do uso de informações trazidas por umas das vítimas ou por outro indivíduo induzido ao erro pela plataforma digital de redes sociais, como também de contatos telefônicos, trotes, envio de correio eletrônico falso, ou por qualquer outro meio fraudulento que possa ludibriar.

A nova lei também viu a necessidade no aumento penal para o crime de estelionato contra idoso ou vulnerável, que não possua escolaridade formada ou alguma fragilidade mental que o impossibilite de entender que está sofrendo um golpe. Segundo o § 4º, artigo 171 do Código Penal a pena pode ser aumentada de 1/3 (um terço) ao dobro, se o crime for cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.

4.2 CRIME DE FURTO

Com base no artigo de Jeferson Botelho Pereira da Lei nº 14.155/2021, a nova lei introduziu sensíveis modificações no artigo 155 do Código Penal, para inserir uma nova qualificadora no § 4º-B. Outro crime a ser ressaltado, que pela nova lei teve mudanças na sua pena, foi o crime de furto, pelo artigo 155, § 4º-B e o § 4º-C do Código Penal determinando que a pena é de reclusão, 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança, com a utilização de programa malicioso ou por qualquer outro meio fraudulento análogo, conforme é mencionado no artigo. (PEREIRA, 2021)

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)

§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)

I – 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; (Incluído pela Lei nº 14.155, de 2021)

II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (Incluído pela Lei nº 14.155, de 2021) (BRASIL, 1940, N.P)

A pretensão do legislador é de causar uma pena mais severa aos crimes já mencionados anteriormente, em face da ampliação assustadora do número de fraudes no meio digital na sociedade atual durante a pandemia e pós-pandemia, inclusive com conta de cartão de crédito clonado ou furtado, o que se tornou um golpe muito comum nos últimos anos no Brasil.

4.3. STALKING

O crime de stalking se origina da palavra em inglês que é utilizada na prática de caça, deriva do verbo *stalk*, que corresponde a perseguir incessantemente. Consiste em forma de violência na qual o sujeito invade repetidamente a esfera da vida privada da vítima, por meio da reiteração de atos de modo a restringir a sua liberdade ou atacar a sua privacidade ou reputação. O resultado é um dano temporário ou permanente à integridade psicológica e emocional. Os motivos dessa prática são os mais variados: violência doméstica, inveja, vingança, ódio ou pretexto de brincadeira.

Há o emprego de táticas de perseguição diversas, a exemplo de ligações telefônicas, envio de mensagens por SMS, aplicativo ou *e-mail*, publicação de fatos ou boatos, remessa de presentes, espera da passagem da vítima pelos lugares que frequenta, invasão de dispositivos eletrônicos, dentre outras.

Com o avanço da sociedade cada vez mais hiperconectada, essa violência passou a ser concretizada também por meio virtual. Daí, chamar-se de *cyberstalking* a perseguição realizada por intermédio da *internet*, seja por redes sociais, *emails*, blogs etc.

A LEI Nº 14.132 de 31/03/2021 acrescentou o art. 147-A ao Decreto-Lei nº 2.848/40 (Código Penal) e estabeleceu o crime de perseguição. A lei ainda revogou o art. 65 do Decreto-Lei nº 3.688/41 (Lei das Contravenções Penais), o qual tratava do assunto de forma mais branda.

Com a mudança a tipificação penal de “Perseguição” ficou assim definida:

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.

§ 1º A pena é aumentada de metade se o crime é cometido:

I – contra criança, adolescente ou idoso;

II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;

III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.

§ 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes violência.

§ 3º Somente se procede mediante representação.

Em se tratando de um delito habitual, a infração penal prevista no art. 147-A do CP se consuma quando há prática reiterada da perseguição, e por qualquer meio, venha a ameaçar a integridade física ou psicológica da vítima, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. O que o agente faz, portanto, não é apenas incomodar a vítima, mas deixá-la sob seu controle, subjugá-la para que sinta constante ansiedade e medo (angústia e temor).

O *stalking* afeta a formação de vontade da vítima e atinge suas decisões e comportamentos, levando-a a mudar seus hábitos, horários, trajetos, número de telefone, e-mail e até mesmo local de residência e trabalho, degradando suas condições de vida e prejudicando, inclusive, sua liberdade de determinação. Isso pode causar crises de ansiedade, pânico, desespero, insônia, angústia etc. Sérios problemas na esfera física, psicológica, profissional e emocional, logo, o *stalking* deve ser punido com o rigor da lei.

4.4 ESTELIONATO AFETIVO

O estelionato sentimental se caracteriza como uma forma de enganar seu cônjuge para obter uso de tal produto ou bem, podendo o criminoso utilizar os meios virtuais para aplicar os golpes, assim, em seguida, safar-se e responsabilizar indevidamente quem assumiu a dívida, agindo de má-fé. Esse é um golpe de extrema covardia, onde o caloteiro(a) abusa psicologicamente do parceiro(a) e infringe os princípios da dignidade da pessoa humana e da boa-fé, como por exemplo.

