FACULDADE DE JUSSARA - FAJ
CURSO DE DIREITO

O COMBATE AOS CRIMES CIBERNÉTICOS COM O AVANÇO DA TECNOLOGIA NA ÓTICA DA LEGISLAÇÃO BRASILEIRA

JUSSARA/GO
NOVEMBRO/2024

CARLOS JOEL RODRIGUES LIMA

O COMBATE AOS CRIMES CIBERNÉTICOS COM O AVANÇO DA TECNOLOGIA NA ÓTICA DA LEGISLAÇÃO BRASILEIRA

Trabalho de Conclusão do Curso de Direito da Faculdade de Jussara-FAJ, para obtenção de nota na disciplina de Trabalho de Conclusão de Curso 2, do docente: Profº Sanderson.
Sob orientação do Professor Esp. Dr. Rodrigo R. Marques.

JUSSARA/GO
NOVEMBRO/2024

Carlos Joel Rodrigues Lima**
Rodrigo R. Marques***

RESUMO: Este trabalho expõe as nuances relativas aos crimes cibernéticos, levando em consideração o aumento expressivo nos últimos anos com o advento da tecnologia. Vale salientar que é possível que a legislação não seja suficientemente capaz de prever e prevenir com a criação de leis e, com elas, mecanismos para se coibir a prática destes. Importa dizer que este artigo busca a compreensão acerca da dificuldade em combater esses tipos de crimes, uma vez que estes vêm aumentando gradativamente, o que impõe uma necessária reposta do poder público com agente punidor. Ademais, este artigo visa entender quais tipos penais podem ser empregados aos crimes cibernéticos e esse ambiente, tendo em vista o demasiado avanço da tecnologia em um ambiente totalmente novo e ainda pouco explorado. Entrementes, visa entender como se classificam esses crimes, se enquadram na legislação vigente para se obter uma investigação e posterior punição por parte do Estado, bem como se a legislação vigente é suficiente para esse combate e se a busca por segurança cibernética frente a legislação seria algo utópico frente a nossa realidade fática e perspectiva de um futuro próximo. Ainda, busca compreender se existe e, em caso afirmativo, quais as consequências do aumento dos casos de crimes cibernéticos na vida da população e como o Estado vem conduzindo as investigações e punições frente a legislação vigente, tendo em vista o respeito ao princípio da legalidade.

Palavras-chaves: Crimes Cibernéticos. Tecnologia. Legislação. Segurança Cibernética.

ABSTRACT: This work exposes the nuances relating to cybercrimes, taking into account the significant increase in recent years with the advent of technology. It is worth noting that it is possible that legislation is not sufficiently capable of predicting and preventing with the creation of laws and, with them, mechanisms to curb their practice. It is important to say that this article seeks to understand the difficulty in combating these types of crimes, since they have been gradually increasing, which requires a necessary response from the public authorities with a punishing agent. Furthermore, this article aims to understand which criminal types can be used for cybercrimes and this environment, given the excessive advancement of technology in a totally new and still little explored environment. Meanwhile, this article aims to understand how these crimes are classified, whether they fit into current legislation to obtain an investigation and subsequent punishment by the State, as well as whether current legislation is sufficient to combat this and whether the search for cyber security in the face of legislation would be something utopian given our factual reality and perspective of the near future. Furthermore, it seeks to understand whether it exists and, if so, what are the consequences of the increase in cases of cybercrime in the lives of the population and how the State has been conducting investigations and punishments in light of current legislation, with a view to respecting the principle of legality.

Keywords: Cybercrimes. Technology. Legislation. Cybersecurity.

1. INTRODUÇÃO

Este trabalho tem como tema: o combate aos crimes cibernéticos com o avanço da tecnologia na ótica da legislação brasileira. Partindo dessa temática é imprescindível a compreensão de que para chegar aos dias atuais passamos por uma grande evolução tecnológica, que marca desenvolvimento da internet, a qual tem grande implicação na vida dos seres humanos haja vista que, a mesma está inserida de forma íntegra em seus cotidianos, por apresentar amplos recursos que proporcionam mais oportunidades e facilidade para a vivência dos cidadãos.

Contudo, com a criação do mundo virtual, surgiram os conhecidos “crimes cibernéticos”, que consiste em delitos cometidos, utilizando ambientes de redes, que podem interferir e sensibilizar a vítima. Uma categoria destes crimes que são mais decorrentes é o *Phishing,* o qual corresponde a uma fraude de dados, onde o infrator objetiva obter informações pessoais do indivíduo e usá-las para seu benefício.

É indispensável salientar, que se teve um avanço no Direito Penal, com a implantação da Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckman”, que simboliza o caso de uma atriz global, a qual teve suas fotos íntimas expostas nas redes sociais, após a invasão do seu computador.

Entretanto, lamentavelmente o Código Penal apresenta retrocesso diante da constante eclosão do estelionato de dados, já que é de extrema dificuldade identificar o infrator e as pessoas continuam desinformadas e ingênuas com relação aos crimes cibernéticos. Desse modo, irei abordar metodologias e técnicas, com o objetivo de informar e propor práticas para se prevenirem e evitarem a propagação dos crimes virtuais. Nesse sentido, a problemática apresentada nesta pesquisa é: A legislação penal brasileira é capaz de coibir os crimes cibernéticos no ano atual de 2024?

A pesquisa tem como objetivo analisar o expressivo aumento dos crimes cibernéticos nos últimos anos frente ao avanço tecnológico tido em todo o mundo, buscando identificar se há e quais são as consequências sociais para as vítimas destes tipos de crimes, bem como quais tipos penais se enquadrará na forma de crimes cibernéticos.

Busco compreender se a legislação vigente é suficientemente capaz de coibir os crimes cibernéticos e se há um efetivo combate e resposta por parte do Estado quanto detentor do *jus puniendi*.

O método a ser utilizado tem um caráter dedutivo, visto que, tem como objetivo quantitativamente apresentar números de elevação dos crimes cibernéticos. Esta pesquisa apresenta três fases de embasamento, sendo elas: examinar o crescimento dos cibercrimes; explorar a legislação através de uma análise ampla e intensificada e propor aplicação para análise de resultados. O estudo foi desenvolvido com o suporte em materiais já elaborados, tendo destaques em artigos, livros, sites e pesquisas científicas.

Nesse sentido, afim de alcançar os objetivos supracitados, a pesquisa foi dividida em 4 (quatros) capítulos, sendo o primeiro acerca do crime cibernético, aduzindo sobre conceituação, surgimento, tipos de crimes e classificação. Em seguida o segundo capítulo trata sobre o crime cibernético e suas diretrizes no que tange a legislação penal brasileira. Logo vem o terceiro capítulo que faz uma abordagem jurídica sobre o crime cibernético bem como aduz sobre diretrizes penais sobre o feito.

