



CRISLANE GOMES PIRES

JORDANA DUARTE DA SILVA

THYAGO TEIXEIRA PINTO

**A CRIMINALIDADE DIGITAL E OS DESAFIOS CONTEMPORÂNEOS PARA
O DIREITO PENAL NA ERA DA INTELIGÊNCIA ALGORÍTMICA**

TERESINA-PI

2025

JORDANA DUARTE DA SILVA

CRISLANE GOMES PIRES

THYAGO TEIXEIRA PINTO

**A CRIMINALIDADE DIGITAL E OS DESAFIOS CONTEMPORÂNEOS PARA O
DIREITO PENAL NA ERA DA INTELIGÊNCIA ALGORÍTMICA**

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Bacharel em Direito.

Orientador(a): Prof.(a) Dr(a). Enedina
Gizeli Albano Moura.

TERESINA – PI

2025

FICHA CATALOGRÁFICA

P667c Pires, Crislane Gomes

A criminalidade digital e os desafios contemporâneos para o direito penal na era da inteligência algorítmica. / Crislane Gomes Pires; Jordana Duarte da Silva; Thyago Teixeira Pinto. – Teresina: UNINOVAFAPI, 2025.

Orientador (a): Prof^o. Dra. Enedina Gizeli Albano Moura – UNINOVAFAPI, 2025.

30.p.; il. 23cm.

Trabalho de conclusão (Graduação em Direito) – UNINOVAFAPI, Teresina, 2025.

* Criminalidade Digital. 2. Direito Digital. 3. Marco Civil. I. Título. II. Silva, Jordana Duarte da. III. Pires, Crislane Gomes. IV. Pinto, Thyago Teixeira Pinto.

CDD 341.5

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

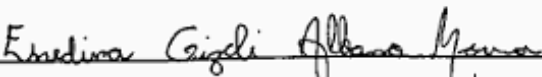
JORDANA DUARTE DA SILVA
CRISLANE GOMES PIRES
THYAGO TEIXEIRA PINTO

**A CRIMINALIDADE DIGITAL E OS DESAFIOS CONTEMPORÂNEOS PARA O
DIREITO PENAL NA ERA DA INTELIGÊNCIA ALGORÍTMICA**

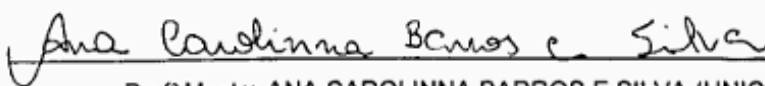
Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 10 / 11 / 25

BANCA EXAMINADORA


Professora Mestra ENEDINA GIZELI ALBANO MOURA
Afya Centro Universitário Uninovafapi
(Orientadora)


Profª Mestre VANESSA NUNES DE BARROS MENDES SAMPAIO
Afya Centro Universitário Uninovafapi
(1º Examinador)


Profª Mestre ANA CAROLINNA BARROS E SILVA (UNICET)
Afya Centro Universitário Uninovafapi
(2º Examinador)

A Deus. A meus pais e familiares, por todo apoio e carinho!

Dedico!

RESUMO

O presente estudo tem como foco tratar da criminalidade digital e os desafios encontrados pelo Direito Penal na aplicação de normas reguladoras. Nesta perspectiva, questionou-se: o ordenamento jurídico brasileiro está preparado para tratar as ocorrências relacionadas a criminalidade digital? Assumiu-se como hipótese a de que, por ser o cibercrime fruto de uma política criminal assente na transnacionalidade do crime, a estilização de novas tipologias jurídicas conduz à expansão do direito penal, todavia, por ser o ordenamento jurídico moroso na expansão legislativa, acarreta em mais demora quando se trata de impor os princípios e regras do Direito Penal e Processual Penal nessa modalidade criminosa. Por meio de uma pesquisa com base metodológica bibliográfica e abordagem qualitativa, esta pesquisa se dividiu em três seções que tiveram como objetivo analisar os principais desafios do Direito Penal na regulamentação de crimes cibernéticos. Como resultados da pesquisa, foi visto que apesar de necessitar de um amparo maior no que tange a criminalidade digital, atualmente, a legislação penal contra os crimes virtuais e/ou cibernéticos representa um importante quadro regulatório no cenário penal e processual penal, decorrente da necessidade de desencadear um processo reflexivo entre as pessoas através da normatização e da interação socioeconômica dos sistemas de informação.

Palavras-chave: Criminalidade Digital; Direito Digital; Marco Civil.

ABSTRACT

This study focuses on digital crime and the challenges faced by criminal law in applying regulatory standards. From this perspective, the question was asked: is the Brazilian legal system prepared to deal with any occurrence related to digital crime? What are the main difficulties in this area? The hypothesis was that, because cybercrime is the result of a criminal policy based on the transnationality of crime, the stylization of new legal typologies leads to the expansion of criminal law; however, because the legal system is slow to expand legislation, this leads to further delays when it comes to imposing the principles and rules of criminal law and criminal procedure on this type of crime. By means of a bibliographical methodological study with a qualitative approach, this study was divided into three sections, the aim of which was to analyze the main challenges facing criminal law when it comes to regulating cybercrime. As a result of the research, it was seen that despite needing greater support with regard to digital crime, criminal legislation against virtual and/or cybercrime currently represents an important regulatory framework in the criminal and criminal procedural scenario, arising from the need to trigger a reflexive process among people through the standardization and socio-economic interaction of information systems.

Keywords: Digital Crime; Digital Law; Civil Rights Framework.

SUMÁRIO

1 INTRODUÇÃO	11
2 ARTIGO	13
1 INTRODUÇÃO	14
2 A INTERNET E DESENVOLVIMENTO DAS TECNOLOGIAS DA INFORMAÇÃO	
16	
3 LEI CAROLINA DIECKMANN E O MARCO CIVIL DA INTERNET	19
4 CIBERCRIMES E OS DESAFIOS PARA O DIREITO PENAL	22
5 CONSIDERAÇÕES FINAIS	26
REFERÊNCIAS	27
ANEXO A - COMPROVANTE DE SUBMISSÃO OU APROVAÇÃO DO ARTIGO NA REVISTA ONDE CONSTE O NOME DE TODOS OS AUTORES DO TRABALHO	32

1 INTRODUÇÃO

A modernidade tem promovido mudanças nas formas de convivência e organização da vida cotidiana, em particular, diante do afastamento gradual entre os membros das famílias, motivado por exigências profissionais, deslocamentos geográficos e novas formas de estruturação social. Nesse contexto, o desenvolvimento da tecnologia e dos meios digitais de comunicação passou a atender à necessidade de manter vínculos e realizar atividades sem a presença física das pessoas envolvidas. O que antes demandava contato direto e presencial, hoje pode ser resolvido por meio de dispositivos conectados à internet, permitindo que tarefas cotidianas, relações pessoais e até mesmo vínculos institucionais sejam mantidos à distância, em um ritmo cada vez mais acelerado (Francisco *et al.*, 2024).

