RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

O Analfabetismo Digital como Fator de Vulnerabilidade nos Crimes de Estelionato Cibernético

Digital Illiteracy as a Vulnerability Factor in Cyber Fraud Crimes
El Analfabetismo Digital como Factor de Vulnerabilidad en los Delitos de Estafa Cibernética

Lucas Sanches Caye – Centro Universitário Itaperuna – Afya, lucasscaye97@gmail.com
Fernanda Rosa Acha – Centro Universitário Itaperuna – Afya, fernanda.acha@afya.com.br

Resumo:
A informatização da sociedade, ao mesmo tempo que democratizou o acesso aos produtos e serviços, aprofundou desigualdades ao criar uma categoria inédita de exclusão: o analfabetismo digital. Milhões de brasileiros, muitos dos quais idosos, foram compelidos a utilizar plataformas digitais complexas sem o devido preparo técnico, tornando-se vítimas fáceis para criminosos. Considerando que essa massa de cidadãos vulneráveis se tornou o alvo preferencial do crime de estelionato cibernético (Art. 171, § 2º-A do CP), que explora a boa-fé e o desconhecimento de suas vítimas, por isso verifica se a emergência de insegurança jurídica e social que demanda respostas urgentes do Estado. O presente artigo se justifica pela urgência humanitária e jurídica de debater a proteção dessas pessoas, objetivando-se, portanto, analisar como o analfabetismo digital se constitui como um fator fático e jurídico de hipervulnerabilidade quando se demonstra que tal condição facilita o "induzimento a erro" e agrava a reprovabilidade da conduta do agente. O artigo busca, em última análise, propor mecanismos de prevenção eficazes. Para tanto, procede-se à uma pesquisa de natureza bibliográfica e documental, com abordagem dedutiva, centrada na análise da doutrina penal (notadamente Guilherme Nucci), na legislação atualizada (Lei nº 14.155/2021) e na análise de dados empíricos sobre as habilidades digitais da população. Parte-se da hipótese de que o foco exclusivo do ordenamento jurídico na repressão penal é insuficiente, sendo importante a criação de mecanismos de prevenção primária — como a educação digital e a responsabilização civil de instituições — para garantir que a inclusão digital no Brasil seja, de fato, segura para todos.

Palavras-chave:
Direito Penal; Estelionato; Analfabetismo Digital; Hipervulnerabilidade.

Abstract:
The computerization of society, while democratizing access to products and services, has deepened inequalities by creating a new category of exclusion: digital illiteracy. Millions of Brazilians, many of whom are elderly, have been compelled to use complex digital platforms without the necessary technical preparation, making them easy targets for criminals. Considering that this mass of vulnerable citizens has become the preferred target of cyber fraud (Article 171, § 2º-A of the Penal Code), which exploits the good faith and lack of knowledge of its victims, the emergence of legal and social insecurity demands urgent responses from the State. This article is justified by the humanitarian and legal urgency of debating the protection of these people, aiming, therefore, to analyze how digital illiteracy constitutes a factual and legal factor of hyper-vulnerability when it is demonstrated that this condition facilitates "inducing error" and aggravates the reprehensibility of the agent's conduct. Ultimately, the work seeks to propose effective prevention mechanisms. To this end, a bibliographical and documentary research is carried out, with a deductive approach, focusing on the analysis of penal doctrine (notably Guilherme Nucci), current legislation (Law No. 14.155/2021), and the analysis of empirical data on the digital skills of the population. The hypothesis is that the exclusive focus of the legal system on criminal repression is insufficient, and that the creation

of primary prevention mechanisms—such as digital education and the civil liability of institutions—is important to ensure that digital inclusion in Brazil is, in fact, safe for everyone.

Keywords:
Criminal Law; Fraud; Digital Illiteracy; Hypervulnerability.

Resumen:
La informatización de la sociedad, al mismo tiempo que democratizó el acceso a productos y servicios, profundizó las desigualdades al crear una nueva categoría de exclusión: el analfabetismo digital. Millones de brasileños, muchos de ellos adultos mayores, fueron obligados a utilizar plataformas digitales complejas sin la preparación técnica necesaria, convirtiéndose en víctimas fáciles de delincuentes. Considerando que esta masa de ciudadanos vulnerables se ha convertido en el objetivo preferente del delito de estafa cibernética (artículo 171, § 2º-A del Código Penal), que explota la buena fe y el desconocimiento de sus víctimas, surge una situación de inseguridad jurídica y social que exige respuestas urgentes por parte del Estado. El presente artículo se justifica por la urgencia humanitaria y jurídica de debatir la protección de estas personas, con el objetivo de analizar cómo el analfabetismo digital constituye un factor fáctico y jurídico de hipervulnerabilidad al demostrarse que esta condición facilita la inducción al error y agrava la reprochabilidad de la conducta del agente. El trabajo busca, en última instancia, proponer mecanismos eficaces de prevención. Para ello, se realiza una investigación bibliográfica y documental, con enfoque deductivo, centrada en el análisis de la doctrina penal (especialmente Guilherme Nucci), la legislación actualizada (Ley n.º 14.155/2021) y el análisis de datos empíricos sobre las habilidades digitales de la población. Se parte de la hipótesis de que el enfoque exclusivo del ordenamiento jurídico en la represión penal es insuficiente, siendo importante la creación de mecanismos de prevención primaria, como la educación digital y la responsabilidad civil de las instituciones, para garantizar que la inclusión digital en Brasil sea realmente segura para todos.

