RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

El analfabetismo digital como factor de vulnerabilidad en los delitos de fraude cibernético.

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

Digital Illiteracy as a Vulnerability Factor in Cyber Fraud Crimes

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

Resumen:
La informatización de la sociedad, si bien 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 ancianos, se han visto obligados a utilizar plataformas digitales complejas sin la preparación técnica necesaria, convirtiéndose así en blancos fáciles para los delincuentes. Dado que esta masa de ciudadanos vulnerables se ha convertido en el objetivo predilecto del fraude cibernético (Artículo 171, § 2-A del Código Penal), que explota la buena fe y la falta de conocimiento de sus víctimas, la aparición de inseguridad jurídica y social exige respuestas urgentes del Estado. Este 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 cuando se demuestra que esta condición facilita la "inducción al error" y agrava la reprobabilidad de la conducta del agente. En última instancia, el artículo busca proponer mecanismos de prevención eficaces. Para ello, se realiza una investigación bibliográfica y documental, con un enfoque deductivo, centrada en el análisis de la doctrina penal (en particular, Guilherme Nucci), la legislación vigente (Ley N° 14.155/2021) y el análisis de datos empíricos sobre las competencias digitales de la población. La hipótesis plantea que el enfoque exclusivo del ordenamiento jurídico en la represión criminal es insuficiente, y que la creación de mecanismos de prevención primaria —como la educación digital y la responsabilidad civil de las instituciones— es fundamental para garantizar que la inclusión digital en Brasil sea, de hecho, segura para todos.

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

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

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

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.

1. Introducción

La evolución humana se ha caracterizado cíclicamente por innovaciones que, en cada momento, redefinen los parámetros fundamentales de la convivencia social. La llegada de la llamada "era tecnológica" o "sociedad de la información" representa uno de estos hitos cruciales, en el que la vida de la mayoría de las personas se ha vuelto completamente dependiente de la tecnología. En principio, este avance es innegablemente positivo, ya que democratiza el acceso a la información, optimiza el tiempo, facilita la comunicación global y propicia el surgimiento de modelos de interacción económica y social sin precedentes. Sin embargo, como consecuencia, esta aceleración ha generado graves perjuicios y desigualdades, que afectan principalmente a los ciudadanos que aún no están familiarizados con estos avances.

Desde esta perspectiva, la exclusión digital emerge como la cara oscura de este progreso, creando una nueva categoría de vulnerabilidad social. Las personas que carecen de las habilidades y los conocimientos técnicos mínimos necesarios para desenvolverse en el

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

entorno digital —los llamados «analfabetos digitales»— se encuentran al margen de una sociedad cada vez más conectada, lo que las hace mucho más vulnerables al cibercrimen. Esta vulnerabilidad es particularmente pronunciada en lo que respecta a la seguridad personal y patrimonial, convirtiendo a este segmento de la población en un objetivo principal para las actividades delictivas organizadas, especialmente el fraude cibernético.

La relevancia social y práctica de este escenario se justifica por el hecho de que Brasil se destaca internacionalmente como uno de los *países* más afectados por el fraude digital, victimizando a millones de ciudadanos anualmente. Este delito no afecta el tejido social de manera homogénea; se aprovecha sistemáticamente de la buena fe y la falta de habilidades técnicas de ciertos grupos, con especial énfasis en la población de la tercera edad. Al verse obligados a interactuar con plataformas virtuales complejas para realizar transacciones bancarias cotidianas o acceder a prestaciones sociales esenciales, estas personas enfrentan pérdidas financieras devastadoras que a menudo comprometen su propia subsistencia, además de sufrir profundos daños morales y psicológicos.

Ante esta situación, surge una pregunta crucial: ¿cómo puede el Estado desarrollar e implementar mecanismos eficaces para proteger a las personas con escasa alfabetización digital del fraude y otros ciberdelitos? La respuesta a esta pregunta es fundamental para garantizar que los beneficios de la era de la información sean, de hecho, universales y seguros para todos. Tradicionalmente, las dificultades del Estado para frenar los delitos en el entorno virtual se analizan a la luz de disposiciones como la Ley N° 12.965/2014 (Carta de Derechos de Internet de Brasil). Esta legislación, si bien es fundamental para regular los derechos y garantías en internet, puede terminar limitando la agilidad y eficacia de la acción directa del Estado para combatir el fraude electrónico de manera oportuna.

