UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

GABRIEL FILGUEIRA SAMPAIO

A EVOLUÇÃO DA LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS: adaptações legais diante do mundo digital em transformação

JUAZEIRO DO NORTE - CE
2023

GABRIEL FILGUEIRA SAMPAIO

A EVOLUÇÃO DA LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS: adaptações legais diante do mundo digital em transformação

Trabalho de Conclusão de Curso – *Artigo Científico,* apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Micael François Gonçalves Cardoso.

JUAZEIRO DO NORTE - CE
2023

GABRIEL FILGUEIRA SAMPAIO

A EVOLUÇÃO DA LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS: adaptações legais diante do mundo digital em transformação

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de GABRIEL FILGUEIRA SAMPAIO

Data da Apresentação 12/12/2023

BANCA EXAMINADORA

_____

Orientador: Prof. Esp. Micael François Gonçalves Cardoso

_____

Membro: Prof. Me. Otto Rodrigo Cruz

_____

Membro: Prof. Esp. Francisco José Martins Bernardo de Carvalho

JUAZEIRO DO NORTE-CE
2023

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

A EVOLUÇÃO DA LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS: adaptações legais diante do mundo digital em transformação

Gabriel Filgueira Sampaio[1]
Micael François Gonçalves Cardoso[2]

RESUMO

Este trabalho discute a progressão da legislação pertinente aos delitos cibernéticos, em resposta ao avanço acelerado da tecnologia. Inicialmente, enfatiza-se a dependência crescente da sociedade em relação à internet, o que torna imprescindível a implementação de normas jurídicas para combater os delitos digitais. A questão central que o trabalho procura responder é como a legislação pode antecipar e se adaptar às ameaças cibernéticas diante do progresso tecnológico acelerado. A pesquisa emprega uma abordagem de revisão bibliográfica para investigar a aplicação da legislação sobre delitos digitais, examinando como as leis se adaptaram ao longo do tempo. O trabalho também analisa brevemente o crescimento dos delitos cibernéticos, os tipos de crimes mais frequentes e a evolução das leis a respeito. Conclui-se que, diante desses delitos, é evidente a falta de tipificações capazes de acompanhar o ritmo de crescimento, bem como o despreparo da sociedade em relação à defesa e reconhecimento de tais crimes. Além da criação de leis mais efetivas, é necessário adotar medidas que promovam a preparação da sociedade e dos agentes responsáveis pela investigação dos delitos cibernéticos, de modo a proporcionar maior segurança à sociedade no ambiente digital.

Palavras-chave: Crimes Cibernéticos. Evolução Legislativa. Pandemia.

ABSTRACT

This article discusses the evolution of legislation related to cybercrime in response to technological advancement. First, we highlight the growing dependence of society on the internet, which makes it crucial to establish legal standards to combat digital crime. The middle problem the article looks to answer is how legislation can anticipate and adapt to cyber threats in the face of rapid technological progress. The research uses a literature review approach to explore the use of legislation on digital crimes, analyzing how laws have adapted over time. The article also briefly examines the rise of cybercrime, the most common types of crime, and the evolution of laws on the subject. In the end, it found that in the face of these crimes, it is notable that there is a lack of legislation capable of keeping up with the pace of growth, as well as a lack of preparation on the part of society about defending and recognizing these crimes. In addition to the creation of more effective laws, it is necessary to adopt measures that promote the preparation of society and agents responsible for the investigation of cybercrimes so that they advance greater security to society in the digital sphere.

Keywords: Cybercrimes. Legislative Evolution. Pandemic.

[1]Discente do Curso de Direito da UNILEÃO. E-mail: gabrielfilgueira44@gmail.com
[2]Professor Orientador. Especialista em Direitos Sociais e professor do Centro Universitário Dr. Leão Sampaio (UNILEÃO). E-mail: micaelcardoso@leaosampaio.edu.br

1 INTRODUÇÃO

Atualmente, a tecnologia permeia a realidade de toda a sociedade, proporcionando inúmeros benefícios. No entanto, juntamente com esses benefícios, surgem grandes desafios que impactam o campo jurídico, forçando-o a evoluir e se adaptar, uma vez que a população está cada vez mais confrontada com crimes cibernéticos. Este trabalho tem como objetivo observar a evolução contínua da legislação para combater os crimes cibernéticos diante do avanço tecnológico.

Anteriormente, a falta de regulamentações específicas resultou no crescimento da criminalidade cibernética. A discussão sobre esse tema torna-se ainda mais relevante, visto que a sociedade se tornou mais dependente da internet, comumente utilizada para transações financeiras, meios de comunicação, armazenamento de dados importantes, criação de empresas, etc., tornando crucial o estabelecimento de normas jurídicas para prevenir os crimes digitais.

Observa-se que o mundo digital está em constante evolução, trazendo inúmeros benefícios para a sociedade desde o seu surgimento. No entanto, para o campo jurídico, essa progressão traz preocupações, pois, com seu avanço, os crimes cibernéticos também evoluem e se aperfeiçoam. Diante disso, este trabalho se propõe a responder à seguinte questão: As leis vigentes são suficientes para a prevenção e repressão dos crimes cibernéticos?