Palabras clave:
Derecho Penal; Estafa; Analfabetismo Digital; Hipervulnerabilidad.

1. Introdução

A evolução humana tem sido ciclicamente marcada por inovações que, a cada momento, redefinem os parâmetros fundamentais para a convivência social. A chegada da chamada “era tecnológica” ou “sociedade da informação” representa um desses marcos divisores, em que a maior parte da vida das pessoas se tornou completamente ligada e dependente da tecnologia. De um ponto de vista inicial, este avanço é inegavelmente positivo, proporcionando a democratização do acesso à informação, a otimização de tempo, a facilitação da comunicação global e o surgimento de inéditos modelos econômicos e de convívio social. Contudo, de forma colateral, essa aceleração acabou por trazer severos malefícios e disparidades, afetando principalmente os cidadãos que ainda não se encontram familiarizados com tais avanços.

Nessa perspectiva, a exclusão digital emerge como uma face sombria desse progresso, criando uma categoria inédita de vulnerabilidade social. Indivíduos que não possuem as

competências e o saber técnico mínimo necessário para navegar no ambiente online — os denominados "analfabetos digitais" — encontram-se à margem de uma sociedade cada vez mais conectada, fator que os torna drasticamente mais suscetíveis a crimes virtuais. Esta vulnerabilidade é particularmente acentuada no que tange à segurança pessoal e patrimonial, transformando essa parcela da população em um alvo preferencial para atividades criminosas organizadas, com especial destaque para o estelionato cibernético.

A relevância social e prática deste cenário justifica-se pelo fato de o Brasil despontar internacionalmente no topo do *ranking* de nações mais afetadas por fraudes digitais, vitimizando milhões de cidadãos anualmente. Essa criminalidade não atinge o tecido social de forma homogênea; ela se aproveita, de maneira sistemática, da boa-fé e da falta de habilidades técnicas de certos grupos, com especial ênfase na população idosa. Ao serem compelidos a interagir com plataformas virtuais complexas para realizar transações bancárias cotidianas ou para acessar benefícios assistenciais essenciais, esses indivíduos enfrentam perdas financeiras devastadoras que muitas vezes comprometem a própria subsistência, além de sofrerem danos morais e psicológicos profundos.

Diante dessa conjuntura, emerge um questionamento imperativo: de que forma o Estado pode desenvolver e implementar mecanismos eficazes para proteger os analfabetos digitais do estelionato e de outros crimes no meio cibernético? A resposta a essa pergunta é crucial para garantir que os benefícios da era da informação sejam, de fato, universais e seguros para todos. Tradicionalmente, as dificuldades estatais em coibir ilícitos penais no ambiente virtual são investigadas à luz de dispositivos como a Lei nº 12.965/2014 (Marco Civil da Internet). Essa legislação, embora fundamental para a regulação de direitos e garantias na rede, pode acabar por limitar a agilidade e a eficácia da atuação estatal direta em repelir as fraudes eletrônicas em tempo hábil.

No entanto, sob o prisma teórico e criminológico, constata-se uma lacuna na produção científica nacional, que ainda se concentra majoritariamente na análise dogmática pós-delitiva e na suficiência da persecução penal (o "depois"). É nesse vácuo que se insere a necessária doutrina crítica de Aury Lopes Jr. e de Nucci acerca do Direito Penal Simbólico. Demonstra-se que o foco exclusivo do ordenamento jurídico na repressão penal e no mero endurecimento de penas — a exemplo das alterações promovidas pela Lei nº 14.155/2021(Brasil, 2021) no crime de estelionato eletrônico — funciona como uma resposta ilusória e paliativa das agências estatais. O agravamento da sanção atua tardiamente, quando o patrimônio do vulnerável já foi dilapidado, revelando a urgência de deslocar o debate para mecanismos de prevenção primária e salvaguardas institucionais antes da consumação do delito.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Para nortear a presente investigação, estabelece-se como objetivo geral demonstrar e verificar criticamente de que maneira o analfabetismo digital se consolida como um fator fático e jurídico de hipervulnerabilidade social e jurídica. Busca-se analisar como essa condição mitiga a capacidade de resistência da vítima, facilitando o seu induzimento a erro no crime de estelionato cibernético (Art. 171, § 2º-A do Código Penal), e, paralelamente, evidenciar a insuficiência da resposta puramente penal do Estado, propondo mecanismos preventivos de ordem jurídica e social aptos a conferir efetiva proteção ao cidadão na sociedade da informação.

2. Metodologia

Para a consecução dos objetivos delineados nesta investigação e a resolução do problema científico proposto — que gravita em torno da eficácia protetiva do Estado face à hipervulnerabilidade do analfabeto digital no crime de estelionato cibernético —, adotou-se um desenho metodológico de matriz eminentemente teórica e qualitativa. O percurso investigativo pautou-se pelo rigor científico necessário para interligar a dogmática penal clássica às transformações fáticas da Sociedade da Informação.