Sin embargo, desde una perspectiva teórica y criminológica, se observa una brecha en la producción científica nacional, que aún se centra principalmente en el análisis dogmático posterior al delito y la suficiencia del enjuiciamiento penal ("a posteriori"). Es en este vacío donde se inserta la necesaria doctrina crítica de Aury Lopes Jr. y Nucci sobre el Derecho Penal Simbólico. Se demuestra que el enfoque exclusivo del sistema jurídico en la represión criminal y el mero endurecimiento de las penas —como lo ejemplifican los cambios promovidos por la Ley N° 14.155/2021 (Brasil, 2021) en el delito de fraude electrónico— funciona como una respuesta ilusoria y paliativa de las agencias estatales. El agravamiento de la sanción actúa tardíamente, cuando los recursos de los vulnerables ya se han agotado , lo que revela la urgencia de reorientar el debate hacia los mecanismos de prevención primaria y las salvaguardias institucionales antes de que se cometa el delito.

Para orientar esta investigación, el objetivo general es demostrar y verificar críticamente cómo el analfabetismo digital se consolida como un factor fáctico y jurídico de hipervulnerabilidad social y legal . Se busca analizar cómo esta condición disminuye la capacidad de resistencia de la víctima, facilitando su inducción al error en el delito de fraude cibernético (Artículo 171, § 2-A del Código Penal) y, simultáneamente, resaltar la insuficiencia de una respuesta puramente penal del Estado, proponiendo mecanismos preventivos de carácter jurídico y social capaces de brindar protección efectiva a los ciudadanos en la sociedad de la información.

2. Metodología

Para alcanzar los objetivos de esta investigación y resolver el problema científico planteado —que gira en torno a la eficacia protectora del Estado frente a la hipervulnerabilidad de las personas con analfabetismo digital en el delito de fraude cibernético— se adoptó un diseño metodológico de carácter eminentemente teórico y cualitativo. El proceso de investigación se guió por el rigor científico necesario para vincular la doctrina clásica del derecho penal con las transformaciones fácticas de la Sociedad de la Información.

El **método deductivo fue el elegido para regir el razonamiento científico** . Partió de premisas macroestructurales generales —en particular, el concepto sociológico de la Sociedad Red y la transición obligatoria de los servicios financieros a los ecosistemas telemáticos— para, mediante una cadena lógica y silogística de razonamiento, llegar al análisis del fenómeno particular y específico, a saber, la vulnerabilidad tecnocognitiva del individuo excluido digitalmente frente al engaño empleado en el fraude agravado por vía electrónica (Artículo 171, § 2-A del Código Penal).

En cuanto a la naturaleza de la investigación y los objetivos perseguidos, el estudio se califica como **exploratorio y descriptivo** . Exploratorio porque profundiza en un campo jurídico en constante y rápida evolución, cuyas repercusiones sociales exigen nuevas categorías hermenéuticas; y descriptivo porque detalla los elementos normativos del delito de fraude, los contornos de la responsabilidad civil objetiva del consumidor y los datos estadísticos que definen el alcance de la exclusión digital y el cibercrimen en el contexto brasileño contemporáneo.

se utilizó el procedimiento combinado de **investigación bibliográfica y documental** , operando estrictamente sobre fuentes secundarias con confiabilidad y reconocimiento académico/institucional .

- **Investigación bibliográfica:** Consistió en una revisión sistemática y crítica de la literatura jurídica y sociológica pertinente. Se examinaron obras consolidadas sobre derecho penal (Guilherme de Souza Nucci y Cezar Roberto Bitencourt), criminología crítica y procedimiento penal (Aury Lopes Jr.), derecho digital y del consumidor (Patrícia Peck Pinheiro), así como la teoría social clásica de Manuel Castells. La selección de este marco doctrinal siguió criterios de relevancia temática y actualidad, garantizando así la base teórica indispensable para la crítica del Derecho Penal Simbólico.
- **Investigación documental:** Esto implicó el análisis del sistema jurídico nacional vigente, que abarca la Constitución de 1988 de la República Federativa de Brasil, el Código Penal brasileño (con un enfoque analítico en los cambios introducidos por la Ley No. 14.155/2021), el Marco Civil da Internet (Ley No. 12.965/2014), el Código de Protección al Consumidor (Ley No. 8.078/1990) y la declaración del Precedente No. 479 del Tribunal Superior de Justicia.

Además, la investigación documental se enriqueció con la incorporación de **datos estadísticos secundarios de carácter empírico** , extraídos de los informes oficiales más recientes de organismos gubernamentales y entidades sectoriales reconocidas. Se integraron en el texto indicadores cuantitativos de la Encuesta Nacional Continua de Hogares (PNAD) del Instituto Brasileño de Geografía y Estadística (IBGE), encuestas del Centro Regional de Estudios sobre el Desarrollo de la Sociedad de la Información (Cetic.br) y volúmenes consolidados de la Encuesta de Tecnología Bancaria de FEBRABAN. La inclusión de estos datos empíricos tuvo como objetivo contrastar la realidad del analfabetismo digital con la respuesta normativa del Estado.