O princípio da dignidade da pessoa humana se contextualiza no estelionato afetivo como uma forma de expressar a frustração da vítima e a vergonha de ter sido enganada. Na fundamentação jurídica na doutrina de Guilherme de Souza Nucci (2015), em seu texto “Princípios Constitucionais Penais e Processuais Penais”, há a seguinte afirmativa:

A referência à dignidade da pessoa humana, feita no art. 1.º, III, da Constituição Federal, “parece conglobar em si todos aqueles direitos fundamentais, quer sejam os individuais clássicos, quer sejam os de fundo econômico e social”.³ É um

princípio de valor pré-constituente e de hierarquia supraconstitucional. (NUCCI, 2015, pág. 31)

Assim, se tratando de um direito fundamental e reconhecido pela Constituição Federal não podendo ser retirado por qualquer ser humano, esse princípio garante que todos os brasileiros têm o direito de serem tratados com igualdade, equidade, respeitado e ser valorizado. É conceituado que cada humano tem dentro de si uma única natureza, onde tem qualidades, defeitos e liberdade de expressão, não sendo tratados com mercadorias ou serem rebaixados por terceiros. (LEMEIRAS, 2023)

O princípio da boa-fé tem como objetivo proteger as duas partes em litígio para seguirem com os fundamentos éticos e profissionais. De acordo com o Código Civil pelo art. 422, “os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé.” (BRASIL, 2002, N.P)

Por esse motivo entende-se que o estelionato sentimental ou afetivo fere também o princípio da boa-fé, na qual exige que as partes estejam corretas e dispostas a assumirem os riscos que se responsabilizaram, arcando com os custos em que seu cônjuge obteve em seu nome. Ao abusar da confiança da vítima com a intenção de conduta ilícita, viola-se então este princípio, enganando a lealdade do parceiro(a), com o intuito de obter vantagem ilícita por meio do namoro.

O estelionato afetivo ou sentimental submete a vítima a um constrangimento, deixa claro suas verdadeiras intenções de buscar o interesse material, contenta-se com o bem que não é seu e não foi gasto com o seu próprio recurso financeiro, o que agreda vários princípios constitucionais que têm valores inalienáveis.

5 CONSIDERAÇÕES FINAIS

Todos esses crimes cometidos no espaço cibernético acontecem simultaneamente em qualquer lugar e momento. Porém, atualmente o Brasil encontra uma dificuldade para que sua legislação consiga acompanhar a constante evolução desse tema e fazer com que suas leis sejam realmente rigorosas para quem comete e, conseqüentemente, proteger quem se torna vítima.

A falta de uma tipificação que seja mais precisa e coercitiva, causa na população uma insegurança na eficácia no âmbito jurídico brasileiro, pois os dados pessoais e empresariais, ou até bens materiais podem definitivamente sofrer perdas irreparáveis, consumando o conceito de crime digital.

Com o advento de novos tipos e meios fraudulentos, houve a necessidade de criação e modificação de instrumentos

normativos que regulam as leis e suas penas, como o caso da Lei n.º 12.737/2012 (LEI CAROLINA DIECKMANN) e a majoração da pena da Lei n.º 14.155/21, foi necessária cautela sob o tema, uma maior compreensão e conhecimento de estudo do legislador de forma adequada para que essas lacunas não voltem a se repetir.

Com toda a evolução das leis e legislações aqui trazidas e explicadas é essencial a elaboração de um único ordenamento jurídico brasileiro que tenha como objetivo a disciplina e o dever do Estado em se utilizar normas objetivas, conexas e justa, objetivando trazer proteger a população brasileira de criminosos que se aproveitam das constantes mudanças das leis sobre o conteúdo em pauta.

Dessa forma, todas as leis relacionadas aos crimes cibernéticos teriam uma mesma característica, que seria a proteção da privacidade do indivíduo, onde qualquer pessoa que tenha um celular ou um dispositivo informático, vá buscar sempre sua proteção quando estiver on-line. Bem como punir as práticas de pessoas e empresas que possam causar prejuízos a terceiros, previstos no artigo já mencionados anteriormente art. 154-A do Código Penal.

Por fim, as tipificações de crimes cibernéticos devem estar sempre abrangentes pela constante evolução da tecnologia, como por exemplo a Lei 14.132/21, Lei do Stalking, que define a proibição, por qualquer razão, de meios de perseguir um indivíduo, infringir sua privacidade e o direito à própria vida que se perde quando é violada sem o consentimento da vítima, prevista também no art. 147-A do Código Penal, arguidas com uma exposição sem precedentes da imagem e reputação da vítima.

