B1 ISSN: 2595-1661

ARTIGO ORIGINAL

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

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

ISSN: 2595-1661
Revista JRG de Estudos Acadêmicos

Os ataques cibernéticos e suas implicações penais

Cyber attacks and their criminal implications

DOI: 10.55892/jrg.v7i14.988
ARK: 57118/JRG.v7i14.988

Recebido: 23/02/2023 | Aceito: 24/03/2024 | Publicado *on-line*: 27/03/2024

Marlon Glauber Marinho[1]
https://orcid.org/0000-0001-7760-6914
http://lattes.cnpq.br/7519180451357839
Instituto Federal de Ciência e Tecnologia de Mato Grosso do Sul
E-mail: marlon.marinho@ifms.edu.br

Danilo Ribeiro de Sá Teles[2]
https://orcid.org/0000-0001-9725-2762
http://lattes.cnpq.br/2528182839566669
Instituto Federal de Ciência e Tecnologia de Mato Grosso do Sul
E-mail: danilo.teles@ifms.edu.br

Resumo

Este artigo visa contribuir para a compreensão dos crimes cibernéticos. Para alcançar tal objetivo, buscou-se elaborar uma linha do tempo com as principais legislações que abordam o conteúdo no ordenamento jurídico pátrio. Discutiu-se alguns dos principais ataques hackers elencados pelo site da Microsoft™, entre eles o do tipo Malware, o DDoS, o phishing, o tipo SQL injection, o botnets e o ataque ransomware. Em seguida, foram apresentados os crimes virtuais próprios, conforme descritos na legislação brasileira, tais como invasão de dispositivo informático, interrupção ou perturbação de serviço informático/telemático, estelionato digital, furto mediante fraude eletrônica, inserção de dados falsos em sistema de informações, modificação ou alteração não autorizada de sistema de informações, e clonagem/falsificação de cartão de crédito e débito. Adicionalmente, foram abordados alguns crimes impróprios. Seguindo entendimentos jurisprudenciais recentes, discutiu-se o crime de estupro por meio virtual de vulnerável, além de analisar a prática do ciberbullying e os delitos decorrentes de sua prática. Considerando que o uso cotidiano das tecnologias requer prudência diante dos potenciais riscos e vulnerabilidades, acredita-se que este artigo possa servir como um instrumento norteador para um aprofundamento na temática proposta, ressaltando a importância de compreender os ataques cibernéticos e suas implicações legais, bem como destacando a relevância da conscientização e adoção de medidas de segurança cibernética para mitigar os riscos associados ao uso das tecnologias.

[1] Mestrando no Programa de Pós-Graduação em Educação Profissional e Tecnológica - ProfEPT.
[2] Doutor em Geofísica Aplicada, pela Universidade Federal da Bahia (UFBA). Professor EBTT de Física, do Instituto Federal de Mato Grosso do Sul (IFMS), Dourados, Mato Grosso do Sul, Brasil.

Palavras-chave: Crimes virtuais. Ataques cibernéticos. Direito penal. Vulnerabilidades. Tecnologia da informação.

Abstract
This article aims to contribute to the understanding of cybercrimes. To achieve this goal, we sought to develop a timeline with the main legislations addressing the subject in the national legal system. Some of the main hacker attacks listed by Microsoft™ were addressed, including Malware, DDoS, phishing, SQL injection, botnets, and ransomware attacks. Next, virtual crimes defined in Brazilian legislation were presented, such as invasion of computer devices, interruption or disturbance of computer/telematic services, digital fraud, electronic fraud theft, insertion of false data into information systems, unauthorized modification or alteration of information systems, and credit card cloning/fraud. Additionally, some improper crimes were discussed. Following recent jurisprudential understandings, the crime of virtual rape of a vulnerable person was discussed, as well as the analysis of cyberbullying and the offenses resulting from its practice. Considering that the daily use of technologies requires caution in the face of potential risks and vulnerabilities, it is believed that this article can serve as a guiding instrument for further exploration of the proposed theme, emphasizing the importance of understanding cyber attacks and their legal implications, as well as highlighting the relevance of awareness and adoption of cybersecurity measures to mitigate the risks associated with the use of technologies.

