ISSN 2675-4398

Transições
Centro Universitário Barão de Mauá

https://doi.org/10.56344/2675-4398.v6n2a2025.6

Título
Crimes cibernéticos: a tipificação penal e os desafios na efetivação das medidas legais de combate

Autor
Vincenzo de Campos Agonilha Fayão
Alcides Belfort da Silva

Ano de publicação
2025

Referência
FAYÃO, Vincenzo de Campos Agonilha; SILVA, Alcides Belfort. Crimes cibernéticos: a tipificação penal e os desafios na efetivação das medidas legais de combate. **Transições**, Ribeirão Preto, v. 6, n. 2, 2025.

Recebimento: 29/05/2025
Aprovação: 04/07/2025

CRIMES CIBERNÉTICOS: A TIPIFICAÇÃO PENAL E OS DESAFIOS NA EFETIVAÇÃO DAS MEDIDAS LEGAIS DE COMBATE

CYBERCRIMES: CRIMINAL CLASSIFICATION AND THE CHALLENGES IN THE IMPLEMENTATION OF LEGAL MEASURES FOR COMBAT

Vicenzo de Campos Agonilha Fayão*
Alcides Belfort da Silva**

Resumo: O presente artigo, com base no método dedutivo e em ampla revisão bibliográfica e legislativa, analisa a tipificação penal dos crimes cibernéticos no ordenamento jurídico brasileiro, bem como os desafios estruturais, técnicos e jurídicos para a efetivação das medidas legais de combate. A partir da análise de diplomas como a Lei nº 12.737/2012, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a recente adesão à Convenção de Budapeste, evidencia-se a evolução normativa frente à criminalidade digital. Contudo, destaca-se que a sofisticação tecnológica dos ataques, aliada à vulnerabilidade de infraestruturas críticas, à dificuldade de obtenção de provas digitais e à natureza transnacional desses delitos, ainda compromete a eficácia da repressão penal. O trabalho também examina experiências internacionais e os esforços de cooperação jurídica global, ressaltando a necessidade de constante atualização normativa, investimentos em segurança cibernética e fortalecimento institucional. Conclui-se que o enfrentamento efetivo ao cibercrime exige uma ação coordenada entre legislação moderna, estrutura técnica adequada e colaboração internacional articulada.

Palavras-chave: Crimes Cibernéticos; Direito Penal; Cibersegurança; Cooperação Internacional; Tipificação Penal.

Abstract: This article, based on the deductive method and an extensive bibliographic and legislative review, examines the criminal classification of cybercrimes within the Brazilian legal system, as well as the structural,

* Graduando em Direito, pelo Centro Universitário Barão de Mauá de Ribeirão Preto. Contato: vicenzo511@gmail.com
** Doutor em Tecnologia Ambiental pela UNAERP, com estágio de pós-doutorado pela Univresidad del Museu Social Argentino (UMSA). Docente do Centro Universitário Barão de Mauá. Contato: belfortalcides@gmail.com

technical, and legal challenges involved in the effective enforcement of legal measures. Through the analysis of key legal instruments such as Law No. 12.737/2012, the Civil Rights Framework for the Internet, the General Data Protection Law, and Brazil's recent accession to the Budapest Convention, the study reveals the normative evolution in response to digital crime. However, the growing sophistication of attacks, the vulnerability of critical infrastructures, the complexity of digital evidence collection, and the transnational nature of cyber offenses continue to hinder the effectiveness of criminal prosecution. The paper also explores international experiences and global legal cooperation efforts, emphasizing the need for constant legislative updating, investments in cybersecurity, and institutional strengthening. It concludes that effective cybercrime control requires coordinated action among modern legislation, technical capacity, and international cooperation.

Keywords: Cybercrimes; Criminal Law; Cybersecurity; International Cooperation; Criminal Typification.

INTRODUÇÃO

O acelerado avanço das tecnologias digitais e a crescente digitalização das relações sociais, econômicas e políticas trouxeram inúmeros benefícios, mas também propiciaram o surgimento de novas modalidades de condutas ilícitas. Os **crimes cibernéticos** – ou cibercrimes – passaram a ocupar posição central nas preocupações das autoridades em todo o mundo, incluindo no Brasil.

Hoje, é possível praticar fraudes bancárias, roubos de dados pessoais, disseminação de notícias falsas (*fake news*), *ciberbullying*, ataques a infraestruturas críticas e diversas outras infrações sem sair de trás de um computador conectado à internet.

Esse fenômeno reflete-se nas estatísticas: somente em 2023 foram registrados quase 2 milhões de casos de estelionato no Brasil, um aumento de 8,2% em relação a 2022, dos quais pelo menos 12% ocorreram por meio eletrônico.Estimativas apontam que, entre julho de

2023 e julho de 2024, mais de 80 milhões de brasileiros foram vítimas de golpes virtuais, causando prejuízos na ordem de R$ 40 bilhões.

Diante desse cenário alarmante, cresce a urgência de adaptação do ordenamento jurídico para enfrentar a criminalidade no meio digital. Nas últimas décadas, o Brasil editou leis específicas e alterou dispositivos do Código Penal visando punir condutas ilícitas praticadas via meios informáticos.

Todavia, a eficácia dessas medidas legais nem sempre acompanha o ritmo das inovações tecnológicas e da audácia dos criminosos virtuais. As investigações esbarram em desafios técnicos e jurídicos, e lacunas legais tornam a tipificação e punição de certos delitos cibernéticos mais complexas do que nos crimes tradicionais.

Este artigo, analisa os crimes cibernéticos sob a perspectiva do ordenamento jurídico brasileiro, abordando sua conceituação e exemplos práticos, a legislação pertinente (Marco Civil da Internet, Lei Carolina Dieckmann, Lei Geral de Proteção de Dados, entre outras), os desafios encontrados pelas autoridades na investigação e repressão desses delitos, a necessidade de constante atualização das normas, e por fim apresenta sugestões para o fortalecimento das medidas legais e institucionais de combate a essa forma de criminalidade.

CRIMES CIBERNÉTICOS: CONCEITO E EXEMPLOS

A expressão, crime cibernético refere-se a toda atividade ilícita praticada no ambiente virtual, por meio da internet, de redes de computadores ou de dispositivos digitais conectados. Em outras palavras, são delitos cuja execução envolve diretamente recursos informáticos, seja como meio para atingir a vítima, seja tendo o próprio sistema computacional como alvo.