O acesso ampliado à internet e a inovação dos recursos tecnológicos tornaram esses meios parte integrante do cotidiano da maior parte da população. A internet se é vista atualmente como ferramenta essencial em diferentes esferas da vida, como na educação, no ambiente de trabalho, na busca por informação, no entretenimento e na manutenção de relações interpessoais. Sua presença passou, inclusive, a influenciar diretamente o modo como as pessoas se comunicam, se expressam, consomem e constroem seus vínculos sociais (Stábile; Santos, 2024).

Ainda que o uso da internet traga facilidades e possibilidades antes inexistentes, também é necessário reconhecer que esse ambiente tem sido utilizado com frequência para práticas ilegais e comportamentos lesivos. A rede mundial de computadores, ao mesmo tempo em que favorece o acesso a serviços e informações, também serve de espaço para a ocorrência de crimes como fraudes, furtos virtuais, chantagens, além de ataques contra a honra e a integridade das pessoas. Entre essas condutas, estão presentes o *cyberbullying*, a calúnia, o preconceito racial e a invasão de privacidade, todos praticados em meios digitais e que causam efeitos concretos nas vidas das vítimas (Masini Neto, 2024).

Dentro desse cenário, observa-se o aumento das ocorrências de crimes digitais, os quais abrangem práticas como estelionato eletrônico, invasão de dispositivos, roubo de dados pessoais, disseminação de conteúdos ofensivos ou discriminatórios, violação de privacidade, entre outros. Essa realidade tem imposto ao Poder Judiciário o dever de se adaptar com agilidade para enfrentar as novas

formas de conduta ilícita que se manifestam nos meios virtuais (Stábile; Santos, 2024).

Partindo dessa premissa, questiona-se: o ordenamento jurídico brasileiro dispõe de mecanismos atualizados para o enfrentamento da criminalidade digital na era da informação? Logo, o objeto deste estudo foi analisar se o ordenamento jurídico penal brasileiro está adequadamente atualizado para enfrentar a criminalidade digital, verificando quais são os principais entraves normativos, estruturais e tecnológicos que comprometem a prevenção, repressão e responsabilização penal nesse contexto.

A justificativa deste estudo se sustenta na necessidade de compreender as causas que levam indivíduos a cometer crimes no ambiente virtual, observando as relações entre comportamento, anonimato digital e ausência de barreiras físicas. Considerando a expansão das tecnologias como parte da rotina cotidiana, torna-se indispensável analisar de que maneira essas práticas ilícitas ocorrem e como interferem na convivência social.

A pesquisa pretende oferecer contribuição ao campo jurídico ao tratar o tema de forma direta, com base em fundamentos legais e na realidade observável. Além disso, busca fornecer elementos que favoreçam a discussão entre estudantes e profissionais do Direito, ampliando a compreensão sobre a aplicação penal no contexto digital e incentivando o desenvolvimento de respostas jurídicas mais coerentes com os desafios contemporâneos.

A presente investigação possui natureza bibliográfica, com abordagem qualitativa, orientada por um método interpretativo-indutivo. Trata-se de um estudo que se apoia na análise de fontes secundárias, compreendidas como o conjunto de produções bibliográficas que, já tornadas públicas, versam sobre a temática em questão.

A pesquisa foi dividida em três seções, nas quais a primeira focou em analisar o avanço da tecnologia e da rede mundial de computadores. A segunda em analisar a Lei Carolina Dieckmann e o Marco Civil da internet como marcos históricos na regulação de crimes cibernéticos e a terceira seção que enfrenta os desafios do direito penal em aplicar as leis existentes aos crimes cibernéticos.

2 ARTIGO

A CRIMINALIDADE DIGITAL E OS DESAFIOS CONTEMPORÂNEOS PARA O DIREITO PENAL NA ERA DA INTELIGÊNCIA ALGORÍTMICA

DIGITAL CRIME AND CONTEMPORARY CHALLENGES FOR CRIMINAL LAW IN THE AGE OF ALGORITHMIC INTELLIGENCE

RESUMO

O presente estudo tem como foco tratar da criminalidade digital e os desafios encontrados pelo Direito Penal na aplicação de normas reguladoras. Nesta perspectiva, questionou-se: o ordenamento jurídico brasileiro está preparado para tratar as ocorrências relacionadas a criminalidade digital? Assumiu-se como hipótese a de que, por ser o cibercrime fruto de uma política criminal assente na transnacionalidade do crime, a estilização de novas tipologias jurídicas conduz à expansão do direito penal, todavia, por ser o ordenamento jurídico moroso na expansão legislativa, acarreta em mais demora quando se trata de impor os princípios e regras do Direito Penal e Processual Penal nessa modalidade criminosa. Por meio de uma pesquisa com base metodológica bibliográfica e abordagem qualitativa, esta pesquisa se dividiu em três seções que tiveram como objetivo analisar os principais desafios do Direito Penal na regulamentação de crimes cibernéticos. Como resultados da pesquisa, foi visto que apesar de necessitar de um amparo maior no que tange a criminalidade digital, atualmente, a legislação penal contra os crimes virtuais e/ou cibernéticos representa um importante quadro regulatório no cenário penal e processual penal, decorrente da necessidade de desencadear um processo reflexivo entre as pessoas através da normatização e da interação socioeconômica dos sistemas de informação.

Palavras-chave: Criminalidade Digital; Direito Digital; Marco Civil.

ABSTRACT

This study focuses on digital crime and the challenges faced by criminal law in applying regulatory standards. From this perspective, the question was asked: is the Brazilian legal system prepared to deal with any occurrence related to digital crime? What are the main difficulties in this area? The hypothesis was that, because cybercrime is the result of a criminal policy based on the transnationality of crime, the stylization of new legal typologies leads to the expansion of criminal law; however, because the legal system is slow to expand legislation, this leads to further delays when it comes to imposing the principles and rules of criminal law and criminal procedure on this type of crime. By means of a bibliographical methodological study with a qualitative approach, this study was divided into three sections, the aim of which was to analyze the main challenges facing criminal law when it comes to regulating cybercrime. As a result of the research, it was seen that despite needing greater support with regard to digital crime, criminal legislation against virtual and/or cybercrime currently represents an important regulatory framework in the criminal

and criminal procedural scenario, arising from the need to trigger a reflexive process among people through the standardization and socio-economic interaction of information systems.

Keywords: Digital Crime; Digital Law; Civil Rights Framework.

1 INTRODUÇÃO

A modernidade tem promovido mudanças nas formas de convivência e organização da vida cotidiana, em particular, diante do afastamento gradual entre os membros das famílias, motivado por exigências profissionais, deslocamentos geográficos e novas formas de estruturação social. Nesse contexto, o desenvolvimento da tecnologia e dos meios digitais de comunicação passou a atender à necessidade de manter vínculos e realizar atividades sem a presença física das pessoas envolvidas. O que antes demandava contato direto e presencial, hoje pode ser resolvido por meio de dispositivos conectados à internet, permitindo que tarefas cotidianas, relações pessoais e até mesmo vínculos institucionais sejam mantidos à distância, em um ritmo cada vez mais acelerado (Francisco *et al.*, 2024).