O método de abordagem eleito para governar o raciocínio científico foi o **método dedutivo**. Partiu-se de premissas gerais macroestruturais — notadamente o conceito sociológico da Sociedade em Rede e a transição compulsória dos serviços financeiros para os ecossistemas telemáticos — para, mediante um encadeamento lógico e silogístico, alcançar a análise do fenômeno particular e específico, qual seja, a vulnerabilidade tecnocognitiva do indivíduo excluído digitalmente frente ao ardil operado no estelionato qualificado pela fraude eletrônica (§ 2º-A do art. 171 do Código Penal).

No que concerne à natureza da pesquisa e aos objetivos perseguidos, o estudo qualifica-se como **exploratório e descritivo**. Exploratório por adentrar em uma seara jurídica em constante e célere mutação, cujos reflexos sociais demandam novas categorias hermenêuticas; e descritivo por pormenorizar os elementos normativos do tipo penal de estelionato, os contornos da responsabilidade civil objetiva consumerista e os dados estatísticos que delimitam a extensão da exclusão digital e da criminalidade virtual no cenário brasileiro contemporâneo.

Como técnica de coleta e levantamento de dados, utilizou-se o procedimento conjugado da **pesquisa bibliográfica e documental**, operando-se estritamente sobre fontes secundárias dotadas de fidedignidade e reconhecimento acadêmicoinstitucional:

- **Pesquisa Bibliográfica:** Consistiu na revisão sistemática e crítica de literatura jurídica e sociológica de referência. Foram examinadas obras consagradas de dogmática penal (Guilherme de Souza Nucci e Cezar Roberto Bitencourt), criminologia crítica e processo penal (Aury Lopes Jr.), Direito Digital e do Consumidor (Patrícia Peck Pinheiro), além da teoria social clássica de Manuel Castells. A seleção desse arcabouço doutrinário obedeceu a critérios de relevância temática e atualidade, garantindo o estofo teórico indispensável para a crítica ao Direito Penal Simbólico.
- **Pesquisa Documental:** Compreendeu a análise do ordenamento jurídico pátrio vigente, englobando a Constituição da República Federativa do Brasil de 1988, o Código Penal brasileiro (com o recorte analítico das alterações promovidas pela Lei nº 14.155/2021), Marco Civil da Internet(Lei Lei nº 12.965/2014), o Código de Defesa do Consumidor (Lei nº 8.078/1990) e o enunciado da Súmula nº 479 do Superior Tribunal de Justiça.

Ademais, a pesquisa documental foi enriquecida com a incorporação de **dados estatísticos secundários de natureza empírica**, extraídos dos relatórios oficiais mais recentes de órgãos governamentais e entidades de classe setoriais reconhecidas. Foram amalgamados ao texto os indicadores quantitativos da Pesquisa Nacional por Amostra de Domicílios (PNAD) Contínua do Instituto Brasileiro de Geografia e Estatística (IBGE), os levantamentos do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) e os volumes consolidados da Pesquisa FEBRABAN de Tecnologia Bancária. A inserção desses dados empíricos objetivou contrastar a realidade fática do analfabetismo digital com a resposta normativa dada pelo Estado.

Por fim, o método de processamento e análise dos dados coletados deu-se por meio da **análise de conteúdo crítica e explicativa**. Os textos legais, as construções doutrinárias e os dados estatísticos não foram meramente reproduzidos, mas sim submetidos a um filtro hermenêutico cruzado. Confrontouse a dogmática jurídica com a criminologia factual para demonstrar as insuficiências do modelo punitivo clássico e fundamentar a urgência de uma mudança de paradigma em direção à prevenção primária e à responsabilização civil proativa do mercado financeiro.

3. Desenvolvimento

3.1. A Sociedade da Informação e o Fenômeno do Analfabetismo Digital como Exclusão Social

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Para compreender o impacto do estelionato cibernético sobre as vítimas vulneráveis, faz-se imperioso mapear as transformações estruturais que culminaram na gênese da chamada Sociedade da Informação. Conforme o pensamento sociológico de Castells (2018), a transição global para a "Sociedade em Rede" operou uma mutação profunda nas matrizes de poder, economia e convivência social. A informação e a tecnologia deixaram de ocupar uma função meramente instrumental para se converterem na própria infraestrutura onde a vida civil se processa. O espaço de fluxos virtuais substituiu, progressivamente, o espaço de lugares físicos, redefinindo as dinâmicas de consumo, lazer e, fundamentalmente, de acesso a serviços públicos e financeiros.

Todavia, o advento dessa nova era não se deu sob o manto da equidade. A transição para o ecossistema hiperconectado expôs um severo paradoxo: ao passo que a tecnologia encurtou distâncias e democratizou o acesso formal a dados para expressiva parcela da população, simultaneamente aprofundou abismos sociais pretéritos e estruturou uma nova modalidade de segregação: a exclusão digital. Castells adverte que na sociedade em rede a exclusão assume contornos dramáticos, uma vez que estar desconectado — ou ser incapaz de interagir de forma autônoma com a rede — equivale à invisibilidade social e à perda das prerrogativas mais básicas da cidadania moderna.

No cenário brasileiro, essa exclusão tecnocognitiva corporifica-se no fenômeno do analfabetismo digital. Este conceito transcende a mera ausência física de aparelhos tecnológicos ou de infraestrutura de conectividade; o analfabetismo digital caracteriza-se pela incapacidade do indivíduo de compreender, interpretar e operar de maneira segura e crítica as ferramentas virtuais que lhe são impostas pelo cotidiano. Trata-se de um deficit de letramento digital, no qual o usuário detém o acesso instrumental de superfície (como ligar um aparelho ou acionar um aplicativo), mas carece das competências necessárias para discernir riscos, validar a legitimidade de interfaces virtuais ou identificar armadilhas operadas por terceiros.