Keywords: *Virtual crimes. Cyber attacks. Criminal law. Vulnerabilities. Information technology.*

Introdução

Recentemente, um hacker conhecido por invadir e vazar mensagens da equipe que atuava na Operação Lava Jato foi condenado a mais de vinte anos de prisão. O juiz que proferiu a sentença condenatória concluiu que os ataques realizados pelo criminoso foram direcionados às autoridades públicas envolvidas na operação. Além disso, ele foi acusado de tentar vender o material hackeado a jornalistas por duzentos mil reais (Falcão, 2023, G1).

Este é somente um dos inúmeros exemplos de condenações advindas das práticas dos crimes virtuais no sistema de justiça brasileiro. Desta forma, conhecer os ataques cibernéticos e suas consequências penais é fundamental tanto para aqueles que têm no ciberespaço o seu principal ambiente de trabalho quanto para aqueles que utilizam qualquer meio tecnológico ligado à internet. Logo, uma breve revisão sobre a legislação brasileira que aborda este tema se faz necessária.

O arcabouço jurídico sobre os crimes virtuais foi se construindo e se solidificando com o passar dos anos. A doutrina jurídica considera que a regulamentação do direito digital se deu legalmente no Brasil com a promulgação da Lei n.º 12.737/2012. Este regramento estabelece a tipificação para alguns delitos informáticos e altera alguns artigos do Código Penal. Esta inovação foi considerada uma resposta do Estado às ações dos infratores que, até então, se aproveitavam de lacunas legais.

Um exemplo de um crime que não detinha uma tipificação penal específica era o delito de cópia indevida de dados ou informações, que, até a aprovação desta lei, não era enquadrado corretamente, ocasionando assim grandes embates jurídicos. Contudo, o processo de atualização do Código Penal foi avançado, quando um

acontecimento envolvendo Carolina Dieckmann, atriz da Rede Globo, repercutiu em escala nacional. A artista foi vítima da obtenção indevida de 36 fotos nuas que estavam em seu computador e, após o vazamento ilegal das imagens, o processo de modernização legislativa foi aprimorado. O dispositivo legal foi aprovado, ficando conhecido como Lei Carolina Dieckmann (GOMES, 2016, p.141).

Em maio de 2021, o Código Penal foi alterado novamente através da lei n.º 14.155/21. Esta atualização entrou em vigor “para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet” (BRASIL, 2021).

No ano de 2014, foi sancionada a Lei n.º 12.965/14, regramento que estabeleceu os princípios, as garantias, os direitos e os deveres para quem utiliza a internet no Brasil, o chamado Marco Civil da Internet (MCI). Brandão (2019) assenta que esta lei tem um caráter civil, visto que não focou em uma linha criminalizadora do uso da internet, sendo considerada uma referência global e elogiada por inúmeros países por seu conteúdo e, principalmente, pelo amplo processo de discussão com a sociedade civil que originou sua elaboração.

As evoluções legislativas, alterações/elaborações de leis, por vezes são morosas, acredita-se, em virtude dos trâmites legislativos que precisam ser seguidos. Por isso, a legislação vem, na maioria das vezes, após as atualizações esperadas pela sociedade.

Em agosto de 2018, foi sancionada a Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que altera o MCI. Esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado, aspirando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Em 2023, no dia 12 de abril, a Presidência da República promulgou o Decreto 11.491/2023. A presente Convenção é considerada necessária para prevenir ações que ameacem a confidencialidade, integridade e disponibilidade de sistemas informáticos, redes e dados, além de combater o abuso desses sistemas, redes e dados. Ela propõe a criminalização de tais condutas, estabelece competências para lidar com esses crimes de forma eficaz, facilita a descoberta, investigação e julgamento dessas infrações, tanto em níveis nacionais quanto internacionais, e estabelece mecanismos para uma cooperação internacional rápida e confiável. (BRASIL, 2023, preâmbulo).

Após a promulgação, é responsabilidade do Brasil desenvolver novas medidas para a tipificação dos crimes virtuais. Esta iniciativa se alinha com as progressões legislativas pelas quais o país tem passado. Espera-se que futuras atualizações estejam conforme o tratado internacional, potencialmente contribuindo para a harmonização das normas em escala global.