O acesso ampliado à internet e a inovação dos recursos tecnológicos tornaram esses meios parte integrante do cotidiano da maior parte da população. A internet se é vista atualmente como ferramenta essencial em diferentes esferas da vida, como na educação, no ambiente de trabalho, na busca por informação, no entretenimento e na manutenção de relações interpessoais. Sua presença passou, inclusive, a influenciar diretamente o modo como as pessoas se comunicam, se expressam, consomem e constroem seus vínculos sociais (Stábile; Santos, 2024).

Ainda que o uso da internet traga facilidades e possibilidades antes inexistentes, também é necessário reconhecer que esse ambiente tem sido utilizado com frequência para práticas ilegais e comportamentos lesivos. A rede mundial de computadores, ao mesmo tempo em que favorece o acesso a serviços e informações, também serve de espaço para a ocorrência de crimes como fraudes, furtos virtuais, chantagens, além de ataques contra a honra e a integridade das pessoas. Entre essas condutas, estão presentes o *cyberbullying*, a calúnia, o preconceito racial e a invasão de privacidade, todos praticados em meios digitais e que causam efeitos concretos nas vidas das vítimas (Masini Neto, 2024).

Dentro desse cenário, observa-se o aumento das ocorrências de crimes

digitais, os quais abrangem práticas como estelionato eletrônico, invasão de dispositivos, roubo de dados pessoais, disseminação de conteúdos ofensivos ou discriminatórios, violação de privacidade, entre outros. Essa realidade tem imposto ao Poder Judiciário o dever de se adaptar com agilidade para enfrentar as novas formas de conduta ilícita que se manifestam nos meios virtuais (Stábile; Santos, 2024).

Partindo dessa premissa, questiona-se: o ordenamento jurídico brasileiro dispõe de mecanismos atualizados para o enfrentamento da criminalidade digital na era da informação? Logo, o objeto deste estudo foi analisar se o ordenamento jurídico penal brasileiro está adequadamente atualizado para enfrentar a criminalidade digital, verificando quais são os principais entraves normativos, estruturais e tecnológicos que comprometem a prevenção, repressão e responsabilização penal nesse contexto.

A justificativa deste estudo se sustenta na necessidade de compreender as causas que levam indivíduos a cometer crimes no ambiente virtual, observando as relações entre comportamento, anonimato digital e ausência de barreiras físicas. Considerando a expansão das tecnologias como parte da rotina cotidiana, torna-se indispensável analisar de que maneira essas práticas ilícitas ocorrem e como interferem na convivência social.

A pesquisa pretende oferecer contribuição ao campo jurídico ao tratar o tema de forma direta, com base em fundamentos legais e na realidade observável. Além disso, busca fornecer elementos que favoreçam a discussão entre estudantes e profissionais do Direito, ampliando a compreensão sobre a aplicação penal no contexto digital e incentivando o desenvolvimento de respostas jurídicas mais coerentes com os desafios contemporâneos.

A presente investigação possui natureza bibliográfica, com abordagem qualitativa, orientada por um método interpretativo-indutivo. Trata-se de um estudo que se apoia na análise de fontes secundárias, compreendidas como o conjunto de produções bibliográficas que, já tornadas públicas, versam sobre a temática em questão.

A pesquisa foi dividida em três seções, nas quais a primeira focou em analisar o avanço da tecnologia e da rede mundial de computadores. A segunda em analisar

a Lei Carolina Dieckmann e o Marco Civil da internet como marcos históricos na regulação de crimes cibernéticos e a terceira seção que enfrenta os desafios do direito penal em aplicar as leis existentes aos crimes cibernéticos.

2 A INTERNET E DESENVOLVIMENTO DAS TECNOLOGIAS DA INFORMAÇÃO

A Internet é caracterizada por uma vasta rede de computadores interconectados em todo o mundo, interligadas por meio de cabos, linhas telefônicas, comunicação via satélite e outros meios de telecomunicações. Seu desenvolvimento foi de cunho militar, como alternativa de comunicação entre os principais centros militares de comando e controle, com o objetivo de que, caso os meios de comunicação utilizados na época fossem destruídos, o exército pudesse manter as informações ligadas eletronicamente por meio de computadores, de modo que não haveria comando central, e em caso de ataque a um dos pontos da rede, a conexão ainda estaria ativa (Souza, 2021).

O desenvolvimento da tecnologia no final do século XX começou a dar origem aos primeiros ambientes virtuais utilizando métodos de comunicação, como o telefone, para estabelecer conexões entre vários usuários simultaneamente, permitindo a comunicação instantânea dentro de um ambiente considerado virtual. Com efeito, pode-se considerar que os ambientes virtuais nasceram nesse período, como resultado do desenvolvimento dos meios de comunicação (Souza, 2021).

Há relatos, no entanto, que definem que o desenvolvimento da revolução da tecnologia da informação e da mídia não ocorreu realmente até o início do século XXI e, com poucas exceções, desenvolveu-se inicialmente em ambientes empresariais, em certos estudos governamentais e em indivíduos de classes econômicas mais altas (Raposo, 2022). Desde o surgimento do uso das tecnologias digitais, seu uso aparenta estar fora do controle de qualquer agência governamental e existindo um ambiente de livres possibilidades de uso.

O crescimento explosivo da Internet e a utilização crescente das redes sociais e dos meios virtuais criaram complexidades que popularizaram os meios digitais e os tornaram facilmente acessíveis a todos, e mesmo com essa explosão, ainda na primeira metade do século XXI não existem regulamentações diretas sobre o uso de

tais meios, apenas normas gerais e abrangentes de direito nacional para punir e prevenir abusos (Buani, 2020).

A Internet é uma importante ferramenta e o seu uso tem trazido inúmeros benefícios em diversas áreas, tornando-se indispensável na vida cotidiana. Contudo, justamente por seu caráter de comunicação em larga escala, pela transferência instantânea de informações e pela substituição de diversas atividades manuais por práticas digitais e online, esse ambiente passou a ser igualmente explorado para a prática de condutas ilícitas, classificadas como crimes virtuais (Souza, 2021). Essa ambivalência entre os avanços tecnológicos e os riscos associados evidencia que, ao mesmo tempo em que a rede mundial conecta pessoas e potencializa oportunidades, também amplia os desafios relacionados à segurança digital e à persecução penal.

Também chamados de cibercrimes, o conceito por trás desse tipo de ação é constituída por todos os atos ilícitos praticados pela Internet que podem causar algum tipo de dano, seja financeiro ou moral, ao ofendido. Os crimes cibernéticos podem ser definidos como crimes que utilizam um sistema eletrônico de processamento de dados como ferramenta ou objeto com diversos métodos de execução e danos a bens jurídicos e está associado ao fenômeno dos crimes de informação, ações que violam direitos básicos, seja pelo uso da tecnologia da informação para cometer um crime, seja como elemento do tipo jurídico da atividade criminosa (Faoro; Jesus; Abreu, 2015).