Com o objetivo de elucidar essa questão, adotamos como metodologia a pesquisa bibliográfica, apresentando informações referentes à aplicação da legislação sobre crimes digitais, elucidando o avanço dos crimes digitais e a evolução da legislação para combatê-los, por meio da consulta em livros, artigos, sites especializados e legislações.

Ao longo deste trabalho, analisaremos momentos relevantes na evolução da legislação de crimes cibernéticos, realizando um estudo de como as leis se adaptaram e foram criadas para combater tais crimes. Também analisaremos os avanços dos crimes cibernéticos, citando os tipos de crimes mais recorrentes, bem como os avanços da legislação sobre o tema.

O objetivo geral desta pesquisa é analisar a evolução da legislação relacionada a crimes cibernéticos em resposta ao avanço tecnológico, destacando como as leis se adaptaram e foram criadas para combater esses tipos de crimes. Os objetivos específicos incluem examinar o aumento dos crimes cibernéticos, incluindo estatísticas e dados relevantes sobre a frequência desses delitos, discutir o contexto dos crimes cibernéticos durante a pandemia do COVID-19 e suas implicações na segurança cibernética, e identificar desafios relacionados à investigação e punição desses crimes.

Os próximos capítulos deste estudo seguem a seguinte estrutura: o Capítulo 2 é o referencial teórico e tratará sobre o conceito, avanço e tipos de crimes cibernéticos, além de discorrer sobre a evolução da legislação e apresentar um panorama conciso sobre os crimes cibernéticos no período da pandemia; o capítulo seguinte apresentará a metodologia utilizada nesta pesquisa; o quarto capítulo tratará sobre os resultados alcançados; e, finalmente, este trabalho científico se encerrará com as Considerações Finais.

2 CRIMES CIBERNÉTICOS: CONCEITO E EVOLUÇÃO

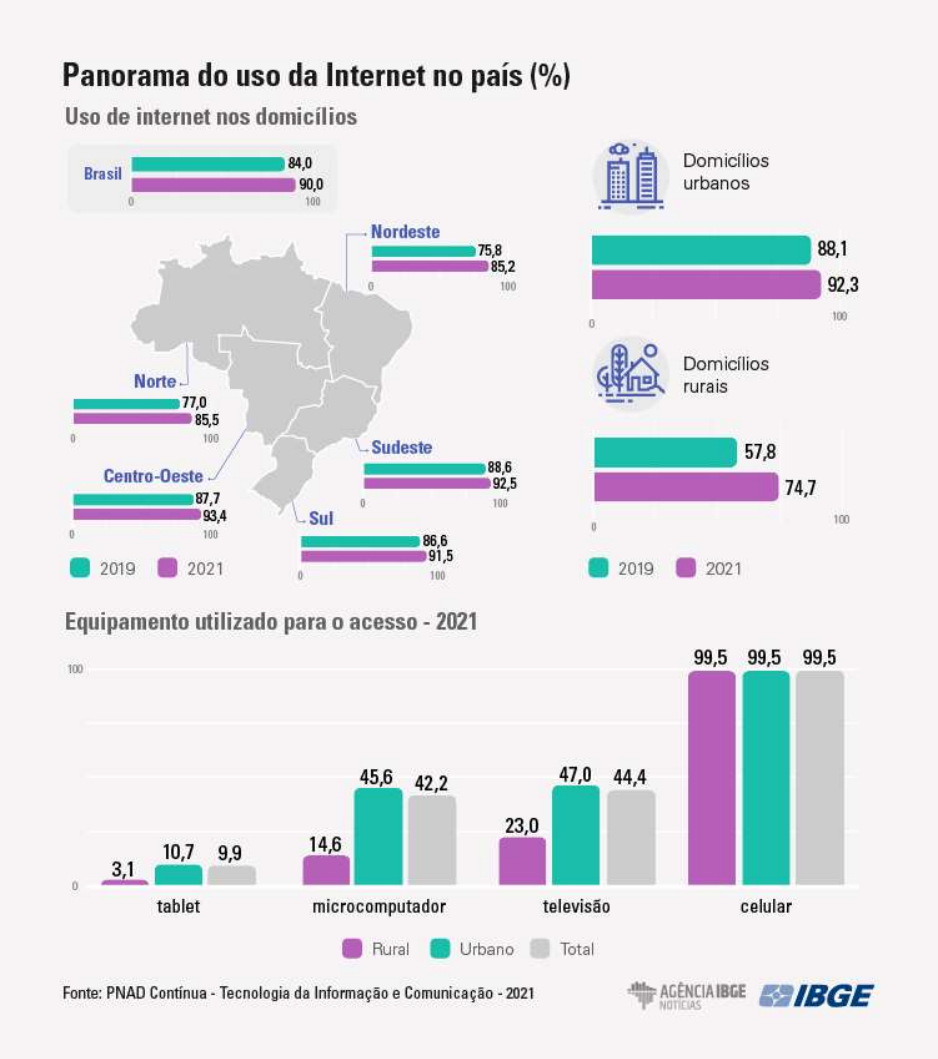
As primeiras ocorrências de crimes cibernéticos datam de meados da década de 1960, com delitos de sabotagem, manipulação, abuso de computadores e espionagem. Por volta da década de 1980, com as transformações econômicas e sociais, iniciou-se o crescimento das ações criminosas no âmbito tecnológico, como manipulações de caixas bancários, pornografia infantil e pirataria de programas (Oliveira Júnior, 2013).

