Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i5.19365

A TIPICIDADE PENAL NO CONTEXTO DO CRIME CIBERNÉTICO DE ROUBO DE INFORMAÇÕES E CLONAGEM DE DADOS

Carlos Andrey Oliveira Martins[1]
Carlos Henrique Martins Pitillo[2]
Willames Castro de Souza[3]
Marcelo Augusto Rebouças Leite[4]

RESUMO: Os crimes cibernéticos tem se mostrado notoriamente difícil de investigar e processar com sucesso. Uma infinidade de questões no policiamento e no direito penal relacionados ao crime cibernético influenciam essa dificuldade. Diante disso, o presente artigo tem como objetivo relacionar a tipicidade penal no contexto do crime cibernético por roubo e clonagem de dados. Foi desenvolvida uma revisão integrativa da literatura. As principais etapas na condução dessa revisão foram as seguintes: elaborar uma questão de pesquisa, conduzir uma busca na literatura, especificar os métodos de seleção e avaliação, detalhar e sintetizar os principais achados sobre o tema. Os resultados encontrados neste estudo mostraram que a tipicidade penal no contexto dos crimes cibernéticos, especialmente aqueles relacionados ao roubo de informações e à clonagem de dados, revela a necessidade de constante atualização e adequação do ordenamento jurídico frente à dinâmica das novas tecnologias. Diante disso, é compreendido que deve haver mais estudos que abordem o tema, devido a importância da disseminação dos conhecimentos do crime cibernético diante do ordenamento jurídico nacional. Sendo relevante para sociedade, para área do direito e podendo servir como subsidio para ajustes legislativos nas políticas referente a essa problemática.

Palavras-chave: Tipicidade penal. Crime. Cyber. Direito.

INTRODUÇÃO

De acordo com Martins et al., (2024) roubo de dados é um tipo de crime cibernético, caracterizado pela transferência ou armazenamento ilegal de informações pessoais, confidenciais ou financeiras. Isso pode incluir senhas, código de software ou algoritmos e processos ou tecnologias proprietárias. O roubo de dados é considerado uma violação grave de segurança e privacidade, com consequências potencialmente severas para indivíduos e organizações.

Os crimes cibernéticos envolvem obter acesso ilegal ou entrada ilegal em um computador ou interagir ilegalmente com outro por meio do uso de um computador. Alguns

[1]Discente do Curso de Direito do Centro Universitário do Norte – UNINORTE.
[2]Discente do Curso de Direito do Centro Universitário do Norte – UNINORTE.
[3]Discente do Curso de Direito do Centro Universitário do Norte – UNINORTE.
[4]Professor Orientador, Marcelo Augusto Rebouças Leite, advogado, especialista em docência do ensino superior e professor do curso de direito do Centro Universitário do Norte – UNINORTE.

crimes cibernéticos são apenas um novo método para cometer crimes antigos contra a propriedade, como roubo e fraude, ou crimes contra a pessoa, como assédio e agressão.

Esse contexto é criminalizado pela Lei Geral de Proteção de Dados (LGPD), a lei nº 13.709, aprovada em agosto de 2018, estabelece regras sobre a coleta, armazenamento e compartilhamento de dados pessoais. Essa medida jurídica possui tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado.

Segundo Garcia et al., (2020) as penalidades pelo descumprimento da LGPD são bem pesadas e compreendem: Multas altíssimas, com potencial de quebrar muitos negócios ou até a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Outra lei é a Lei Carolina Dieckmann, é a Lei Nº 12.737/2012 e é uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos informáticos. Essa norma estabeleceu no Brasil, que a invasão de computadores ou celulares é crime tipificado no brasil desde 2012. a pena prevista é de um a quatro anos de reclusão e multa.

No entanto, as leis tradicionais de propriedade podem ser inadequadas e inapropriadas no mundo cibernético, as leis locais de muitas jurisdições podem não identificar o crime como um ato ilegal. Por isso, as vítimas de crimes cibernéticos acabam não denunciando os crimes imediatamente devido à percepção de que as autoridades policiais e jurídicas podem identificar o ato de acordo com o princípio da insignificância, tornando assim o contexto de tipicidade criminal.