Com a objetividade de somar com toda a pesquisa o capítulo quarto traz consigo a metodologia aplicada para a solução da problemática e a seguir há o resultado de toda a pesquisa estudada onde pode-se absorver que as tipificações legislativas, principalmente no que se refere as leis penalistas, não conseguiram acompanhar de modo que penalize da forma adequada, sendo assim, não conseguindo coibir com os crimes cibernéticos nos últimos anos.

2. ASPECTOS GERAIS DO CRIME CIBERNÉTICO

Inicialmente, pode se dizer que as denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso acerca da melhor denominação para os delitos que se relacionam com a tecnologia.

Entre outros, temos crimes de computação, delitos de informática, abuso de computador, fraude informática, enfim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia e, portanto, se deve ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual.

Segundo Antônio Chaves, cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação”. (Chaves, 2019, p. 19). Já Sérgio Marcos Roque conceitua crimes cibernéticos como sendo “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. (Roque, 2007, p. 25).

Conseguinte, Carla R. Castro leciona que “os crimes de informática são aqueles perpetrados por meio dos computadores e a maioria dos crimes são praticados através da internet, e o meio usualmente utilizado é o computador”. (Castro, 2003, p. 9).

2.1 Do surgimento

Com o avanço da tecnologia, as pessoas introduziram a “Internet” em suas vidas, que desempenha um papel importante no seu dia a dia. Com a adoção do mundo virtual, tornou-se possível fazer tudo o que precisamos sem sair de casa e num piscar de olhos, pois a sociedade passou a fazer quase tudo através de meios tecnológicos.

A rede trouxe vasto conhecimento à população, além disso, favoreceu a possibilidade de manter a comunicação entre indivíduos distantes, trabalhar em casa, obter informações com um simples clique e entre muitas outras vantagens.

Dessa forma, essa virtualidade está sempre presente no cotidiano das pessoas, facilitando as relações sociais e tornando o modo de vida mais cômodo e rápido. Portanto, esse universo digital trouxe tanta comodidade para a vida das pessoas que hoje é impossível sobreviver sem ele, por isso se tornou, antes de tudo, um objeto de necessidade diária.

Os computadores foram originalmente criados com o propósito de proporcionar comunicação entre as pessoas, transmissão de informações e aprendizado. No entanto, com o desenvolvimento da tecnologia, também surgiram crimes cibernéticos conhecidos, o que equivale a uma fraude cometida com um computador (tecnologia da informação) e conectado a uma rede.

> [...] os primeiros casos de crimes cibernéticos foram na década de sessenta. Eram utilizados computadores como forma de cometimento do crime virtual, como o estelionato. Na referida década foi que começaram a ser relatados pela imprensa os primeiros casos de crimes cibernéticos. A partir da década de setenta, c começaram os primeiros estudos empíricos sobre a criminalidade cibernética (ALBUQUERQUE, 2006, p.35).

É um fato que a Internet contribuiu e tem contribuído de forma sublime para a vida humana, mas ainda há pessoas que viram esta situação para o lado negativo e a exploram, porque há indivíduos que veem a tecnologia como uma oportunidade. Ser capaz de praticar ações ilegais para gerar seu lucro.

Na década de 1960, o termo *hacker* parecia referir-se a indivíduos que queriam programar. Porém, com o avanço da Internet, essa definição mudou para invasores de computadores de outras pessoas.

> [...] os transgressores da lei penal logo viram no computador e na Internet formidáveis instrumentos à consecução de vários delitos. Como se não bastasse, essa revolução tecnológica também deu azo à criatividade delituosa, gerando comportamentos inéditos que, não obstante o alto grau de reprovabilidade social, ainda permanecem atípicos (FURLANETO; GUIMARÃES, 2003, p.264).

De referir que nem sempre os criminosos cometeram fraudes electrónicas para obter ganhos financeiros, mas na maioria dos casos fizeram-no apenas por diversão, para demonstrarem os seus conhecimentos informáticos e curiosidade, porque os *hackers* sabem que todo sistema de segurança tem uma falha que lhe dá abertura para invadir computadores de outras pessoas e controlá-los remotamente.

Visto que esses comportamentos já eram considerados atos ilícitos, que consequentemente causam danos, deterioração e podem gerar grandes prejuízos, uma vez que alguns programas ou dados de computador não têm possibilidade de serem reutilizados pelo proprietário.

2.2 Tipos de crimes cibernéticos

Sendo a cibernética uma ciência da comunicação e dos sistemas de informação, parece o termo mais amplo e apropriado para a denominação dos delitos tratados nessa pesquisa de crimes cibernéticos.

Entretementes, Fabrizio Rosa conceitua o crime de informática como, *in verbis*:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. (Rosa, 2002, p. 53).

Já nas palavras de Alexandre Júnior, o cibercrime é definido da seguinte maneira, *ipsis literis*:

> O cibercrime nada mais é que todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia de informação é objeto de um crime. O cibercrime está associado ao fenômeno da criminalidade informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para a prática do crime ou como elemento de tipo legal de crime. (Alexandre Júnior, 2019).

O sítio eletrônico especializado em crimes cibernéticos denominado Kaspersky traz o seguinte conceito, senão vejamos:

> O crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou hackers que querem ganhar dinheiro. No entanto, ocasionalmente, o crime cibernético visa danificar computadores ou redes por outros motivos que não o lucro. Nesses casos, os motivos podem ser pessoais ou políticos. O crime cibernético pode ser realizado por indivíduos ou organizações. (Kaspersky, 2024).

Partindo do conceito de crimes cibernéticos, vislumbra-se a necessidade de se analisar a legislação vigente em relação aos tipos penais existentes que podem ser cometidos pela internet e por meio de computadores, celulares, tablets, ou seja, por meio de dispositivos eletrônicos.

Diante disso, convém salientar acerca da pedofilia, também considerada um crime virtual, a qual é considerada um crime gravíssimo, que consiste em um transtorno psiquiátrico crônico, onde o indivíduo tem desejos e fantasias de modo sexual por crianças, sendo muito praticado de forma virtual a venda de pornografia infantil.

Ademais, para este crime específico foi implementada a Lei nº 8.069/1990, mais conhecida como ECA (Estatuto da Criança e do Adolescente), mais especificamente no art. 240, §§ 1º e 2º e seus incisos.