Como mencionado anteriormente, com o desenvolvimento da internet, paralelamente aos benefícios trazidos, surgiram os crimes cibernéticos, que são atos delituosos no universo digital. De acordo com Rocha (2017, p. 13), os crimes virtuais são aqueles cometidos utilizando algum tipo de dispositivo tecnológico, deixando claro que tais crimes são realizados na esfera virtual. Mais especificamente, a autora Rosa (2002) explica que os crimes cibernéticos compreendem procedimentos que afetam dados em qualquer estágio, seja armazenados, compilados ou em transmissão, e requerem dois elementos indissociáveis: atentado contra dados preparados para operações computacionais e a utilização de hardware e software para perpetrar essas ações.

Na prática, esses crimes podem ser direcionados contra ou pela utilização de sistemas de informática, afetando interesses juridicamente protegidos, como ordem econômica, integridade corporal, liberdade individual, privacidade, honra, patrimônio público ou privado, e a Administração Pública, entre outros. Este tipo de crime tem aumentado à medida que as pessoas armazenam dados importantes em meios virtuais, acessam sites de segurança duvidosa, têm seus dispositivos pessoais hackeados e utilizados para golpes.

Notadamente, crimes cibernéticos e o mundo digital estão intrinsecamente ligados. Assim, é de se esperar que, com o crescimento do uso da internet, também haja um aumento no número deste tipo de crime. Sobre o uso de internet no Brasil, cerca de 84% dos domicílios possuíam acesso em 2019. Já em 2021, houve um aumento de 6 pontos percentuais, chegando à marca de 90%, de acordo com o gráfico a seguir:

Gráfico 1 - Panorama do uso da internet no país (%)



Fonte: IBGE, 2022.

Com o aumento do uso das redes, as tentativas e a realização de crimes cibernéticos aumentaram drasticamente. O FortiGuard Labs (2021), em seu relatório, revela que no ano de 2020 o Brasil sofreu 8,5 bilhões de tentativas de ataques, sendo a maior parte (5 bilhões) nos meses de outubro, novembro e dezembro. Já em 2021, foram registradas 88,5 bilhões de investidas neste sentido, um aumento de 950% em relação a 2020. O Brasil chegou a ocupar a segunda posição com mais ataques na América Latina e Caribe, conforme é possível observar na tabela a seguir:

Tabela 1: Ranking de tentativas de ataques cibernéticos na América Latina e Caribe.

País	**Nº de tentativas de ataques**
México	156,000,000,000
Brasil	88,500,000,000
Peru	11,500,000,000
Colômbia	11,200,000,000
Chile	9,400,000,000
Argentina	3,200,000,000
Panamá	3,200,000,000
Costa Rica	2,500,000,000
República Dominicana	2,200,000,000
Porto Rico	926,000,000

Fonte: fortinet.com São Paulo, 2022.

No primeiro semestre de 2022, o Brasil registrou 31,5 bilhões de tentativas de ataques a empresas. Esse número é 94% superior ao do primeiro semestre do ano anterior, quando foram registrados 16,2 bilhões de tentativas de ataques (Portal CNN, 2022). Esse crescimento se deve à dificuldade de combater os referidos crimes, uma vez que, nos meios digitais, existem formas de deixar o mínimo de vestígios possíveis, agindo de forma anônima e silenciosa, o que tem dificultado as prisões em flagrante e até mesmo a constituição de prova.

Segundo o advogado criminalista, especialista em cibercrimes, D'URSO (2019), em entrevista ao Jornal Estadão, a maior dificuldade com relação ao combate desses crimes está relacionada à dificuldade de se fazer prova e investigar a origem do delito, a materialidade e a autoria. Qualquer pessoa pode ser autora de um crime cibernético, tendo em vista que para acessar as redes não é necessária autorização nem identificação, dificultando ainda mais o reconhecimento do autor de tais delitos.

De acordo com Harakemiv e Vieira (2014), a facilidade de identificação de crimes cibernéticos contrasta-se com a extrema dificuldade em determinar o autor do delito. Isso se deve à ausência de controle efetivo e à não exigência de identificação para o acesso à internet. Nesse cenário, qualquer pessoa pode se tornar autora do crime, e a identificação torna-se um desafio considerável (HARAKEMIV; VIEIRA, 2014).

Os usuários, ao se conectarem à rede por meio do protocolo TCP/IP, compartilham um único número de IP, que se altera automaticamente a cada acesso, dificultando a rastreabilidade do agente que, após desconectar-se da internet, elimina qualquer possibilidade de identificação por meio do número de IP utilizado durante a prática do delito.

Outra questão que dificulta a apuração policial é a imprescindibilidade de profissionais especializados na área para acompanhar esse desenvolvimento tecnológico. A própria Lei 12.735/2012 (Brasil, 2012) prevê em seu artigo 4º que "os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado".

Uma vez que foi realizada uma contextualização da evolução dos crimes cibernéticos no Brasil e no mundo, torna-se imperativo apresentar como os legisladores vêm, durante os últimos anos, tentando conter este problema.