Esse conceito abrangente inclui tantos crimes estritamente digitais – por exemplo, invasão de sistemas, roubo de dados eletrônicos ou disseminação de vírus (*malware*) – quanto crimes tradicionais cometidos via internet, como estelionatos on-line (golpes financeiros) ou difamação em redes sociais.

Diversos exemplos práticos ilustram a amplitude dos cibercrimes. Entre os delitos contra o patrimônio, destacam-se as fraudes bancárias on-line, o furto de dados de cartões de crédito e as fraudes de pagamento eletrônico (como o golpe do Pix). No campo contra a pessoa, têm-se casos de *hacking* (invasão de dispositivos informáticos) para subtrair informações confidenciais, a espionagem digital e a divulgação não autorizada de conteúdos íntimos – prática conhecida como **"**revenge porn**"** (pornografia de vingança).

Há também crimes contra a honra e a dignidade, como o *cyberbullying* e o assédio on-line, além de ameaças e extorsões virtuais. Outros exemplos incluem ataques de ransomware (sequestro de dados mediante criptografia e pedido de resgate), phishing (roubo de credenciais através de páginas ou e-mails falsos) e até o terrorismo cibernético, em que sistemas de infraestrutura (energética, financeira, governamental) são atacados com intenção de causar danos em larga escala. Importante notar que muitas dessas condutas correspondem a versões digitais de crimes já existentes no "mundo real" (fraude, furto, calúnia, etc.), porém potencializadas pela rapidez, anonimato e alcance global proporcionados pela rede mundial de computadores.

Em função dessas particularidades, a legislação e a justiça criminal precisaram evoluir para adequar definições e prever punições adequadas a esses novos delitos digitais.

LEGISLAÇÃO BRASILEIRA PERTINENTE

O ordenamento jurídico brasileiro não conta com um código penal exclusivamente dedicado aos crimes cibernéticos; em vez disso, a abordagem tem sido a edição de leis específicas e a alteração pontual de leis vigentes para abarcar condutas informáticas ilícitas.

Destacam-se, nesse contexto, três marcos normativos de grande importância: o Marco Civil da Internet (Lei nº 12.965/2014), a chamada Lei Carolina Dieckmann (Lei nº 12.737/2012) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Cada qual, a seu modo, contribuiu para o enfrentamento dos cibercrimes, seja tipificando novas condutas como crime, seja estabelecendo direitos, deveres e mecanismos de responsabilização no contexto digital.

Lei nº 12.737/2012 – "Lei Carolina Dieckmann"

Um importante marco inicial na evolução da legislação penal digital no Brasil foi a Lei nº 12.737, de 30 de novembro de 2012, conhecida popularmente como Lei Carolina Dieckmann. Essa lei ganhou esse apelido em referência a um caso envolvendo a atriz Carolina Dieckmann, que teve fotos pessoais roubadas de seu computador invadido e divulgadas na internet sem autorização, fato que evidenciou a ausência de tipificação específica para invasões de dispositivos na época.

A Lei 12.737/2012 veio suprir tal lacuna ao introduzir o artigo 154-A no Código Penal, tipificando expressamente o crime de invasão de dispositivo informático.

Conforme o art. 154-A do CP, passou a ser crime invadir, sem autorização do titular, computador, tablet, celular ou outro dispositivo informático alheio, conectado ou não à internet, com o objetivo de

obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades para obter vantagem ilícita.

A pena inicialmente prevista era relativamente branda: detenção de 3 meses a 1 ano e multa, aumentada para até 2 anos se da invasão resultasse a obtenção de conteúdo privado (como segredos industriais ou informações sigilosas). Além do 154-A, a lei também criou o art. 154-B (que pune quem produz, oferece ou vende programas de computador destinados à invasão de dispositivos alheios) e fez pequenos ajustes em artigos existentes.

A Lei Carolina Dieckmann representou um passo importante na adaptação do direito penal à realidade digital brasileira, ao criminalizar condutas comuns de hackers até então não abrangidas claramente pela legislação. Entretanto, doutrinadores e juristas logo apontaram limitações na nova lei – por exemplo, penas consideradas baixas para a gravidade de algumas invasões e dificuldades na aplicação prática diante da sofisticação dos ataques cibernéticos (tanto que, em 2021, reformas posteriores vieram endurecer essas punições, como será adiante mencionado).

Ainda assim, a Lei 12.737/2012 inaugurou formalmente a categoria de "delitos informáticos" no Código Penal brasileiro, servindo de base para legislações subsequentes.

Marco Civil Da Internet (Lei Nº 12.965/2014)

Outro marco jurídico relevante é a Lei nº 12.965, de 23 de abril de 2014, apelidada de Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diferentemente da Lei 12.737/2012, o Marco Civil não é uma lei penal, mas sim uma lei de caráter civil-regulatório que delineia diretrizes gerais

sobre o ambiente on-line. Ainda assim, ele possui reflexos importantes na prevenção e responsabilização de ilícitos cibernéticos.

O Marco Civil da Internet consagra princípios como a neutralidade da rede, a liberdade de expressão, a privacidade e a proteção de dados pessoais na internet. Em termos de combate a abusos, um de seus pontos centrais é delinear a responsabilidade dos provedores de conexão e de aplicações pela veiculação de conteúdos de terceiros.

A lei adotou, por exemplo, um mecanismo de *notice and takedown* moderado: provedores de aplicações de internet (como sites e redes sociais) só poderão ser responsabilizados civilmente por conteúdos ilícitos de terceiros se, após ordem judicial específica, não tomarem as providências para remover o material.

Essa previsão incentiva a remoção diligente de conteúdos criminosos (como apologia a crimes, discursos de ódio, pornografia infantil, etc.) mediante acionamento da Justiça, funcionando como instrumento coadjuvante no combate a certos cibercrimes.

Além disso, o Marco Civil determinou a guarda de registros de conexão e acesso a aplicações por parte de provedores, sob sigilo, pelo prazo legal, o que auxilia investigações policiais ao permitir a identificação de usuários mediante ordem judicial.

Estabeleceu também direitos dos usuários quanto à inviolabilidade de suas comunicações on-line, impondo limites à entrega de dados a autoridades, sempre exigindo devido processo legal. Em suma, embora não tipifique crimes novos, o Marco Civil da Internet criou um arcabouço jurídico para o ambiente virtual brasileiro, equilibrando liberdade e responsabilidade.