Finalmente, el método de procesamiento y análisis de los datos recopilados se llevó a cabo mediante **un análisis crítico y explicativo del contenido** . Los textos legales, las construcciones doctrinales y los datos estadísticos no se reprodujeron meramente, sino que se sometieron a un filtro hermenéutico transversal. La dogmática jurídica se contrastó con la criminología fáctica para demostrar las deficiencias del modelo punitivo clásico y fundamentar la urgencia de un cambio de paradigma hacia la prevención primaria y la responsabilidad civil proactiva del mercado financiero.

3. Desarrollo

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

3.1. La sociedad de la información y el fenómeno del analfabetismo digital como exclusión social.

Para comprender el impacto del fraude cibernético en las víctimas vulnerables, es fundamental analizar las transformaciones estructurales que culminaron en la génesis de la denominada Sociedad de la Información. Según el pensamiento sociológico de Castells (2018), la transición global a la «Sociedad Red» ha provocado una profunda mutación en las matrices de poder, economía y convivencia social. La información y la tecnología han dejado de tener una función meramente instrumental para convertirse en la infraestructura misma donde se desarrolla la vida civil. El espacio de los flujos virtuales ha sustituido progresivamente al espacio físico, redefiniendo la dinámica del consumo, el ocio y, fundamentalmente, el acceso a los servicios públicos y financieros.

Sin embargo, el advenimiento de esta nueva era no se produjo bajo el manto de la equidad. La transición al ecosistema hiperconectado puso al descubierto una grave paradoja: si bien la tecnología acortó distancias y democratizó el acceso formal a los datos para una parte significativa de la población, al mismo tiempo profundizó las divisiones sociales preexistentes y estructuró una nueva forma de segregación: la exclusión digital. Castells advierte que, en la sociedad red, la exclusión adquiere proporciones dramáticas, ya que estar desconectado —o ser incapaz de interactuar de forma autónoma con la red— equivale a la invisibilidad social y a la pérdida de las prerrogativas más básicas de la ciudadanía moderna.

exclusión tecnocognitiva se materializa en el fenómeno del analfabetismo digital. Este concepto trasciende la mera ausencia física de dispositivos tecnológicos o infraestructura de conectividad; el analfabetismo digital se caracteriza por la incapacidad de una persona para comprender, interpretar y utilizar de forma segura y crítica las herramientas virtuales que le impone la vida cotidiana. Se trata de un déficit de alfabetización digital , en el que el usuario tiene acceso instrumental superficial (como encender un dispositivo o abrir una aplicación), pero carece de las habilidades necesarias para discernir riesgos, validar la legitimidad de las interfaces virtuales o identificar trampas tendidas por terceros.

La dimensión empírica de este problema se evidencia en los datos estadísticos oficiales. Según los informes consolidados de la Encuesta Nacional Continua de Hogares (PNAD Contínua), publicada por el Instituto Brasileño de Geografía y Estadística (IBGE), si bien la inclusión digital formal de la población de la tercera edad ha aumentado del 44,8% al 69,4%, el contingente que permanece al margen de la red revela la raíz de la exclusión. Entre los millones de brasileños de 60 años o más que declaran no tener acceso a internet, el **66%** señala

explícitamente el desconocimiento de las tecnologías como la razón determinante de su aislamiento digital (IBGE, 2025).

Complementando este diagnóstico, la encuesta nacional **sobre hogares con acceso a las TIC** , realizada por el Centro Regional de Estudios sobre el Desarrollo de la Sociedad de la Información (Cetic.br), demuestra que la mayoría de los no usuarios de internet en Brasil se concentran en el grupo de edad mayor de 60 años, sumando más de 16 millones de personas completamente desconectadas de las habilidades digitales básicas. Paralelamente, el avance vertiginoso de las herramientas de transacciones instantáneas, impulsado por la adopción masiva de Pix, ha provocado que el acceso a los canales bancarios y a las instituciones financieras a través de internet aumente hasta el **71,2% de los usuarios** (IBGE, 2025).

Esta migración rápida, forzada y, en ocasiones, sin orientación pedagógica a los entornos digitales ha creado un escenario de extrema vulnerabilidad, como señala Patricia Peck Pinheiro al hablar de seguridad y educación en la era digital:

> «La evolución tecnológica sin una adecuada aculturación digital y educación preventiva crea una sociedad expuesta a riesgos incalculables. El Derecho Digital exige que la inclusión vaya acompañada de alfabetización digital, ya que simplemente entregar herramientas tecnológicas complejas a personas vulnerables, sin enseñarles medidas de seguridad, equivale a colocarlas en un terreno peligroso sin ningún mecanismo de defensa.» (PINHEIRO, 2021).