Este recorte faz parte da pesquisa em desenvolvimento no programa de Mestrado Profissional em Educação Profissional e Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul. O trabalho tem por título “Implicações Penais dos Cibercrimes: Um estudo visando aprimorar a formação do técnico em informática para internet”, que busca identificar quais os crimes virtuais e as implicações legais devem ser compreendidas pelos estudantes, visando o enriquecimento de sua capacitação profissional e, ao mesmo tempo, possibilitar que o estudante formado nas bases da EPT, construa esses conhecimentos para o pleno exercício de sua cidadania também no ciberespaço.

Este estudo é relevante, pois os ataques cibernéticos estão intrinsecamente ligados aos estudantes de informática, devido à sua familiaridade e acesso privilegiado às ferramentas e tecnologias digitais. Esses futuros profissionais frequentemente possuem um profundo conhecimento técnico dos sistemas de informação, o que os coloca em posição de potencialmente explorar brechas de segurança ou desenvolver métodos mais sofisticados de invasão. No entanto, a maioria dos estudantes de informática são, na verdade, defensores da segurança cibernética, trabalhando para identificar e mitigar vulnerabilidades em sistemas de informação. A educação e conscientização sobre ética digital são fundamentais para orientar esses estudantes para o uso responsável e ético de suas habilidades técnicas.

Os Ataques cibernéticos mais recorrentes

Segundo o site da Microsoft (2023), os ataques virtuais visam causar danos ou obter acesso a documentos e sistemas relevantes, tanto pessoais quanto comerciais. Os ataques cibernéticos mais comuns incluem Malware, Ataque de DDoS (ataque de negação de serviço), Phishing, Ataques de injeção de SQL, Cross-site scripting (XSS), Botnets e Ransomware. A seguir, esses ataques serão contextualizados de forma resumida.

O termo "Malware" abrange uma ampla gama de programas destinados a realizar atividades prejudiciais em sistemas computacionais. Dentre os exemplos de códigos maliciosos estão vírus, worms, bots, cavalos de tróia, rootkits, entre outros (PINHEIRO, 2021, p. 363).

De acordo com Teixeira (2020, p. 682), os trojans são conhecidos como cavalos de Tróia ou backdoors, sendo programas enviados a um sistema alvo que possibilitam que o computador infectado se conecte ao computador do invasor sem a necessidade de autorização prévia.

O ataque DDoS é operacionalizado da seguinte forma: em um cenário desse tipo, um conjunto de computadores designados como mestres recebe uma instrução. Esses mestres têm controle sobre uma rede de computadores "zumbis", que são principalmente computadores domésticos infectados por vírus. Todos esses computadores acessam um site ao mesmo tempo, conforme ordenado (TEIXEIRA, 2020, p. 667).

O Phishing é descrito como uma "mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros" (PINHEIRO, 2021, p. 370). Um relatório recente da Kaspersky revelou que um em cada cinco usuários da internet no Brasil foi alvo de pelo menos uma tentativa de ataque de phishing em 2020 (RODRIGUES, 2021).

O ataque do tipo SQL injection, segundo Ferreira (2017, p. 35), está entre os dez mais realizados no meio informático. Sua execução não é considerada uma tarefa complicada; ao contrário, resume-se a digitar comandos SQL nos campos de entrada de formulários da aplicação, não exigindo conhecimentos técnicos avançados por parte do invasor. Essas ações podem ser utilizadas, entre outras coisas, para apagar todos os registros de aplicação, manipular um banco de dados ou obter informações dos usuários, como dados de cartões de crédito.

Segundo Ferreira (2017, p. 48), o ataque XSS assemelha-se ao ataque SQL Injection, pois exploram a mesma vulnerabilidade: o tratamento incorreto das informações digitadas pelos usuários. O objetivo dessa ação é enviar comandos em

JavaScript com o objetivo de enganar o usuário, levando-o a fornecer suas informações pessoais, realizar ações sem perceber ou ser redirecionado para aplicações fraudulentas.

O termo "botnets" advém da união das palavras "robot" (robô) e "network" (rede). Isso ocorre quando vários computadores, geralmente em uma rede privada, são infectados por vírus e outros tipos de software malicioso, como mensagens pop-up ou spam (MICROSOFT, 2023).

