

O LOCUS DELICTI NA ERA DIGITAL: COMPETÊNCIA JURISDICIONAL E OS DESAFIOS INVESTIGATIVOS DO ESTELIONATO ELETRÔNICO

LOCUS DELICTI IN THE DIGITAL AGE: JURISDICTIONAL COMPETENCE AND THE INVESTIGATIVE CHALLENGES OF ELECTRONIC FRAUD

Adriano Nazareno Soares Miranda Junior

Faculdade Regional do Amazonas – FAM, Brasil

Elaine Silva Rodrigues

Faculdade Regional do Amazonas – FAM, Brasil

Marvyson Darley Albuquerque Alves

Faculdade Regional do Amazonas – FAM, Brasil

DOI: <https://doi.org/10.46550/ilustracao.v7i3.560>

Publicado em: 08.03.2026

Resumo: O presente artigo analisa o fenômeno do estelionato virtual no contexto da consolidação da Sociedade da Informação, examinando os desafios enfrentados pelo ordenamento jurídico brasileiro diante da crescente digitalização das relações sociais e econômicas. Parte-se da premissa de que os crimes cibernéticos decorrem da ampliação do uso das tecnologias digitais, distinguindo-se entre delitos informáticos próprios e impróprios, categoria na qual se insere o estelionato ao transpor uma tipificação penal tradicional para o ambiente virtual. Por meio de abordagem dedutiva e pesquisa bibliográfica, o estudo examina a origem conceitual e a tipicidade do crime previsto no artigo 171 do Código Penal, confrontando sua estrutura normativa com novas modalidades de fraude eletrônica, como phishing e utilização de páginas espelhadas. A análise evidencia que, embora instrumentos normativos como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 12.965/2014 (Marco Civil da Internet) tenham representado avanços na regulação do ambiente digital, ainda persistem lacunas normativas e operacionais que dificultam a repressão eficaz de fraudes virtuais, sobretudo aquelas praticadas em ambientes de maior anonimato. Ademais, identificam-se desafios relevantes na persecução penal, como a definição da competência jurisdicional e a necessidade de maior capacitação técnica das instituições responsáveis pela investigação. Conclui-se que o enfrentamento do estelionato eletrônico demanda não apenas o aperfeiçoamento legislativo, mas também investimentos em infraestrutura tecnológica, formação especializada e estratégias de prevenção baseadas em educação digital, de modo a fortalecer a proteção dos direitos fundamentais no ambiente informacional.

Palavras-chave: Crimes cibernéticos. Estelionato virtual. Direito digital. Deficiência legislativa. Sociedade da informação.

Abstract: This article analyzes the phenomenon of online fraud in the context of the consolidation of the Information Society, examining the challenges faced by the Brazilian legal system in the face of the increasing digitalization of social and economic relations. It starts from the premise that cybercrimes stem from the increased use of digital technologies, distinguishing between proper and improper computer crimes, a category into which fraud falls by transposing a traditional criminal classification to the virtual environment. Through a deductive approach and bibliographic research, the study examines the conceptual origin and the typicality of the crime foreseen in article 171 of the Penal Code, confronting its normative structure with new modalities of electronic fraud, such as phishing and the use of mirrored pages. The analysis shows that, although normative instruments such as Law No. 12,737/2012 (Carolina Dieckmann Law) and Law No. 12,965/2014 (Marco Civil da Internet) have represented advances in the regulation of the digital environment, normative and operational gaps still persist that hinder the effective repression of virtual fraud, especially those practiced in environments of greater anonymity. Furthermore, relevant challenges in criminal prosecution are identified, such as the definition of jurisdictional competence and the need for greater technical capacity of the institutions responsible for the investigation. It is concluded that tackling electronic fraud requires not only legislative improvement, but also investments in technological infrastructure, specialized training, and prevention strategies based on digital education, in order to strengthen the protection of fundamental rights in the informational environment.

Keywords: Cybercrimes. Virtual fraud. Digital law. Legislative deficiency. Information society.