A dimensão empírica dessa problemática é evidenciada pelos dados estatísticos oficiais. Segundo os relatórios consolidados da Pesquisa Nacional por Amostra de Domicílios (PNAD) Contínua, publicada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), embora a inclusão digital formal da população idosa tenha saltado de 44,8% para 69,4%, o contingente que permanece à margem da rede revela o cerne da exclusão. Dentre os milhões de brasileiros com 60 anos ou mais que declaram não acessar a internet, **66%** apontam explicitamente o "não saber usar a tecnologia" como o motivo determinante para o seu isolamento digital (IBGE, 2025).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Complementando esse diagnóstico, o levantamento nacional **TIC Domicílios**, conduzido pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), demonstra que a maior parte dos não usuários de internet no Brasil concentra-se na faixa etária acima dos 60 anos, somando mais de 16 milhões de indivíduos completamente apartados das competências digitais básicas. Concomitantemente, o avanço meteórico de ferramentas de transação instantânea, capitaneado pela massificação do Pix, fez com que o acesso a canais bancários e instituições financeiras por meio da internet saltasse para **71,2% dos usuários** (IBGE, 2025).

Essa migração célere, forçada e por vezes desprovida de transição pedagógica para os ambientes digitais gerou um cenário de extrema vulnerabilidade, tal como pondera Patrícia Peck Pinheiro ao tratar da segurança e da educação na era digital:

> "A evolução tecnológica sem a devida aculturação digital e sem educação preventiva gera uma sociedade exposta a riscos imensuráveis. O Direito Digital exige que a inclusão seja acompanhada do letramento, pois a simples entrega de ferramentas tecnológicas complexas a indivíduos vulneráveis, sem o ensino de salvaguardas de segurança, equivale a colocá-los em uma arena de perigos sem qualquer mecanismo de defesa." (PINHEIRO, 2021).

Verifica-se, portanto, que a confluência entre a bancarização digital obrigatória — intensificada pela desmaterialização das agências físicas — e o analfabetismo digital crônico pavimenta o caminho para a vitimização em massa. O indivíduo desprovido de discernimento tecnológico é inserido compulsoriamente em um mercado de transações digitais complexas, operando sob o constante risco de interagir com engenharia social fraudulenta.

Nesse contexto, o analfabetismo digital deixa de ser apenas uma questão de isolamento social e assume contornos de uma autêntica **hipervulnerabilidade jurídica**, transformando o idoso e o hipossuficiente técnico nos alvos prediletos de organizações criminosas especializadas na exploração do vácuo cognitivo tecnológico, conforme restará detalhado nas seções dogmáticas e criminológicas subsequentes deste estudo.

3.2. O Estelionato Cibernético: Análise Dogmática, o Meio Fraudulento e criação da Qualificadora (Lei nº 14.155/2021)

O estudo da vitimização do analfabeto digital exige, invariavelmente, a dissecação dogmática do crime de estelionato, tipificado no artigo 171 do Código Penal brasileiro.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Considerado pela doutrina tradicional como o crime patrimonial fraudulento por excelência, o estelionato não se perfaz por meio do emprego de violência ou grave ameaça, mas sim através de um vício de consentimento provocado no sujeito passivo. O agente delitivo induz ou mantém a vítima em erro para que esta, voluntariamente, porém ludibriada, realize a disposição patrimonial prejudicial.

Para a configuração do tipo básico, a doutrina penal exige a concorrência de quatro elementos fundamentais, que se encadeiam em um duplo nexo causal: o emprego de meio fraudulento; o induzimento ou manutenção da vítima em erro; a obtenção de vantagem ilícita; e o consequente prejuízo alheio. Conforme a precisa lição de Guilherme de Souza Nucci (2014), o núcleo do tipo penal reside na conduta enganosa:

> *"A ação do estelionato consiste em obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Artifício é a fraude material (ex: a utilização de um documento falso); ardil é a fraude moral ou intelectual (ex: a conversa enganosa, a astúcia). O meio fraudulento é a fórmula genérica (procedimento enganoso de qualquer outra natureza)."* (Nucci, 2014).

No ecossistema cibernético, as tradicionais figuras do artifício e do ardil ganham contornos tecnológicos complexos. O *artifício* materializa-se por meio de engenharia de software maliciosa, tais como páginas de internet clonadas de instituições bancárias legítimas, aplicativos fraudulentos e hiperlinks capciosos (*phishing*). O *ardil*, por sua vez, manifesta-se através da engenharia social, na qual o criminoso, valendo-se do manto de anonimato da rede, adota uma identidade falsa (falsos funcionários de suporte de segurança de bancos, parentes simulados em aplicativos de mensagens) para enredar a vítima em uma narrativa fictícia altamente verossímil.