Em sua grande maioria, esses ilícitos são cometidos por pensarem os criminosos estarem protegidos pelo anonimato. Nos dias atuais, o anonimato no ambiente virtual é um tema polêmico, pois geralmente não há informações sobre essa pessoa e como ela está agindo, se de forma automatizada ou por computador. “Essa sensação impulsiona alguns indivíduos a ir de encontro a lei, na ilusória sensação de que não serão descobertos, de que agirão sem serem percebidos ou julgados” (Fernandes, 2022, p. 12).

Dado que a Internet constitui uma rede informática global, não é incomum que fatores geopolíticos transnacionais tornem as investigações ainda mais complexas em situações desse tipo. Cada país dispõe de arcabouço jurídico próprio para o enfrentamento desses delitos, sendo que alguns contam com estruturas técnicas

especializadas, enquanto outros ainda apresentam fragilidades legislativas e investigativas, o que compromete a efetividade no combate a tais práticas, consideradas altamente prejudiciais (Coltro; Waldman, 2021).

O termo “transnacionalidade”, aplicado à rede mundial de computadores, significa que não existem fronteiras nacionais que restrinjam a divulgação de informações e a transferência de dados, exceto em países que não possuem neutralidade de rede ou outros tipos de regulação de acesso dentro do provedor. Por um lado, o carácter transnacional traz benefícios, garantindo e promovendo o livre exercício da democracia, mas por outro lado, também cria obstáculos ao exercício efetivo da proteção judicial, como é o caso do Brasil, onde o art. 11 da Lei 12.965/2014 (Marco Civil da Internet) discorre,

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. 23 § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (Brasil, 2014).

Além disso, o maior problema causado pela transnacionalidade da rede se deve ao fato de os provedores de aplicações de Internet hospedarem suas atividades ilegais alocando servidores em países com legislação diferente da brasileira, em relação aos crimes digitais.

Conceituando os crimes digitais, estes são atos realizados contra os sistemas de computador, que são subespécies de atos contra dados ou programas destinados às pessoas, logo, os atos praticados e incluídos em um sistema são considerados crimes digitais, podendo ser classificados como crimes contra a propriedade e/ou crimes contra a liberdade pessoal e crimes contra a propriedade imaterial (Pereira, 2022).

Atualmente, se tornou comum a prática de crimes virtuais, onde a grande maioria das vítimas não busca a justiça, por não acreditar que o criminoso possa ser

devidamente punido, pois o crime foi cometido pela internet, não havendo como “identificar o autor do crime”. Sobre esse ponto de vista, evidencia-se que o cometimento de crimes cibernéticos inclui fraude, roubo, extorsão, além de crimes contra a dignidade humana, como cyberbullying, calúnia, racismo e violação da intimidade (Pereira, 2022).

Em outros casos, o infrator tem em mente que, por se tratar da realização de um ilícito em um local onde não há rastreamento e, portanto, sem projeção legal, não haverá punição por ser uma “terra sem lei”. Porém, os crimes de extorsão, ameaça, furto, estelionato já havia tutela no Código Penal (1940), o que ocorre nesses casos é uma extensão para o ambiente virtual (Theuherz; Santos, 2023).

Milhares de pessoas em todo o Brasil são atacadas diariamente por golpistas que tentam roubar seus dados, só em 2020, o Brasil foi o país mais atingido por tentativas de roubo de dados pessoais ou financeiros de pessoas na internet, prática denominada em inglês phishing. Com as essas informações, golpistas prejudicam a vítima de diversas forma, seja acessando recursos ou enganado pessoas se fazendo passar por ela. As tentativas de golpes se dão por diversos meios, inclusive de situações atuais, como no caso do cadastramento do auxílio emergencial, cadastro para vacinação, tentativas de golpe usando o PIX e através do WhatsApp, onde o aplicativo é clonado (Silva, 2022, p. 03).

Esta inevitável adaptação do *modus operandi* dos crimes digitais revelou também as disputas existentes sobre terminologia, conceito e classificação que são utilizadas neste profícuo campo que se apresenta. Além dessas questões relevantes, é importante destacar aquelas relacionadas ao bem jurídico a ser tutelado, havendo ou não necessidade de ampliação do escopo de proteção, ou seja, o instituto de novos bens jurídicos decorrentes do atual processo de cometimento esses crimes digitais (Santos, 2021).

O cometimento dos crimes cibernéticos ocorre, em sua maioria, através das mídias sociais, que tem um forte poder de transmissão de informações, seja via Instagram, *WhatsApp* ou Facebook. A situação muda quando lidamos com internautas que cometem crimes nas redes sociais, porém, ignoram que suas ações são criminosas (Santana; Santos, 2023). Não é incomum o comportamento criminoso nessas redes, como a divulgação e compartilhamento de fotos, vídeos e mensagens com conteúdo ofensivo e, em muitos casos, publicações com informações falsas, desacreditando as vítimas e ferindo sua reputação. No entanto,

o descumprimento da lei não isenta o infrator da pena aplicável.

3 LEI CAROLINA DIECKMANN E O MARCO CIVIL DA INTERNET

O direito digital surgiu como uma área recente dentro do campo jurídico, construída a partir da necessidade de lidar com as demandas específicas originadas pelo uso das tecnologias da informação e da comunicação, em especial da internet. Sua finalidade é enfrentar os novos desafios que se apresentam diante da reorganização das relações sociais, do modo de vida contemporâneo e das práticas que se estabelecem em ambientes virtuais (Lantyer; Carvalho, 2024).

Essa nova realidade gerou situações inéditas que não encontram correspondência direta nas legislações tradicionais, o que tem exigido adaptações e reflexões contínuas por parte dos operadores do direito. De acordo com Pimentel (2018), essa nova disciplina se estrutura justamente para responder a questões ligadas ao impacto das inovações tecnológicas sobre o comportamento humano e sobre a forma como as pessoas interagem, consomem conteúdos, trabalham e se relacionam nos espaços digitais, dentro daquilo que se convencionou chamar de “sociedade da informação”.

Com a globalização, a expansão da tecnologia e o uso de mídias virtuais, surgiu uma nova categoria de crime denominada crime virtual informático, crime eletrônico ou crime cibernético, onde a falta de legislação específica regulamentando esse tema deixou os usuários desprotegidos (Pompeu, 2022). Sob este ponto de vista, a sociedade na era da informação precisa refletir sobre a cultura, a justiça e as regras que permeiam esta sociedade e como utilizá-las para alcançar uma convivência equilibrada entre todas as pessoas.

Como regra, os usuários de tecnologias devem estar atentos aos perigos advindos das violações de dados e informações privadas, bem como aos ataques de *hackers* e vírus que podem comprometer a segurança dos seus dados pessoais. Além disso,

A disponibilização de informações pessoais na rede faz com que se criem verdadeiros dossiês de perfil de usuários, seu comportamento pessoal, econômico e social, informações que podem ser utilizadas para diversos fins, inclusive comerciais. Tal exposição está diretamente ligada à invasão de privacidade. Os dados compartilhados permanecem sobre o controle dos

operadores de rede, que os armazenam muitas vezes para fins econômicos próprios ou venda para terceiros (Castro, 2021, online).