Introdução

A revolução tecnoindustrial, intensificada desde o século XX, transbordou a economia para reconfigurar as relações sociais e os padrões de consumo, estabelecendo uma singular, porém excludente, forma de vida. Esse cenário de informatização da existência não apenas estreita distâncias, mas impõe novas dependências e vulnerabilidades, expondo a sociedade a riscos que vão da desinformação sistêmica, como as fake news, a novas modalidades de submissão digital. “A intensificação do uso das tecnologias da informação transformou profundamente as relações sociais, econômicas e jurídicas, deslocando grande parte das interações humanas para o ambiente digital”.¹

O Direito, enquanto produto cultural que tradicionalmente caminha a reboque dos fatos sociais, enfrenta hoje o desafio hercúleo de tutelar transações instantâneas e comportamentos fluidos sem se distanciar da realidade que pretende regular. A migração forçada do espaço físico

1 ALVES, Marvysen Darley Albuquerque; JUNIOR, Adriano Nazareno Soares Miranda; SOUSA, Larissa Freire de; LAVAREDA, Priscila da Silva; SANTOS, Anarienda Cristina Muniz dos; JESUS, Lucas Caravetto de. **SEGURANÇA DA INFORMAÇÃO E CONTRAINTELIGÊNCIA DIGITAL: UMA ANÁLISE COMPARADA ENTRE OS PATRIOT ACTS, A LGPD E O MARCO CIVIL DA INTERNET.** Revista Políticas Públicas & Cidades, [S. l.], v. 15, n. 2, p. e3176, 2026. DOI: 10.23900/2359-1552v15n2-26-2026. Disponível em: <https://journalppc.com/RPPC/article/view/3176>. Acesso em: 3 mar. 2026.

para o virtual, catalisada pela pandemia da Covid-19, escancarou o despreparo técnico dos usuários e a obsolescência das ferramentas de repressão estatal.

Neste hiato entre a inovação e a norma, proliferam-se vantagens ilícitas facilitadas pela fragilidade dos sistemas e pela complexidade na identificação de agentes em ambientes de endereços IP mascarados. A presente análise propõe, portanto, enfrentar os vácuos legislativos e a insuficiência das sanções penais vigentes, os quais, ao falharem na inibição de condutas criminosas, comprometem a segurança jurídica nesta novel conjuntura digital.

A investigação desenvolve-se por meio de metodologia dedutiva, documental e bibliográfica, com base na Constituição Federal, na legislação infraconstitucional e na jurisprudência dos tribunais superiores, além do diálogo com diversas doutrinas e produções acadêmicas.

A sociedade da informação e a fenomenologia dos crimes virtuais

O desenvolvimento tecnológico contemporâneo impulsionou a transição para a denominada Sociedade da Informação, conforme Castelles, já Vargas Losa prefere “Civilização do Espetáculo” e Toffler de “Powershift. Segundo a exegese de Werthein (2000), tal expressão substitui o conceito de sociedade pós-industrial, estabelecendo um novo paradigma organizacional e administrativo. Nesse cenário, o eixo central de produção desloca-se dos insumos energéticos tradicionais para os insumos informacionais de baixo custo, viabilizados pelos avanços disruptivos nas tecnologias eletrônicas e comunicativas.

Sob a ótica de Savegnago e Woltmann (2015), o crime cibernético emerge organicamente nesse contexto, no qual bens tecnológicos, produtos de entretenimento e a própria circulação de dados assumem proeminência política e econômica. Por conseguinte, as tecnologias de comunicação tornam-se ferramentas indispensáveis à gestão da vida em sociedade, conforme asseveram Cruz e Rodrigues (2018), mediando interações que transcendem as limitações geográficas tradicionais através do ciberespaço, este ambiente de interconexão humana via redes de telecomunicação descrito por Thing (2003).

A despeito da natureza imaterial do ciberespaço, Dullius, Hipller e Franco (2012) argumentam que este domínio não deve ser compreendido como uma realidade dissociada, mas como um espaço intermediário que se integra à cotidianidade. É nesta zona de intersecção que Cassanti (2014) define o crime virtual pela ausência física do agente, caracterizando-o por atividades em que a tecnologia da informação, conectada à rede, atua como ferramenta, base ou meio de execução. O agente delituoso, portanto, utiliza sua expertise técnica para subverter sistemas e lesar direitos individuais ou coletivos no ambiente digital.