Nesse diapasão, Cezar Roberto Bitencourt (2020) acentua que, para a tipificação do estelionato, o meio fraudulento adotado pelo agente deve ser idôneo e possuir a capacidade concreta de enganar o homem médio. Há de existir uma relação de causalidade direta entre a fraude e o erro:

> *"Entre a fraude e o erro deve existir uma relação de causa e efeito, isto é, o erro deve ser a consequência direta da fraude. Se o erro decorre de outra causa que não a conduta fraudulenta do sujeito ativo, não haverá o crime de estelionato. Exige-se que o meio empregado seja idôneo para enganar, induzir ou*

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

> *manter alguém em erro, retirando-lhe a exata percepção da realidade."* (Bitencourt, 2020).

É precisamente nessa junção dogmática que a presente investigação localiza o ponto de ruptura em relação ao analfabeto digital. O conceito de "homem médio" ou de "meio fraudulento idôneo" torna-se difuso e insuficiente quando confrontado com a exclusão tecnológica. Uma fraude eletrônica que se apresenta como manifestamente grosseira ou facilmente detectável para um usuário nativo digital ou letrado tecnologicamente, assume contornos de fidedignidade absoluta para o indivíduo afetado pelo analfabetismo digital.

A ausência de letramento impede a identificação de sinais básicos de alerta, tais como desvios em URLs, falta de certificados de segurança digitais ou a atipicidade de solicitações de senhas master via telefone. Por conseguinte, a idoneidade do meio fraudulento deve ser aferida em concreto, considerando a hiper vulnerabilidade técnica do sujeito passivo.

Atento à proliferação massiva dessas condutas no ambiente de rede, o legislador federal editou a Lei nº 14.155/2021, a qual inseriu a qualificadora da fraude eletrônica no § 2º-A do artigo 171 do Código Penal. O dispositivo preceitua que a pena será de reclusão, de 4 a 8 anos, e multa, se o estelionato for cometido:

> *"[...] com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo."* (BRASIL, 2021).

A criação desta qualificadora deslocou o foco do estelionato comum para o desvalor da conduta digital, reconhecendo que o emprego de sistemas telemáticos automatizados amplia exponencialmente o alcance do dano e a velocidade da dilapidação patrimonial.

3.3. A Resposta Punitiva e a Ilusão Protetiva: O Populismo Penal à Luz de Aury Lopes Jr.

A edição da Lei nº 14.155/2021, conforme analisado na seção anterior, inseriu amarras dogmáticas mais severas ao crime de estelionato eletrônico, elevando significativamente as balizas penais abstratas. (BRASIL, 2021) Ocorre que, sob o prisma da criminologia crítica contemporânea, essa incessante atividade legislativa de recrudescimento penal revela uma faceta sintomática do Estado moderno. Em vez de solucionar as causas estruturais da

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

criminalidade cibernética — as quais fincam raízes na exclusão tecnológica —, o poder público recorre à expansão do direito de punir como um mecanismo paliativo de satisfação da opinião pública.

(LOPES JR., 2025).

Essa dinâmica insere-se perfeitamente no conceito que Aury Lopes Jr. (2025) cunha como **populismo penal** ou **Direito Penal Simbólico**. Na obra *Fundamentos do Processo Penal*, o autor adverte que o legislador brasileiro padece de uma crônica "neurose legislativa", operando sob a falsa premissa de que a mera criação de tipos qualificados ou o aumento das penas possui o condão mágico de estancar o fenômeno delitivo. Produz-se, com isso, uma lei simbólica: uma resposta rápida e de forte apelo midiático que gera uma ilusória sensação de segurança jurídica e de eficiência estatal, enquanto a vulnerabilidade fática do cidadão permanece intocada.

No contexto dos crimes cometidos contra o analfabeto digital, a seletividade e a ineficácia desse modelo simbólico tornam-se flagrantes. A exasperação da pena com a criação do parágrafo 2º-A do artigo 171 do Código Penal fundamenta-se na lógica clássica da prevenção geral negativa, isto é, na crença de que o rigor da sanção irá dissuadir o criminoso de praticar o delito. Todavia, a lição criminológica de Lopes Jr. reconduz o debate à realidade empírica, demonstrando o erro metodológico dessa premissa:

> *"O criminoso não calcula a pena com o Código Penal na mão. O fator de dissuasão real não é o quantum da pena cominada em abstrato, mas sim a certeza da punição, a eficácia do aparato investigatório e a probabilidade real de captura. Quando o sistema investigativo é ineficaz, o aumento da pena funciona apenas como um espetáculo pirotécnico legislativo que acalma os ânimos sociais, mas não intimida o infrator." (LOPES JR., 2025).*

Transpondo esse ensinamento para o ambiente virtual, constata-se que o estelionatário cibernético opera sob o manto do anonimato telemático, valendo-se de redes privadas virtuais (VPNs), servidores hospedados em outros países, criptografia de dados e a utilização de dados de terceiros ("laranjas") para ocultar o produto do crime.(PINHEIRO, 2021) O agente delitivo atua com a plena convicção da impunidade, ciente de que o aparato policial e investigativo estatal carece de estrutura tecnológica e de pessoal especializado para rastrear infrações em larga escala no ciberespaço. (LOPES JR., 2025).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Portanto, se a probabilidade de identificação e captura do criminoso virtual é estatisticamente ínfima, torna-se inócua a previsão de uma pena de reclusão de quatro a oito anos; o desvalor da lei abstrata perde-se diante da certeza factual da impunidade.