> Art. 240_ Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente. Pena_ reclusão, de 4 (quatro) a 8 (oito) anos, e multa. § 1º_ Incorre nas mesmas penas quem: I_ agencia, facilita, recruta, coage ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. II_ exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de criança ou adolescente. § 2º_ Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: I_ no exercício de cargo ou função pública ou a pretexto de exercê-la. II_ prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou III_ prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento. (ECA, 1990).

O *phishing* é o crime virtual mais eficaz porque tem potencial de transformação. O tribunal Regional Federal da 3º Região (TRF-3) trouxe em sua página o seguinte conceito:

> Phishing uma forma de fraude na qual um invasor mal-intencionado tenta coletar informações confidenciais de uma vítima se passando por uma pessoa, departamento ou organização legítima. Os invasores tentarão obter dados privados, como credenciais de contas, números de contas bancárias, informações de identificação pessoal (como números de CPF) ou qualquer outra informação que possa ser valiosa para o invasor. (TRF-3, 2023).

Os crimes contra a honra também são considerados crimes virtuais e se caracterizam conforme expostos nos artigos 138, 139 e 140, todos do Código Penal.

É importante destacar algumas das leis que tratam da proteção de dados relacionadas ao crime cibernético, entre elas a Lei nº 12.735/2012, conhecida como Lei Azeredo, a Lei nº 12.737/2012, conhecida como Lei Carolina Dickmann e a Lei nº 12.965/2014, conhecida como Lei do Marco Civil.

Em explanação perfunctória, entendendo-se suficiente para o momento, a Lei Azeredo define os crimes cometidos no domínio digital e através das tecnologias de informação, cuja forma determina as medidas a tomar, como a necessidade de criação de uma esquadra virtual, conforme prevê o art. 4º, vejamos:

> Art. 4º_ 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. (Lei Azeredo, 2012).

Quanto à Lei Carolina Dickmann, ela define crimes cometidos na internet, como hacker, roubo de senhas e conteúdo de e-mails, exclusão intencional de *sites*, entre outros, conforme consta no artigo 1º da referida Lei e acrescentou o art. 154-A ao Código Penal.

> Art. 1º_ Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. (Lei Caroline Dickmann, 2012).

> Art. 154-A_ Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. Pena_ reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Código Penal, 1940).

Por fim, a Lei nº 12.965/2014, conhecida como “Marco Civil da Internet”, regulamenta os conceitos, benefícios, direitos e obrigações do uso da internet no Brasil e inclui, entre seu art. 3º que “a disciplina do uso da internet no Brasil tem os seguintes princípios: garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade”. (Lei do Marco Civil da Internet, 2014).

Ademais, a legislação prevê como crime a divulgação e partilha de tipos de imagens ou materiais de vídeo íntimos ou sexuais obtidos ilegalmente Lei nº 13.772/18 (Lei Rose Leonel) e Lei 13.718/18, o que demonstra que está havendo um avanço legislativo no combate aos crimes cibernéticos.

A Lei 13.772/18 em seus arts. 1º e 2º aduzem o seguinte:

> Art. 1º_ Esta Lei reconhece que a violação da intimidade da mulher configura violência doméstica e familiar e criminaliza o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado.

> Art. 2º O inciso II do caput do art. 7º da Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), passa a vigorar com a seguinte redação: Art. 7º_ [...] II_ a violência psicológica, entendida como qualquer conduta que lhe cause danos emocional e diminuição da autoestima ou que lhe prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, violação de sua intimidade, ridicularização, exploração e limitação do direito de ir e vir ou qualquer outro meio que lhe cause prejuízo à saúde psicológica e à autodeterminação. (Lei 13.772 de 2018).

Com isso, vislumbra-se que o sistema legislativo brasileiro vem trabalhando incessantemente para que as normas vigentes acompanhem os novos crimes que surjam com o avanço da tecnologia, bem como trazendo formas atualizadas de combate à criminalidade digital.

2.3 Classificação dos crimes cibernéticos

Com o advento da internet, a tecnologia já percorreu um longo caminho. Essa expansão fica evidente quando notamos que os meios de comunicação tornaram-se mais desenvolvidos e acessíveis a grande parte da população. Fazer compras online, conversar com amigos e até namorar agora são completamente normais e possíveis.

A Internet veio para ficar, mas diante de toda essa comodidade, o crime neste caso assumiu uma forma mais sutil e se tornou bastante comum, aumentando a cada dia, causando cada vez mais vítimas e tornando o ambiente virtual cheio de perigos e armadilhas. Não existe uma nomenclatura adequada para esse tipo de crime, pois ainda é uma vertente nova no mundo jurídico. Portanto, estes crimes, entre outros, também são chamados de crimes virtuais, crimes digitais, crimes informáticos.

Para que haja uma melhor compreensão acerca desse assunto, é necessário compreendermos o conceito de crime. Conforme aduz Carvalho (2008, não paginado), crime é:

> [...] material, como “todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade da paz social”. E, formal, onde o “crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo”.

Já no conceito mais minucioso, o crime informático (sendo também um crime cibernético) é “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão”. (VELLOSO, 2015 apud FERREIRA, 2000, p. 210).

Conforme aduzido anteriormente, uma grande parcela dos doutrinadores não possui um consenso no que tange este instituto, contudo existe uma classificação que atua de forma evidente nas literaturas atuais. Conforme leciona Velloso (2015 apud CORRÊA, 2000b, p. 43), os crimes cibernéticos, são “todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar”.

É importante ressaltar que, conforme parágrafo anterior, o crime será cometido contra a máquina, o próprio computador, ou seja, contra os dados presentes no dispositivo. Destruição de software e dados, roubo de informações, etc. são exemplos de alguns danos que seu computador pode sofrer.

Assim, para classificar de forma mais informativa, a classificação mais aceita da doutrina é a divisão entre crimes cibernéticos puros, impuros ou mistos.

2.3.1 Crimes Cibernéticos puros

Embora o crime cibernético ocorra quando um ator precisa absolutamente de um computador para atacar remotamente ou diretamente com um sistema de computador, e todos os interesses legítimos já estão protegidos. Neste caso, não se trata apenas de *hackear* e capturar dados massivos armazenados, mas também da intenção de modificar, inserir, falsificar ou destruir dados existentes no computador.

Nessa perspectiva Viana (2003, p. 13-26), destaca que “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)”. Ainda nesse sentido, Damásio de Jesus (2003) traz consigo o posicionamento de que os crimes eletrônicos puros ou próprios são crimes cometidos por computador e cometidos ou consumidos em meio eletrônico. Dentre eles, a tecnologia da informação (segurança do sistema, propriedade da informação e integridade dos dados, máquinas e periféricos) é o objeto jurídico protegido.