Segundo Almeida e Soares (2022) os crimes cibernéticos tem se mostrado notoriamente difícil de investigar e processar com sucesso. Uma infinidade de questões no policiamento e no direito penal relacionados ao crime cibernético influenciam essa dificuldade. Diante disso, o presente estudo tem como justificativa a importância da disseminação dos conhecimentos do crime cibernético diante do ordenamento jurídico nacional. Sendo relevante para sociedade, para área do direito e podendo servir como subsidio para ajustes legislativos nas políticas referente a essa problemática.

Os crimes cibernéticos tem se mostrado notoriamente difícil de investigar e processar com sucesso. Uma infinidade de questões no policiamento e no direito penal relacionados ao crime cibernético influenciam essa dificuldade. Dessa forma, de que forma o crime cibernético entra em um contexto de tipicidade penal?

O presente artigo tem como objetivo relacionar a tipicidade penal no contexto do crime cibernético por roubo e clonagem de dados. Tendo como objetivos específicos o intuito de analisar os entendimentos doutrinários e jurisprudenciais acerca dos crimes cibernéticos no âmbito nacional, relacionar os fatores de análise para aplicação da tipicidade penal em crimes cibernéticos e identificar os crimes cibernéticos que podem ser tipificados, no Código Penal.

2 Tipos de crime cibernético

De acordo com Martins et al., (2024) o crime cibernético é um termo amplo que abrange muitas atividades maliciosas que exploram tecnologias digitais, afetando indivíduos, empresas e governos em todo o mundo. O crime cibernético continua a aumentar, causando impactos financeiros e psicológicos significativos. À medida que a tecnologia evolui, também evoluem os métodos empregados pelos criminosos cibernéticos, tornando crucial manter-se informado sobre as ameaças mais recentes e empregar medidas preventivas.

A tabela 1 apresente os principais tipos de crimes cibernéticos.

Tabela 1 Principais tipos de crimes cibernéticos.

CRIME CIBERNÉTICO	DESCRIÇÃO
Ataques de phishing	Os invasores se passam por organizações legítimas, como bancos ou repartições governamentais, por e-mail, texto ou telefonemas, para enganar indivíduos e fazê-los compartilhar informações confidenciais.
Distribuição de malware	. Tipos comuns de malware incluem ransomware, spyware, trojans, worms e keyloggers, que roubam dados confidenciais, registram pressionamentos de tecla ou criam backdoors para exploração posterior e interrupção de negócios.
Ataques de Ransomware	Esses ataques podem paralisar organizações inteiras, de hospitais a instituições financeiras, e resultar em danos financeiros significativos. Existem muitos tipos de vetores de ataque de ransomware , como anexos de e-mail, pop-ups de sites ou mensagens de texto.
Roubo de identidade	Os criminosos cibernéticos roubam informações pessoais — como números de previdência social, detalhes bancários e senhas para cometer fraudes.
Ataques de negação de serviço (DoS)	Em ataques DoS e DDoS, os cibercriminosos inundam uma rede, servidor ou site com tráfego excessivo, fazendo com que ele trave ou fique inacessível.
Espionagem cibernética e ataques patrocinados pelo Estado	Esses ataques têm como alvo governos, infraestrutura crítica, instituições financeiras e grandes empresas para roubar inteligência, interromper operações ou obter uma vantagem geopolítica.
Ataques à cadeia de suprimentos	Em vez de mirar diretamente nas organizações, os cibercriminosos se infiltram em suas cadeias de suprimentos, fornecedores terceirizados, provedores de nuvem ou fornecedores de software, para obter acesso não autorizado a dados ou sistemas confidenciais.

Cyberstalking e assédio online	s criminosos cibernéticos exploram mídias sociais, e-mail e serviços de mensagens para monitorar vítimas, roubar informações pessoais ou manipular reputações online.
Fraude Financeira e Bancária	Os criminosos cibernéticos exploram fraquezas em sistemas bancários, transações on-line e carteiras digitais para cometer fraudes.