Ele serve como parâmetro interpretativo inclusive na área penal, ao definir balizas sobre o que se espera de comportamentos na internet e ao oferecer ferramentas para coletar provas e imputar responsabilidade em casos de ilícitos digitais.

Lei Geral De Proteção De Dados (Lei Nº 13.709/2018 – LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, consiste em outra peça legislativa fundamental no contexto digital brasileiro. Inspirada em legislações estrangeiras como o GDPR europeu, a LGPD foi uma resposta direta ao aumento de incidentes envolvendo uso indevido e vazamento de dados pessoais no meio eletrônico.

Embora a LGPD não seja uma lei penal, ela estabelece diretrizes abrangentes sobre como empresas e entidades devem coletar, armazenar, tratar e compartilhar dados pessoais, criando mecanismos de responsabilização administrativa e civil em caso de violações.

No âmbito de prevenção e combate a crimes cibernéticos, a LGPD traz impactos importantes. Primeiro, ao impor padrões de segurança da informação e obrigação de reporte de incidentes de segurança (como vazamentos) à Autoridade Nacional de Proteção de Dados (ANPD), a lei estimula a melhoria das práticas de segurança digital nas organizações, dificultando assim a ação de cibercriminosos que buscam explorar dados sensíveis.

Segundo, ao prever sanções administrativas severas (multas que podem chegar a 2% do faturamento, bloqueio de dados, etc.), a LGPD funciona como um desestímulo à negligência com informações pessoais – muitas vezes alvo de ataques cibernéticos. Além disso, a existência de direitos assegurados aos titulares de dados (como acesso, exclusão, etc.) e a maior transparência forçada pela lei podem ajudar vítimas de crimes cibernéticos a identificar e provar usos indevidos de seus dados, subsidiando eventuais ações penais ou civis contra os responsáveis.

É importante destacar que a LGPD alterou o Marco Civil da Internet em alguns pontos e complementa a legislação penal: embora não tipifique novos crimes, casos graves de violação de dados pessoais

envolvendo dolo ou finalidade econômica podem ser enquadrados em delitos já existentes, como extorsão, estelionato, ou mesmo na própria invasão de dispositivo informático quando esta ocorrer para obter dados pessoais alheios.

Assim, a LGPD integra o rol de medidas legais que, ainda que indiretamente, fortalecem o combate aos crimes cibernéticos, na medida em que protegem um dos ativos mais visados na era digital – os dados – e estabelecem um ambiente de maior responsabilização pelo seu uso.

Outras Atualizações Legislativas Recentes

A legislação brasileira vem passando por atualizações constantes para acompanhar a evolução dos delitos informáticos. Um exemplo significativo é a Lei nº 14.155, de 27 de maio de 2021, que endureceu as penas e criou novas figuras típicas no Código Penal relacionadas a crimes cibernéticos. Essa lei alterou o art. 154-A do CP (invasão de dispositivo informático), aumentando sua pena básica de detenção (3 meses a 1 ano) para reclusão de 1 a 4 anos, além de ampliar as causas de aumento de pena para esse delito.

Também introduziu disposições específicas para crimes patrimoniais praticados por meios eletrônicos: por exemplo, incluiu o §4º-B no art. 155 do CP, prevendo como furto qualificado (pena de 4 a 8 anos de reclusão) a subtração de valores mediante fraude cometida via dispositivo eletrônico ou informático – caso típico de invasão de conta bancária on-line para desviar dinheiro.

Adicionalmente, a Lei 14.155/2021 criou causas de aumento de pena para esses furtos eletrônicos quando praticados por meio de servidor estrangeiro ou contra vítimas vulneráveis (idosos, por exemplo), e também agravou a punição do estelionato eletrônico, inserindo o §2º-A

no art. 171 do CP para casos de fraude digital (como golpes pela internet) e prevendo aumento de pena se cometidos contra idosos ou por meio de servidor fora do país.

Essas modificações recentes demonstram a preocupação do legislador em manter a legislação atualizada frente às novas modalidades de golpes virtuais, tornando mais efetiva a resposta penal.

Por fim, no campo da cooperação internacional, merece menção o Decreto nº 11.491/2023, pelo qual o Brasil promulgou a Convenção de Budapeste sobre o Crime Cibernético – tratado internacional desenvolvido no âmbito do Conselho da Europa. Com a adesão brasileira a esse instrumento multilateral, espera-se aprofundar a cooperação jurídica internacional para investigação e obtenção de provas eletrônicas em casos transnacionais, de forma mais ágil e eficaz.

Essa iniciativa reflete o reconhecimento de que o enfrentamento aos cibercrimes extrapola as fronteiras nacionais e requer harmonização legislativa e parceria com autoridades estrangeiras.

DESAFIOS NA INVESTIGAÇÃO E PUNIÇÃO DOS CRIMES CIBERNÉTICOS

Apesar do arcabouço legal em constante construção, diversos desafios dificultam a efetiva investigação, tipificação e punição dos crimes cibernéticos pelas autoridades brasileiras. Um dos principais entraves é a natureza transnacional e anônima da maioria dessas condutas. Diferentemente dos crimes comuns, os delitos digitais podem ser praticados por agentes localizados em qualquer parte do mundo, vitimando pessoas ou organizações no Brasil sem que o autor jamais pise em território nacional.

A internet confere aos criminosos uma camada de anonimato – através de redes privadas virtuais (VPNs), *dark web*, criptografia de comunicações, perfis falsos etc. – que torna extremamente difícil

identificá-los e atribuir-lhes responsabilidade. Como ressalta Beatriz Borges, "*o anonimato e a consequente dificuldade de identificação dos criminosos, características inerentes aos crimes cibernéticos, dificultam a aplicação das normas tradicionais do direito penal*", especialmente quando a conduta ilícita ocorre simultaneamente em múltiplas jurisdições de forma muito rápida.

Ou seja, os marcos territoriais que orientam a atuação policial e judiciária tornam-se nebulosos no ciberespaço: um crime pode iniciar-se em um país, ter efeitos em outro e utilizar infraestrutura de servidores em diversos outros, demandando uma coordenação internacional complexa para sua apuração.

A questão da jurisdição e cooperação internacional é, portanto, um desafio de primeira ordem. Crimes cibernéticos envolvendo autores estrangeiros contra vítimas brasileiras exigem mecanismos legais de auxílio mútuo entre países, tratados de extradição, cartas rogatórias e outros instrumentos que muitas vezes são lentos e burocráticos.