É também fundamental notar a presença de duas figuras, a saber: *hackers e crackers*. Os *hackers*, por outro lado, são pessoas que utilizam o seu conhecimento técnico para obter acesso a sistemas privados substanciais. Analisando esse contexto, podemos concluir que os hackers possuem um conhecimento único sobre esse tema e não necessariamente o utilizam para fins ilegais, pois a partir desse conhecimento podemos concluir que o campo pode ser considerado algo positivo ou não.

Já os *crackers* são aqueles que focam em ganhos ilegais. Eles invadem e comprometem qualquer site, quebram senhas e desenvolvem softwares capazes de comprometer diversas máquinas ao mesmo tempo.

2.3.2 crimes cibernéticos impuros ou mistos

O crime cibernético feio ou inapropriado é um crime cometido com computadores. Ao contrário do crime cibernético puro, esta forma de crime utiliza apenas computadores como ferramentas para cometer o crime. Porém, os crimes cometidos nesta “ajuda” já estão representados pelo Código Penal Brasileiro, o que indica que o uso do computador pessoal não é o fator principal, mas sim uma das diferentes formas de cometer os delitos já protegidos. Desta forma, aduz Damásio de Jesus (2003) aduz que o crime eletrônico impuro ou impróprio é quando um agente usa um computador como meio de produzir um resultado natural que ofende o mundo físico ou o espaço "real" e ameaça ou prejudica outros ativos não computacionais.

Graças a isso, fica mais fácil entender o que são crimes cibernéticos puros e crimes cibernéticos não puros, enfatizando sempre que uma pessoa precisa de um computador, enquanto o outro modelo não precisa apenas de um PC como meio de cometer o crime.

3. EVOLUÇÃO DO CRIME CIBERNÉTICO E SUAS DIRETRIZES NO QUE TANGE A LEGISLAÇÃO PENAL BRASILEIRA

Com os avanços contínuos da tecnologia, o ciberespaço tornou-se um terreno fértil para atividades ilegais. Neste contexto, o cibercrime ganhou importância devido à sua complexidade e escala. Cazaroti e Pinheiro (2021) ressaltam que essa nova modalidade de crime se desenvolve em um ritmo vertiginoso, exigindo do Estado uma constante atualização legislativa para a devida persecução penal.

A história do cibercrime está fundamentalmente ligada à evolução tecnológica e à utilização de redes informáticas. À medida que a sociedade adotou o uso da Internet nas suas atividades diárias, surgiram novos desafios para a lei. Dornelas (2019) destaca que a resposta estatal frente a esse fenômeno e fundamental, sendo as Leis nº 12.735/2012 e 12.737/2012 marcos legais importantes na tentativa de coibir tais práticas.

Contudo, não basta criar leis para combater o crime cibernético. Também é necessário compreender plenamente a materialidade das provas nos crimes digitais. Souza (2021) analisa o caso específico do ataque cibernético na rede de informática do Superior Tribunal de Justiça em 2020, destacando a relevância da preservação e análise de evidências digitais para uma efetiva responsabilização dos agentes infratores.

Ao contrário da rápida evolução dos mecanismos e métodos utilizados pelos criminosos no ciberespaço, o desenvolvimento de ferramentas legais para combater tais práticas tem sido mais lento. Krieguer, Ceron e Marcondes (2021) argumentam que o gap entre a evolução social e tecnológica global e a resposta legislativa tem permitido que crimes cibernéticos proliferem em um cenário de relativa impunidade.

Por outro lado, à medida que a sociedade passa por uma revolução tecnológica, a legislação luta para enfrentar os desafios desta nova realidade. Hernandez e De Toledo (2021) salientam que os crimes cibernéticos têm efeitos revolucionários no cenário jurídico, demandando uma legislação que esteja em constante evolução para garantir a proteção dos direitos e a punição dos infratores.

Outra preocupação que emerge deste contexto é a necessidade de adaptação das instituições judiciais e policiais. Cazaroti e Pinheiro (2021) pontuam que o combate efetivo aos crimes cibernéticos exige não apenas um arcabouço legal robusto, mas também profissionais capacitados e estruturas especializadas para investigar e processar tais delitos.

Portanto, a evolução do cibercrime representa um dos maiores desafios do século XXI para o direito penal. As transformações tecnológicas, a rapidez da difusão da informação e o carácter global da Internet exigem uma resposta rápida, integrada e eficaz por parte das organizações responsáveis por garantir a segurança e a justiça. Hernandez e De Toledo (2021) reiteram que, diante deste cenário, é imperativo que o ordenamento jurídico esteja em constante atualização, de forma a responder adequadamente aos novos desafios impostos pelos crimes cibernéticos.

3.1 Origem e primeiras ocorrências

O advento da era digital traz consigo uma ampla gama de oportunidades e desafios. Neste contexto, a origem do cibercrime está fundamentalmente ligada à expansão da utilização de computadores e redes de comunicação. Conforme apontado por Cazaroti e Pinheiro (2021), os primeiros vestígios de crimes cibernéticos datam das décadas de 1970 e 1980, quando os sistemas informatizados começaram a ser amplamente adotados por empresas e instituições.

Nesta fase inicial, os crimes estavam mais relacionados com tentativas de intrusão de sistemas por parte de entusiastas e curiosos, muitos dos quais procuravam apenas o desafio de *hackear* sistemas, sem necessariamente terem intenções maliciosas ou lucrativas. Dornelas (2019) destaca que o cenário da época era menos complexo do que o atual, uma vez que a internet ainda não era uma realidade globalizada e os sistemas eram menos interconectados.

No entanto, à medida que a Internet se tornou mais popular e os sistemas se tornaram mais complexos, o cibercrime começou a evoluir, tanto tecnicamente como em termos de motivação. Krieguer, Ceron e Marcondes (2021) enfatizam que essa transição marcou a passagem de invasões inocentes para ações com propósitos claros de roubo de dados, espionagem ou vantagem financeira.

O desenvolvimento tecnológico acelerado dos anos 1990 e a expansão da World Wide Web intensificaram a problemática. Lima et al. (2022) pontuam que foi nesse período que surgiram as primeiras legislações específicas para combater os crimes cibernéticos em diversos países, dado o aumento exponencial desses delitos.

Hernandez e De Toledo (2021) sublinham a maneira como, paralelamente ao desenvolvimento tecnológico, surgiu uma subcultura de hackers, que, motivados por diversas razões – desde a busca por reconhecimento até objetivos políticos ou financeiros –, desafiavam constantemente as medidas de segurança existentes.