Ademais, a intervenção do Direito Penal e, por conseguinte, do Processo Penal, caracteriza-se por sua natureza essencialmente retrospectiva e repressiva. O aparato punitivo é desenhado para atuar *ex post facto*, ou seja, somente após a violação do bem jurídico tutelado. É nesse ponto que a lente crítica de Aury Lopes Jr. define o processo penal como um **"ritual tardio"**. Trata-se de uma engrenagem burocrática, morosa e ritualística que se inicia quando a lesão ao patrimônio e à dignidade do indivíduo já se consolidou por completo no plano da realidade.

Para o sujeito afetado pelo analfabetismo digital — frequentemente idosos, aposentados e indivíduos de baixa renda —, o caráter tardio do direito penal assume contornos devastadores. Quando o inquérito policial é instaurado ou a ação penal é proposta, os ativos financeiros subtraídos através do Pix ou de empréstimos consignados fraudulentos já foram pulverizados em uma cadeia infinita de contas bancárias fantasmas, tornando a reparação civil praticamente impossível (CONTELLI, 2022). O idoso hipervulnerável, desprovido do discernimento técnico para repelir a fraude eletrônica no momento de sua execução, assiste ao desfalque de suas economias de subsistência enquanto o Estado lhe oferece, tardiamente, a promessa simbólica de punir um réu muitas vezes inalcançável.

Conclui-se, fundamentando-se na doutrina de Lopes Jr. (2025), que a obsessão pelo punitivismo e o abandono de políticas de prevenção primária representam uma falha estrutural do ordenamento. O foco exclusivo na repressão penal pós-delito mascara a omissão estatal em tutelar preventivamente o vulnerável técnico na Sociedade da Informação. Torna-se imperativo, portanto, retirar o Direito Penal do centro das soluções e deslocar o eixo do debate jurídico para o campo da responsabilidade preventiva, exigindo do Estado e das instituições privadas mecanismos de blindagem tecnológica e letramento digital que impeçam a consumação do engano antes que o "ritual tardio" da sanção se faça necessário.

3.4. Mecanismos de Prevenção Primária: Educação Digital e a Responsabilidade Civil Objetiva das Instituições Financeiras

A constatação de que o aparato repressivo do Estado atua de forma retrospectiva e eminentemente simbólica — conforme as contundentes críticas de Aury Lopes Jr. (2025) analisadas na seção precedente — impõe o deslocamento do eixo de gravidade do debate

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

jurídico. Para além da ilusão protetiva do punitivismo penal, torna-se imperioso arquitetar mecanismos de prevenção primária que neutralizem o estelionato cibernético antes de sua consumação fática.

Essa engenharia preventiva estrutura-se sob dois pilares indissociáveis: as políticas públicas de letramento digital direcionadas à população hipervulnerável e a responsabilização civil objetiva do setor bancário, cujo modelo de negócios impulsionou a digitalização financeira compulsória da sociedade.(PINHEIRO, 2021).

O primeiro pilar assenta-se na necessidade de mitigar o *deficit* cognitivo gerado pelo analfabetismo digital por meio de uma pedagogia pública e inclusiva. Se o meio fraudulento eletrônico adquire contornos de fidedignidade absoluta para o indivíduo desprovido de letramento técnico, a resposta mais eficaz reside em fornecer a este sujeito os instrumentos conceituais para decodificar o engano virtual. Campanhas governamentais de educação financeira e digital devem abandonar a comunicação genérica e focar em diretrizes comportamentais específicas para idosos e vulneráveis, ensinando-os a identificar anomalias sistêmicas, tais como o desvio de URLs, solicitações telefônicas atípicas de dados sigilosos e o caráter irreversível das transações imediatas. (PINHEIRO, 2021).

Ocorre que a transferência da governança das transações econômicas para o ciberespaço não decorreu de uma escolha deliberada do cidadão, mas sim de uma escolha estratégica de eficiência corporativa das grandes corporações bancárias.

Os dados empíricos publicados pela Federação Brasileira de Bancos (FEBRABAN) evidenciam a magnitude dessa migração. Conforme o segundo volume da Pesquisa FEBRABAN de Tecnologia Bancária (2025), as operações realizadas em canais físicos (agências bancárias e caixas eletrônicos) registram quedas contínuas, ao passo que as transações via *mobile banking* consolidaramse de forma absoluta. O ecossistema do Pix, isoladamente, apresentou um crescimento vertiginoso de 41% em relação ao período anterior, alcançando a marca histórica de quase **25 bilhões de operações** concentradas majoritariamente nos canais digitais de dispositivos móveis (FEBRABAN, 2025).

Essa hiperconectividade e aceleração das transações eletrônicas, embora gerem otimização operacional bilionária para as instituições de crédito, expandiram exponencialmente a superfície de ataque para a criminalidade cibernética, tornando o analfabeto digital o alvo preferencial das fraudes em rede. Estudos setoriais repercutidos pela própria plataforma FEBRABAN Tech (2024) apontam que aproximadamente **15,8% dos usuários** entrevistados já foram vítimas diretas de golpes ou fraudes financeiras perpetradas por meio da internet ou de aparelhos celulares.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

Diante desse cenário, a indústria bancária tem elevado sistematicamente seus aportes tecnológicos. O primeiro volume da Pesquisa FEBRABAN de Tecnologia Bancária (2025) revela que as projeções de investimentos totais dos bancos em inovação e tecnologia devem alcançar a cifra histórica de **R$ 47,8 bilhões**, dos quais estima-se que cerca de **R$ 5 bilhões anuais** (aproximadamente 10% do orçamento tecnológico setorial) sejam destinados especificamente ao desenvolvimento de sistemas de tecnologia da informação voltados à segurança e à blindagem cibernética (FEBRABAN, 2025; BRASSCOM, 2025).