Mesmo com a adesão à Convenção de Budapeste e outros acordos, a articulação entre diferentes ordens jurídicas nem sempre acontece no tempo necessário para uma investigação ágil. Enquanto isso, os criminosos podem ocultar evidências em serviços de nuvem no exterior ou se valer de legislações mais permissivas de proteção de dados para se esquivar da lei.

Outro obstáculo está na prova e na perícia digital. Coletar evidências eletrônicas confiáveis exige equipamentos adequados e pessoal altamente especializado em computação forense. Muitas vezes, é preciso quebrar criptografias fortes, rastrear endereços de IP que podem ter sido mascarados ou múltipla e rapidamente reencaminhados (*spoofing*), recuperar dados apagados e estabelecer a autoria de ações realizadas em ambientes virtuais compartilhados.

A volatilidade das provas digitais (que podem ser deletadas ou alteradas remotamente em instantes) impõe às autoridades a necessidade de rapidez e de procedimentos técnicos rigorosos para garantir a cadeia de custódia e a validade jurídica desses vestígios. No Brasil, embora existam núcleos de perícia cibernética nas polícias (especialmente na Polícia Federal e em alguns estados), ainda há deficiências de recursos e de capacitação.

Há um volume crescente de casos que dependem de análise de computadores, celulares e tráfego de internet, gerando filas e atrasos que podem comprometer investigações. Além disso, a cooperação de empresas provedoras de serviços de internet é fundamental para obtenção de dados (como registros de acesso, conteúdos de comunicações, dados de usuários), mas essa cooperação enfrenta limites legais (devido à privacidade e à necessidade de ordens judiciais) e práticos (empresas sediadas fora do país, diferença de fuso horário, barreiras linguísticas, etc.).

No que tange à tipificação penal em si, ainda há lacunas e interpretações controversas. Mesmo após as leis específicas já mencionadas, a legislação nem sempre consegue abranger toda a gama de condutas lesivas que surgem com as inovações tecnológicas.

Por vezes, autoridades precisam recorrer à analogia ou enquadrar um ato novo em um tipo penal preexistente semelhante, o que pode gerar debates jurídicos. Por exemplo, antes de 2012, uma invasão de sistema para roubar dados poderia ser tratada como furto, violação de segredo ou mesmo *delito atípico* por ausência de previsão clara.

Hoje ainda há discussões: *stalking* on-line, criação e disseminação de *fake news* com fim de prejudicar eleições, ataques de *DDoS* (negação de serviço) – todas essas práticas nem sempre se encaixam perfeitamente nas figuras penais vigentes. Essa dificuldade de tipificação pode levar à impunidade ou a punições menos adequadas.

Soma-se a isso o fato de que a legislação geralmente reage atrasada às novidades: entre o surgimento de uma nova modalidade de golpe digital e a aprovação de uma lei específica, os criminosos já exploraram por anos a brecha legal.

A gravidade das sanções penais aplicáveis também impacta a efetividade do combate. Penas muito baixas reduzem o efeito dissuasório da lei e dificultam a aplicação de medidas cautelares e prisões preventivas durante o processo. Nesse sentido, a alteração promovida em 2021 (Lei 14.155) buscou corrigir um problema: sob a lei de 2012, invadir um dispositivo para subtrair dados sigilosos era punido com detenção máxima de 1 ano (pena que frequentemente resultava em transação penal ou suspensão condicional do processo, por tratar-se de menor potencial ofensivo); agora, com pena de até 4 anos de reclusão, o crime ganhou status mais grave, permitindo resposta mais enérgica.

No entanto, ainda há crimes cibernéticos cuja punição é considerada branda ou cujas consequências legais não parecem proporcionalmente rígidas dado o dano que causam – por exemplo, casos de vazamento massivo de dados pessoais não estão tipificados como crime específico e podem, quando muito, ser enquadrados em delitos genéricos com penas baixas, como infração a sigilo ou omissão de responsável (se houver negligência).

Por fim, há os desafios institucionais e culturais. As autoridades tradicionais (polícias, Ministério Público, Judiciário) precisam constantemente se atualizar em relação às técnicas de investigação digital e às nuances da prova eletrônica. Nem todos os operadores do Direito estão familiarizados com conceitos técnicos de TI, o que pode dificultar desde a fase de inquérito (como elaborar pedidos de quebra de dados eficazes) até o julgamento (como valorar uma perícia digital, ou compreender a dinâmica de um ataque cibernético).

A necessidade de capacitação especializada é premente. Iniciativas de treinamento e criação de delegacias especializadas em crimes cibernéticos ainda apresentam cobertura desigual pelo país. Além disso, a resposta estatal costuma ser mais lenta que a agilidade dos criminosos virtuais.

Essa disparidade gera sensação de impunidade: não raramente, quadrilhas virtuais se sentem fora do alcance da polícia e da Justiça, continuando a lesar milhares de pessoas antes que alguma ação efetiva as interrompa.

A cada hora, estima-se que cerca de 4,6 mil brasileiros sejam alvo de tentativas de golpes financeiros via mensagens ou ligações, e outros milhares efetivamente caem em fraudes on-line – um volume que sobrecarrega as estruturas de segurança pública e judiciária.

Esse cenário reforça a importância de aprimorar tanto as leis quanto as estratégias institucionais de combate, sob pena de o cibercrime consolidar-se como uma prática de alto lucro e baixo risco para os perpetradores.

NECESSIDADE DE ATUALIZAÇÃO CONSTANTE DA LEGISLAÇÃO

A natureza dinâmica do mundo digital impõe ao legislador o desafio de manter as normas sempre atualizadas diante de novas tecnologias e táticas criminosas. Inovações como inteligência artificial, Internet das Coisas (IoT), criptomoedas e redes 5G trazem consigo oportunidades de desenvolvimento, mas também ampliam a superfície de exposição a delitos inéditos ou variantes sofisticadas de crimes já conhecidos.

Assim, a legislação de combate aos cibercrimes não pode estagnar – deve ser flexível e evolutiva, passando por revisões e acréscimos constantes para cobrir brechas legais emergentes.

No Brasil, verifica-se que muitas mudanças legais ocorrem de forma reativa, após a divulgação de casos de grande repercussão que expõem fragilidades nas leis vigentes.