Aprofundando a tipificação, Jesus e Milagres (2016) sustentam que o crime virtual extrapola a mera infração penal comum, configurando-se como conduta antijurídica perpetrada contra ou por intermédio de sistemas informáticos e redes de computadores. Tais ilícitos possuem particularidades que desafiam a análise criminal convencional. Conforme Sydow (2009), a

ausência de contato físico entre as partes mitiga a percepção imediata de violência, conferindo ao ato um caráter discreto e silencioso, desprovido de padrões comportamentais rígidos.

No plano da dogmática jurídica, a doutrina diferencia os delitos em próprios e impróprios. Rocha (2017) esclarece que os crimes cibernéticos próprios visam a violação direta de dados ou sistemas. Complementando tal entendimento, Almeida et al. (2015) explicam que, nestes casos, o sistema do sujeito passivo é o meio e o fim da infração. O bem jurídico tutelado, como aponta Carneiro (2012), é a inviolabilidade das informações automatizadas, protegendo-se a segurança, a integridade dos dados e a disponibilidade dos sistemas.

Em contrapartida, os crimes cibernéticos impróprios referem-se a condutas já tipificadas no ordenamento jurídico que utilizam a informática apenas como instrumento facilitador. Segundo Almeida et al. (2015) e Assunção (2018), as modalidades mais recorrentes envolvem abusos da liberdade de expressão, como o discurso de ódio. Outrossim, crimes como a pedofilia, que prescindem da tecnologia para sua existência, são classificados como impróprios quando mediados pela rede, conforme a lição de Carneiro (2012).

A expansão do acesso à rede mundial de computadores correlaciona-se diretamente com a ascensão dos índices de criminalidade virtual, exemplificada por episódios de exfiltração massiva de dados em plataformas como o Facebook. O incidente ocorrido em outubro de 2021, que resultou na exposição de dados de 530 milhões de usuários em fóruns especializados, ilustra a vulnerabilidade sistêmica da era digital (PORTAL G1, 2021). No Brasil, Deslandes e Arantes (2017) observam um crescimento anual de denúncias, com destaque para crimes contra a honra, ameaças, extorsões e delitos sexuais, frequentemente operacionalizados em redes sociais (JESUS; MILAGRES, 2016).

O tipo penal do estelionato

Gênese etimológica

A compreensão da figura típica do estelionato perpassa, inicialmente, por sua arqueologia linguística. Conforme leciona Ribeiro (2019), o termo origina-se do vocábulo grego *stellio*, designação de uma espécie de lagarto notável por sua capacidade de mimetismo para iludir presas. Esta metáfora biológica fundamenta a essência do delito: o emprego de um estratagema enganoso para a obtenção de vantagem indevida. Nesse sentido, Greco (2012) define o estelionato como a utilização de qualquer meio fraudulento que induza a vítima a erro, enquanto Campos et al. (2016) ratificam que o cerne da conduta reside na aferição de benefício próprio ou alheio mediante o artifício do engodo.

No ordenamento jurídico brasileiro, o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), consagra em seu artigo 171 a obtenção de vantagem ilícita, em prejuízo alheio, mediante induzimento ou manutenção de alguém em erro através de artifício, ardil ou qualquer outro meio fraudulento. Sob a ótica de Capez (2016), trata-se de um crime essencialmente

doloso, no qual a vontade livre e consciente de ludibriar é acompanhada da má-fé voltada à causação de prejuízo alheio em proveito do agente.

A análise doutrinária de Baldan (2020) classifica o estelionato como um crime patrimonial que se distancia da violência ou grave ameaça, operando-se através da vulnerabilidade da vítima e do abuso de confiança. O objeto da tutela jurídica transcende o patrimônio móvel ou imóvel da pessoa física ou jurídica, alcançando o próprio interesse público na manutenção da lisura e da boa-fé nas relações sociais. Enquanto o sujeito ativo pode ser qualquer indivíduo, o polo passivo abarca tanto a pessoa enganada quanto o titular da lesão patrimonial, admitindo-se que uma fraude perpetrada contra um preposto cause prejuízo à entidade jurídica que este representa.