No Brasil, a alta incidência de crimes cibernéticos impulsionou o desenvolvimento de leis de proteção de dados em ambientes virtuais. Essas ações, embora mais conhecidas atualmente, já ocorrem desde muito tempo. No Brasil, antes do ano de 2012, não havia nenhuma lei que regulasse totalmente o direito a intimidade e vida privada. Todavia, a Lei nº 12.737, de 30 de novembro de 2012, conhecida como “Lei Carolina Dieckmann”, foi considerado como um caso simbólico de inovação legislativa para combater esse tipo de crime, além do Marco Civil da Internet publicado na Lei nº 12.965 de 2014.

Antes da lei, invadir um ambiente virtual e roubar dados pessoais já era crime, mas não havia regulamentação específica. Para muitos especialistas, a ausência de leis próprias ou de algum meio de coibir a criminalidade informática em 2012 levou a sérios atrasos na legislação brasileira. Assim, o surgimento desta nova Lei veio para proteger os interesses jurídicos da liberdade pessoal e do sigilo profissional e pessoal, tendo impacto no código penal, acrescentando dois artigos 154-A e 154-B intitulados “invasão de dispositivo informático” e alterando o artigo 266 e 298 no que diz respeito à segurança em ambientes virtuais, regulamenta o uso indevido de informações e materiais na Internet correspondentes à privacidade humana, como fotos e vídeos (Pompeu, 2022).

Todo o cenário construído pelo processo de virtualização da informação ao longo dos anos, em conformidade com a legislação específica sobre lei de proteção de dados, representa o conflito contínuo em que o Estado, através da utilização de recursos e meios legais, tenta coibir este tipo de crime, que ampliou o escopo de suas operações em diferentes ambientes do ciberespaço. Porém, nesta política de confronto algumas leis se destacam, mas ainda existem crimes praticados de forma cotidiana e crimes que exigem respostas legislativas cada vez mais rápidas e eficazes (Meinero; Dalzotto, 2021).

O Marco Civil da Internet surgiu no cenário nacional para regular os direitos, obrigações e princípios que devem ser observados na utilização da Internet. As questões que envolvem liberdade de expressão, inclusão digital, segurança da informação, proteção de dados pessoais, provas eletrônicas e a responsabilidade

dos prestadores são objeto desta Lei (Meinero; Dalzotto, 2021).

Embora os princípios que regem a Lei nº 12.737/2012 e a Lei nº 12.695/2014 sejam teoricamente harmoniosos, na prática apresentam divergências dominantes que requerem a ajuda do princípio da proporcionalidade. Assim, para resolver esta questão, o Marco Civil introduziu a possibilidade de responsabilizar os prestadores de serviços de *internet* como medida para garantir que os direitos fundamentais sejam respeitados quando forem violados.

Respaldado no Código Civil vigente, ao se analisar o artigo 927 do texto legislativo, e em especial o parágrafo único, verifica-se que a definição nele contida sustenta a responsabilidades dos fornecedores envolvidos no processo de comunicação midiática. De acordo com esta disposição, “quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem” (Brasil, 2002), há a obrigação de se reparar o dano sem apurar se houve culpa, aplicando-se, neste contexto, o instituto da responsabilidade objetiva do agente.

Mas, apesar da implementação dessa lei, o Ministro Rogerio Schietti, explanou que o direito penal não está preparado para receber os desafios envolvendo os crimes cibernéticos. Segundo ele “os danos potenciais que esses delitos podem causar ainda não são totalmente conhecidos” (Galli, 2017, s/p), e isso pode levar a uma estrutura de interpretação totalmente incoerente do que é o direito e a sua aplicabilidade.

No âmbito penal, apesar de esforços, a legislação brasileira ainda é atrasada e desatualizada no combate direto ao crime cibernético, que tem tratado esses tipos penais como meras contravenções crimes comuns desde que o país iniciou a sua enorme explosão tecnológica, e, apesar dos institutos legislativos citados nesta seção serem consideradas como um grande avanço tecnológico para o sistema Penal ainda existem muitas críticas em relação ao sistema legislativo e penal, sendo imprescindível um olhar mais cauteloso do legislador para essa lacuna normativa, principalmente devido ao grande aumento do uso tecnológico dos últimos anos e a sua progressão na chamada “era da tecnologia”.

4 CIBERCRIMES E OS DESAFIOS PARA O DIREITO PENAL

Quanto mais a tecnologia incorpora-se ao cotidiano humano, mais importante se torna que os sujeitos comecem a adquirir conhecimento dos elementos virtuais para fazer frente à modernidade e assim, participar de modo ativo. Este campo de estudo se tornou importante não apenas para os estudos de tecnologia, mas também para os cidadãos, que em alguns casos buscam aprender e desenvolver a tecnologia de acesso a redes de comunicação e outras ferramentas como forma de trabalho (Fiorillo; Conte, 2016).

O mundo da tecnologia tem se expandido cada vez mais e isso pode ser evidenciado nas seções anteriores. Todo esse processo de globalização trouxe a necessidade de mudanças importantes para a sociedade e baseado nisso, a legislação também teve que se adequar a esse processo expansivo. Com o desenvolvimento da tecnologia virtual, os crimes cibernéticos apenas continuaram a desenvolver-se e as suas formas passaram a mudar rapidamente, havendo, pois, uma necessidade de formular legislação penal especial para prevenir e combater novos crimes virtuais.

Deve-se ressaltar que a expansão do Direito Penal é causada por uma série de fatores que iniciam-se através da globalização, tais como: novos interesses, novos riscos, a insegurança social e o reconhecimento das vítimas de crimes pela maioria das pessoas na sociedade. Neste contexto, mesmo reconhecendo os problemas envolvidos na expansão do direito penal, é necessário analisar como o problema pode ser reorganizado de modo a levar em conta o surgimento de novas realidades, a fim de garantir ou pelo menos contribuir para a proteção da legalidade da lei (Silva, 2023).

Autores como D'Ávila e Santos (2016), defendem que os principais problemas do Direito Penal contemporâneo não são de ordem quantitativa, ou seja, não surgiram da sua expansão para abarcar novos assuntos, do aumento da área de regulamentação ou mesmo do simples fato de o Direito Penal ter proliferado, o seu real problema se dá em como essa expansão é aplicada qualitativamente.

Devido às mudanças no campo tecnológico e ao crescimento desenfreado do crime digital, novos direitos relacionados aos ambientes virtuais começam a ser reconhecidos até mesmo em nível internacional, como por exemplo o direito de

acesso à Internet, que foi declarado um Direito Humano em relatórios elaborados pelas Nações Unidas, cuja violação constitui crime (Taveski; Silva, 2023). Contudo, deve-se destacar que esses novos direitos específicos de que tratam deste tema não abrangem toda a área de atuação do cibercrime, o que representa outro desafio à aplicação do direito penal.