Exemplos disso foram a edição da Lei Carolina Dieckmann em 2012 após o incidente com a atriz, e as alterações de 2021 após o boom de golpes eletrônicos durante a pandemia de COVID-19, quando estelionatos virtuais e invasões de contas se tornaram epidêmicos.

Porém, idealmente, a atualização legislativa deve antever tendências tecnológicas. Nos últimos anos, o Congresso Nacional tem debatido projetos como a regulamentação da inteligência artificial, justamente com o intuito de prevenir usos abusivos dessa ferramenta – por exemplo, *deepfakes* usados para extorsão ou golpes, ou algoritmos que possam ameaçar direitos fundamentais.

Em 2023, o Senado aprovou um projeto de lei para estabelecer um marco legal da IA, incorporando diversos dispositivos de propostas em tramitação.

Embora essa lei ainda esteja pendente de aprovação final, ela ilustra um esforço de atualizar o ordenamento antes que determinados usos de IA gerem problemas incontroláveis.

Outra frente de constante atenção é a proteção de dados e privacidad**e**. A LGPD de 2018 foi um passo fundamental, mas já se discute a necessidade de aperfeiçoar pontos da lei diante de novas ameaças, bem como a criação de tipos penais específicos para condutas maliciosas envolvendo dados (por exemplo, comércio ilegal de grandes volumes de dados pessoais obtidos em vazamentos).

Da mesma forma, a expansão das criptomoedas e ativos virtuais trouxe desafios relacionados a lavagem de dinheiro e golpes financeiros (como esquemas de pirâmide com bitcoins), levando à edição recente da Lei nº 14.478/2022 (Marco Legal dos Criptoativos) e exigindo

possivelmente novas tipificações penais para fraudes envolvendo moedas virtuais.

No âmbito internacional, a atualização contínua também significa harmonizar a legislação doméstica com padrões globais. A adesão do Brasil à Convenção de Budapeste em 2023, já mencionada, é um marco nesse sentido, pois implica o compromisso de manter nossa legislação e procedimentos alinhados às melhores práticas internacionais no combate ao cibercrime.

Além disso, participam-se das discussões em fóruns multilaterais, como a ONU, para a elaboração de uma possível convenção global de cibercrimes, garantindo que o país não fique isolado nas soluções jurídicas adotadas.

Por fim, é válido ressaltar que a atualização legislativa deve vir acompanhada de melhoria institucional. Muitas vezes, não basta editar uma nova lei: é preciso regulamentá-la, difundir seu conteúdo entre os operadores e dotar as instituições dos meios para aplicá-la.

Leis mais modernas que prevejam, por exemplo, técnicas especiais de investigação (como agentes infiltrados em fóruns da *dark web*, ou acesso remoto a computadores de criminosos sob autorização judicial) só terão efeito prático se houver órgãos preparados para utilizá-las e orçamento destinado a essas operações. Assim, a evolução normativa deve ser pensada em conjunto com políticas públicas de aparelhamento das forças de segurança e do sistema de Justiça.

Em suma, legislar sobre crimes cibernéticos é um processo contínuo, que deve acompanhar o rápido ciclo de inovação tecnológica. Novos riscos exigirão novos remédios jurídicos. A falta de atualização legal pode transformar o ordenamento em ferramenta obsoleta diante de modalidades sofisticadas de ataque digital.

O Estado brasileiro, portanto, necessita permanecer vigilante e proativo, revisitando periodicamente seu aparato normativo e adotando uma postura preventiva, e não apenas reativa, frente ao cibercrime.

AVANÇOS TECNOLÓGICOS E DESAFIOS TÉCNICOS NO CIBERCRIME

A rápida evolução tecnológica tem fornecido aos cibercriminosos novas ferramentas e métodos, muitas vezes antes que as autoridades consigam se adaptar. Inovações como a inteligência artificial (IA), a Internet das Coisas (IoT) e as criptomoedas ampliaram o alcance e a sofisticação dos delitos digitais. Criminosos virtuais vêm empregando técnicas avançadas – desde deepfakes (vídeos ou áudios falsificados por IA que simulam pessoas reais) usados para fraudes e extorsões, até malwares complexos que exploram vulnerabilidades em sistemas conectados.

Da mesma forma, o uso disseminado de criptoativos facilita atividades ilícitas como lavagem de dinheiro e extorsão via ransomware, pois transações em moedas digitais oferecem alto grau de anonimato e descentralização, dificultando o rastreio pelos órgãos de segurança.

Adicionalmente, quadrilhas especializadas aplicam engenharia social hiperpersonalizada – muitas vezes com auxílio de IA – para enganar vítimas em golpes on-line, criando páginas falsas e esquemas sob medida que burlam camadas tradicionais de segurança.

Esses exemplos ilustram como a tecnologia, ao mesmo tempo em que impulsiona a economia digital, é desviada para potencializar condutas criminosas de forma inédita.

Do ponto de vista das autoridades, esses avanços técnicos impõem desafios consideráveis na investigação e persecução penal. Ferramentas de anonimização e criptografia robustas permitem que

ofensores escondam sua identidade e atividade on-line, tornando difícil atribuir autoria aos crimes.

Como ressaltam especialistas, o anonimato inerente ao ambiente virtual e a possibilidade de um delito ocorrer simultaneamente em múltiplas jurisdições "dificultam a aplicação das normas tradicionais do direito penal".

Hackers podem operar de qualquer lugar do mundo, utilizando redes privadas virtuais (VPNs), navegadores anônimos (como Tor) e comunicações cifradas de ponta a ponta, o que complica a obtenção de provas eletrônicas e a identificação dos responsáveis.

Além disso, a velocidade com que ataques digitais ocorrem – muitas vezes automatizados por bots ou scripts maliciosos – exige uma capacidade de resposta imediata das equipes de segurança, sob pena de evidências voláteis serem perdidas em instantes.

Para enfrentar esse cenário, é necessária uma constante atualização técnica por parte do Estado. As forças de segurança precisam incorporar ferramentas de ponta em cibersegurança e investigações digitais, tais como sistemas de monitoração de tráfego anômalo, análise de big data e técnicas de computação forense avançada para decodificar malware, quebrar criptografias ou rastrear transações em blockchain.

No Brasil, começa-se a reconhecer essa necessidade: propõe-se a criação de laboratórios forenses digitais aparelhados para a investigação e produção de provas eletrônicas, bem como programas de capacitação especializada para delegados, peritos e agentes atuarem eficientemente no ambiente cibernético.