De acordo com Heleno Fragoso, “o antigo direito romano desconhecia o crime hoje denominado estelionato. Era integrado ao *dolus malus* que, juntamente com a *fraus* e o *metus*, constituía crime privado, produto de criação pretoriana. Na Grécia antiga a fraude era severamente reprimida².” Noronha traz em seu livro que a fraude, bem como a figura de estelionato, vem antes de qualquer civilização, “bastando considerar que leis, as mais antigas, como os Códigos de Hammurabi e de Manu, dela já se ocupavam”.³

Segundo o entendimento consolidado pelo Tribunal de Justiça do Distrito Federal e Territórios, a tipicidade do estelionato pressupõe o preenchimento cumulativo de quatro requisitos: a obtenção de vantagem ilícita; a ocorrência de prejuízo alheio; o emprego de ardis ou artimanha; e o induzimento ou manutenção em erro. A inexistência de qualquer um desses vetores desfigura a conduta típica. Ademais, ressalta-se a inexistência da modalidade culposa, exigindo-se invariavelmente o dolo específico de lesar para que se verifique a consumação ou a tentativa, conforme as balizas da bilateralidade entre vantagem e prejuízo discutidas por Campos et al. (2016).

Historicamente, o estelionato reflete uma conduta inerente às tensões das relações interpessoais. Ribeiro (2019) observa que o sujeito ativo frequentemente instrumentaliza a confiança e até a fé alheia para consolidar a fraude, uma prática que encontra ecos em narrativas mitológicas de diversas culturas. Essa perenidade demonstra que a falsificação da verdade em busca de proveito próprio acompanha a evolução social, adaptando-se às novas ambiências de interação humana, como ocorre hodiernamente no cenário digital.

A transposição dessas práticas para o ciberespaço confere ao estelionato uma nova e complexa dimensão. Ferreira (2019) salienta que a configuração do estelionato virtual demanda a coexistência da tipificação legal, da conduta autoral e do dano efetivo. Entretanto, o autor adverte que a carência de legislações específicas e as dificuldades na identificação da autoria e da competência jurisdicional geram uma percepção de impunidade. Esse descompasso entre a velocidade tecnológica e a resposta estatal, como pontua Pinheiro (2014), exige que os sistemas

2 FRAGOSO, Heleno Cláudio. **Lições de Direito Penal**. v.1. São Paulo: Jose Bushatsky, 1977, p. 444.

3 ORONHA, E. Magalhães. **Direito Penal**. ed. 13. v. 2. São Paulo: Saraiva, 1979, p.377.

jurídicos globais se reorganizem para tutelar relações cada vez mais mediadas por sistemas informáticos cujas fragilidades são exploradas por agentes criminosos.

Por fim, Pereira (2018) identifica três modalidades operacionais preponderantes no estelionato eletrônico. A primeira envolve a criação de sites espelhados ou falsas plataformas de e-commerce, visando a captura de dados financeiros ou a venda de produtos inexistentes. A segunda manifesta-se através de e-mails fraudulentos, conhecidos como phishing, que mimetizam comunicações de órgãos públicos ou instituições bancárias. Por fim, as correntes de mensagens em aplicativos como o WhatsApp funcionam como vetores para o direcionamento a sites maliciosos, expondo a vulnerabilidade do usuário médio diante da sofisticação dos novos estratagemas digitais.

Legislação pertinente

A análise da evolução legislativa atinente aos delitos informáticos no Brasil exige o resgate histórico da Convenção sobre o Cibercrime, celebrada em Budapeste no ano de 2001, que reconheceu a premência de se estabelecer, mediante cooperação transnacional, uma política criminal compartilhada voltada à proteção das sociedades frente à criminalidade em rede. Conquanto a Convenção não tenha instituído normas impositivas imediatas, ela delineou orientações e definições basilares, preservando a autonomia e a soberania de cada Estado signatário para a construção de seus próprios aparatos normativos internos.

No cenário nacional, observa-se a ausência de uma codificação única e abrangente dedicada exclusivamente aos crimes virtuais, o que impõe desafios dogmáticos significativos. Conforme adverte Feitosa (2012), a interpretação do crime cibernético exige cautela exegética, uma vez que o ordenamento jurídico pátrio se submete ao princípio da reserva legal, segundo o qual não há crime sem lei anterior que o defina. Tal circunstância confere certa fragilidade jurídica à repressão de condutas como o estelionato virtual, dada a necessidade de adequação dessas novas práticas aos tipos penais clássicos ou a leis esparsas que tentam suprir lacunas do Código Penal.