O ataque ransomware é um tipo de software malicioso que ameaça uma vítima bloqueando o acesso a dados críticos ou sistemas até que um resgate seja pago (MICROSOFT, 2023).

Existem outros tipos de ataques que podem ser realizados no meio informático, mas esses exemplos demonstram como os invasores podem articular vários desses ataques/ferramentas para praticar crimes cibernéticos.

Crimes Virtuais

Os crimes virtuais próprios estão dispostos tanto no Código Penal quanto em leis esparsas. Esses crimes exigem uma tipificação específica dos sujeitos ativos ou passivos. Por outro lado, o crime impróprio virtual é aquele em que a internet é utilizada como meio para cometer o crime, não exigindo uma qualificação específica dos sujeitos (GRECO, 2017, p. 239).

Portanto, os cibercrimes podem ser cometidos de duas maneiras: primeiro, quando a internet é utilizada como meio (sendo considerado ilícito mesmo fora dela) para se chegar ao crime; segundo, quando o tipo penal exige uma qualificação específica (somente podendo ser praticado através da internet). A seguir, será apresentado um compêndio desses delitos próprios dispostos no ordenamento jurídico pátrio.

A Invasão de Dispositivo Informático, já mencionada anteriormente, requer uma análise detalhada. O tipo penal está previsto no artigo Art. 154-A do Código Penal, com o objetivo 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" (BRASIL, 2021). Recentemente, com a última alteração legislativa, este crime teve sua pena agravada, passando para "Reclusão, de um a quatro anos, e multa" (BRASIL, 2021).

Além disso, responde por este crime "quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir tais condutas" (BRASIL, 2021). Cabe acrescentar que o tipo penal previu alguns agravantes, como por exemplo, se da invasão resultar prejuízo econômico, se resultar na obtenção de conteúdo de comunicações eletrônicas privadas, se a invasão objetivar segredos comerciais ou industriais, ou se os crimes foram praticados contra Presidente da República, governadores e prefeitos.

Existem centenas de exemplos de condenações a hackers que tentam praticar este crime. Por exemplo, a assessoria de comunicação social do Tribunal Regional Federal da 3ª Região publicou uma nota em dezembro de 2021, onde a Justiça Federal "(...) condenou, por falsificação de documento público e invasão de dispositivo informático, dois homens acusados de tentar invadir, entre os meses de janeiro e fevereiro deste ano, sistemas eletrônicos utilizados pela Justiça Federal da 3ª Região" (TRF3, 2023). A pena de um dos réus passou de nove anos de prisão, iniciando o cumprimento de pena em regime fechado.

A Interrupção ou perturbação de Serviço Informático/Telemático é prevista no art. 266 do Código Penal, incorrendo neste delito quem "Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa" (BRASIL, 2012). Além disso, equipara as mesmas penas do artigo, "quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (BRASIL, 2012). Penalizando em dobro quem praticar a conduta por conjuntura de calamidade pública. Essa tipificação "Trata-se de verdadeira punição por ataques DoS (Denial of Service) praticados em face de sites públicos, algo que se tornou muito comum no Brasil, principalmente como forma de protesto por grupos de hacktivistas" (GOMES, 2016, p.155).

O Estelionato Digital ou Fraude Eletrônica é um desdobramento do crime previsto no art.171 do Código Penal, que se caracteriza por causar prejuízo alheio, obtendo vantagens ilícitas, enganando a vítima. Com o avanço tecnológico, evoluiu também as práticas ilícitas nesses ambientes, forçando o legislador a criar um novo tipo penal. Desta forma, este crime é praticado no momento em que o "criminoso consegue enganar alguém, por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento, a fornecer dados confidenciais, tais como, senhas de acesso, bancos ou número de cartão de crédito ou débito" (TJDFT, 2021).

A tipificação prevista no Art.171, parágrafo segundo, que "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" (BRASIL, 2021). Estipula uma pena partindo de quatro anos de reclusão e podendo chegar a oito, além da multa. Ademais, pode ser agravada se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e/ou se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

O Furto Mediante Fraude Eletrônica também é uma inovação recente. Com a previsão no Art. 155, parágrafo quarto-b do Código Penal, é descrito como aquele praticado "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" (BRASIL, 2021). O sujeito ativo do crime estará sujeito a uma pena de reclusão, de quatro a oito anos, e multa. Assim como no estelionato digital, a pena é agravada se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e/ou se o crime é praticado contra idoso ou vulnerável.