Tais medidas técnicas – aliadas ao intercâmbio de informações com o setor privado, que frequentemente detém expertise em cibersegurança – são essenciais para reduzir a defasagem entre a

criatividade dos criminosos virtuais e a capacidade do poder público em reagir.

Contudo, esse é um esforço contínuo e de largo espectro: exige investimentos permanentes em atualização tecnológica, recursos humanos altamente qualificados e protocolos ágeis de atuação, de modo que a lei e a tecnologia caminhem juntas no combate ao cibercrime.

SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

Entre as facetas mais sensíveis da criminalidade digital estão os ataques contra sistemas de informática de infraestruturas críticas – aqueles que sustentam serviços essenciais como justiça, energia, comunicações, finanças e saúde.

Nos últimos anos, incidentes desse tipo evidenciaram o enorme potencial de dano social e econômico causado por brechas de segurança nesses ambientes.

Um caso emblemático foi o ataque de ransomware sofrido pelo Superior Tribunal de Justiça (STJ) em novembro de 2020, no qual hackers invadiram a rede do tribunal e criptografaram todo o acervo de processos, bloqueando o acesso a dados judiciais vitais.

O STJ teve de suspender serviços por dias, até conseguir restaurar os sistemas via backup, em um episódio sem precedentes na história do judiciário brasileiro – considerado "um dos mais graves já efetuados contra uma instituição de Estado" no país.

Poucos meses depois, em 2021, um ataque similar atingiu o Tribunal de Justiça do Rio Grande do Sul, comprometendo cerca de 12 mil computadores e paralisando diversas operações.

Esses eventos expõem fragilidades importantes na proteção de dados governamentais e demonstram que nenhum órgão está imune: se

até Cortes Supremas enfrentam invasões, infraestruturas críticas de outras áreas também estão sob risco constante.

No setor privado e em utilities, o cenário não é menos preocupante. Ataques cibernéticos a operadoras de energia, telecomunicações, transporte e outras redes vitais têm se multiplicado globalmente – muitas vezes perpetrados por grupos financiados pelo crime organizado ou até com possíveis motivações geopolíticas.

Um relatório do Centro de Tratamento e Resposta a Incidentes Cibernéticos Gov destaca que casos internacionais recentes, como o ataque à Colonial Pipeline (oleoduto nos EUA) em 2021, expuseram a baixa maturidade de certas empresas em lidar com ameaças digitais nas operações industriais.

Mesmo no Brasil, onde tradicionalmente adotava-se o isolamento físico ("air gap") de redes industriais como principal forma de proteção, a crescente conexão dessas redes à internet aumenta a superfície de ataque disponível.

Estatísticas de segurança indicam que a maioria esmagadora das organizações com sistemas de controle industrial já sofreram incidentes: segundo dados da empresa Fortinet, 9 em cada 10 empresas com ambiente de Tecnologia Operacional tiveram algum tipo de incidente cibernético apenas no ano de 2021.

Esses números refletem a sofisticação crescente dos ataques – incluindo ransomwares direcionados, sabotagens e espionagem industrial – e a urgência de fortalecer a cibersegurança nessas infraestruturas.

A proteção efetiva das infraestruturas críticas demanda uma abordagem integrada de tecnologia, processos e legislação.

Do ponto de vista técnico, é imperativo adotar medidas robustas de segurança: segmentação de redes, monitoramento em tempo real

de intrusões, redundância de dados, backups offline e planos de resposta a incidentes bem estruturados.

Empresas e órgãos públicos que operam serviços essenciais precisam implementar padrões rigorosos (por exemplo, conformidade com a Lei de Segurança de Informações Críticas caso exista, ou boas práticas como as normas ISO/IEC 27001 e 27002) e investir em atualizações constantes de seus sistemas legados.

Sob o prisma legal, o ordenamento brasileiro vem buscando acompanhar essas necessidades – seja prevendo agravantes penais para crimes cibernéticos que afetem sistemas de utilidade pública (como feito pela Lei 14.155/2021, que qualificou furtos praticados mediante invasão eletrônica a sistemas bancários), seja elaborando estratégias nacionais de cibersegurança. Em 2020, o governo federal lançou a Estratégia Nacional de Segurança Cibernética (E-Ciber), e mais recentemente discute-se no Congresso a criação de uma Agência Nacional de Segurança Cibernética dedicada a coordenar a defesa dessas infraestruturas.

Tais iniciativas, aliadas à cooperação com o setor privado (por exemplo, empresas de TI auxiliando investigações, como a Microsoft fez no caso do ataque ao STJ são caminhos para aumentar a resiliência do país.

Em suma, assegurar a inviolabilidade de sistemas críticos na era digital tornou-se questão de segurança nacional, exigindo a conjugação de avanços técnicos, gestão de risco e aprimoramento legal contínuo.

PANORAMA INTERNACIONAL E COMPARATIVO LEGAL

O enfrentamento aos crimes cibernéticos não é um desafio exclusivo do Brasil – pelo contrário, trata-se de uma preocupação global

que tem levado diversos países a reformular suas legislações e políticas de segurança digital.

Historicamente, algumas nações saíram na frente na tipificação de delitos informáticos. Os Estados Unidos, por exemplo, já em 1986 editaram uma lei federal específica para crimes de computador, o Computer Fraud and Abuse Act (CFAA), que criminaliza acessos não autorizados a sistemas computacionais e outras atividades de hacking, prevendo sanções penais severas para tais condutas.

Desde então, a CFAA foi emendada repetidas vezes para acompanhar novas modalidades de fraude eletrônica, demonstrando uma postura proativa na atualização legal.

De modo semelhante, países europeus vêm adaptando seus ordenamentos desde o início dos anos 2000, muitos seguindo as diretrizes da Convenção de Budapeste sobre Cibercrime – tratado internacional pioneiro (de 2001) que serviu de base para harmonizar as definições de delitos cibernéticos e orientar a cooperação jurídica entre dezenas de nações. Membros da União Europeia, em especial, incorporaram as disposições da Convenção e de diretivas comunitárias correlatas, criando leis nacionais que cobrem ilícitos como intrusão em sistemas, interferência em dados, fraudes on-line, pornografia infantil e outros crimes cometidos via internet de forma relativamente padronizada entre si.

Isso significa que um ataque digital que ocorreria na França, na Alemanha ou em Portugal tende a estar sujeito a tipos penais equivalentes, facilitando ações coordenadas. Mesmo com pontos em comum, diferenças legislativas e institucionais persistem no plano comparado.