2.1 AVANÇO DA LEGISLAÇÃO

Até o passado recente, não havia legislação específica para tratar de crimes cibernéticos, recorrendo-se ao Código Civil, ao Código Penal, à Lei 9.296/96, que dispõe sobre crimes nas interceptações de comunicação em sistema de telefonia, informática e telemática, e à Lei 9.609/98, que tipifica sobre a propriedade intelectual de programas de computadores, na aplicação dos casos concretos ao que fosse cabível.

Com os crimes cibernéticos se tornando cada vez mais frequentes no dia a dia, os casos e relatos aumentaram de forma exponencial. Um desses casos, que teve grande repercussão no Brasil, foi o da atriz Carolina Dieckmann que, em 2012, teve seu aparelho invadido e fotos pessoais divulgadas.

O episódio serviu de fato gerador para a criação da Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipifica a invasão de dispositivos como crime, incluindo no Código Penal os artigos 154-A e 154-B, configurando como crime o ato de invadir dispositivo informático alheio, seja ele conectado ou não à rede de computadores, por meio da violação indevida de mecanismo de segurança, com o objetivo de obter, adulterar ou destruir dados sem a autorização do titular do dispositivo.

A penalidade para tal conduta inclui detenção, variando de 3 meses a 1 ano, além da aplicação de multa. Adicionalmente, aqueles que produzem, oferecem, distribuem, vendem ou propagam dispositivos ou programas de computador com o intuito de facilitar tal prática também estão sujeitos às mesmas penalidades. O legislador estabelece um aumento de pena,

entre um sexto e um terço, nos casos em que a invasão resulta em prejuízo econômico (Brasil, 2012).

Posteriormente, em 23 de abril de 2014, foi criada a Lei 12.965, também conhecida como o Marco Civil da Internet, que estabelece os princípios que regulam o uso da internet. Os artigos da referida lei dispõem, por exemplo, sobre os princípios do uso da internet no Brasil e os direitos garantidos aos usuários. Veja-se:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei (Brasil, 2014).

Segundo Alves (2020), todos os usuários da internet são regidos pelas normas e princípios que regulam as interações que ocorrem na rede. Tais princípios têm como objetivo garantir que as interações online sejam justas, preservando assim, os direitos à liberdade, privacidade e o bom funcionamento dos serviços de internet contratados (ALVES, 2020).

A Lei n° 14.132, de 31 de março de 2021, trouxe a criação do crime de perseguição, popularmente conhecido como stalking, que se dá com perseguições e ameaças quando a vítima não quer ter contato com o criminoso. Crime bastante recorrente, atingindo a marca, no ano de 2021, de 115 casos diários. Em 2022, esse número passou a 155. Antes da referida lei, as denúncias eram registradas como contravenções e perturbação (Portal G1, 2022). O art. 147-A da Lei nº 14.132/21 (Brasil, 2021) define o crime de stalking:

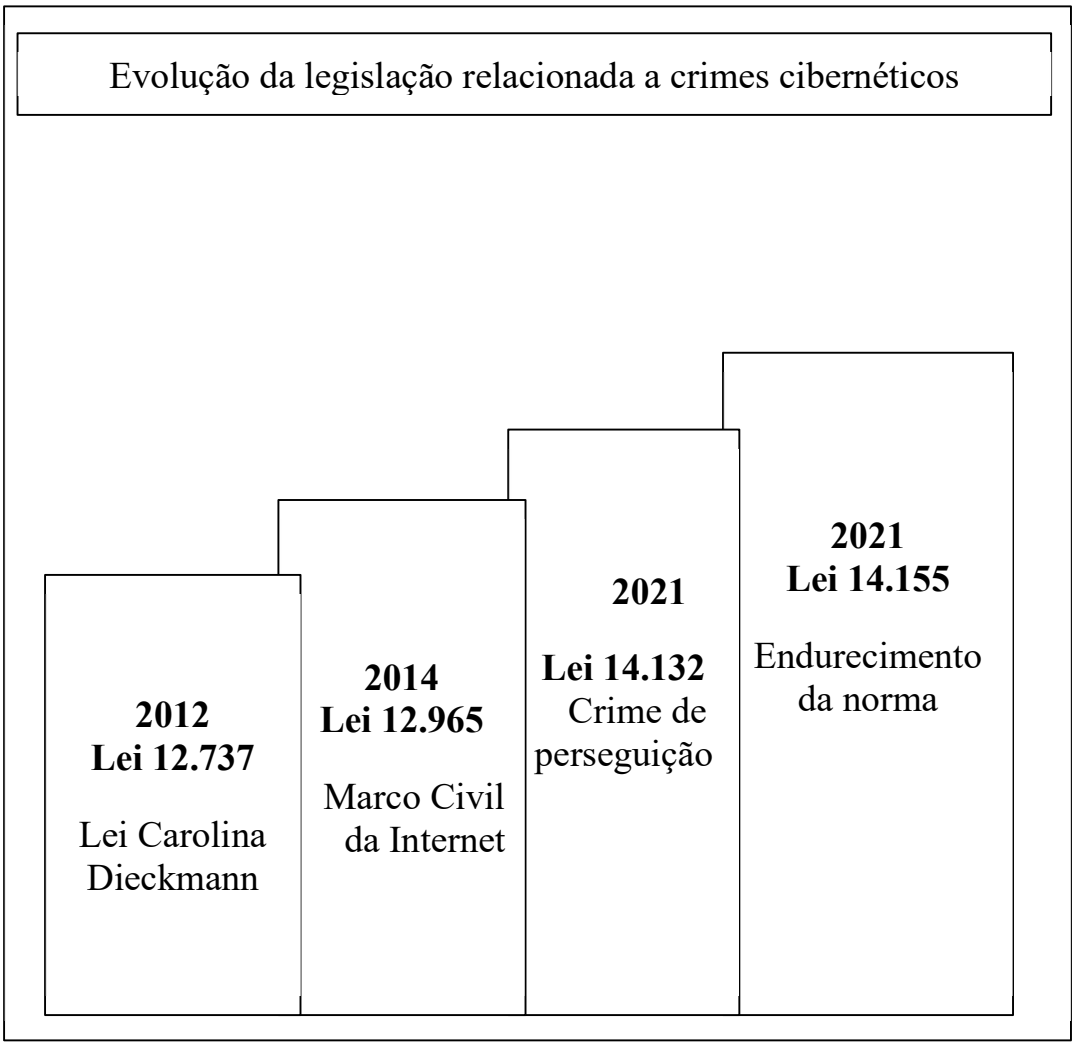
> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa (BRASIL, 2002).