Conforme mencionado por Pinheiro (2021, p. 230), este delito está se tornando cada vez mais comum, especialmente no que concerne à prática de furto mediante fraude, na qual ocorre o envio de e-mails falsos (phishing) para os usuários. Isso resulta na captura de dados de suas contas bancárias por meio da instalação de arquivos maliciosos em seus dispositivos.

A inserção de dados falsos em sistemas de informações é uma prática criminalizada pelo Art. 313-A do Código Penal. Este dispositivo legal abrange a ação de inserir ou facilitar, por parte de funcionários autorizados, a inclusão de informações falsas, assim como a modificação ou eliminação indevida de dados corretos nos sistemas informatizados ou bancos de dados sob responsabilidade da Administração Pública. Aqueles que cometem essa conduta geralmente têm a intenção de obter

vantagem indevida ou causar danos. A penalidade estabelecida para essa infração é a reclusão, com duração variando de dois a doze anos, além da imposição de multa (BRASIL, 2000). Este ato ilícito é caracterizado pelos seguintes elementos: a ação de inserir ou facilitar, por parte do funcionário público, a inclusão de dados falsos; e a modificação ou exclusão indevida de dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública. (GRECO, 2017, p. 769). Acrescenta que o agente deve estar "atuando, sempre, com a finalidade especial de obter vantagem indevida para si ou para outrem ou para causar dano" (GRECO, 2017, p. 769).

A modificação ou alteração não autorizada de sistemas de informações está prevista no Art. 313-B do Código Penal. A conduta se consuma quando "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de três meses a dois anos, e multa" (BRASIL, 2000). Além disso, agrava-se a pena se a modificação resultar dano para a Administração Pública ou para o administrado. Ademais, "as condutas previstas pelo tipo penal em estudo devem ser praticadas por funcionário público" (GRECO, 2017, p. 775). Outra observação enriquecedora deste autor refere-se aos alvos da conduta: "Os objetos materiais das condutas praticadas são o sistema de informações ou programa de informática. Por sistema de informações podemos entender o sistema que manipula informações por meio do uso de banco de dados; programa de informática é o software" (GRECO, 2017, p. 775).

A clonagem/falsificação de cartão de crédito e débito está disposta no Art. 298 do Código Penal, prevendo uma pena de reclusão, de um a cinco anos, e multa. O tipo equipara-se a documento particular, o cartão de crédito ou débito e penaliza quem "Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro" (BRASIL, 2021). Logo,"o legislador brasileiro optou por tipificar tal conduta, que anteriormente era tratada como crime informático impróprio, sustentado pelo artigo 155 do Código Penal (Furto). Neste caso, a clonagem do cartão fica equiparada à falsificação de documento particular" (GOMES, 2016, p.155).

Existe alguma divergência doutrinária a respeito do enquadramento dos crimes próprios. Alguns juristas defendem a inserção de mais crimes nesse rol; todavia, esta é uma discussão jurídica e acadêmica que, na prática, não influi na penalização dos atos praticados.

Com vistas a complementar este estudo, neste momento, será apresentados alguns crimes que podem ser cometidos utilizando o ambiente virtual como meio para se chegar à prática criminosa, os crimes impróprios.

Estupro por meio virtual de vulnerável. O crime de estupro está disposto no art. 217-A do Código Penal: “Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos: Pena - reclusão, de 8 (oito) a 15 (quinze) anos” (BRASIL, 2009).

Embora o termo “estupro por meio virtual de vulnerável” não esteja especificamente previsto na norma jurídica, esse enquadramento penal decorre da interpretação dos magistrados, tanto em primeira instância quanto nos Tribunais Regionais. Segundo informações do site do TJMS (2023), o Estado de Mato Grosso do Sul registrou sua primeira condenação por estupro virtual. Na sentença proferida, o juiz condenou um homem a uma pena de 13 anos e 24 dias de reclusão, em regime inicial fechado.