A virada do milênio inaugurou uma nova era para o crime cibernético. Com o surgimento e a popularização das redes sociais, do comércio eletrônico e dos serviços bancários online, os criminosos encontraram novos alvos. Souza e Cervinski (2021) discorrem sobre como a crescente digitalização de serviços e informações pessoais tornou-se um chamariz para ações mal-intencionadas.

De acordo com Souza (2021) é relevante destacar que além das motivações financeiras, houve um aumento nos crimes de natureza pessoal, como *cyberbulling*, difamação e invasão de privacidade, refletindo as transformações sociais e a maneira como interagimos no mundo virtual.

Além disso, a evolução global da internet trouxe desafios jurisdicionais. Cazaroti e Pinheiro (2021) ressaltam a dificuldade em lidar com crimes que transcendem fronteiras nacionais, exigindo cooperação internacional para rastrear e punir responsáveis que podem estar atuando em qualquer canto do mundo.

Em suma, a trajetória do cibercrime reflete a evolução da tecnologia e da própria sociedade digital. Desde seus primórdios, marcados por invasões de curiosos, até os ataques sofisticados de hoje, que abrangem desde grandes empresas até pessoas físicas, a necessidade de compreender e combater eficazmente esses crimes tornou-se prioridade no cenário jurídico global (LIMA et al., 2022).

3.2 PRINCIPAIS MODALIDADES E SUA PREVALÊNCIA

No contexto digital contemporâneo, os tipos de crimes cibernéticos diversificaram-se e adquiriram importância nos campos jurídico e social.

Os crimes de hacking, conforme explica Souza (2021), têm aumentado em prevalência, dada a profunda integração das tecnologias no cotidiano das pessoas. Invadir sistemas privados, seja para obter dados pessoais ou para outros fins maliciosos, constitui uma violação grave da privacidade e dá segurança da informação.

O *phishing*, que envolve enganar indivíduos para que forneçam dados pessoais através de sites falsos ou mensagens de e-mail, tornou-se uma das práticas mais comuns entre os cibercriminosos.

Este tipo de crime, como aponta Dornelas (2019), tem se beneficiado da falta de informação e do despreparo dos usuários diante da sofisticação das ameaças digitais. Além disso, a distribuição de programas maliciosos, chamados *malware,* surge como outro tipo de crime virtual com consequências significativas.

Esses softwares, uma vez instalados, podem coletar dados, danificar sistemas ou inutilizar dispositivos. Conforme observado por Lima et al. (2022), o surgimento diário de novos *malwares* representa um grande desafio para os mecanismos de defesa cibernética.

Os crimes de calúnia e difamação na esfera digital também merecem atenção, dado o alcance alargado das redes sociais e plataformas online. A velocidade com que as informações são compartilhadas online, muitas vezes sem verificação, aumenta os ataques à honra e à imagem das vítimas (CRUZ; RODRIGUES, 2018).

Outra forma alarmante é o *ransomware*, que envolve *hackear* dados de um sistema, seguido de um pedido de resgate para sua liberação. Muitas empresas e indivíduos, como explicam Hernandez e De Toledo (2021), enfrentam dilemas éticos e financeiros ao decidir pagar ou não criminosos em situações em que informações essenciais são mantidas como reféns.

No domínio do comércio eletrónico, os crimes de fraude financeira estão a aumentar. A utilização de cartões de crédito clonados ou de dados bancários obtidos ilegalmente representa um grande obstáculo ao pleno desenvolvimento do comércio eletrônico (KRIEGUER; CERON; MARCONDES, 2021).

Além dessas formas, o *cyberbullying*, principalmente entre jovens e adolescentes, tem despertado a atenção da sociedade e do mundo jurídico. Este tipo de violência psicológica, amplificada pelo anonimato da Internet, pode ter consequências devastadoras para as vítimas (MARRA, 2019).

Neste contexto, é essencial compreender que a natureza dinâmica e em constante mudança da tecnologia amplifica os desafios de combate ao cibercrime. Os tipos de crimes virtuais não são estáticos e evoluem junto com os avanços tecnológicos (ALMEIDA; DE OLIVEIRA, 2022).

Silva e Da Silva (2019) enfatizam a necessidade urgente de novas ferramentas investigativas eficazes diante do crescente número e sofisticação dos crimes cibernéticos. Além disso, é essencial que o sistema de justiça também se desenvolva, para proporcionar o enquadramento adequado e combater estes crimes.

Concluindo, os tipos de cibercriminalidade não estão apenas a crescer, mas também a diversificar-se, refletindo mudanças e inovações no ambiente digital. Cabe ao direito e à sociedade se atualizarem constantemente para identificar, prevenir e combater essas ameaças, garantindo a segurança e a integridade dos usuários na era digital (MARTINS FILHO; LEITE; CEREWUTA, 2022).

4. DESAFIOS DA LEGISLAÇÃO BRASILEIRA

4.1 panorama atual da legislação sobre crimes virtuais no Brasil

A legislação brasileira tem enfrentado desafios contínuos ao tentar acompanhar o ritmo acelerado da evolução tecnológica e, consequentemente, dos crimes cibernéticos. Esse panorama torna-se ainda mais complexo ao analisarmos a dinâmica intrínseca desses delitos, que frequentemente ultrapassam fronteiras nacionais, exigindo uma atuação jurídica extraterritorial. Lira e Salgado (2021), apontam a importância do princípio da extraterritorialidade, especialmente no contexto da era digital, o que implica na necessidade de adaptação do direito penal nacional para contemplar essa nova realidade.

A Lei 12.965/2014, conhecida como Marco Civil da Internet, representou um marco importante para regular a internet no Brasil, especialmente em relação ao direito à privacidade online. Entretanto, Calgaroto (2021), ressalta que, apesar das inovações trazidas por esta lei, ainda há desafios pendentes em relação à responsabilização civil e à proteção efetiva dos direitos dos usuários.

Outra preocupação que surge é com a omissão legislativa em relação a determinados crimes cibernéticos, especialmente os que atentam contra a honra. Stephane e De Andrade (2022), discutem essa lacuna e enfatizam a necessidade de uma atuação mais robusta do Estado para proteger a dignidade das vítimas.

No entanto, é relevante destacar os esforços recentes para modernizar a legislação. Gomes e Medrado (2023), trazem uma ponderação sobre a Lei 14.155 de 2021, que trata especificamente do crime de estelionato virtual, demonstrando um movimento legislativo em busca de respostas mais atuais aos desafios impostos pelo ambiente digital.

Theuherz e Santos (2023), por sua vez, abordam a temática dos crimes virtuais de uma forma mais ampla, destacando a importância de uma legislação específica, atualizada e eficiente, capaz de enfrentar a crescente criminalidade cibernética que ameaça tanto indivíduos quanto instituições.