Em 27 de maio de 2021, com um cenário de grande avanço dos crimes cibernéticos devido à pandemia, foi sancionada a Lei Nº 14.155, que trouxe consigo o endurecimento das normas já existentes em seus artigos. Tornou a violação de dispositivos informáticos mais rígida em suas penas e definiu como crime a fraude eletrônica e o estelionato, que são as atividades fraudulentas no mundo digital com a intenção de enganar, captar dados e obter ganhos financeiros. Trouxe também agravantes para os mesmos crimes, quando cometidos, no caso da

fraude, com servidores fora do território nacional, e no caso do estelionato, quando cometido contra idosos ou vulneráveis.

Sobre a tipificação de cibercrimes, Cunha (2021) argumenta que o "tipo penal surgiu com a justificativa de preencher uma lacuna e de tornar proporcional a pena para uma conduta que, embora muitas vezes tratada como algo de menor importância, pode ter efeitos - especialmente psicológicos - muito prejudiciais na vida de quem a sofre" (CUNHA, 2021).

Figura 1 - Evolução da legislação relacionada a crimes cibernéticos



Fonte: Elaborado pelos autores, 2023.

2.2 CRIMES CIBERNÉTICOS NA PANDEMIA

A pandemia do COVID-19 no Brasil desencadeou consequências imensuráveis, como crises política, econômica e emocional. Com o isolamento social, o teletrabalho, o ensino a

distância, as transações financeiras digitais e a grande expansão do e-commerce se tornaram realidade para os brasileiros, intensificando o uso expressivo das redes.

De acordo com a Aser Security, os crimes virtuais mais comuns são a engenharia social, que consiste na manipulação da vítima para que clique em links maliciosos, permitindo a conexão de material infectado em seu aparelho e a revelação de informações sigilosas. O backdoor, que se assemelha a um cavalo de Tróia, permite que os invasores assumam o controle do aparelho contaminado, possibilitando a realização de transações bancárias, envio de e-mails, eliminação de arquivos, entre outros. Outro crime bastante comum é a manipulação de URL, onde os criminosos conseguem redirecionar páginas para outros sites.

O Eavesdropping, bastante conhecido por violar o princípio da confidencialidade, configura-se pela ação do agente inspecionar as informações dos dispositivos ou sistemas, sem a devida autorização do usuário, podendo se deparar com informações de cunho sigiloso da vítima. Outra modalidade bastante comum é o Phishing, que é a criação de sites e aplicativos falsos usados para enganar os usuários, levando-os a clicar em links contaminados ou preencher dados e informações pessoais.

Um exemplo bastante recorrente é a clonagem de WhatsApp. Muitos golpes também ocorrem por meio de sites de vendas falsos, onde, além de sequestrar dados dos compradores, os criminosos também conseguem o valor do objeto falso vendido. Durante a pandemia, o número de vendas online aumentou bastante, e, consequentemente, golpes como esse. Em levantamento realizado pelo Procon (2022) junto à Conferência Nacional do Comércio, foi constatado que em junho de 2020 houve um aumento de 73% no e-commerce em relação ao ano anterior, já em 2021 o aumento foi de 48,2% em relação a 2020.