Por lo tanto, resulta evidente que la confluencia entre la banca digital obligatoria —intensificada por la desmaterialización de las sucursales físicas— y el analfabetismo digital crónico allana el camino a la victimización masiva. Las personas que carecen de discernimiento tecnológico se ven forzadas a entrar en un mercado de transacciones digitales complejas, operando bajo el riesgo constante de interactuar con ingeniería social fraudulenta.

En este contexto, el analfabetismo digital deja de ser simplemente una cuestión de aislamiento social y adquiere los contornos de una auténtica **hipervulnerabilidad legal** , transformando a las personas mayores y a las técnicamente desfavorecidas en los objetivos preferidos de las organizaciones criminales especializadas en explotar el vacío cognitivo tecnológico, como se detallará en las secciones dogmáticas y criminológicas posteriores de este estudio.

3.2. Ciberfraude: Análisis dogmático, el medio Fraude y creación de la circunstancia calificativa (Ley nº 14.155/2021)

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

El estudio de la victimización de las personas con analfabetismo digital requiere invariablemente un análisis exhaustivo del delito de fraude, tal como se define en el artículo 171 del Código Penal brasileño. Considerado por la doctrina tradicional como el delito de fraude patrimonial por excelencia, el fraude no se comete mediante el uso de violencia o amenazas graves, sino mediante la virulencia del consentimiento inducido en la víctima. El perpetrador induce o mantiene a la víctima en el error, de modo que esta, voluntaria pero engañada, realiza la transferencia financiera perjudicial.

Para que se configure el delito básico, la doctrina penal exige la concurrencia de cuatro elementos fundamentales, vinculados por un doble nexo causal: el uso de medios fraudulentos; la inducción o mantenimiento de la víctima en el error; la obtención de una ventaja ilícita; y el consiguiente daño a otra persona. Según la precisa lección de Guilherme de Souza Nucci (2014), el núcleo del delito reside en la conducta engañosa:

> *El acto de fraude consiste en obtener una ventaja ilícita, en detrimento de otro, induciendo o manteniendo a alguien en el error mediante artificio, engaño o cualquier otro medio fraudulento. El artificio es fraude material (p. ej. , el uso de un documento falso); el engaño es fraude moral o intelectual (p. ej. , conversación engañosa, astucia). El medio fraudulento es la fórmula genérica (procedimiento engañoso de cualquier otra naturaleza).* (Nucci, 2014).

En el ecosistema cibernético, los conceptos tradicionales de artificio y engaño adquieren formas tecnológicas complejas. *El artificio* se materializa mediante la ingeniería de software malicioso, como sitios web clonados de instituciones bancarias legítimas, aplicaciones fraudulentas e hipervínculos engañosos (*phishing*). *El engaño* , por su parte, se manifiesta a través de la ingeniería social, en la que el delincuente, aprovechando el anonimato de la red, adopta una identidad falsa (falsos empleados de seguridad bancaria, familiares simulados en aplicaciones de mensajería) para atrapar a la víctima en una narrativa ficticia altamente creíble.

En este sentido, Cezar Roberto Bitencourt (2020) subraya que, para que el delito de fraude se clasifique como tal, los medios fraudulentos empleados por el perpetrador deben ser adecuados y tener la capacidad concreta de engañar a la persona promedio. Debe existir una relación causal directa entre el fraude y el error:

> *Entre fraude y error debe existir una relación de causa y efecto; es decir, el error debe ser consecuencia directa del fraude. Si el error se origina por una causa distinta a la conducta*

> *fraudulenta del perpetrador, no habrá delito de fraude. Se requiere que los medios empleados sean adecuados para engañar, inducir o mantener a alguien en el error, privándolo de una percepción precisa de la realidad.* (Bitencourt, 2020).

Es precisamente en este punto crucial donde la presente investigación sitúa el punto de inflexión en relación con las personas con analfabetismo digital. El concepto de "hombre común" o "medios fraudulentos adecuados" se vuelve difuso e insuficiente ante la exclusión tecnológica. Un fraude electrónico que para un usuario nativo digital o con conocimientos tecnológicos resulta manifiestamente burdo o fácilmente detectable, adquiere características de absoluta fiabilidad para la persona con analfabetismo digital.

La falta de alfabetización digital impide identificar señales de alerta básicas, como desviaciones en las URL, la ausencia de certificados de seguridad digital o solicitudes atípicas de contraseñas maestras por teléfono. Por consiguiente, es fundamental evaluar de forma concreta la idoneidad de los métodos fraudulentos, teniendo en cuenta la extrema vulnerabilidad de las habilidades técnicas de la víctima.