Veiga e Da Silveira (2022) discutem a (in)eficácia da lei conhecida como "Lei de Carolina Dieckmann", enfatizando a necessidade constante de revisões e atualizações legislativas, bem como a implementação efetiva das normas existentes.

Nogueira e Nolasco (2022) argumentam que os crimes cibernéticos representam um importante desafio para o direito, pois sua natureza e métodos de atuação são diferentes dos crimes tradicionais, o que exige uma abordagem jurídica diferenciada, mais adaptada à realidade virtual.

Bonini et al. (2018) reforçam a importância de se ter uma compreensão clara e profunda do crime cibernético para que haja uma aplicação eficaz da legislação, garantindo assim a punição e a proteção adequadas das vítimas.

Por fim, a investigação de provas em atos criminosos relacionados a crimes virtuais é um dos maiores desafios do sistema judiciário brasileiro. Santana (2019) indica que o caráter transitório das provas digitais exige uma abordagem técnica e especializada para garantir a equidade e a correta aplicação da lei.

4.2 Lacunas e limitações identificadas

O mundo digital, apesar de todas as vantagens que traz, torna-se um ambiente favorável ao desenvolvimento de práticas criminosas. A legislação brasileira, para tentar acompanhar essa evolução, enfrenta muitos desafios, como indicam Lopes e Lopes (2023). Esse autores ressaltam que as regulamentações existentes ainda não são capazes de abranger todos os crimes que podem ser cometidos neste ambiente virtual, gerando lacunas significativas no ordenamento jurídico brasileiro.

Calgaroto (2021) examina a privacidade online e suas implicações. Ele ressalta que, apesar dos avanços do Marco Civil a partir da Internet, a responsabilidade civil em caso de infrações ainda permanece em território incerto. Esta legislação, embora tenha sido uma tentativa de modernização e adaptação da lei à era digital, não resolveu todos os problemas relacionados com os crimes virtuais.

Uma lacuna importante na lei diz respeito às diretrizes probatórias em julgamentos criminais envolvendo crimes cibernéticos. Santana (2019) destaca os desafios que surgem ao tentar coletar e autenticar provas de tais crimes, uma vez que a natureza volátil e difundida do ambiente virtual dificulta a identificação e preservação de provas concretas.

Bonini et al. (2018) analisam os crimes cibernéticos em geral e identificam que a velocidade dos desenvolvimento tecnológico exige a atualização constante da legislação. Muitas vezes, quando uma lei é finalmente aprovada, os criminosos já desenvolveram novas formas de operar, tornando a legislação rapidamente obsoleta ou inadequada.

Um dos crimes cibernéticos que tem ganhado importância é o peculado virtual. Gomes e Medrado (2023) refletem sobre a recente Lei 14.155 de 2021 que combate esse crime. Argumentam que, embora represente um progresso, a lei ainda deixa espaço para diferentes interpretações e não abrange todas as formas possíveis deste crime.

As omissões legislativas também são problemáticas, especialmente quando se trata de crimes cibernéticos contra a honra. Stephane e De Andrade (2022) criticam a falta de regulamentação clara e específica para combater esta categoria de crimes, o que torna o processo de responsabilização e sanção mais complexo e, em muitos casos, ineficaz.

Nogueira e Nolasco (2022) discutem os desafios que a lei enfrenta no crime cibernético. Sublinham a necessidade de um equilíbrio entre as garantias individuais e a segurança coletiva, um dilema que a legislação atual não resolve bem.

O Brasil, comparado a outros países, ainda tem um longo caminho a percorrer em termos de eficácia de suas leis contra o crime cibernético. Veiga e Da Silveira (2022) fazem uma análise crítica da Lei Carolina Dieckmann e de sua efetividade, concluindo que embora represente um progresso, ainda hà muito a ser feito. No contexto dos crimes virtuais, Theuherz e Santos (2023) chamam a atenção para o cenário de Mato Grosso. Sublinham que, tal como noutros países, a falta de legislação específica e a dificuldade de adaptação do sistema judicial constituem os principais obstáculos a um combate eficaz a estes crimes.

Por fim, a era digital trouxe consigo o debate sobre o princípio da extraterritorialidade. Lira e Salgado (2021) analisam como os crimes cibernéticos podem ser cometidos em qualquer lugar do mundo, tornando complexa a determinação da jurisdição e aplicação de leis específicas. Assim, a internacionalização do crime cibernético constitui mais um desafio para o sistema judiciário brasileiro. Essas reflexões mostram que, apesar dos esforços recentes para atualizar a legislação, ainda existem lacunas e limitações significativas quando se trata de crimes cibernéticos no Brasil. As constantes mudanças e a evolução tecnológica exigem uma resposta ágil e adaptada do direito, o que ainda hoje é um desafio.

4.3 A complexidade na aplicação das leis em casos cibernéticos

A complexidade da aplicação da lei em casos de crimes cibernéticos supera as barreiras tradicionais do direito penal. O crescimento exponencial da internet e das tecnologias digitais sempre desafiou o sistema jurídico brasileiro a se adaptar aos novos paradigmas (LOPES; LOPES, 2023).

No contexto do cibercrime, determinar a responsabilidade e identificar o autor do crime são tarefas hercúleas. Com a globalização das redes e a multiplicidade de jurisdições envolvidas em um único ato criminoso, o princípio da extraterritorialidade torna-se cada vez mais importante, mas ao mesmo tempo complexo (LIRA; SALGADO, 2021).

Uma das maiores preocupações reside na aplicação de provas em ações penais relacionadas a crimes virtuais. A natureza intangível e volátil dos dados digitais e a falta de formação técnica limitam frequentemente a ação judicial. Não é incomum que evidências cruciais sejam perdidas ou inacessíveis antes de serem devidamente coletadas e analisadas (SANTANA, 2019).

A evasão legislativa é outro aspecto deste cenário. Em algumas situações, os crimes cibernéticos contra a honra, por exemplo, encontram-se num vazio jurídico, devido à incapacidade do legislador de antecipar e reagir rapidamente às mudanças tecnológicas e comportamentais dos cidadãos (STEPHANE; DE ANDRADE, 2022).

Lei nº 12.965/2014, também conhecida como Marco Civil da internet, trouxe avanços importantes, especialmente no que diz respeito ao direito à privacidade na internet. Contudo, as questões relacionadas à responsabilidade civil e à efetiva proteção dos direitos dos usuários ainda são objeto de intensos debates e estudos (CALGAROTO, 2021).