Alguns países adotam penas mais rígidas ou enquadramentos específicos dependendo da gravidade do ataque ou do bem jurídico lesado. No Reino Unido, por exemplo, a legislação de crimes de

computação (Computer Misuse Act) foi alterada em 2015 para elevar a até prisão perpétua a punição de ataques que causem danos muito graves à infraestrutura nacional (como apagões ou riscos de morte) – uma resposta a temores de terrorismo cibernético. Já nos EUA, além da CFAA, há uma miríade de leis complementares abordando desde fraude de identidade até espionagem digital, e casos de crimes cibernéticos de alto impacto frequentemente resultam em condenações exemplares.

Em contraste, países com recursos limitados ou estrutura investigativa incipiente enfrentam maior dificuldade em atualizar suas leis e combater efetivamente esses crimes, o que acaba os tornando territórios atraentes para hackers internacionais. Por isso, organismos multilaterais têm enfatizado a necessidade de elevação do padrão normativo em escala global.

A recém-aprovada Convenção da ONU sobre Crimes Cibernéticos (2024) vai nessa direção: além de criar novos mecanismos de auxílio mútuo, deverá servir "como base normativa aos países que não têm legislação nacional" robusta sobre o tema, estimulando que Estados menos adiantados implementem leis modernas. Em outras palavras, busca-se evitar "brechas geográficas" – isto é, nações onde criminosos se refugiam devido à legislação obsoleta ou pouco aplicada.

Outro aspecto relevante na comparação internacional são as estruturas dedicadas ao combate do cibercrime. Na União Europeia, foi estabelecido em 2013 o European Cybercrime Centre (EC3) no âmbito da Europol, com a função de centralizar expertise e apoiar investigações transnacionais de delitos informáticos.

A existência de unidades especializadas como o EC3, o FBI Cyber Division nos EUA, ou forças-tarefa nacionais (a exemplo da Divisão de Crimes Cibernéticos da Polícia Federal brasileira) evidencia um consenso: tão importante quanto a lei em si é ter instituições preparadas e integradas internacionalmente.

Nota-se que Brasil, EUA, UE e diversos outros já convergem na adoção de estratégias nacionais de cibersegurança e planos de proteção de infraestruturas críticas, compartilhando informações sobre ameaças emergentes.

Assim, do ponto de vista comparativo, o Brasil está alinhado a uma tendência global de aprimorar o arcabouço legal e estrutural contra crimes cibernéticos – embora com o desafio adicional de acelerar a implementação dessas medidas para equiparar-se aos países mais avançados no tema.

COOPERAÇÃO INTERNACIONAL NO COMBATE AO CIBERCRIME

Dada a natureza transnacional da maioria dos delitos cibernéticos, a cooperação internacional desponta como pilar indispensável para uma repressão eficaz. Nenhum país, isoladamente, consegue investigar e punir todas as infrações digitais que frequentemente atravessam fronteiras físicas em segundos.

Por isso, o Brasil tem buscado inserir-se nos principais acordos multilaterais e estreitar laços bilaterais visando aprimorar o intercâmbio de informações e a assistência jurídica mútua.

A adesão brasileira à Convenção de Budapeste em 2023 foi um passo fundamental nesse sentido: ao tornar-se parte do tratado, o país passou a contar com "mais um recurso nas investigações de crimes cibernéticos" – um canal formal que promete cooperação "mais intensa, rápida e eficaz" na obtenção de provas eletrônicas armazenadas no exterior.

Autoridades do Ministério da Justiça estimam que a implementação plena da Convenção permitirá não só agilizar pedidos de dados a provedores estrangeiros, como também modernizar normativas internas relacionadas à coleta e preservação de evidências

digitais, equilibrando a persecução penal com a proteção de dados pessoais.

Essa expectativa já começa a se concretizar: desde a promulgação do tratado, houve aumento no número de pedidos de cooperação jurídica internacional expedidos pelo Brasil, reforçando investigações que dependiam de informações hospedadas fora do país. Em paralelo, o Brasil tem participado ativamente da construção de um novo regime global de combate ao cibercrime no âmbito da Organização das Nações Unidas.

Em agosto de 2024, o Comitê de Cibercrime da ONU aprovou o texto de uma convenção internacional inédita contra crimes cibernéticos, do qual o Brasil foi vice-presidente negociador.

Essa convenção – que segue para apreciação final da Assembleia Geral da ONU – amplia os instrumentos de cooperação, prevendo um canal global célere e seguro para tramitação de pedidos de assistência entre países, além de medidas coordenadas para crimes como fraude digital, ataques a sistemas e abuso sexual infantil on-line.

Como destacou o Secretário Nacional de Justiça, Jean Uema, na ocasião, "o cibercrime ultrapassa as fronteiras geográficas dos países e essa convenção vai contribuir para a colaboração entre os países no seu enfrentamento".

Ou seja, há um reconhecimento uníssono de que "se o crime se tornou transnacional e organizado, precisamos de uma resposta internacional e unida para combatê-lo com sucesso", nas palavras do Ministro da Justiça Ricardo Lewandowski.

A cooperação não se limita aos aspectos formais: forças-tarefa conjuntas, intercâmbio de agentes de inteligência e operações coordenadas via Interpol e outras agências têm desmantelado algumas das maiores redes criminosas cibernéticas. Um exemplo emblemático foi a Operação Emotet (2021), em que autoridades de diversos países, sob

coordenação da Europol, derrubaram a maior botnet de malware bancário do mundo.

Essa ação só foi possível graças ao compartilhamento ágil de informações e ao esforço combinado de unidades policiais de vários continentes – ilustrando na prática como a colaboração internacional pode alcançar criminosos que atuam globalmente.

Por fim, vale mencionar que a cooperação internacional no ciberespaço também engloba parcerias público-privadas em escala global. Empresas de tecnologia sediadas em diferentes países frequentemente auxiliam investigações fornecendo dados técnicos ou soluções para decifrar mecanismos usados por hackers.

A troca de conhecimentos sobre novas ameaças e vulnerabilidades – seja em conferências internacionais, seja em plataformas de alerta mantidas por coalizões de países – tem se mostrado crucial para antecipar ataques.