Conforme relatado, o magistrado, ao proferir a sentença, observou que, por meio da internet, o réu chantageava a vítima, uma menor de 14 anos, exigindo fotos de suas partes íntimas e ordenando que praticasse atos libidinosos para satisfazê-lo,

destacando-se a introdução de objeto na vagina (TJMS, 2023). Adicionalmente, uma decisão semelhante foi confirmada pela 8ª Câmara Criminal do TJRS, na qual um estudante de medicina foi condenado a 12 anos, 9 meses e 20 dias de reclusão por estupro virtual contra uma criança de 10 anos (TJMS, 2023).

A expressão "Ciberbullying" refere-se a uma forma específica de bullying praticada através de meios digitais. A Lei n.º 13.185 de 2015, instituiu o Programa de Combate à Intimidação Sistemática (Bullying), definindo-o em seu artigo 2º como uma prática que envolve "violência física ou psicológica em atos de intimidação, humilhação ou discriminação" (BRASIL, 2015). Essa intimidação pode ocorrer de diversas formas, como verbal, moral, sexual, social, psicológica, física, material e até mesmo virtual, incluindo ações como depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social (BRASIL, 2015).

No contexto penal, a prática do ciberbullying pode desencadear uma série de crimes. A seguir, será apresentado um quadro com alguns dos crimes que podem ocorrer em decorrência do ciberbullying.

Quadro 1: Alguns crimes que podem ser cometidos através do ciberbullying

Crime	Conduta	Pena
Difamação (art.139, CP)	Imputar algo ofensivo à reputação de outrem.	Pena - detenção, de três meses a um ano, e multa.
Calúnia (art.138, CP)	Dizer de forma mentirosa que alguém cometeu crime. Propagar/Divulgar sabendo ser falsa a imputação.	Pena - detenção, de seis meses a dois anos, e multa.
Incitação ao crime (art.286,CP)	Incitar, publicamente, a prática de crime	Pena - detenção, de três a seis meses, ou multa.
Ameaça (art.147,CP)	Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.	Pena - detenção, de um a seis meses, ou multa.
Injúria (art.140, CP)	Ofender a dignidade ou o decoro.	Pena - detenção, de um a seis meses, ou multa.
Constrangimento Ilegal (art. 146, CP)	Constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda:	Pena - detenção, de três meses a um ano, ou multa.
Falsa identidade (art.307, CP)	Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:	Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.
Racismo (art. 20, lei n.º 7.716/89)	Praticar, induzir ou incitar a discriminação ou preconceito	Pena: reclusão de um a três anos e multa.

	de raça, cor, etnia, religião ou procedência nacional.	
Apologia do Nazismo (parágrafo 1º do art. 20, lei n.º 7.716/89)	Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.	Pena: reclusão de dois a cinco anos e multa.

Fonte: elaborado com base no DECRETO-LEI Nº 2.848/1940 e na Lei nº 7.716/1989.

Considerações Finais

É possível inferir que uma pessoa que faz uso diário das tecnologias da informação, tanto no trabalho quanto no cotidiano, deve estar atenta, não deixando de se preocupar com os riscos e as vulnerabilidades que essas ferramentas apresentam. Dessa forma, as considerações anotadas nesta síntese destacam a relevância da temática em questão, tornando a análise realizada sobre os ataques cibernéticos e as consequências advindas dessas invasões no âmbito penal extremamente relevante.

Foi possível, embora brevemente, apresentar as evoluções legislativas que regulamentam a internet e, de maneira mais específica, os crimes virtuais. Este percurso teve início na primeira lei aprovada no Brasil em 2012, a chamada "Lei Carolina Dieckmann", e foi até a última atualização nesse âmbito, com a promulgação do Decreto que ratificou a Convenção Internacional sobre o Crime Cibernético.

Os exemplos de ataques virtuais mencionados no texto dão uma noção clara de como o usuário está exposto na sua relação com o ciberespaço. São invasões que executam ações maliciosas nos aplicativos, roubam informações financeiras e instalam programas que capturam tudo que se passa em seu computador ou celular. Portanto, a preocupação e os cuidados devem ser constantes.