O reconhecimento formal desses delitos ganhou relevo apenas em 2012, com a promulgação da Lei nº 12.737, popularmente denominada Lei Carolina Dieckmann. O diploma, originado de um episódio de invasão de privacidade e extorsão contra a referida atriz, logrou tipificar infrações relacionadas à invasão de dispositivos informáticos. Todavia, Ferreira (2019) observa que, embora a norma estabeleça jurisdição para a sanção de ilícitos cibernéticos, ela possui um escopo limitado, concentrando-se na violação técnica do dispositivo e não exaurindo a vasta gama de possibilidades de afronta à privacidade e à segurança jurídica nos ambientes digitais.

Complementarmente, a Lei nº 12.965 de 2014, o Marco Civil da Internet, instituiu o estatuto de garantias, direitos e deveres para o uso da rede no Brasil. Este marco regulatório visa não apenas normatizar a utilização da internet, mas assegurar a proteção de dados e definir diretrizes para a atuação entes federativos. Em conjunto com a Lei Carolina Dieckmann, o

Marco Civil busca mitigar as lacunas do sistema jurídico. Segundo Siqueira et al. (2017), além de enumerar as prerrogativas dos usuários, a lei autoriza a atuação do Poder Público frente aos ilícitos digitais, em um esforço para consolidar um ambiente virtual dotado de maior segurança jurídica.

Por fim, a estruturação institucional para o combate a essas práticas foi impulsionada pela Lei nº 12.735 de 2012, que determinou a criação de setores especializados nas polícias judiciárias para a investigação de delitos em sistemas informatizados. Caetano (2015) ressalta que tal exigência demandou um esforço logístico e de treinamento das polícias civis em todo o território nacional. Soma-se a este arcabouço a Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018), que disciplina o tratamento de informações pessoais por entes públicos e privados. O objetivo da LGPD, conforme seu artigo 1º, é salvaguardar os direitos fundamentais de liberdade, privacidade e o desenvolvimento da personalidade, consolidando a defesa do indivíduo na era dos dados.

A investigação do estelionato virtual e os desafios da persecução penal

A defasagem entre a agilidade das práticas delitivas no ciberespaço e a resposta estatal brasileira é evidente, especialmente no que tange ao estelionato virtual. Sob a ótica de Paulino (2018), a persecução penal deste delito apresenta-se de forma acanhada em comparação a outras infrações patrimoniais, fenômeno atribuído à percepção de ineficácia do aparato judiciário. Esta subnotificação, ou “cifra negra” dos crimes cibernéticos, decorre das barreiras técnicas e procedimentais que permeiam a colheita de provas e a identificação de autoria em ambientes de alta volatilidade informacional.

Um dos nós críticos da investigação reside na fixação da competência jurisdicional e na definição do locus delicti. O Código de Processo Penal estabelece a competência, via de regra, pelo lugar da consumação da infração; todavia, o estelionato virtual fragmenta essa lógica territorial, uma vez que o agente, a infraestrutura de rede e a vítima podem estar situados em jurisdições ou países distintos. Conforme adverte Nauata (2018), a utilização de redes públicas e pontos de acesso anônimos mascara a origem da conexão, dificultando a individualização da conduta e gerando conflitos de atribuição que fragilizam o inquérito policial e a subsequente instrução processual.

A carência de estrutura técnica e capilaridade das forças de segurança pública constitui outro óbice relevante no cenário nacional. A escassez de delegacias especializadas em crimes de alta tecnologia limita a capacidade de resposta imediata, essencial para a preservação de evidências digitais que se perdem com celeridade. Esse quadro de vulnerabilidade investigativa é potencializado quando as práticas fraudulentas migram para a Deep Web, onde o anonimato é garantido por camadas de criptografia. Segundo Paulino (2018), o arcabouço legal vigente revela-se insuficiente e por vezes ambíguo para orientar diligências em camadas ocultas da rede, tornando as investigações de estelionato eletrônico complexas e, frequentemente, inconclusivas.