Consciente de la proliferación masiva de estas conductas en el entorno digital, la legislatura federal promulgó la Ley N° 14.155/2021, que añadió la circunstancia agravante de fraude electrónico al inciso 2-A del artículo 171 del Código Penal. Dicha disposición estipula que la pena será de prisión de 4 a 8 años y multa, en caso de cometerse el fraude.

> *"[...] utilizando información proporcionada por la víctima o por un tercero engañado a través de redes sociales, contactos telefónicos o envío de correos electrónicos fraudulentos, o por cualquier otro medio fraudulento similar."* (BRASIL, 2021).

La creación de esta circunstancia agravante desplazó la atención del fraude común a la devaluación de la conducta digital, reconociendo que el uso de sistemas telemáticos automatizados amplía exponencialmente el alcance del daño y la velocidad de disipación de los activos.

3.3. La respuesta punitiva y la ilusión protectora: el populismo penal a la luz de Aury Lopes Jr.

La promulgación de la Ley N° 14.155/2021, analizada en la sección anterior, introdujo restricciones dogmáticas más severas al delito de fraude electrónico, elevando significativamente los límites abstractos del castigo. (BRASIL, 2021) Sin embargo, desde la

perspectiva de la criminología crítica contemporánea, esta incesante actividad legislativa de creciente severidad penal revela una faceta sintomática del Estado moderno. En lugar de abordar las causas estructurales del ciberdelito —que tienen su origen en la exclusión tecnológica—, las autoridades públicas recurren a la ampliación del derecho a castigar como mecanismo paliativo para satisfacer a la opinión pública.

(LOPES JR., 2025).

Esta dinámica encaja a la perfección con el concepto que Aury Lopes Jr. (2025) denomina **populismo penal** o **derecho penal simbólico** . En su obra **Fundamentos do Processo Penal* (Fundamentos del Proceso Penal*), el autor advierte que el legislador brasileño padece una neurosis legislativa crónica, operando bajo la falsa premisa de que la mera creación de delitos calificados o el aumento de las penas tiene el poder mágico de detener el fenómeno delictivo. Esto produce un derecho simbólico: una respuesta rápida con gran impacto mediático que genera una ilusoria sensación de seguridad jurídica y eficiencia estatal, mientras que la vulnerabilidad real del ciudadano permanece intacta.

En el contexto de los delitos cometidos contra personas con analfabetismo digital, la selectividad e ineficacia de este modelo simbólico se hacen patentes. El aumento de la pena con la creación del apartado 2-A del artículo 171 del Código Penal se basa en la lógica clásica de la prevención general negativa, es decir, en la creencia de que la severidad de la sanción disuadirá al delincuente de cometer el delito. Sin embargo, la lección criminológica de Lopes Jr. devuelve el debate a la realidad empírica, demostrando el error metodológico de esta premisa:

> *El delincuente no calcula la pena con el Código Penal en la mano. El verdadero factor disuasorio no es la cuantía de la pena prescrita en abstracto, sino la certeza del castigo, la eficacia del aparato de investigación y la probabilidad real de captura. Cuando el sistema de investigación es ineficaz, aumentar la pena solo funciona como un espectáculo legislativo pirotécnico que calma las inquietudes sociales, pero no intimida al delincuente. (LOPES JR., 2025).*

Trasladando esta lección al entorno virtual, se observa que el ciberdelincuente opera bajo el manto del anonimato telemático, utilizando redes privadas virtuales (VPN), servidores alojados en otros países, cifrado de datos y el uso de datos de terceros ("intermediarios") para ocultar las ganancias del delito. (PINHEIRO, 2021) El agente criminal actúa con la plena convicción de impunidad, consciente de que la policía estatal y el aparato de investigación

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

carecen de la estructura tecnológica y el personal especializado necesarios para rastrear delitos a gran escala en el ciberespacio. (LOPES JR., 2025).

la predicción de una pena de prisión de cuatro a ocho años pierde sentido ; la devaluación de la ley abstracta se pierde ante la certeza fáctica de la impunidad.

Además, la intervención del Derecho Penal y, por consiguiente, del Procedimiento Penal, se caracteriza por su carácter esencialmente retrospectivo y represivo. El aparato punitivo está diseñado para actuar *ex post facto* , es decir, solo después de la violación del derecho legal protegido. Es en este punto donde la perspectiva crítica de Aury Lopes Jr. define el procedimiento penal como un **«ritual tardío** ». Se trata de un mecanismo burocrático, lento y ritualista que comienza cuando el daño a la propiedad y la dignidad del individuo ya se ha consolidado plenamente en la realidad.