Fonte: Adaptado de

De acordo com Maia e Costa (2023) os cibercriminosos se adaptam à tecnologia. Eles estão usando tecnologias emergentes como criptomoeda e blockchain para roubar fundos de exchanges, carteiras e contratos inteligentes e até mesmo usando blockchain para lavagem de dinheiro. Os ataques de phishing também ficaram mais sofisticados com os cibercriminosos usando eventos do mundo real, como temporada de impostos e promoções de compras para atrair vítimas.

Outras tendências emergentes são o ciberativismo, o hacking automotivo e o impacto da inteligência artificial (IA) no crime cibernético. De fato, estudos recentes mostraram que 85% do aumento nas ameaças cibernéticas é atribuído a atores mal-intencionados usando IA generativa, então os desafios na segurança digital estão evoluindo. À medida que o crime cibernético continua a evoluir com novas tecnologias e táticas, o impacto financeiro na economia e no PIB global é enorme (Costa e Bruno, 2024).

2.1 Métodos utilizados no crime de roubo e clonagem de dados

Silveira e Santos (2024) um dos métodos é a exploração de senhas fracas. Usar a mesma senha para várias contas ou uma senha fácil de adivinhar, como o ano de nascimento, facilita o acesso de agentes de ameaças aos seus dados. Praticar hábitos ruins de senha, como compartilhá-la com outras pessoas ou escrevê-la em um pedaço de papel (é recomendável que você escolha uma senha fácil de lembrar) também pode resultar em perda de dados.

Silva e Pinto (2023) apresenta que a Engenharia social é outra forma de ataque cibernético usada por hackers para roubar dados. Embora existam várias formas de engenharia social, o phishing é o mais prevalente. Ele ocorre quando um ator malicioso se disfarça como uma entidade confiável para enganar a vítima e fazê-la abrir uma mensagem de texto, e-mail ou mensagem instantânea.

Ameaça interna também é considerada uma forma de roubo, quando os funcionários de uma organização podem, às vezes, ter acesso a dados confidenciais de clientes. Um funcionário descontente ou desonesto pode potencialmente alterar, roubar ou vender esses dados. Ameaças

internas também podem vir de contratados, parceiros ou ex-funcionários que têm acesso aos dados confidenciais de uma organização (Fernandes, 2021).

Além dessas, a vulnerabilidades do sistema também são utilizadas como uma forma de prática desses criminosos. Segundo Silveira e Santos (2024) os sistemas de rede instalados incorretamente e aplicativos de software mal escritos criam vulnerabilidades que os agentes de ameaças podem explorar e usar para roubar dados. Deixar de atualizar seu software antivírus também pode criar brechas de segurança.

De acordo com Prokisch (2023) problemas no servidor também são estratégias identificadas pelos criminosos. Quando os servidores ou bancos de dados de uma organização estão mal protegidos ou protegidos, eles podem acessar informações confidenciais, como informações pessoais de clientes. As violações de dados nem sempre são causadas por ações maliciosas. Há momentos em que elas ocorrem como resultado de erro humano. Alguns dos erros comuns incluem enviar arquivos confidenciais para a pessoa errada, anexar o documento errado ou deixar informações confidenciais online sem instituir restrições de senha.

O roubo de dados também pode ocorrer devido a ações físicas. Silva e Pinto (2023) descrevem que isso pode incluir o roubo de documentos confidenciais ou dispositivos como telefones, laptops ou dispositivos de armazenamento. Assim como as informações disponíveis ao público, visto que muitas informações estão disponíveis em domínio público, também chamadas de inteligência de código aberto. Isso pode ser por meio de pesquisas na internet ou por meio de postagens em mídias sociais.