No plano da prova material, a identificação de dispositivos eletrônicos por meio do protocolo de internet (IP) representa o rastro fundamental para a persecução, contudo, tal elemento é passível de manipulação através de servidores proxy ou redes VPN, que ocultam a real localização do criminoso. Paulino (2018) assevera que a ausência de diretrizes investigativas padronizadas e a morosidade na obtenção de ordens judiciais para a quebra de sigilo de dados facilitam a eliminação de vestígios digitais. A investigação, portanto, demanda um esforço hercúleo de inteligência para correlacionar dados telemáticos a comportamentos humanos no mundo físico.

A complexidade técnica do estelionato virtual impõe ao Direito Penal uma necessária transposição de paradigmas, distanciando-se de conceitos puramente geográficos para abraçar a ubiquidade digital. Como aponta Pinheiro (2014), a modernização das técnicas de investigação é imperativa para que o sistema jurídico não se torne obsoleto diante da sofisticação dos novos estratagemas de engenharia social e fraude bancária. Sem o devido investimento em capacitação de peritos e em cooperação jurídica internacional, o hiato entre a inovação criminosa e a repressão estatal tende a se expandir, consolidando o ciberespaço como um campo fértil para a lesão de direitos patrimoniais.

No âmbito da processualística penal aplicada ao cenário digital, a definição da competência jurisdicional para o estelionato virtual sofreu uma alteração paradigmática com a promulgação da Lei nº 14.155/2021, que introduziu o § 4º ao art. 70 do Código de Processo Penal⁴. Conforme consolidado pela Terceira Seção do Superior Tribunal de Justiça (STJ) no julgamento do CC 180.832/RJ, a regra de fixação da competência nos casos de estelionato mediante transferência de valores ou depósito bancário deslocou-se do local da obtenção da vantagem para o domicílio da vítima.

Essa transição jurisprudencial visa mitigar as dificuldades de acesso à justiça e facilitar a instrução probatória, reconhecendo que o efetivo prejuízo patrimonial se concretiza no local onde o ofendido mantém seus ativos financeiros, independentemente da ubiquidade do agente no ciberespaço

Conclusão

A presente investigação permitiu diagnosticar que a transição para a Sociedade da Informação, embora tenha potencializado a conectividade global, institucionalizou o ciberespaço como um novo locus para a fenomenologia delitiva.

Conclui-se que o crime virtual, caracterizado pela dispensabilidade da presença física do agente e pela ausência de violência imediata, impõe desafios inéditos ao Poder Público, uma vez que as tecnologias voltadas ao bem-estar social são subvertidas para fins escusos. No decorrer

4 § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

da exegese, identificou-se que o estelionato virtual se amolda à categoria de crime impróprio, transpondo condutas já tipificadas na vida analógica para o meio digital, aproveitando-se da mediação tecnológica para a reiteração de ilicitudes patrimoniais.

A análise crítica revela que o descompasso entre a celeridade das inovações tecnológicas e a resposta do Direito é um fenômeno global. Observa-se que a Convenção de Budapeste (2001), embora pioneira, ao privilegiar estritamente a soberania nacional e limitar-se a recomendações, abdicou de estabelecer diretrizes internacionais mais cogentes que poderiam ter fomentado mecanismos repressivos transnacionais mais eficazes.

No cenário brasileiro, esse vácuo legislativo é evidente, uma vez que, a elaboração normativa, sujeita aos ritos políticos, não tem sido capaz de suprir a carência de uma estrutura investigativa robusta, resultando em baixos investimentos em capacitação técnica e em uma rede de proteção judiciária ainda incipiente para lidar com a complexidade do estelionato eletrônico.

Infere-se que, enquanto for possível ocultar vestígios digitais com facilidade, a eficácia do Estado permanecerá comprometida. Portanto, a conclusão central aponta para a necessidade premente de investimentos não apenas em tecnologia de ponta, mas em treinamento humano especializado, superando a fragmentação da Lei Carolina Dieckmann para alcançar uma reforma do Código Penal que dialogue com a informatização das relações financeiras no século XXI.