Para quienes sufren analfabetismo digital —a menudo ancianos, jubilados y personas de bajos ingresos— la tardanza en la aplicación de la ley penal adquiere proporciones devastadoras. Para cuando se inicia una investigación policial o se presentan cargos penales, los activos financieros robados a través de Pix (el sistema de pagos instantáneos de Brasil) o préstamos fraudulentos de nómina ya se han dispersado en una cadena interminable de cuentas bancarias fantasma, lo que hace que la reparación civil sea prácticamente imposible (CONTELLI, 2022). Los ancianos, altamente vulnerables y sin la capacidad técnica para rechazar el fraude electrónico en el momento de su ejecución, ven cómo se agotan sus ahorros de subsistencia mientras el Estado, tardíamente, les ofrece la promesa simbólica de castigar a un acusado que a menudo es inaccesible.

En conclusión, según la doctrina de Lopes Jr. (2025), la obsesión por el punitivismo y el abandono de las políticas de prevención primaria representan una falla estructural en el sistema jurídico. El enfoque exclusivo en la represión penal posterior al delito oculta la omisión del Estado de proteger preventivamente a las personas tecnológicamente vulnerables en la Sociedad de la Información. Por lo tanto, es imperativo apartar el Derecho Penal del centro de las soluciones y reorientar el debate jurídico hacia el ámbito de la responsabilidad preventiva, exigiendo al Estado y a las instituciones privadas que implementen mecanismos de protección tecnológica y alfabetización digital que impidan la consumación del engaño antes de que se haga necesario el "ritual tardío" de la sanción.

3.4. Mecanismos de prevención primaria: Educación digital y responsabilidad objetiva de las instituciones financieras

La constatación de que el aparato represivo del Estado actúa de manera retrospectiva y eminentemente simbólica —como señalan las contundentes críticas de Aury Lopes Jr. (2025), analizadas en la sección anterior— exige un cambio en el centro del debate jurídico. Más allá de la ilusión protectora del punitivismo penal, resulta imperativo diseñar mecanismos de prevención primaria que neutralicen el fraude cibernético antes de su consumación.

Esta ingeniería preventiva se estructura sobre dos pilares inseparables: las políticas públicas de alfabetización digital dirigidas a la población hipervulnerable y la responsabilidad civil objetiva del sector bancario, cuyo modelo de negocio ha impulsado la digitalización financiera obligatoria de la sociedad. (PINHEIRO, 2021).

El primer pilar se basa en la necesidad de mitigar el *déficit.* El deterioro cognitivo derivado del analfabetismo digital puede abordarse mediante la educación pública e inclusiva. Si los medios electrónicos fraudulentos adquieren una apariencia de absoluta fiabilidad para las personas con escasa alfabetización digital, la respuesta más eficaz consiste en proporcionarles las herramientas conceptuales necesarias para detectar el engaño virtual. Las campañas gubernamentales de educación financiera y digital deberían abandonar la comunicación genérica y centrarse en directrices de comportamiento específicas para las personas mayores y vulnerables, enseñándoles a identificar anomalías sistémicas como la distorsión de URL, las solicitudes telefónicas atípicas de datos confidenciales y la naturaleza irreversible de las transacciones instantáneas. (PINHEIRO, 2021).

Lo cierto es que la transferencia de la gobernanza de las transacciones económicas al ciberespacio no fue resultado de una decisión deliberada de los ciudadanos, sino más bien de una elección estratégica en aras de la eficiencia corporativa por parte de las grandes corporaciones bancarias.

Los datos empíricos publicados por la Federación Brasileña de Bancos (FEBRABAN) ponen de manifiesto la magnitud de esta migración. Según el segundo volumen de la Encuesta de Tecnología Bancaria de FEBRABAN (2025), las transacciones realizadas a través de canales físicos (sucursales bancarias y cajeros automáticos) muestran un descenso continuo, mientras que las transacciones mediante *banca móvil van en aumento.* Se han consolidado por completo. El ecosistema Pix, de forma aislada, mostró un crecimiento vertiginoso del 41% en comparación con el período anterior, alcanzando la cifra histórica de casi **25 mil millones de operaciones** concentradas principalmente en canales digitales de dispositivos móviles (FEBRABAN, 2025).

Esta hiperconectividad y aceleración de las transacciones electrónicas, si bien genera miles de millones en optimización operativa para las entidades de crédito, ha expandido

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

exponencialmente la superficie de ataque para el cibercrimen, convirtiendo a las personas con escasa alfabetización digital en el objetivo predilecto del fraude en línea. Estudios sectoriales publicados por la propia plataforma FEBRABAN Tech (2024) indican que aproximadamente el **15,8 % de los usuarios** encuestados ya han sido víctimas directas de estafas o fraudes financieros perpetrados a través de internet o dispositivos móviles.