A despeito dos vultosos investimentos em *softwares* e ferramentas de segurança da informação, a persistência e a sofisticação das fraudes — que vitimizam quase um sexto dos usuários digitais do país — sinalizam que o aparato corporativo ainda falha em tutelar o consumidor hipervulnerável no momento da transação. É precisamente nesse vácuo que o ordenamento jurídico convoca as normas de Direito Civil e do Consumidor para equilibrar a assimetria técnica. (BRASIL, 1990).

O segundo pilar de prevenção, delineado para solucionar essa assimetria, consolida-se na atribuição jurídica de responsabilidade às instituições financeiras. Essa responsabilização fundamenta-se na Teoria do Risco do Empreendimento, positivada no artigo 14 da Lei nº 8.078/1990 (Código de Defesa do Consumidor). O diploma legal preceitua que o fornecedor de serviços responde de forma objetiva — isto é, independentemente da demonstração de culpa — pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (BRASIL, 1990).

O defeito no serviço bancário eletrônico configura-se quando o sistema de segurança da instituição não obsta movimentações financeiras manifestamente atípicas, desproporcionais e incompatíveis com o perfil socioeconômico de um cliente vulnerável ou idoso, permitindo a imediata pulverização de ativos subtraídos por engenharia social. Essa interpretação dogmática consolidou-se em âmbito nacional por meio da edição da **Súmula nº 479 do Superior Tribunal de Justiça (STJ)**, cujo texto pacifica a matéria ao dispor:

> *"As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias." (STJ, 2012).*

O conceito fundamental cunhado pela Súmula repousa na distinção entre o fortuito externo e o fortuito interno. Enquanto o fortuito externo rompe o nexo de causalidade por se tratar de um evento totalmente alheio à atividade (como uma força da natureza), o fortuito

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

interno compreende todos os riscos inerentes à própria organização e exploração econômica do negócio.

O vazamento de dados que viabiliza a abordagem fraudulenta, a abertura de contas correntes fictícias por falsários ("contas laranjas") utilizadas para o recebimento do produto do estelionato e a fragilidade dos algoritmos de detecção de fraudes em tempo real integram o risco inerente à atividade bancária moderna.

Por conseguinte, a imputação da responsabilidade civil objetiva e integral às instituições financeiras pelas fraudes que atingem o analfabeto digital opera como o mecanismo mais potente de indução econômica à prevenção. Ao transferir o ônus financeiro do prejuízo do elo mais vulnerável da corrente (o indivíduo excluído digitalmente) para o agente econômico detentor dos lucros decorrentes da digitalização, o Direito força o mercado financeiro a desenhar barreiras tecnológicas proativas, sistemas de dupla validação humana e travas de segurança cognitiva aptas a impedir a consolidação do erro do vulnerável, superando de vez a ineficácia retrospectiva da sanção criminal. (BRASIL, 1990; SUPERIOR TRIBUNAL DE JUSTIÇA, 2012).

4. Considerações finais

O presente artigo propôs-se a analisar o analfabetismo digital não apenas como um fenômeno de exclusão social, mas como um vetor fático e jurídico de hipervulnerabilidade no âmbito do Direito Penal contemporâneo, com especial enfoque no crime de estelionato cibernético. Ao término deste percurso acadêmico, resta evidente que a transição abrupta e compulsória das relações civis e econômicas para o ambiente telemático — impulsionada pela busca de eficiência e otimização por parte das instituições financeiras — gerou um contingente de cidadãos marginalizados, cuja ausência de letramento tecnológico os transforma em alvos preferenciais da criminalidade informática.

Em resposta ao influxo inflacionário dos delitos virtuais, o Estado brasileiro editou a Lei nº 14.155/2021, introduzindo a qualificadora da fraude eletrônica (§ 2ºA do artigo 171 do Código Penal). Todavia, a análise dogmática e criminológica empreendida revelou a insuficiência desse modelo. A exegese tradicional que ancora a tipicidade do estelionato na figura abstrata do "homem médio" claudica diante da exclusão tecnológica; artifícios e ardis cibernéticos que se afiguram evidentes ou rudimentares para um usuário digitalmente letrado assumem contornos de fidedignidade intransponível para o analfabeto digital. Por conseguinte,

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 10/06/2026 | aceito: 13/06/2026 | publicação: 16/06/2026

demonstrou-se a necessidade imperiosa de que a idoneidade do meio fraudulento seja aferida em concreto, sopesando a vulnerabilidade tecnocognitiva da vítima.

Ademais, respaldando-se na lente crítica de Aury Lopes Jr., constatou-se que o endurecimento das balizas penais abstratas amolda-se ao fenômeno do populismo penal legislativo. Trata-se de uma resposta meramente simbólica do Estado, que visa aplacar o clamor social e mitigar a sensação de insegurança jurídica, mas que falha estruturalmente em sua função dissuasória. Como os criminosos virtuais operam sob a garantia do anonimato telemático e cientes da defasagem estrutural dos órgãos de investigação penal, o aumento de pena tornase inócuo. O Direito Penal e o processo manifestam-se, assim, como um "ritual tardio": uma burocracia morosa que intervém de forma puramente retrospectiva, quando o patrimônio e a subsistência do vulnerável já foram irremediavelmente pulverizados no ciberespaço.