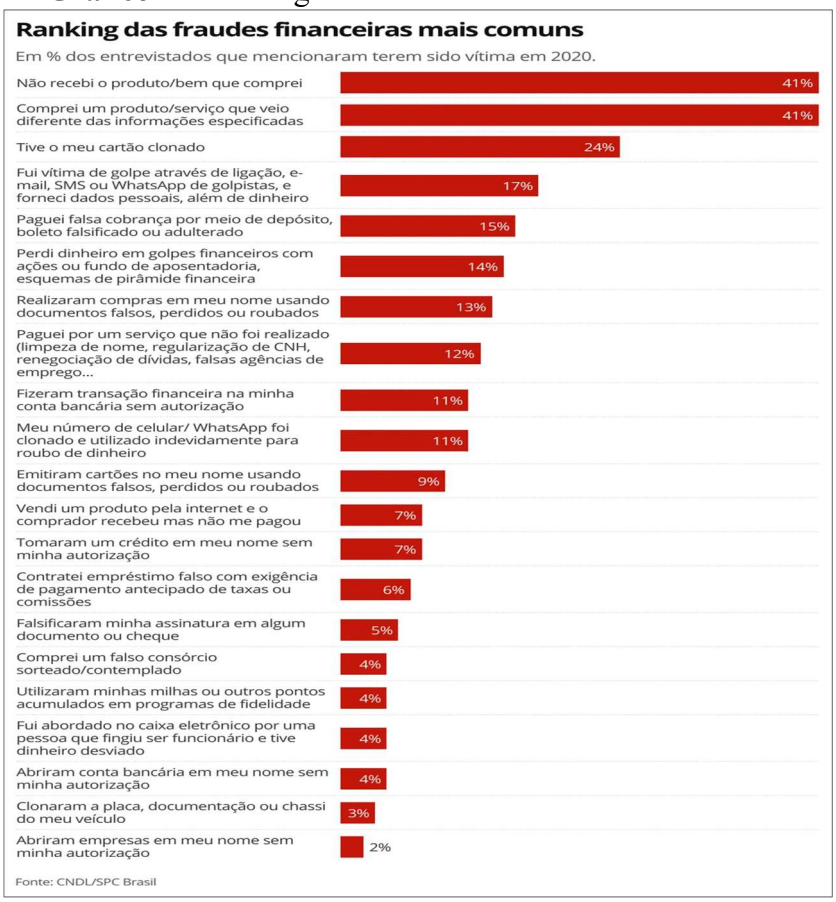
A Confederação Nacional de Dirigentes Lojistas (CNDL) juntamente ao Serviço de Proteção de Crédito (SPC Brasil), em pesquisa realizada recentemente, constataram que o crescimento das compras online no período pandêmico resultou em um aumento significativo das fraudes na internet. Em parceria com o SEBRAE, foram entrevistados 949 internautas com idade igual ou maior a 18 anos. A coleta foi feita entre 15 de abril e 30 de abril de 2021. De acordo com o resultado da pesquisa, 59% dos internautas sofreram algum tipo de fraude financeira nos últimos 12 meses, contra 46% em 2019, correspondendo a um contingente de 16,7 milhões de brasileiros (Alvarenga, 2021).

O estudo supracitado conseguiu estimar o possível prejuízo trazido pelas fraudes, chegando a R$2,7 bilhões nos últimos 12 meses, já incluído os gastos com a busca da recuperação, tendo o valor médio da fraude de R$512,4 (Alvarenga, 2021). Entre os principais

locais do golpe, as lojas online estão com maior incidência, 38,8%, seguidos pelos bancos com 8,9% e as financeiras 7,7%.

No ranking das fraudes mais comuns, estão no topo o não recebimento de produto comprado, a clonagem de cartão e os golpes através de ligações ou mensagens, conforme gráfico 2.

Gráfico 2 - Ranking das fraudes financeiras mais comuns



Fonte: Dados extraídos do site do Procon (2023)

Durante a pandemia, em face das dificuldades que os cidadãos estavam enfrentando, foi criada a Lei 13.982, de 2 de abril de 2020 (Lei Auxílio Emergencial), que proporcionou uma renda mínima, o chamado "Coronavoucher", aos cidadãos brasileiros mais vulneráveis durante a pandemia. Os trâmites até a fase do recebimento do auxílio foram realizados por meio de um aplicativo.

> Art. 20-A. Em razão do estado de calamidade pública reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020 , e da emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19), o critério de aferição da renda familiar mensal **per capita** previsto no inciso I do § 3º do art. 20 poderá ser ampliado para até 1/2 (meio) salário-mínimo (BRASIL, 2020).

Um dia após o início do cadastramento no programa, já havia 26,6 milhões de pessoas inscritas, 217 milhões de acessos ao site e 22,5 milhões de downloads do aplicativo (Portal G1, 2020). Diante de tantos dados importantes sendo compartilhados e dinheiro sendo transferido, os golpistas vislumbraram oportunidades para fraudar. Muitos golpes foram realizados no período (PORTAL G1, 2020).

Uma das fraudes mais comuns nesta época foi conhecida como golpe do auxílio emergencial, que consistia em sites e aplicativos que se passavam por oficiais. Em pesquisa realizada pela Psafe, em 2020, foram 7 milhões de compartilhamentos e acesso aos sites usados neste tipo de golpe (Portal UOL, 2020).

3 METODOLOGIA

Neste capítulo, é crucial compreender inicialmente o que se entende por método. Conforme definido por Marconi & Lakatos (2006, p. 83), método é um "conjunto de atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros -, traçando o caminho a ser alcançado, detectando erros e auxiliando as decisões do cientista". Após a explanação do conceito de método, optou-se por elucidar a metodologia deste trabalho em três campos distintos: o método de abordagem, a classificação da pesquisa com base em seus objetivos e o método de procedimento (MARCONI; LAKATOS, 2006, P. 83).