Mesmo que hoje em dia exista diversos trabalhos e mecanismos de controle social e virtual que possam retirar fotografias, proteger a vítima e zelar por sua reputação, uma vez postadas na internet sempre permanecerão disponíveis para serem acessadas. Isso faz com que a vítima seja constantemente constrangida, impedindo-a de ter uma vida de liberdade sem intimidações. Dessa forma, leis mais severas podem coibir os criminosos e o incentivo a não violência virtual podem conscientizar a população a não cometer esses crimes.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado, 1988. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 23.out.2023

BRASIL. Lei nº 12.737, de 30 de novembro de 2012 e Lei nº 14.155, de 27 de maio de 2021. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em 17 de outubro de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre proteção de dados pessoais, instituído no site do planalto. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em 18 de outubro de 2023.

BRASIL. Lei nº 10.406, 10 de janeiro de 2002 – Código Civil; https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acessado em 21 de outubro de 2023.

BRASIL. Código Penal (1940). Constituição da República Federativa do Brasil. Brasília: Senado, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 23.out.2023.

FILHO, Eduardo Tomás Evicius. **A Lei Geral de Proteção de Dados Brasileira**. São Paulo: Almedina, 2021.

HOBBSAWM, Eric. **Era dos Extremos O breve século XX 1914 - 1991**. 2. ed. São Paulo: companhia das letras, 1995.

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

JORGE, Emerson Wendt Higor Vinicius Nogueira. **Crimes cibernéticos ameaça e procedimentos de investigação**. 25 nov. 2013. Disponível em:

<https://books.google.com.br/books?hl=pt-BR&lr=&id=iGY-AgAAQBAJ&oi=fnd&pg=PA1&dq=o+que+são+crimes+ciberneticos&ots=OsJ-SLd8Vm&sig=SfNMkR->

[HJTIAYO5TpOB_sO9iKKc#v=onepage&q=o%20que%20são%20crimes%20ciberneticos&f=false](https://books.google.com.br/books?hl=pt-BR&lr=&id=iGY-AgAAQBAJ&oi=fnd&pg=PA1&dq=o+que+são+crimes+ciberneticos&ots=OsJ-SLd8Vm&sig=SfNMkR-HJTIAYO5TpOB_sO9iKKc#v=onepage&q=o%20que%20são%20crimes%20ciberneticos&f=false). Acesso em: 13 set. 2023.

JUNIOR, OCTAHYDES BALLAN. TEORIA TRIDIMENSIONAL DO DIREITO DE MIGUEL REALE NAS DECISÕES DOS TRIBUNAIS SUPERIORES. **Revista Pensamento Jurídico**, v. 12, n. 2, p. 262, 2018.

LAMEIRAS, Vanessa Assis Vieira. **A RESPONSABILIDADE CIVIL DO ESTELIONATO SENTIMENTAL**. Disponível em:

<<https://repositorio.animaeducacao.com.br/bitstream/ANIMA/36467/1/Tcc%20versa%CC%83o%20final%20-%20Vanessa%20Lameiras.%20.pdf>>. Acessado em: 09 de outubro de 2023.

NUCCI, Guilherme de Souza. **Princípios Constitucionais Penais e Processuais Penais**. 4. ed. Rio de Janeiro: Forense, 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em:

<https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/por.pdf>. Acessado em: 04 de agosto de 2023. DF

PINHEIRO, Patricia Peck. **Direito Digital**. 8ª edição. São Paulo: Saraiva Educação, 2018.

PEREIRA, Jeferson Botelho. **Aspectos Jurídicos da Novíssima Lei nº 14.155/2021, de 27 de maio de 2021**. Jus.com.br. 2021. Disponível em: <<https://jus.com.br/artigos/90857/aspectos-juridicos-da-novissima-lei-n-14-155-de-27-de-maio-de-2021>>. Acessado em 14 de set. 2023.

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

TEIXEIRA, Tarcísio; GUERREIRO, Ruth. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 4. ed. São Paulo: Saraiva, 2022.

XAVIER, Marcelo de Freitas Crespo. **Crimes digitais**. São Paulo: Saraiva, 2011.

DECLARAÇÃO DE REVISÃO ORTOGRÁFICA

Eu, Mariana Maia dos Reis, graduada em Letras pela Universidade Estadual do Piauí, declaro para o Centro Universitário UNINOVAFAPI que revisei o Trabalho de Conclusão de Curso de Bacharelado em Direito intitulado "Crimes Cibernéticos: análise evolutiva na perspectiva da legislação penal brasileira" dos alunos Israel Dourado de Barros e José Lucas Oliveira Arruda. Declaro ainda que o presente trabalho encontra-se de acordo com as normas ortográficas e gramaticais vigentes.

Teresina, 10 de novembro de 2023

Mariana Maia dos Reis
CPF- 043 357 173-00

Nome completo e Registro do Conselho Letras ou Português/ ou
CPF/RG