A própria legislação, apesar de esforços, anda a passos lentos no que diz respeito ao acompanhamento dos avanços provocados pela tecnologia, e é a partir dessa falha legislativa, que o desenvolvimento de práticas delituosas ocorre, por meio de agentes que se utilizam do anonimato para realizá-los.

Diante delas, as liberdades e garantias penais, a tanto custo conquistadas, veem-se hoje fragilizadas e não raramente são afastadas, sob o argumento da necessidade de otimização das pretensões político-criminais de combate à criminalidade. Uma espécie de entronização da ideia de segurança que, por vezes, a depender do âmbito em que se projeta, como, aliás, bem ilustra o terrorismo, parece não conhecer limites dogmáticos ou político-criminais (D'Avila; Santos, 2016, p. 101).

Barroso (2013), explicou que, de acordo com o artigo 1º, inciso III da Constituição Federal de 1988, a dignidade da pessoa humana é o fundamento da República Federativa do Brasil e é o valor fundamental que orienta os princípios e normas considerados fundamentais. Os direitos fundamentais incluem no seu âmbito o direito à integridade moral ou mental, incluindo a privacidade, a honra e a publicidade. Em suma, vários sistemas jurídicos, incluindo o sistema brasileiro, consideram a proteção de dados um importante meio de proteção pessoal e um direito fundamental. Isto requer mecanismos que permitam às pessoas compreenderem e controlar os seus próprios dados como uma expressão direta da sua personalidade.

Dadas as possibilidades apresentadas por este instrumento normativo, suas premissas focam em representar o desejo de proporcionar a proteção adequada aos indivíduos e seus respectivos bens. Obviamente, uma tarefa desta magnitude não é tão fácil de realizar, pois o mundo digital está repleto de inúmeros desafios, entre os quais a dificuldade de identificar possíveis atos criminosos, incluindo aqueles que ocorrem através do acesso e utilização inadvertida de dados pessoais por parte de terceiros (Stacchini, 2022).

Como o desenvolvimento da Internet trouxe conveniência à vida moderna, deve-se considerar que este desenvolvimento também levou a um aumento da criminalidade, uma vez que é utilizada para realizar atividades ilegais, sendo um grande desafio para o Direito Penal para a regulamentação dessas atividades (Conte; Santos, 2008). É importante ter em mente que num mundo cada vez mais globalizado, o direito penal precisa acompanhar o contínuo desenvolvimento da tecnologia para garantir a correta aplicação da lei e, assim, alcançar o ideal de justiça, bem como promover a paz social.

Além disso, a sociedade deve considerar que o Direito Penal não pode atingir um efeito preventivo esclarecendo todos os casos existentes. É necessário implementar diversas formas de proteção para que os usuários tenham consciência dos perigos que a Internet representa, uma vez que a rede de computadores disponibiliza atualmente informações gratuitas e diversificadas sobre a vida pública e privada (Freitas; Gonçalves, Torres, 2023).

O legislador direciona sua atuação para atender às demandas mais enfáticas da mídia e da sociedade, recorrendo muitas vezes à matéria penal, considerando-a a área do direito mais rigorosa e relevante para a proteção da sociedade. Contudo, em muitos casos, esta instrução é realizada de forma desproporcional e desorganizada, contrariando a filosofia de intervenção mínima do direito penal.

De acordo com Silva (2023), a utilização do direito penal como único mecanismo para combater o cibercrime resulta muitas vezes na formulação aleatória de leis sem conhecimentos técnicos. Comparando outros casos, verifica-se que os crimes ambientais e os crimes relacionados com drogas não foram completamente resolvidos através da aplicação separada do direito penal, e ainda têm um impacto negativo noutras questões jurídicas, como o encarceramento excessivo.

À medida que o ciberespaço avança, embora as fraquezas naturais das relações de consumo sejam expostas à criminalidade informática, muitas vezes desenfreada, é necessária uma melhor legislação penal específica, incluindo a proteção de dados. Face a esta realidade, foi desenvolvido um projeto de Lei de Proteção de Dados para a segurança pública e investigações criminais, que inclui as seguintes disposições do texto do Código Penal: “Art. 154-C. Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou

interconectar bancos de dados pessoais sem autorização legal: (NR) Pena - reclusão, de 1 (um) a 4 (quatro), anos e multa” (Brasil, 1940).

Considera-se, portanto, que um dos principais desafios da política criminal de proteção de dados no ciberespaço não é apenas a falta de disciplina jurídica, mas principalmente a sua eficácia. Face à nova transformação digital, e por força dos preceitos constitucionais, o direito penal baseado unicamente na repressão estritamente punitiva pode carecer de real eficácia (Taveski; Silva, 2023). Portanto, além da necessidade de uma descrição típica dos tipos de crimes virtuais que violam a proteção de dados do consumidor, outro desafio é também a adoção de diferentes medidas que vão além de uma perspectiva punitiva, como a abolição das penas privativas de liberdade e a implementação de medidas alternativas, para atingir a finalidade social da pena imposta para garantir a máxima eficácia da segurança digital.

Outrossim, o Tribunal Superior de Justiça considerou que as provas obtidas diretamente de um *smartphone*, como mensagens de texto, aplicativos como WhatsApp ou mensagens recebidas e enviadas por e-mail, obtidas no momento da conduta, mas sem prévia autorização legal para analisar dados de dispositivos móveis será considerada ilegal, necessitando, portanto de autorização para utilizá-las como meio probatório (Zaniolo, 2021).

Apesar de necessitar de um amparo maior no que tange a criminalidade digital, atualmente, a legislação penal contra os crimes virtuais e/ou cibernéticos representa um importante quadro regulatório no cenário penal e processual penal, decorrente da necessidade de desencadear um processo reflexivo entre as pessoas através da normatização e da interação socioeconômica dos sistemas de informação. No entanto, não se refere a uma forma concreta de normas, mas a um processo contínuo de filosofia normativa no qual todos devem estar envolvidos: o Estado e a sociedade civil.

5 CONSIDERAÇÕES FINAIS

Este estudo teve como foco analisar os principais desafios do Direito Penal na regulamentação de crimes cibernéticos. De modo a verificar-se que, embora o

ordenamento jurídico brasileiro ainda não disponha de um conjunto normativo unificado e sistemático dedicado exclusivamente ao tratamento de delitos cibernéticos, o Direito Penal tem sido o principal instrumento utilizado para combater essas práticas.

Verificou-se que há uma busca permanente para atualizar interpretações jurídicas e encontrar respostas compatíveis com as novas modalidades de violação de bens jurídicos, partindo do princípio de que o espaço virtual, embora tenha características distintas do espaço físico, não está isento da aplicação das normas jurídicas que regem a convivência social. Como apontam Coltro e Waldman (2021), um dos fatores que agrava o cenário dos crimes virtuais é a existência de indivíduos ou grupos que se especializam na elaboração de métodos e estratégias para cometer esses delitos, por meio de redes clandestinas. É dizer, os desafios para o enfrentamento da criminalidade digital, ultrapassa a falta de legislação, permeando o próprio campo da estruturação estatal.