O método de abordagem empregado nesta pesquisa é o indutivo, caracterizado pela análise do objeto de estudo, partindo de premissas menores e particulares, culminando em conclusões universais. O trabalho aqui proposto visa à observação de casos reais com o objetivo de obter uma resposta de caráter generalista. No que tange ao método de procedimento, este projeto se enquadra na categoria observacional. Optou-se por este método na presente pesquisa por se tratar de um estudo que observa fatos passados e recentes. Quanto à técnica, adota-se uma pesquisa bibliográfica. A pesquisa é realizada por meio do levantamento de literatura em livros, artigos e revistas digitais.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Este trabalho buscou realizar uma análise meticulosa, por meio de consultas a dados e legislações relacionados aos avanços dos crimes cibernéticos, bem como da evolução da própria

legislação para combatê-los. O objetivo era determinar se as leis e formas de enfrentamento estão sendo realmente eficazes para mitigá-los.

É notável que o aumento dos crimes cibernéticos está diretamente ligado ao avanço da tecnologia. Para cada inovação ou aperfeiçoamento nas leis, em contrapartida, novos crimes são criados ou, no caso dos existentes, aprimorados. Assim, é imprescindível que a legislação referente à temática acompanhe o ritmo acelerado do crescimento tecnológico.

O estudo destaca a trajetória das criações das leis para o enfrentamento dos crimes, mostrando como um incidente notório se transformou em lei específica, como no caso da Lei Carolina Dieckmann, que surgiu após a atriz ter seu computador invadido e suas fotos íntimas vazadas. Enfatiza também, nesse trajeto, a necessidade do endurecimento das normas pela Lei 14.155.

No entanto, os resultados apontam desafios na investigação dos referidos crimes, tendo em vista a grande dificuldade de coletar provas, identificar autores e a possibilidade do anonimato oferecida pela internet, tornando a prisão em flagrante e a produção de provas mais difíceis, destacando a complexidade do ambiente digital.

Em relação à pandemia, os resultados mostram que o aumento das atividades online, como teletrabalho e compras na internet, ocasionou um aumento substancial nos crimes cibernéticos. Houve uma grande incidência no período do auxílio emergencial.

5 CONSIDERAÇÕES FINAIS

De 2012 até os dias atuais, foram promulgadas as leis 12.737/12 (Lei Carolina Dieckmann), 12.735/12 (Lei Azeredo), 12.965/14 (Marco Civil da Internet), 14.155/21 e 14.132/21 (Crime de Perseguição). A última lei relacionada diretamente ao tema foi criada em 2021. No entanto, os dados mostram que houve um aumento no número de ataques entre 2021 e 2022, sugerindo que as leis vigentes ainda não conseguiram acompanhar os crimes cibernéticos.

Tais crimes são mais complexos de serem resolvidos e solucionados, uma vez que na internet é possível o anonimato, tornando a identificação do autor bastante difícil de ser revelada. Outro fator que dificulta é que nos crimes cometidos nas redes, são quase impossíveis de acontecer flagrante delito.

Entre as inúmeras modalidades de cibercrimes, muitas têm em comum a intenção de ludibriar ou mascarar informações com a finalidade de enganar as vítimas. Logo, quanto menos

experiência tecnológica e conhecimento dos meios usados pelos criminosos, mais difícil se torna escapar dos golpes.

Assim, é indiscutível que para enfrentar esses desafios se faz necessário, não somente a criação de leis, mas também, em paralelo a isto, investimentos em recursos especializados e tecnológicos, capacitação e conscientização da sociedade, capacitação dos agentes para o combate, maior vazão de casos e medidas de prevenção, cooperação internacional e constante atualização de técnicas de segurança.

REFERÊNCIAS

ASER SECURITY. **Crimes cibernéticos comuns**. Disponível em: <https://www.aser.com.br/os-7-tipos-de-ataques-ciberneticos-mais-comuns/>. Acesso em 28 set. 2023.

ALVES, Matheus de Araújo. **Crimes Digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova**. São Paulo, SP: Editora Dialética, 2020.

ALVARENGA, Darlan. **Cresce número de consumidores vítimas de fraudes financeiras no Brasil**. G1 - Globo. Disponível em: <https://g1.globo.com/economia/noticia/2021/06/24/cresce-no-de-consumidores-vitimas-de-fraudes-financeiras-no-brasil-veja-ranking-das-mais-recorrentes.ghtml#>. Acesso em: 12 out. 2023.

BRASIL. **Lei Nº 9.296, de 24 de Julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal**. Brasília, 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 14 out. 2023.

BRASIL. Lei Nº 9.609, de 19 de fevereiro de 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências**. Brasília, 1998. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 15 out. 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos.** Brasília. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 out. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasília. 2014. Disponível

em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965>.htm. Acesso em: 18 out. 2023.

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. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Acesso em: 25 out. 2023.

BRASIL. Lei nº 14.132, de 31 de março de 2021. **Tipificando o crime de perseguição (stalking)**. Brasília. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm>. Acesso em: 12 out. 2023.