Por fim, o estudo demonstra que a pandemia de COVID-19 atuou como um catalisador dessa vulnerabilidade, ao acelerar a migração compulsória de transações presenciais para o ambiente on-line sem a devida literacia digital da população. Sustenta-se que a solução para a segurança jurídica na rede não reside exclusivamente na sanção penal, mas na educação tecnológica preventiva.

Conclui-se, portanto, pela urgência na aprovação de projetos de lei que abranjam as especificidades do estelionato virtual e na estruturação de uma rede de investigação integrada. Somente através do diálogo entre o saber jurídico e o investimento em campanhas educativas será possível mitigar a fragilidade estrutural que hoje favorece a impunidade e a exploração de terceiros no ciberespaço.

Referências

ALMEIDA, Jéssica de Jesus et al. **Crimes Virtuais**. Cadernos de Graduação - Ciências Humanas e Sociais Unit, Aracaju, v. 2, n. 3, p. 215-236, 2015.

ALVES, A. B. da C. S.; ALVES, M. D. A.; SANTOS, A. A. **A judicialização da censura no Brasil: do controle prévio ao assédio processual como limite à liberdade de expressão digital**. Revista Ilustração, [S. l.], v. 7, n. 1, p. 263–273, 2026. Disponível em: <https://journal.editorailustracao.com.br/index.php/ilustracao/article/view/547>. Acesso em: 3 mar. 2026.

ALVES, Marvyson Darley Albuquerque et al. **Segurança da informação e contrainteligência digital: uma análise comparada entre os Patriot Acts, a LGPD e o Marco Civil da Internet**. Revista Políticas Públicas & Cidades, [S. l.], v. 15, n. 2, p. e3176, 2026. Disponível em:

<https://journalppc.com/RPPC/article/view/3176>. Acesso em: 3 mar. 2026.

ASSUNÇÃO, Ana Paula Souza. **Crimes virtuais**. 2018. Monografia (Graduação em Direito) – Centro Universitário de Anápolis (UniEvangélica), Anápolis, 2018.

BALDAN, Édson Luís. **Estelionato**. In: Enciclopédia jurídica da PUC-SP. Tomo: Direito Penal. 1. ed. São Paulo: PUC-SP, 2020. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/425/edicao-1/estelionato>. Acesso em: 16 out. 2025.

BRASIL. [Código Penal (1940)]. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Rio de Janeiro, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 8 set. 2025.

BRASIL. [Código de Processo Penal (1941)]. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Brasília, DF: Presidência da República, [1941]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 1 mar. 2026.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. **Tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares**. Brasília, DF, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 16 out. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação **criminal de delitos informáticos**. Brasília, DF, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16 out. 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, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 out. 2025.

CAETANO, Aldo Maxwell Pereira de Mesquita. **Crimes virtuais: Aplicação, Falibilidade e impunidade**. 2015. Monografia (Graduação em Direito) – Universidade Tiradentes, Aracaju, 2015.

CAMPOS, Pedro Franco et al. **Direito penal aplicado: parte geral e parte especial do Código Penal**. São Paulo: Saraiva, 2016.

CASTELLS, M. **A galáxia da internet**. Trad. Maria Luiza X de A. Borges. Rio de Janeiro: Zahar, 2003.

CASTELLS, M. **A sociedade em rede**. Trad. Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999.

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

CARNEIRO, Adenele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico, São Paulo, v. 15, n. 99, abr. 2012.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport,

2014.

CONVENÇÃO SOBRE O CIBERCRIME (2001). **Convenção de Budapeste. Budapeste, 2001.** Disponível em: http://www.mpf.mp.br/atualizacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 13 out. 2025.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista Científica Eletrônica do Curso de Direito, Garça, v. 13, n. 1, p. 1-18, 2025.

DESLANDES, Maria; ARANTES, Álisson. **Os perigos dos crimes virtuais nas redes sociais.** Sinapse Múltipla, Belo Horizonte, v. 6, n. 2, p. 175-178, 2017.

DULLIUS, Aladino Anastácio; HIPLER, Aldair; FRANCO, Elisa Lunardi. **Dos crimes praticados em ambientes virtuais.** 2012. Disponível em: <https://egov.ufsc.br/portal/conteudo/dos-crimes-praticados-em-ambientes-virtuais>. Acesso em: 10 out. 2025.