2.2 Fatores de riscos para o crime cibernético

De acordo com Nolasco e Silva (2022) devido às ameaças crescentes que representa para as empresas, o crime cibernético tornou-se uma grande preocupação. Apesar dos muitos avanços na tecnologia de segurança cibernética, as empresas ainda são vítimas de ataques cibernéticos, e a um ritmo alarmante.

Silva e Silva (2015) os fatores de riscos se referem a capacidade intrínseca de um equipamento ou ação de causar danos. No caso da cibersegurança, os vírus representam, por exemplo, um perigo, uma ameaça por natureza para os sistemas de informação de uma empresa. O que gera riscos em relação ao resultado da exposição da empresa ao perigo. É sempre caracterizado de acordo com a probabilidade e o nível potencial de gravidade das consequências do evento para o que tem valor para o seu titular.

Dessa forma, clicar em um link não identificado em um e-mail expõe você ao perigo representado por e-mails de phishing, por exemplo. Clicar neste link e o malware se espalhar pela rede da estação de trabalho, impedindo os funcionários de trabalhar, é um risco.

Embora a fraca segurança do sistema e o software desatualizado sejam frequentemente responsabilizados como um fator de riscos pelas violações de dados, a verdade é que o erro humano é um fator de risco responsável por 80% dos casos. Os humanos são a maior vulnerabilidade na estratégia de segurança cibernética de uma organização. Em mais de 8 em cada 10 casos, a origem do comprometimento dos dados é atribuível ao usuário.

De acordo Holt (2019), 62% dos incidentes de intrusão de sistemas envolvem um parceiro externo. Isso é chamado de ataque à cadeia de suprimentos. Quando um software ou serviço é fornecido por uma empresa terceira, se esta deixou escapar uma violação de segurança e se infiltrou, são todas as empresas às quais prestou o seu serviço (cadeia de abastecimento) que correm o risco de serem comprometidas.

Segundo Prokisch (2023) outro fator que pode explicar o aumento dos ataques cibernéticos é o risco causado ou agravado pela computação paralela. Isso pode acontecer por ignorância ou quando certos departamentos de uma organização têm poder demais. Este sistema paralelo dos serviços de TI cria um ponto de acesso inseguro à rede e, portanto, um ponto de entrada para hackers. Isto pode acontecer, por exemplo, em sistemas hospitalares, devido ao grande número de máquinas médicas ligadas à web, como ressonâncias magnéticas ou scanners.

No contexto dos riscos cibernéticos, trata-se de riscos que envolvem informação em formato digital ou elementos de um sistema de informação. Alguns métodos de análise distinguem os riscos intencionais dos riscos acidentais com base no facto de poderem ser abordados a priori através da conformidade.

No entanto, segundo Santos et al., (2023) o risco associado à segurança informática está por vezes oculto em hábitos diários, como utilização de computadores no âmbito de transferências financeiras ou manipulação de contas bancárias de empresas, especialmente se esses computadores forem portáteis e utilizados em modo nómada. Também ocorre a utilização remota do sistema informático, por exemplo em contexto de teletrabalho, assim como a política de segurança de senha fraca e política de segurança de TI mal atualizada.

3 O crime cibernético no contexto do direito penal

De acordo com Freitas et al., (2023) o mundo está constantemente desenvolvendo novas tecnologias, então agora, ele tem uma grande dependência da tecnologia. A maioria dos dispositivos inteligentes está conectada à internet. Há benefícios e também há riscos. Um dos riscos é o grande aumento no número de crimes cibernéticos cometidos, não há medidas e operações de segurança suficientes para ajudar a proteger essas tecnologias.

As redes de computadores permitem que as pessoas no ciberespaço alcancem qualquer parte conectada do mundo em segundos. Cruz e Rodrigues (2018) o que pode facilitar crimes, esses crimes cibernéticos podem ser definidos como "O uso ilegal de qualquer dispositivo de comunicação para cometer ou facilitar a prática de qualquer ato ilegal". Um crime cibernético é explicado como um tipo de crime que tem como alvo ou usa um computador ou um grupo de computadores em uma rede com o propósito de causar danos.