Ao mesmo tempo, leis como a Lei 14,155 de 2021, que trata especificamente da aquisição virtual, representam esforços louváveis de adaptação à realidade digital. Contudo, a velocidade com que os criminosos digitais evoluem seus métodos e a globalização do crime mostram que uma abordagem nacional pode não ser suficiente (GOMES; MEDRADO, 2023).

Outro desafio constante diz respeito à eficácia da legislação existente. A Lei Carolina Dieckmann, por exemplo, embora seja um passo importante no combate ao crime cibernético, é alvo de críticas quanto à sua aplicabilidade prática e à extensão de sua proteção (VEIGA; DA SILVEIRA, 2022).

De modo geral, a interdisciplinaridade apresenta-se como elemento fundamental no combate ao cibercrime. A tecnologia da informação e os profissionais jurídicos devem trabalhar juntos para garantir uma aplicação eficaz e justa da lei. Também é necessária uma análise mais ampla, envolvendo a sociologia, a psicologia e outras áreas do conhecimento (BONINI, 2018).

O problema dos crimes virtuais não se limita à responsabilidade e à punição. Aumentar a consciência social e construir uma cultura digital segura são parte integrante de uma estratégia eficaz. A educação, formal e informal, desempenha um papel decisivo nesse processo (THEUHERZ; SANTOS, 2023).

Portanto, a complexidade da aplicação da lei em casos de crimes cibernéticos reflete o dinamismo e a variabilidade do mundo digital. As soluções exigem uma abordagem multifacetada, colaborativa e, acima de tudo, adaptativa. O direito, como instrumento de ordem social, deve enfrentar os desafios apresentados pela era digital (NOGUEIRA; NOLASCO, 2022).

5. CONCLUSÃO

Existe um paradoxo que ainda hoje permeia a Internet, nota-se que a mesma atua de forma diversa e está presente em quase todos os momentos de nossas vidas, é notório que ela traz consigo benefícios diversos, porém, é de suma importância analisar os pontos negativos intrínsecos a esta tecnologia.

Internet é uma poderosa ferramenta de comunicação, porém, quando usada de forma incorreta, de modo que afeta de forma intensificada outras pessoas, é exigindo a intervenção do Estado, em sentimentos sobre práticas restritivas que podem estar além do escopo da liberdade. Nesse sentido, é necessário tipificar esses comportamentos para que assim o Estado possa exercer suas funções, o que infelizmente não está acontecendo.

Como observado, o principal motivo para atualizações do Direito Penal sobre as leis com amparo a segurança à cibercrimes ocorre principalmente em casos de repercussões na mídia, seja nacional ou internacional, a partir dessa conjuntura foi criada a Lei Carolina Dieckmann e o Marco Civil da Internet.

Porém, o Marco Civil não regulamenta o lado Penal devidamente, sendo essa questão pouco elaborada, e com algumas leis dentro de outros contextos para a regulamentação, sem uma “Constituição” voltada para essa área.

Como foi possível identificar as principais características do método de ataque *phishing*, que é o ataque mais comum no país para aplicação de golpes, ao adquirir dados sigilosos das pessoas. Deve ler, compreender, aplicar e testar no cotidiano os métodos de prevenção à ataques no Brasil. As pessoas devem se conscientizar e não serem inocentes quando abrirem determinado site ou aplicação, seja pelo computador ou celular.

Isso ocorre porque os golpes podem ocorrer em qualquer hora, local e equipamento, seja através do *hardware, software* ou pelo ser humano, por isso, saber que esses problemas são possíveis com qualquer pessoa, representa o necessário para aprender a combater estes males, tornando a internet do país um local mais seguro para todos.

6. REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 2006. AMBITO JURIDICO. Crimes Cibernéticos: Phishing. Disponível em: https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/.htm.

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 2006. AMBITO JURIDICO.

ALEXANDRE JÚNIOR, Júlio César. **Cibercrime: um estudo acerca do conceito de crimes informáticos**. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/download/602/pdf.

ALMEIDA, Haian de Assis Lopes; DE OLIVEIRA, Tamar Ramos. CRIMES VIRTUAIS: O AVANÇO DOS CRIMES ELETRÔNICOS E A EVOLUÇÃO DAS LEIS ESPECÍFICAS NO BRASIL. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 11, p. 277-294, 2022.

BONINI, Luci Mendes et al. Crimes Cibernéticos. **Diálogos Interdisciplinares**, v. 7, n. 3, p. 223-236, 2018.

BRASIL. **Código Civil**. Disponível em: http://www.planalto.gov.br/ccivil _03/Leis/2002/l10406.htm. Acesso em: 8 set. 2021. BRASIL. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848 de 07 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRASIL. **Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em 8 set. 2021. BRASIL. Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **Lei 12.737/2012.** Disponível em: http://www.planalto.gov.br/ccivil _03/_ato2011-2014/2012/lei/l12737

BRASIL. **Lei nº 13.772**, de 19 de dezembro de 2018. Altera o Decreto Lei nº 2.848/40. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm.

BRASIL. Lei nº 13.772, de 19 de dezembro de 2018. **Lei Rose Leonel**. Altera a Lei nº 11.340/06 (Lei Maria da Penha) e o Decreto Lei nº 2.848/40. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13772.htm.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.

CALGAROTO, Cleber. O direito à privacidade na internet: panorama, responsabilização civil e inovações do marco civil da internet (Lei nº 12.965/2014). **Direito-Unisul Virtual**, 2021. CAZAROTI, Tatiane Martins Barros; PINHEIRO, Eduardo Fernandes. Crimes Cibernéticos. **TCC-Direito**, 2021.

CANAL TECH. **Hackers usam mensagens sobre corona vírus para roubar dados no Brasil.** Disponível em: https://canaltech.com.br/seguranca/hackers-usam-mensagens-sobre-coronaviruspara-roubar-dados-bancarios-no-brasil-160465/.htm.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003, p.9.

CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. São Paulo: Saraiva, 2019, p. 19.

CORREIO BRASILIENSE. **Estudo aponta 1,6 bilhão de casos de roubo de dados pessoais na internet.** Disponível em: https://www.correiobraziliense.com.br /brasil/2021/06/4928596-estudo-aponta-16- bilhao-de-casos-de-roubo-de-dados-pessoais-na-internet.html.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, 2018.

DORNELAS, Natália Alves. A Resposta Estatal Quanto Aos Crimes Cibernéticos: Uma Análise Direcionada Às Leis Nº 12.735/2012 E 12.737/2012. **Repositório de Trabalhos de Conclusão de Curso**, 2019.

Extraterritorialidade. **Criminalidade Na Era Digital**, v. 58046, p. 68. 2021.