Ante este panorama, el sector bancario ha incrementado sistemáticamente sus inversiones tecnológicas. El primer volumen de la Encuesta de Tecnología Bancaria de FEBRABAN (2025) revela que las proyecciones de inversión total de los bancos en innovación y tecnología deberían alcanzar la cifra histórica de **R$ 47.800 millones** , de los cuales se estima que alrededor de **R$ 5.000 millones anuales** (aproximadamente el 10% del presupuesto tecnológico del sector) se destinarán específicamente al desarrollo de sistemas de tecnología de la información enfocados en seguridad y ciberseguridad (FEBRABAN, 2025; BRASSCOM, 2025).

A pesar de las importantes inversiones en *software* y herramientas de seguridad informática, la persistencia y sofisticación del fraude —que victimiza a casi una sexta parte de los usuarios digitales del país— indican que el aparato empresarial aún no logra proteger al consumidor, altamente vulnerable , en el momento de la transacción. Es precisamente ante este vacío que el sistema jurídico recurre a las normas del Derecho Civil y del Derecho del Consumidor para equilibrar la asimetría técnica. (BRASIL, 1990).

El segundo pilar de la prevención, diseñado para abordar esta asimetría, se consolida en la atribución legal de responsabilidad a las instituciones financieras. Esta responsabilidad se fundamenta en la Teoría del Riesgo Empresarial, consagrada en el artículo 14 de la Ley n.º 8.078/1990 (Código de Protección al Consumidor). Dicho instrumento legal estipula que el prestador del servicio es objetivamente responsable —es decir, independientemente de la prueba de culpa— de la reparación de los daños causados a los consumidores por defectos relacionados con la prestación de servicios, así como por información insuficiente o inadecuada sobre su uso y riesgos (BRASIL, 1990).

Se produce un defecto en los servicios de banca electrónica cuando el sistema de seguridad de la institución no logra impedir transacciones financieras manifiestamente atípicas, desproporcionadas e incompatibles con el perfil socioeconómico de un cliente vulnerable o anciano, permitiendo la inmediata dispersión de activos robados mediante ingeniería social. Esta interpretación dogmática se ha consolidado a nivel nacional mediante la emisión del **Precedente N° 479 del Tribunal Superior de Justicia (TSJ)** , cuyo texto zanja la cuestión al afirmar:

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 10/06/2026 | Aceptado: 13/06/2026 | Publicación: 16/06/2026

> *"Las entidades financieras son objetivamente responsables de los daños causados por sucesos fortuitos internos relacionados con el fraude y los delitos cometidos por terceros en el ámbito de las operaciones bancarias." (STJ, 2012).*

El concepto fundamental que plantea el Resumen se basa en la distinción entre eventos fortuitos externos e internos. Mientras que los eventos fortuitos externos rompen el vínculo causal, ya que son sucesos completamente ajenos a la actividad (como un fenómeno natural), los eventos fortuitos internos abarcan todos los riesgos inherentes a la organización y la explotación económica de la propia empresa.

Las filtraciones de datos que permiten prácticas fraudulentas, la apertura de cuentas corrientes ficticias por parte de los estafadores ("cuentas ficticias") utilizadas para recibir el producto del fraude y la fragilidad de los algoritmos de detección de fraude en tiempo real son riesgos inherentes a la banca moderna.

Por lo tanto, imputar responsabilidad civil objetiva y plena a las instituciones financieras por el fraude que afecta a las personas con escasa alfabetización digital constituye el mecanismo más eficaz de incentivo económico para la prevención. Al transferir la carga financiera de la pérdida del eslabón más vulnerable de la cadena (la persona excluida digitalmente) al agente económico que se beneficia de la digitalización, la ley obliga al mercado financiero a diseñar barreras tecnológicas proactivas, sistemas de doble validación humana y salvaguardias de seguridad cognitiva capaces de prevenir la consolidación del error de la parte vulnerable, superando definitivamente la ineficacia retroactiva de las sanciones penales. (BRASIL, 1990; TRIBUNAL SUPERIOR DE JUSTICIA, 2012).

4. Consideraciones finales

Este artículo tuvo como objetivo analizar el analfabetismo digital no solo como un fenómeno de exclusión social, sino también como un vector fáctico y jurídico de hipervulnerabilidad en el marco del Derecho Penal contemporáneo, con especial énfasis en el delito de fraude cibernético. Al final de este recorrido académico, resulta evidente que la transición abrupta y obligatoria de las relaciones civiles y económicas al entorno telemático —impulsada por la búsqueda de eficiencia y optimización por parte de las instituciones financieras— ha generado un contingente de ciudadanos marginados cuya falta de alfabetización tecnológica los convierte en blancos fáciles para el cibercrimen.