De acordo com Caldeira e Caldeira (2023) o crime cibernético refere-se ao uso de computadores para cometer ações maliciosas. Esta ameaça moderna é uma das maiores ameaças que as empresas enfrentam neste momento. Pode até afetar a segurança nacional e a privacidade dos cidadãos. Ou seja, o crime cibernético é um termo usado para descrever atividades criminosas que ocorrem no ciberespaço. Pode assumir várias formas.

Os crimes cibernéticos são cometidos usando computadores e redes de computadores. Eles podem ter como alvo indivíduos, grupos empresariais ou até mesmo governos. Os investigadores tendem a usar várias maneiras de investigar dispositivos suspeitos de serem usados ou alvos de um crime cibernético (Silva, 2018).

Rodrigues et al., (2023) descreve que os cibercriminosos aproveitam falhas de segurança e vulnerabilidades encontradas nos sistemas e as exploram para se estabelecerem no ambiente alvo. As falhas de segurança podem ser uma forma de utilização de métodos de autenticação e senhas fracas, mas também podem ocorrer pela falta de modelos e políticas de segurança rigorosos.

Segundo Caldeira e Caldeira (2023) os crimes cibernéticos podem ter leis e regulamentações diferentes de um país para outro, mencionando também que esconder rastros é muito mais fácil quando se comete um crime cibernético do que quando se comete um crime real.

Para combater essa ameaça crescente, pessoas e organizações devem estar vigilantes e se proteger proativamente contra crimes cibernéticos.

3.1 Doutrina jurídica e a criminalidade

De acordo com o direito penal brasileiro para um comportamento ser típico, ele deve ser especificamente e detalhadamente declarado como crime na jurisprudência. No entanto, alguns casos enquadrados nos crimes cibernéticos podem ser avaliados com uma tipicidade penal de acordo com a possível e adequada aplicabilidade de casos que possam ser considerados insignificantes para lei. Ou seja, essa relação envolve atos que podem ser considerados, em caso de análise adequada e criteriosa, como um ato e sujeitos que não possuem características e fatores considerados na violação da legislação nacional, de forma a ser criminalizado pelo contexto cometido, sendo aplicado assim a tipicidade penal.

Segundo Costa e Pacheco (2018) é compreendido que o cibercrime se tornou uma grande preocupação nos dias de hoje, devido à forte dependência da sociedade moderna das tecnologias de informação e comunicação. Esta forma de crime envolve o uso ilegal de computadores e da Internet para cometer atos maliciosos. Os cibercriminosos exploram vulnerabilidades de segurança em sistemas e redes informáticas para obter acesso não autorizado a dados sensíveis ou para perturbar as operações normais de empresas e instituições.

Gama (2021) descreve que os cibercriminosos são indivíduos ou grupos organizados que utilizam conhecimentos informáticos e de redes para cometer atos ilegais online. São motivados por vários motivos, como ganho financeiro, espionagem, reconhecimento dos seus pares ou o desejo de prejudicar as suas vítimas.

Geralmente operam de forma independente ou como membros de grupos organizados, por vezes apoiados por governos ou organizações criminosas. Seu perfil é variado, desde hackers amadores até especialistas em segurança altamente qualificados. Para atingir o seu objetivo, utilizam a exploração de vulnerabilidades de segurança em sistemas informáticos e técnicas de manipulação psicológica.

Diante disso e levando em consideração o crime de roubo e clonagem de dados, e os os custos crescentes dessas violações, é vital que os indivíduos e as organizações estabeleçam medidas sólidas de proteção de risco de dados para manter seus dados seguros. Algumas das medidas que podem ser colocadas em prática incluem: uso de senha seguras, use autenticação multifator (MFA), Atualização regular de programas e sistemas se segurança, cuidados ao

compartilhamento de dados pessoais. Além disso, em casos de meios corporativos deve haver gerenciamento de seus endpoints e monitoramento das atividades dos funcionários.