FEDERAL, Tribunal Regional. TRF-3. **O que é phishing**. Disponível em: https://www.trf3.jus.br/dica-phishing.

GOMES, Walyson Milhomem; MEDRADO, Lucas Cavalcante. CRIMES CIBERNÉTICOS UMA PONDERAÇÃO SOBRE A LEI 14.155 DE 2021 APLICÁVEL AO CRIME DE ESTELIONATO VIRTUAL. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 9, p. 1870-1894, 2023.

HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. **Revista Jurídica da UniFil**, v. 17, n. 17, p. 72-84, 2021.

KASPERSKY. **O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos**. Disponível em https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime.

KRIEGUER, André Lemuel Ferreira; CERON, Antonio Luciano Bairros; MARCONDES, Aldair. A Acelerada Evolução Social E Tecnológica Global Como

Viabilizadores De Crimes Cibernéticos, Frente Ao Lento Desenvolvimento De Freios Legais Para Sua Contenção. **Ponto de Vista Jurídico**, p. 128-143, 2021.

LIMA, Yasmin Victoria et al. Direito digital: aplicação nos crimes cibernéticos. **Anais da Semana de Pesquisa Jurídica**, v. 1, p. 42-42, 2022.

LIRA, Caio César Dutra; SALGADO, Ana Alice Ramos Tejo. A Era Digital E A Prática De Crimes Cibernéticos: Uma Análise Sobre O Princípio Da

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. CRIMES VIRTUAIS NO ORDENAMENTO JURÍDICO BRASILEIRO. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 8, p. 462-472, 2023.

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. **Journal of Law and Sustainable Development**, v. 7, n. 2, p. 145-167, 2019.

MARTINS FILHO, Rogério; LEITE, Roniel Bispo; CEREWUTA, Pollyanna Marinho Medeiros. A ASCENSÃO DOS CRIMES CIBERNÉTICOS NO CONTEXTO CONTEMPORÂNEO. **Facit Business and Technology Journal**, v. 1, n. 37, 2022.

NOGUEIRA, Flavio Mirã De Souza; NOLASCO, Loreci Gottschalk. Crimes Cibernéticos Desafios Para O Direito. **Revista Jurídica Direito, Sociedade E Justiça**, v. 9, n. 13, p. 133- 140, 2022.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007. p. 25.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002. p. 53.

SANTANA, Denayde Rodrigues. [Graduação| Monografia] Sistema De Provas Nos Crimes Virtuais Os Desafios Da Instrução Probatória Em Ações Penais Relativas Aos Crimes Virtuais No Brasil. **Portal de Trabalhos Acadêmicos**, v. 6, n. 1, 2019.

SILVA, Kaique Rodrigues; DA SILVA, Rubens Alves. Crimes cibernéticos: necessidade de novas ferramentas de investigação com encargos no ônus da prova. **Revista Artigos**. Com, v. 12, p. e2480-e2480, 2019.

SOUZA, Alexandre Dourado Gomes de. **O avanço dos crimes cibernéticos: um estudo sobre os crimes previstos nas leis 12.737/2012 e 12.735/2012 e a importância da materialidade da prova e seus reflexos no ataque cibernético na rede de informática do superior tribunal de justiça em 2020**. 2021.

SOUZA, Luiza Ananda Queiroz; CERVINSKI, Yasmin. É POSSÍVEL A PREVENÇÃO E COMBATE AOS TEMIDOS CRIMES VIRTUAIS? **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, v. 6, p. e27776-e27776, 2021.

STEPHANE, Tawane; DE ANDRADE, Gleidson Henrique Antunes. A Omissão Legislativa Do Estado Nos Crimes Cibernéticos Contra A Honra. **Praxis Jurídic@**, v. 6, n. 2, 2022. THEUHERZ, Nycolas Gava Baesso; SANTOS, Kaully Furiama. Crimes virtuais. **Revista Mato-grossense de Direito**, v. 1, n. 1, p. 146-160, 2023.

VEIGA, Deivid Jonas Silva; DA SILVEIRA, Dieison Prestes. Joselia Cristina Siqueira da Silva et al.“.**O cibercrime no brasil: uma análise da (in) eficácia da lei carolina dieckmann”, International Journal of Development Research**, v. 11, n. 01, p. 43466- 43469.

FACULDADE DE JUSSARA
Compromisso com o futuro!
Rod. BR-070, KM 24, saída para Goiás, CEP 76.270-000, Jussara/GO.
Telefax: (62) 3373-1219 / www.unifaj.edu.br

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos **22** dias do mês de **novembro** do ano de **2024**, às **17** horas, por meio de recurso eletrônico: *Google Meet* (e-mail: **faj@faculdadedejussara.page**), realizou-se a sessão pública de defesa do trabalho de conclusão de curso intitulado **O COMBATE AOS CRIMES CIBERNÉTICOS COM O AVANÇO DA TECNOLOGIA NA ÓTICA DA LEGISLAÇÃO BRASILEIRA,** apresentado pelo (a) acadêmico (a) **Carlos Joel Rodrigo Lima**, do **Curso de Direito**. Os trabalhos foram iniciados pelo (a) **Professor (a) Orientador (a) Esp. Rodrigo R. Marques**, presidente da banca examinadora, composta pelos (as) professores (as) convidados (as) **Profa. Esp. Thais Alves de Morais Fernandes** e **Prof. Esp. Gisley Alves Faria.**

A banca examinadora, tendo terminado a apresentação do conteúdo do artigo, passou a arguição do(a) candidato(a). Em seguida, os examinadores reuniram-se para avaliação e deram o parecer final sobre o trabalho apresentado pelo (a) acadêmico (a), tendo sido atribuída a nota final **9,0**, com a consequente **APROVAÇÃO** do artigo em comento.

Docente Orientador	Avaliador 1	Avaliador 2	Nota Final
9,0	9,0	9,0	9,0

Proclamados os resultados pelo(a) presidente da banca examinadora, foram encerrados os trabalhos e, para constar, eu, **Rodrigo R. Marques**, lavrei a presente ata que assino juntamente com os demais membros da banca examinadora.

Banca Examinadora:

Assinado eletronicamente por:
Rodrigo Rosa Marques
CPF: ***.681.161-**
Data: 09/12/2024 15:05:45 -03:00

Professor Orientador

Assinado eletronicamente por:
THAIS ALVES DE MORAIS FERNANDES
CPF: ***.198.451-**
Data: 13/12/2024 10:44:39 -03:00

Professor Avaliador 1

Assinado eletronicamente por:
Gisley Alves de Faria
CPF: ***.241.231-**
Data: 09/12/2024 15:04:02 -03:00

Professor Avaliador 2