O Brasil, ao lado de nações aliadas, tem participado desses esforços multilaterais, enviando peritos para capacitações no exterior e firmando acordos como o celebrado em 2025 entre a Polícia Federal e a Europol, que estabelece bases para investigações conjuntas e intercâmbio de dados de inteligência

Em suma, no combate ao crime cibernético a máxima "unidos venceremos" aplica-se de forma categórica: somente através de uma ampla aliança internacional – envolvendo Estados, organismos multilaterais e o setor privado global – é possível reduzir a sensação de impunidade no ciberespaço e levar os criminosos diante da justiça, independentemente de onde operem.

CONSIDERAÇÕES FINAIS

Na sociedade contemporânea, os crimes cibernéticos despontam como uma das maiores ameaças à segurança jurídica, à ordem pública e à efetividade do Direito Penal.

O Brasil tem realizado avanços relevantes nesse campo ao promulgar leis fundamentais como o Marco Civil da Internet, a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei Geral de Proteção de Dados Pessoais (LGPD), além de promover alterações importantes no Código Penal, como a Lei nº 14.155/2021.

Tais medidas foram essenciais para consolidar a tipificação penal de condutas ilícitas digitais e permitir alguma responsabilização dos agentes ofensores. No entanto, a existência de normas legais, por si só, não é suficiente.

Persistem desafios significativos que envolvem aspectos técnicos, institucionais, jurídicos e até mesmo internacionais.

Conforme analisado neste trabalho, o avanço tecnológico acelerado tem sido acompanhado por métodos criminosos cada vez mais sofisticados.

O uso de inteligência artificial, criptografia, dark web, engenharia social e criptoativos representa um novo arsenal à disposição de cibercriminosos, ampliando a complexidade das investigações e demandando do Estado uma resposta igualmente avançada.

A criação de laboratórios forenses digitais, a capacitação de peritos em computação forense e a integração com o setor privado são passos cruciais para mitigar a defasagem tecnológica e fortalecer a produção de provas digitais válidas.

Além disso, a proteção das infraestruturas críticas – como sistemas judiciais, bancos de dados públicos, redes de energia e telecomunicações – revela-se imperiosa, visto que ataques como os que

paralisaram o STJ e o TJ-RS demonstram o impacto potencial dessas investidas.

A adoção de protocolos de segurança cibernética robustos, aliados à regulamentação mais rigorosa e a estratégias nacionais coordenadas (como a E-Ciber), deve ser prioridade para garantir a continuidade dos serviços essenciais e preservar a soberania digital do país.

No plano internacional, o Brasil encontra-se em processo de aproximação com modelos jurídicos mais desenvolvidos, como os dos Estados Unidos e da União Europeia, por meio da adesão à Convenção de Budapeste e da participação ativa na elaboração da Convenção da ONU sobre Crimes Cibernéticos.

Essa inserção em tratados multilaterais e o fortalecimento de mecanismos de cooperação internacional – inclusive com o apoio de forças-tarefa conjuntas e empresas transnacionais – é condição *sine qua non* para enfrentar a natureza transfronteiriça dos delitos digitais.

O cibercrime, por sua essência, ignora fronteiras; logo, a resposta estatal também deve ser transnacional, articulada e técnica.

Portanto, o enfrentamento eficaz dos crimes cibernéticos no Brasil demanda um enfoque multifacetado, que considere simultaneamente: (a) o aperfeiçoamento contínuo do arcabouço legal, com atualização de tipos penais e agravamento proporcional das penas; (b) o investimento técnico-institucional, com infraestrutura moderna e recursos humanos especializados; (c) a proteção sistêmica das infraestruturas críticas, sob perspectiva de segurança nacional; e (d) a cooperação internacional ampliada, com protagonismo nos fóruns multilaterais e integração com organismos e redes globais de combate ao cibercrime. Ao mesmo tempo, é fundamental promover a conscientização social, por meio de educação digital e canais de denúncia acessíveis, para engajar a sociedade na prevenção e repressão a essas condutas.

Em suma, o combate ao cibercrime exige leis modernas, instituições preparadas e cooperação internacional efetiva. O desafio é complexo, mas inadiável. Na era da informação, proteger o ciberespaço não é apenas uma questão de política criminal: é assegurar a integridade das relações sociais, econômicas e democráticas no século XXI.

REFERÊNCIAS

BORGES, Beatriz. **Crimes Cibernéticos**: Como a Legislação Penal está se Adaptando à Nova Realidade Digital. Blog do Direito IDP, 25 nov. 2024. Disponível em: https://pos.idp.edu.br/idp-learning/direito-penal/crimes-ciberneticos-como-a-legislacao-penal-esta-se-adaptando-a-nova-realidade-digital/. Acesso em: 17 maio 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012, Seção 1, p.1.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 24 abr. 2014, Seção 1, p.1.

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, de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018, Seção 1, p.59.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 1940 (Código Penal), para dispor sobre crimes informáticos (invasão de dispositivo informático) e sobre crimes cometidos mediante fraude eletrônica; e dá outras providências. Diário Oficial da União, Brasília, DF, 28 mai. 2021, Seção 1, p.2.

BRASIL. Decreto nº 11.491, de 11 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, adotada em Budapeste em 23 de novembro de 2001. Diário Oficial da União, Brasília, DF, 12 abr. 2023, Seção 1, p.5.

CARVALHO, Leonardo de. Os crimes cibernéticos na realidade brasileira: breve panorama e desafios. **Fonte Segura (Fórum Brasileiro de Segurança Pública)**, 26 mar. 2025.

GOMES, Júlio Cesar L. C.; MEDRADO, Lucas C.; ALBUQUERQUE, Giliarde B. Crimes cibernéticos: desafios jurídicos no processo e julgamento de infrações penais virtuais cometidas por agentes estrangeiros contra vítimas brasileiras. **Revista JRG de Estudos Acadêmicos**, v. 7, n. 15, p. 1-20, 2024.

SENADO FEDERAL. Golpes virtuais aumentam e não fazem distinção de idade. **Senado Notícias**, 11 abr. 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade. Acesso em: 18 maio 2025.

ZIVIANI, Gabriel F.; GUIMARÃES, Fábio L. Crimes cibernéticos na legislação penal brasileira: prevenção e repressão. In: **III Simpósio de Pesquisa do Ecossistema Ânima**, [S.l.: s.n.], [2021]. Disponível em: https://simposiodepesquisa.animaeducacao.com.br/doc_pro/projeto_6747cf1d3217b.pdf. Acesso em: 17 maio 2025.