4 Fundamentação jurídica do crime de roubo de dados: Lei 12.737/2012 e Lei nº 13.709

Segundo Santos et al., (2023) o roubo de dados é um grande crime cibernético cujo crescimento foi alimentado por rápidos avanços digitais nos últimos anos. Ele envolve o armazenamento ilegal ou infiltração de dados ou informações financeiras. Isso pode incluir senhas, algoritmos, código de software, tecnologias proprietárias ou outros dados confidenciais.

Os crimes cibernéticos envolvem obter acesso ilegal ou entrada ilegal em um computador ou interagir ilegalmente com outro por meio do uso de um computador. Alguns crimes cibernéticos são apenas um novo método para cometer crimes antigos contra a propriedade, como roubo e fraude, ou crimes contra a pessoa, como assédio e agressão.

No entanto, segundo Garcia et al., (2020) as leis tradicionais de propriedade podem ser inadequadas e inapropriadas no mundo cibernético, as leis locais de muitas jurisdições podem não identificar o crime como um ato ilegal. Por isso, as vítimas de crimes cibernéticos acabam não denunciando os crimes imediatamente devido à percepção de que as autoridades policiais e jurídicas podem identificar o ato de acordo com o princípio da insignificância, tornando assim o contexto de tipicidade criminal.

Esse contexto é criminalizado pela Lei Geral de Proteção de Dados (LGPD), a lei nº 13.709, aprovada em agosto de 2018, estabelece regras sobre a coleta, armazenamento e compartilhamento de dados pessoais. Essa medida jurídica possui tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado.

A Lei Geral de Proteção de Dados (LGPD), é uma estrutura legal para regular a coleta e o uso de dados pessoais no Brasil. Entrou em vigor em 16 de agosto de 2020 e é aplicada pela Autoridade Nacional de Proteção de Dados.

A Lei Geral de Proteção de Dados (LGPD) é uma lei federal no Brasil criada para unificar 40 leis existentes para regular o tratamento de dados pessoais de indivíduos. Foi aprovada em 18 de setembro de 2020 e tornou-se retroativa, entrando em vigor em 16 de agosto de 2020. As penalidades tornaram-se executáveis em 1º de agosto de 2021, e os titulares dos dados e as autoridades públicas puderam fazer valer seus direitos a partir de 18 de setembro de 2020.

A lei de proteção de dados do Brasil é composta por 65 artigos em 10 capítulos. O Artigo 2 lista os sete fundamentos da lei de proteção de dados pessoais:

> respeito pela privacidade
> autodeterminação informacional
> liberdade de expressão, informação, comunicação e opinião
> inviolabilidade da intimidade, da honra e da imagem
> desenvolvimento económico e tecnológico e inovação
> livre iniciativa, livre concorrência e defesa do consumidor
> direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas singulares

As penalidades pelo descumprimento da LGPD são bem pesadas e compreendem: Multas altíssimas, com potencial de quebrar muitos negócios ou até a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Outra fundamentação jurídica é a Lei Carolina Dieckmann, é a Lei Nº 12.737/2012 e é uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos informáticos. Essa norma estabeleceu no Brasil, que a invasão de computadores ou celulares é crime tipificado no brasil desde 2012. a pena prevista é de um a quatro anos de reclusão e multa.

CONCLUSÃO

O desenvolvimento deste artigo permitiu compreender que a tipicidade penal no contexto dos crimes cibernéticos, especialmente aqueles relacionados ao roubo de informações e à clonagem de dados, revela a necessidade de constante atualização e adequação do ordenamento jurídico frente à dinâmica das novas tecnologias. Tais condutas, embora muitas vezes não envolvam violência física ou contato direto com a vítima, configuram ataques graves ao patrimônio, à privacidade e à integridade digital dos indivíduos.

A análise da tipicidade exige a interpretação dos tipos penais tradicionais à luz das novas realidades virtuais, ou a criação de normas específicas que abranjam as particularidades desses delitos. Dessa forma, a efetiva repressão aos crimes informáticos depende não apenas da tipificação clara das condutas, mas também da capacitação técnica das autoridades e da atuação preventiva do Estado na proteção dos dados pessoais e da segurança digital da sociedade.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados-LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 03, p. 26-45, 2022.