Por esta razão, a terceira seção mostrou que os desafios do direito penal em aplicar a lei penal aos crimes cibernéticos vão além da existência de legislação atualizada. É que com a popularidade da Internet, a criação de um novo domínio faz com que as relações humanas ocorram sem precedentes. Essas mudanças ocorreram de forma tão repentina que se pode notar que a maioria dos países tem demonstrado grande dificuldade em exercer a proteção judicial para regular e controlar comportamentos em ambientes virtuais.

Assim, ao buscar responder o problema de pesquisa, foi possível perceber que, apesar dos esforços legislativos, o ordenamento jurídico brasileiro ainda não se encontra totalmente preparado para regular sobre a matéria, pois a sua adequação as realidades sociais ainda ocorrem a passos lentos. E, por ser o cibercrime fruto de uma política criminal assente na transnacionalidade do crime, a estilização de novas tipologias jurídicas conduz à expansão do direito penal, todavia, por ser o ordenamento jurídico moroso na expansão legislativa, acarreta em mais demora quando se trata de impor os princípios e regras do Direito Penal e Processual Penal nessa modalidade criminosa.

REFERÊNCIAS

BARROSO, Luís Roberto. **O novo direito constitucional brasileiro**: contribuições para a construção teórica e praticada jurisdição constitucional no Brasil. Belo Horizonte – Ed. Fórum, 2013. Disponível em: https://loja.editoraforum.com.br/pdf/O_NOVO_DIREITO_CONSTITUCIONAL_BRASIL_EIRO.pdf. Acesso em: 16 nov. 2025.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html>. Acesso em: 16 nov. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 16 nov. 2025.

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, DF, abril 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 de out. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 de out. 2025.

BUANI, Patrícia Berto. **A compatibilidade entre o ordenamento jurídico brasileiro e a convenção sobre cibercrimes**. 2020. 44 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2020. Disponível em: <https://repositorio.idp.edu.br/handle/123456789/2808>. Acesso em: 13 de out. 2023.

CASTRO, Bárbara Brito de. Direito digital na era da Internet das coisas-O direito à privacidade e o sancionamento da Lei Geral de Proteção de Dados Pessoais. **Caderno Âmbito jurídico** v. 26, 2021. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-civil/direito-digital-na-era-da-internet-das-coisas-o-direito-a-privacidade-eo-sancionamento-da-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 20 out. 2025.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. **Criminalidade digital no Brasil**: a problemática e a aplicabilidade da convenção de budapeste. Revista Em Tempo, v. 21, n. 1, p. 104-123, 2021. Disponível: <https://revista.univem.edu.br/emtempo/article/view/3247>. Acesso em: 20 out. 2025.

CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. Desafios do direito penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos. **Revista de Direito de Informática e Telecomunicações**, v. 3, n. 4, 2008. Disponível em: <https://www.oabma.org.br/public/uploads/files/siteComissoes/2017100510283859d63386ebf0a.pdf>. Acesso em: 20 out. 2025.

D'AVILA, Fabio Roberto; DOS SANTOS, Daniel Leonhardt. Direito Penal e Criminalidade Informática. Breves Aproximações Dogmáticas Criminal Law And Cybercrimes. Briefdogmatic Approaches. **Duc In Altum-Cadernos de Direito**, v. 8, n. 15, 2016. Disponível em: <https://www.revistas.faculadadedamas.edu.br/index.php/cihjur/article/view/369>. Acesso em: 20 out. 2025.

FAORO, Roberta Rodrigues; JESUS, Betina Ribeiro; ABREU, Marcelo Faoro. Um estudo sobre crimes digitais: detecção e prevenção. **Anais do IV SINGEP**, p. 1-17, 2015. Disponível em: <https://www.singep.org.br/4singep/resultado/139.pdf>. Acesso em: 30 out. 2025.

FERNANDES, Marquésia Pereira. Crimes digitais na era do metaverso no Brasil. Goiânia, 2022. 38f. **Artigo Científico** (Graduação em Direito) – Pontifícia Universidade Católica de Goiás (PUCGOIÁS), 2022. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/4923>. Acesso em: 30 out. 2025.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. Crimes no Meio Ambiente Digital. 2. ed. São Paulo: **Saraiva**, 2016. Disponível em: <https://ifrs.pergamum.com.br/acervo/41567>. Acesso em: 19 nov. 2025.

FLOWTI. **A importância da LGPD no combate aos cibercrimes**. Brasil, 12 nov. 2021. Disponível em: <https://flowti.com.br/blog/a-importancia-da-lgpd-no-combateaos-cibercrimes>. Acesso em: 20 out. 2025.

FRANCISCO, Joao *et al.* A Criminalidade Informática: Análise do Sistema Jurídico Angolano. **Revista Eletrônica de Direito Penal e Política Criminal**, v. 12, n. 1/2, p. 15-36, 2024. Disponível em: <https://seer.ufrgs.br/redppc/article/view/137821>. Acesso em: 20 out. 2025.

FREITAS, Camila Cristina Gonzaga; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. **Revista JRG de Estudos Acadêmicos**, v. 6, n. 12, p. 296-311, 2023. Disponível em: <https://revistajrg.com/index.php/jrg/article/view/520>. Acesso em: 19 nov. 2025.

GALLI, Marcelo. Direito não está preparado para enfrentar criminalidade digital, diz Rogério Schietti. 26 mai. 2017. **Conjur**. Disponível em: <https://www.conjur.com.br/2017-mai-26/direito-nao-preparado-enfrentar-crime-digital->

schietti. Acesso em: 25 de mai. 2025.

LANTYER, Victor; CARVALHO, Fábila Ribeiro Carvalho. O Direito fundamental à desconexão no contexto do trabalho remoto: desafios e perspectivas na era digital. **Direitos Democráticos & Estado Moderno**, v. 3, n. 12, p. 115-130, 2024. Disponível em: <https://revistas.pucsp.br/DDEM/article/view/67444>. Acesso em: 19 nov. 2025.

MARCONI, Marina de Andrade. LAKATOS, Eva maria. Fundamentos de metodologia científica. São paulo: **Atlas**, v6. 2003. Disponível em: https://docente.ifrn.edu.br/olivianeta/disciplinas/copy_of_historia-i/historia-ii/china-e-india/view. Acesso em: 19 nov. 2025.

MASINI NETO, Ameleto. **Crimes Cibernéticos**. Editora Foco, 2024. Disponível em: https://konektacommerce.nyc3.cdn.digitaloceanspaces.com/TEXT_SAMPLE_CONTENT/crimes-ciberneticos-1a-ed-2025-251764-1.pdf. Acesso em: 19 nov. 2025.