Frente a esse diagnóstico de ineficácia repressiva, este trabalho responde ao seu problema central ao propor o deslocamento do eixo jurídico da repressão penal pós-delito para os mecanismos de prevenção primária. A proteção efetiva do analfabeto digital não será alcançada por meio de um expansionismo punitivo estéril, mas sim através de uma pedagogia pública de letramento digital aliada à mobilização do instrumental civil e consumerista.

Nesse quadrante, conclui-se que a responsabilização civil objetiva das instituições financeiras, alicerçada na Teoria do Risco do Empreendimento e cristalizada na Súmula nº 479 do Superior Tribunal de Justiça, desponta como o mecanismo mais potente de indução preventiva. Ao imputar o ônus financeiro decorrente das fraudes eletrônicas e da engenharia social ao setor bancário — o qual lucra bilhões com a desmaterialização dos canais de atendimento e o fluxo instantâneo de transações como o Pix —, o ordenamento jurídico constrange o mercado a investir na criação de travas cognitivas, inteligências artificiais preditivas de atipicidade e sistemas proativos de segurança da informação.

Em última análise, salvaguardar o analfabeto digital no ecossistema cibernético é um imperativo de dignidade humana e de justiça social. O progresso tecnológico não pode caminhar dissociado da inclusão e da segurança dos vulneráveis. Espera-se que este trabalho possa contribuir para o debate acadêmico e pretoriano, evidenciando que o papel do Direito na Sociedade da Informação não deve ser o de um espectador tardio armado com sanções ineficazes, mas o de um agente indutor de um ambiente digital ético, protetivo e verdadeiramente democrático.

Referências

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: crimes contra o patrimônio. 20. ed. São Paulo: Saraiva Educação, 2020. v. 3.

BRASIL. [Código de Defesa do Consumidor]. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 7 jun. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, abr. 2014. (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 nov. 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), e a Lei nº 9.296, de 24 de julho de 1996, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou na internet. Brasília, DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20192022/2021/lei/l14155.htm. Acesso em: 6 jun. 2026.

BRASSCOM (Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias em Rede). **Brasil deve investir R$ 104,6 bilhões em cibersegurança até 2028**. São Paulo: Febraban Tech, 2025. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-deve-investir-r-104-6bilhoes-em-ciberseguranca-ate-2028. Acesso em: 7 jun. 2026.

CASTELLS, Manuel. **A Sociedade em Rede** (A Era da Informação: Economia, Sociedade e Cultura - Volume 1). 19. ed. São Paulo: Paz e Terra, 2018.

CETIC.BR (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação). **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – TIC Domicílios 2023**. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Acesso em: 23 mai. 2026.

CONTELLI, Éverson Aparecido. Tragédia PIX - Medidas Assecuratórias per saltum: em busca da efetividade da persecução criminal patrimonial. **Migalhas**, 5 ago. 2022. Disponível em: https://www.migalhas.com.br/depeso/371148/tragedia-pix-medidas-assecuratorias-per-saltum. Acesso em: 12 jun. 2026.

FEBRABAN (Federação Brasileira de Bancos). **Investimento dos bancos em tecnologia deve crescer 13% em 2025 e chegar a R$ 47,8 bilhões**. São Paulo: Portal Febraban, 2025. Disponível em: https://portal.febraban.org.br/noticia/4278/pt-br/. Acesso em: 7 jun. 2026.

FEBRABAN (Federação Brasileira de Bancos). **Pesquisa FEBRABAN de Tecnologia Bancária 2025**: Volume 2. São Paulo: Deloitte, 2025. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_2%20%20VF.pdf. Acesso em: 7 jun. 2026.

FEBRABAN TECH. **Investimento em segurança da informação deve crescer 15% em 2025**. São Paulo: Febraban Tech, 2024. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/investimento-emseguranca-da-informacao-deve-crescer-15-em-2025. Acesso em: 7 jun. 2026.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Pesquisa Nacional por Amostra de Domicílios Contínua**: Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal. Rio de Janeiro: IBGE, 2025. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012agencia-noticias/noticias/44031-internet-chega-a-74-9-milhoes-de-domicilios-dopais-em-2024. Acesso em: 6 jun. 2026.

LOPES JR., Aury. **Fundamentos do Processo Penal**: introdução crítica. 11. ed.

Rio de Janeiro: EMERJ/SRV, 2025. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553625611/. Acesso em: 7 jun. 2026.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 10. ed. rev., atual. e ampl.

Rio de Janeiro: Forense, 2014.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. Rio de Janeiro: Saraiva Jur, 2021.

E-book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/. Acesso em: 6 jun. 2026.

SOUSA, J. **Brasil está no topo do ranking mundial de vítimas de fraudes digitais**. Canaltech, [S. l.], 2025. Disponível em: https://canaltech.com.br/seguranca/brasil-esta-no-topo-do-ranking-mundial-devitimas-de-fraudes-digitais/. Acesso em: 31 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). **Súmula nº 479**. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF: STJ, [2012]. Disponível em: https://scon.stj.jus.br/SCON/.
Acesso em: 7 jun. 2026.