DE ARAÚJO FREITAS, Elison; SILVA, Pedro Henrique Aguiar; DE SOUZA, Márcio Cabral. CRIMES CIBERNÉTICOS: DESAFIOS DA INVESTIGAÇÃO E PRESERVAÇÃO DAS PROVAS. **Facit Business and Technology Journal**, v. 1, n. 44, 2023.

CALDEIRA, Marina de Andrade Figaro; CALDEIRA, Rodrigo de Andrade Figaro. A COMPETÊNCIA PENAL EM CRIMES CIBERNÉTICOS. **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, v. 23, 2023.

COSTA, Renato Lopes; PACHECO, Gisele Freitas. Crimes virtuais e a legislação penal brasileira. **Revista Eletrônica de Ciências Jurídicas**, v. 8, n. 1, 2018.

COSTA, Alan Aquino; BRUNO, Diego Renan. IA–INTELIGENCIA ARTIFICIAL: IMPACTOS, RISCOS E BENEFICIOS QUE DESAFIAM A SOCIEDADE MODERNA. **Revista Interface Tecnológica**, v. 21, n. 1, p. 76-87, 2024.

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

DA SILVA, Angelo Roberto Ilha (Ed.). **Crimes cibernéticos**. Livraria do Advogado Editora, 2018.

FERNANDES, Matheus Pierre. **Os cibercrimes e o direito brasileiro: as limitações da legislação em vigor, considerando a realidade tecnológica**. 2021. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte.

GAMA, João Pedro Senra Pimenta. Cibercriminalidade organizada: os modelos de organização em rede e o cibercriminoso. 2021.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD): guia de implantação**. Editora Blucher, 2020.

GOTTSCHALK NOLASCO, Loreci; MACIEL SILVA, Bruno Dutra. CRIMES CIBERNÉTICOS, PRIVACIDADE E CIBERSEGURANÇA. **Quaestio Iuris (QI)**, v. 15, n. 4, 2022.

HOLT, Thomas J. **The human factor of cybercrime**. Routledge, 2019.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. CRIMES CIBERNÉTICOS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 10, p. 109-126, 2023.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. CRIMES CIBERNÉTICOS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 10, p. 109-126, 2023.

MARTINS, Adeliane Siqueira Picoli et al. CRIMES CIBERNÉTICOS E INVASÃO DE REDES SOCIAIS. **RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218**, v. 5, n. 10, p. e5105810-e5105810, 2024.

NOLASCO, Loreci Gottschalk; SILVA, Bruno Dutra Maciel. Crimes cibernéticos, privacidade e cibersegurança. **Revista Quaestio Iuris**, v. 15, n. 4, p. 2353-2389, 2022.

PROKISCH, Carlos A. **Soluções para a proteção de redes e sistemas**. Editora Senac São Paulo, 2023.

RODRIGUES, Mariane; DE LIMA, Inayá Farias; DE FREITAS, Rafael. Crimes cibernéticos à luz dos crimes contra a honra. **ANAIS CONGREGA MIC-ISBN 978-65-86471-05-2**, v. 16, p. 354-359, 2020.

SANTOS, EDINILSON et al. **Crimes Cibernéticos**. VISEU, 2023.

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

SILVA BISPO, Adrielle; BINTO, Emanuel Vieira. CRIMES CIBERNÉTICOS: DA INEFICÁCIA DA LEI CAROLINA DIECKMANN NA PRÁTICA DE CRIMES VIRTUAIS. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 11, p. 354-369, 2023.

SILVEIRA, MARCELO; DOS SANTOS, CLAYTON EDUARDO. CRIMES CIBERNÉTICOS: UM PANORAMA GERAL SOBRE AS PRINCIPAIS AMEAÇAS. **Revista Científica e-Locução**, v. 1, n. 25, p. 25-25, 2024.