Além disso, foi possível acompanhar na legislação brasileira os crimes próprios e alguns crimes impróprios. O profissional da tecnologia que usa suas habilidades para cometer ilícitos ou o curioso que escolhe se envolver no mundo obscuro da criminalidade virtual será rigorosamente alcançado pela lei. Tipos penais que não eram tipificados de forma específica, como o furto mediante fraude eletrônica e o estelionato digital ou fraude eletrônica, hoje podem ser rigorosamente punidos. Também foi demonstrado um resumo dos crimes, classificados doutrinariamente como impróprios, praticados em decorrência da prática do ciberbullying. Práticas como a calúnia, injúria, difamação, racismo, entre outros, têm sua punibilidade assegurada para quem pratica esses atos no ambiente virtual.

Por fim, acredita-se que este texto possa contribuir tanto para o profissional da tecnologia da informação quanto para os operadores do direito. Esta temática é atual e carece de atualizações periódicas, então, que este estudo sirva como um guia para quem se propuser a aprofundar-se nos crimes virtuais e suas consequências legais.

Referências

BRANDÃO, Luíza Couto Chaves. **O Marco Civil da Internet e a Proteção de Dados**: diálogos com a LGPD. Cadernos Adenauer, Rio de Janeiro, n. 3, p. 35-48, out. 2019.

BRASIL. **Decreto n.º 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste em 23 de novembro de 2001. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 13 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 25 abr. 2023.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 16 fev. 2023.

BRASIL. **Lei n.º 7.716, de 5 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 6 jan. 1989. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 15 fev. 2023.

BRASIL. **Lei n.º 9.983, de 14 de julho de 2000**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 17 jul. 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm#art1. Acesso em: 26 set. 2023.

BRASIL. **Lei n.º 12.015, de 7 de agosto de 2009**. Altera o Título VI da Parte Especial do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, e o art. 1o da Lei no 8.072, de 25 de julho de 1990, que dispõe sobre os crimes hediondos, nos termos do inciso XLIII do art. 5o da Constituição Federal e revoga a Lei no 2.252, de 1o de julho de 1954, que trata de corrupção de menores. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 ago. 2009. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm. Acesso em: 25 abr. 2023.

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 1 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 fev. 2023.

BRASIL. **Lei n.º 13.185, de 6 de novembro de 2015**. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 7 nov. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 26 Set. 2023.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 abr. 2023.

BRASIL. **Lei n.º 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. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 14 fev. 2023.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 Set. 2023.

FALCAO, Mario. **Hacker Delgatti é condenado a 20 anos de prisão por invadir celulares de autoridades da Lava Jato e vazar mensagens**. G1, Brasília, 21 ago. 2023. Disponível em: https://g1.globo.com/politica/noticia/2023/08/21/hacker-delgatti-e-condenado-a-20-anos-na-operacao-que-investiga-o-vazamento-de-conversas-da-lava-jato.ghtml. Acesso em: 25 set. 2023.

FERREIRA, Rodrigo. **Segurança em Aplicações Web**. São Paulo: Editora Casa do Código, 2017.

GOMES, Frederico Félix. **Direito eletrônico e internet**. Londrina: Editora e Distribuidora Educacional S.A., 2016.

GRECO, Rogério. **Curso de Direito Penal**: parte geral, volume I. 19. ed. Niterói, RJ: Impetus, 2017.

MICROSOFT. **O que é um ataque cibernético**?. Microsoft, 2023. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-cyberattack. Acesso em: 10 set. 2023.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021. E-book (573 p.).

RODRIGUES, Renato. **Brasileiros são principais alvos de ataques de phishing no mundo**. kaspersky, 2021. Disponível em: https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/. Acesso em: 10 set. 2023.

TEIXEIRA, Tarcisio**. Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). Edição semanal - Estelionato. TJDFT, 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=A%20fraude%20eletr%C3%B4nica%20ocorre%20quando,cart%C3%A3o%20de%20cr%C3%A9dito%20ou%20d%C3%A9bito. Acesso em: 10 set. 2023.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO DO SUL (TJMS). Homem é condenado a 13 anos de reclusão por estupro virtual de vulnerável. TJMS, 2023. Disponível em: https://www.tjms.jus.br/noticia/63121. Acesso em: 26 Set. 2023.

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO (TRF3). Justiça Federal condena hackers por falsificação de documento público em sistema processual. TRF3, 2021. Disponível em: https://web.trf3.jus.br/noticias/Noticiar/ExibirNoticia/414225-justica-federal-condena-hackers-por-falsificacao-de. Acesso em: 10 set. 2023.