BRASIL. **Lei Nº 13.982, de 2 de abril de 2020**. Altera a Lei nº 8.742, de 7 de dezembro de 1993, para dispor sobre parâmetros adicionais de caracterização da situação de vulnerabilidade social para fins de elegibilidade ao benefício de prestação continuada (BPC), e estabelece medidas excepcionais de proteção social a serem adotadas durante o período de enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19) responsável pelo surto de 2019, a que se refere a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13982.htm>. Acesso em: 26 out. 2023.

BRASIL. **Código Penal: promulgado em 7 de dezembro de 1940**. Lei Nº 12.735, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/DecretoLei/Del2848.htm>. Acesso em: 28 set. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 28 set. 2023.

CUNHA, Rogério Sanches. **Lei 14.132/21: Insere no Código Penal o art. 147-A para tipificar o crime de perseguição**. Meu Site Jurídico, Editora Juspodvim, 01 de abril de 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/04/01/lei-14-13221-insere-no-código-penaloart>. Acesso em: 15 de out. 2023.

CNN BRASIL. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%. 2022**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em: 10 out. 2023.

FORTIGUARD LABS. **Relatório sobre ciberataques no Brasil. 2021**. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em: 07 out. 2023.

HARAKEMIW, Rafael Antônio; VIEIRA, Tiago Vidal. **Crimes Cibernéticos**. Anais do 2º Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais, 2014. Disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-análise-doprocesso-investigatório-e-desafios-enfrentado>. Acesso em: 10 out. 2023.

IBGE. **Uso de internet, televisão e celular no Brasil**. Educa, 2019. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisaoe-celular-no-brasil.html. Acesso em: 14 out. 2023.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 6. ed. São Paulo: Atlas, 2006.

OLIVEIRA JÚNIOR, Eudes Quitino de. **A nova Lei Carolina Dieckmann.** Disponível em: <http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolinadieckmann>. Acesso em: 01 out. 2023.

PROCON. **Compras realizadas através da internet durante a pandemia elevam número de crimes virtuais**. 2022. Disponível em: <https://tribunahoje.com/noticias/economia/2022/02/07/97217-compras-realizadas-atraves-da-internet-durante-a-pandemia-elevam-numero-de-crimes-virtuais>. Acesso em: 03 out. 2023.

PORTAL G1. **Denúncias de stalking passaram de 56 mil casos no Brasil em 2022**. 2023. Disponível em: <https://g1.globo.com/bom-dia-brasil/noticia/2023/09/26/denuncias-de-stalking-passaram-de-56-mil-casos-no-brasil-em-2022.ghtml>. Acesso em: 08 out. 2023.

PORTAL G1. **26,6 milhões já se cadastraram para receber o auxílio emergencial de R$ 600**. 2020. Disponível em: <https://g1.globo.com/economia/noticia/2020/04/08/266-milhoes-ja-se-cadastraram-para-receber-o-auxilio-emergencial-de-r-600.ghtml>. Acesso em: 08 out. 2023.

ROCHA, A. A**. Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet**. São Paulo: Faculdade de Ensino Superior e Formação Integral, Curso de Direito, 2017. Disponível em: https://www.faef.br/userfiles/files/23. Acesso em 10 de mai. 2023.

ROSA, Fabrízio. **Crimes de Informática.** Campinas: Bookseller, 2002. p. 53-54.

UOL. **Golpe do auxílio emergencial atinge mais de 7 milhões de pessoas**. 2020. Disponível em: <https://economia.uol.com.br/noticias/redacao/2020/04/22/golpe-auxilio-emergencial-whatsapp.htm>. Acesso em: 09 out. 2023.

PARECER DE REVISÃO ORTOGRÁFICA E GRAMATICAL

Eu, Aline Rodrigues Ferreira, graduada em Biblioteconomia pela Universidade Federal do Cariri, atesto que realizei a revisão ortográfica e gramatical do trabalho intitulado "**A EVOLUÇÃO DA LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS: adaptações legais diante do mundo digital em transformação**", de autoria de Gabriel Filgueira Sampaio, sob orientação do (a) Prof.(a) Micael François Gonçalves Cardoso. Declaro que este TCC está em conformidade com as normas da ABNT e apto para ser submetido à avaliação da banca examinadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 15/11/2023

gov.br
Documento assinado digitalmente
ALINE RODRIGUES FERREIRA
Data: 16/11/2023 14:55:35-0300
Verifique em https://validar.iti.gov.br

ALINE RODRIGUES FERREIRA

PARECER DE TRADUÇÃO DO RESUMO PARA LÍNGUA INGLESA

Eu, Patrícia Karla Filgueira Borja Almeida, professor(a) com formação Pedagógica em Letras: Língua Inglesa-Licenciatura, pela Instituição de Ensino Superior URCA – Universidade Regional do Cariri, realizei a tradução do resumo do trabalho intitulado A EVOLUÇÃO DA LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS: ADAPTAÇÕES LEGAIS DIANTE DO MUNDO DIGITAL EM TRANSFORMAÇÃO do(a) aluno(a) Gabriel Filgueira Sampaio e orientador(a) Prof. Esp. Micael François Gonçalves Cardoso. Declaro que o ABSTRACT inserido neste TCC está apto à entrega e análise da banca avaliadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 18/11/2023

Patrícia Karla Filgueira B. Almeida

Assinatura do professor (a)

Patrícia Karla Filgueira B. Almeida
Professora de Inglês e Espanhol