MEINERO, Fernanda Sartor; DALZOTTO, Júlia Valandro. A responsabilidade civil dos provedores de internet nos casos de pornografia de vingança. **Revista de Direito**, v. 13, n. 01, p. 01-30, 2021. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Vi%C3%A7osa_v.13_n.1.07.pdf. Acesso em: 19 nov. 2025.

PATIAS, Naiana Dapieve; HOHENDORFF, Jean Von. Critérios de qualidade para artigos de pesquisa qualitativa. **Psicologia em estudo**, v. 24, p. e43536, 2019. Disponível em: <https://www.scielo.br/j/pe/a/BVGWD9hCCyJrSRKrsp6XfJm/?lang=en>. Acesso em: 19 nov. 2025.

PEREIRA, Valéria de Oliveira Machado. **Estelionato Virtual: O click do crime**. 2022. 41f. Trabalho de Conclusão de Curso (graduação em Direito) Universidade São Judas Tadeu, 2022. Disponível em: https://oasisbr.ibict.br/vufind/Record/%C3%82nima_fea5e9da7968a37fa0a5df6191f5f56b. Acesso em: 19 nov. 2025.

PIMENTEL, Jose Eduardo de Souza. **Introdução ao direito digital**. Revista Jurídica da Escola Superior do Ministério Público de São Paulo, v. 13, n. 1, p. 16-39, 2018. Disponível em: https://es.mpsp.mp.br/revista_esmp/index.php/RJESMPSP/article/view/352. Acesso em: 19 nov. 2025.

POMPEU, Ana Luiza Brandão Calil et al. Crimes Cibernéticos: A Ineficácia da Lei Carolina Dieckmann. 2022. 41f. **Monografia** (Curso de Direito) – Faculdade de Inhumas (FACMAIS), 2022. Disponível em: <http://65.108.49.104/bitstream/123456789/509/2/Template%20de%20TCC%20Direito%202021%20%281%29.docx.pdf>. Acesso em: 19 nov. 2025.

RAPOSO, Jair Antonio. A criminalidade e impunidade frente aos delitos praticados

no ambiente virtual. **Praxis Jurídica**, v. 6, n. 1, p. 1-17, 2022. Disponível em: <https://anais.unievangelica.edu.br/index.php/praxisjuridica/article/view/8143>. Acesso em: 19 nov. 2025.

SANTANA, Katiene Gouveia; SANTOS, Keila Oliveira. Crimes contra a honra no ambiente virtual. **Dat@ venia**, v. 11, n. 1, p. 34-34, 2023. Disponível em: https://revista.uepb.edu.br/Datavenia/pt_BR/article/view/1778. Acesso em: 19 nov. 2025.

SANTOS, Rosangela dos. Criminalidade digital em tempos de pandemia: principais ocorrências em Sergipe no ano de 2020. São Cristóvão, 2021. **Monografia** (graduação em Direito) – Departamento em Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão, SE, 2021. Disponível em: <https://ri.ufs.br/handle/riufs/14606>. Acesso em: 19 nov. 2025.

SILVA, Gilsimar. Crimes digitais: evolução dos crimes e a aplicação do direito. **Artigo Científico** – Universidade Potiguar, 2022. Disponível em: <https://repositorio.animaeducacao.com.br/items/868d4293-822f-40df-9c02-8e1c15d02839>. Acesso em: 19 nov. 2025.

SILVA, Matheus Faraco de Medeiros da. A proteção dos dados pessoais contra cibercrimes frente ao projeto de lei nº 879 de 2022. **Trabalho de Conclusão de Curso** (curso de Direito) - Universidade Federal de Santa Catarina, 2023. Disponível em: <https://repositorio.ufsc.br/handle/123456789/248640>. Acesso em: 19 nov. 2025.

SOUZA, Mykaelly Silva. Cibercrimes e os reflexos no direito brasileiro. **Monografia Jurídica** (Graduação em direito) - Pontifícia Universidade Católica de Goiás (PUCGOIÁS), 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2659>. Acesso em: 19 nov. 2025.

STÁBILE, Fábio Rogério Lima; SANTOS, Carlos Henrique Locatelli. **Direito digital, direito internacional e novas tecnologias**: um caminho para a decolonialidade. Revista Tema On-Line, v. 2, n. 2, 2024. Disponível em: <https://publicacoes.uniesp.edu.br/index.php/9/article/view/214>. Acesso em: 19 nov. 2025.

STACCHINI, Isabella Soares. Proteção de dados pessoais no campo do direito penal à luz da lei geral de proteção de dados (lei Nº 13.709/2018). 2022. 52f. **Trabalho de Conclusão** (Faculdade de Direito) – Universidade Presbiteriana Mackenzie, 2022. Disponível em: <https://dspace.mackenzie.br/handle/10899/32639>. Acesso em: 19 nov. 2025.

TAVESKI, Felipe; SILVA, Elcio Domingues. Desafios políticos criminais no combate aos cibercrimes praticados contra a proteção de dados do consumidor. **Anais do Salão de Iniciação Científica Tecnológica** ISSN-2358-8446, 2023. Disponível em: <https://www.phantomstudio.com.br/index.php/sic/article/view/2820>. Acesso em: 19 nov. 2025.

THEUHERZ, Nycolas Gava Baesso; SANTOS, Kaully Furiama. Crimes virtuais. **Revista Mato-grossense de Direito**, v. 1, n. 1, p. 146-160, 2023. Disponível em: <https://revistas.fasipe.com.br/index.php/REMAD/article/view/213>. Acesso em: 19 nov. 2025.

ZANIOLO, Pedro Augusto. Crimes Modernos: O impacto da tecnologia no direito. 4^a ed. Salvador: **JusPodvm**, 2021. Disponível em: <https://bibliotecadigital.stf.jus.br/xmlui/bitstream/handle/123456789/10133/in00001503448.pdf?sequence=1>. Acesso em: 19 nov. 2025.

**ANEXO A - COMPROVANTE DE SUBMISSÃO OU APROVAÇÃO DO ARTIGO NA
REVISTA ONDE CONSTE O NOME DE TODOS OS AUTORES DO TRABALHO**



Jordana Duarte <jordannaduartee@gmail.com>

[RDU] Agradecimento pela submissão

ALEXANDRE AUGUSTO BATISTA DE LIMA via Portal de Revistas <pen-
bounces@emnuvens.com.br>

sáb., 1 de nov.,
15:22

Responder para: ALEXANDRE AUGUSTO BATISTA DE LIMA <alexandre.lima@uninovafapi.edu.br>
Para: Jordana Duarte <jordannaduartee@gmail.com>

Jordana Duarte,

Agradecemos a submissão do trabalho "A CRIMINALIDADE DIGITAL E OS DESAFIOS CONTEMPORÂNEOS PARA O DIREITO PENAL NA ERA DA INTELIGÊNCIA ALGORÍTMICA" para a revista Revista de Direito UNINOVAFAPI. Acompanhe o progresso da sua submissão por meio da interface de administração do sistema, disponível em:

URL da submissão: <https://uninovafapi.emnuvens.com.br/revinterdireito/authorDashboard/submission/2293>

[Texto das mensagens anteriores oculto]