FEITOZA, Luis Guilherme de Matos. **Crimes Cibernéticos: O estelionato virtual.** 2012. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro Universitário de Brasília, Brasília, 2012.

FERREIRA, Pedro Henrique Gomes. **Crimes cometidos através da internet.** 2019. Monografia (Graduação em Direito) – Centro Universitário de Maringá (UniCesumar), Maringá, 2019.

G1. Facebook atribui vazamento de dados de 530 milhões de usuários a ‘raspagem’. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/04/07/facebook-atribui-vazamento-de-dados-de-530-milhoes-de-dados-a-raspagem.ghtml>. Acesso em: 8 out. 2021.

GRECO, Rogério. **Resumos Gráficos de Direito Penal, Parte Especial – vol III.** Niterói: Impetus, 2012.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

LEAL, Luziane de Figueiredo Simão. **Inteligência Artificial nas Campanhas Eleitorais: a democracia das plataformas no banco dos réus.** Belo Horizonte: Dialética, 2020.

MATOS M., Alexandre. **Crimes na Internet.** 4. ed. Rio de Janeiro: Espaço Jurídico, 2012.

NAUATA, Felipe Macedo. **Crimes Virtuais: estelionato.** Revista Jus Navigandi, abr. 2018. Disponível em: <https://jus.com.br/artigos/65242/crimes-virtuais-estelionato>. Acesso em: 16 out. 2021.

PAULINO, Fabiana da Silva. **A ineficácia da legislação nos crimes virtuais.** 2018. Monografia (Graduação em Direito) – Faculdade Raízes, Anápolis, 2018.

PEREIRA, Ana Carolina dos Santos. **O Estelionato Virtual: Com o advento da tecnologia, golpistas se aproveitam de meios virtuais para realizar crimes.** 2018. Disponível em: anacarolinas-pereira.jusbrasil.com.br. Acesso em: 16 out. 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3. ed. São Paulo: Saraiva, 2009.

PINHEIRO, Patrícia Peck. **Regulamentação da Web**. Cadernos Adenauer, Rio de Janeiro, v. 15, n. 4, p. 33-44, out. 2014.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à Lei nº 13.709/2018 (LGPD)**. São Paulo: Saraiva, 2018.

RIBEIRO, Eliete da Silva. **Crime de estelionato – uma análise da evolução sob a égide da impunidade na cidade de Manaus**. Revista Científica Semana Acadêmica, Fortaleza, v. 1, n. 169, p. 1-16, 2019.

ROCHA, Adriano Aparecido. **Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet**. 2017. Monografia (Graduação em Direito) – Faculdade de Ensino Superior e Formação Integral, São Paulo, 2017.

SAVEGNAGO, Jéssica Uliana; WOLTMANN, Angelita. **A regulamentação dos cibercrimes no Brasil: uma análise jurídica dos “três pilares” norteadores do marco civil da internet**. In: Congresso Internacional de Direito e Contemporaneidade, 3., 2015, Santa Maria. Anais [...]. Santa Maria: UFSM, 2015.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. 2. ed. Rio de Janeiro: Elsevier, 2014.

SIQUEIRA, M. S. et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Revista do Curso de Graduação em Direito da Faculdade CNEC, Santo Ângelo, v. 7, n. 13, p. 119-130, 2017.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. 2009. Dissertação (Mestrado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

TOFFLER, Alvim. **Powershift - As mudanças do poder**. Trad. Luiz Carlos do Nascimento Silva. Rio de Janeiro: Record, 2010.

THING, L. **Dicionário de tecnologia Whatis.com**. São Paulo: Futura, 2003.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Estelionato. [s. d.]. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato>. Acesso em: 8 out. 2025.

VARGAS LLOSA, Mario. **A civilização do espetáculo [recurso eletrônico]: uma radiografia do nosso tempo e da nossa cultura**. Tradução Ivone Benedetti. Rio de Janeiro: Objetiva, 2013.

WERTHEIN, Jorge. **A sociedade da informação e seus desafios**. Ciência da Informação, Brasília, v. 29, n. 2, p. 71-77, 2000.