En respuesta al aumento vertiginoso de los ciberdelitos, el Estado brasileño promulgó la Ley N° 14.155/2021, que introduce la circunstancia agravante de fraude electrónico (§ 2A del artículo 171 del Código Penal). Sin embargo, el análisis dogmático y criminológico realizado reveló la insuficiencia de este modelo. La interpretación tradicional que basa la tipicidad del fraude en la figura abstracta de la "persona promedio" flaquea ante la exclusión tecnológica; los artificios y trucos cibernéticos que parecen evidentes o rudimentarios para un usuario con conocimientos digitales adquieren contornos de fiabilidad insuperable para el analfabeto digital. En consecuencia, se demostró la necesidad imperiosa de evaluar concretamente la idoneidad de los medios fraudulentos, ponderando la vulnerabilidad tecnocognitiva de la víctima .

Además, desde la perspectiva crítica de Aury Lopes Jr., se constató que el endurecimiento de las directrices penales abstractas se ajusta al fenómeno del populismo penal legislativo. Se trata de una respuesta meramente simbólica del Estado, destinada a apaciguar la indignación social y mitigar la sensación de inseguridad jurídica, pero que estructuralmente fracasa en su función disuasoria. Dado que los ciberdelincuentes operan bajo la garantía del anonimato telemático y son conscientes de las deficiencias estructurales de los órganos de investigación criminal, el aumento de las penas se vuelve... inocuo . El derecho penal y el proceso legal se manifiestan así como un "ritual tardío": una burocracia lenta que interviene de forma puramente retrospectiva, cuando los bienes y el sustento de los vulnerables ya han sido pulverizados irrevocablemente en el ciberespacio.

Ante este diagnóstico de ineficacia represiva, este trabajo aborda su problema central proponiendo un cambio en el enfoque jurídico, pasando de la represión penal posterior al delito a los mecanismos de prevención primaria. La protección efectiva de las personas con analfabetismo digital no se logrará mediante un expansionismo punitivo estéril, sino a través de una pedagogía pública de la alfabetización digital combinada con la movilización de herramientas de protección civil y del consumidor.

En este contexto, se puede concluir que la responsabilidad objetiva de las instituciones financieras, basada en la Teoría del Riesgo Empresarial y consagrada en el Precedente N.º 479 del Tribunal Superior de Justicia, emerge como el mecanismo más eficaz de disuasión preventiva. Al imputar la carga financiera derivada del fraude electrónico y la ingeniería social al sector bancario —que obtiene miles de millones de beneficios gracias a la desmaterialización de los canales de servicio y al flujo instantáneo de transacciones como Pix—, el ordenamiento jurídico obliga al mercado a invertir en la creación de salvaguardias cognitivas, inteligencia

artificial predictiva para la detección de situaciones atípicas y sistemas proactivos de seguridad de la información.

En definitiva, salvaguardar a las personas con escasa alfabetización digital en el ecosistema cibernético es un imperativo de dignidad humana y justicia social. El progreso tecnológico no puede avanzar desvinculado de la inclusión y la seguridad de las personas vulnerables. Se espera que este trabajo contribuya al debate académico y jurídico, demostrando que el papel del Derecho en la Sociedad de la Información no debe ser el de un mero espectador con sanciones ineficaces, sino el de un agente que promueva un entorno digital ético, protector y verdaderamente democrático.

Referencias

BITENCOURT, Cezar Roberto. **Tratado de derecho penal** : delitos contra la propiedad. 20ª edición. São Paulo: Saraiva Educação, 2020. v.3.

BRASIL. [Código de Protección al Consumidor]. **Ley N° 8.078, del 11 de septiembre, 1990.** Establece medidas de protección al consumidor y otras medidas. Brasilia, DF: Presidencia de la República, 1990. Disponible en: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm . Consultado el 7 de junio de 2026.

BRASIL. **Ley N° 12.965, de 23 de abril de 2014.** Establece principios, garantías, derechos y deberes para el uso de Internet en Brasil. Gaceta Oficial de la Unión, Brasilia, DF, abril de 2014. (Marco Civil da Internet). Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Consultado el: 3 de noviembre de 2025 .

BRASIL. **Ley N° 14.155, del 27 de mayo de 2021.** Modifica el Decreto Ley N° 2.848, del 7 de diciembre de 1940 (Código Penal), el Decreto Ley N° 3.689, del 3 de octubre de 1941 (Código de Procedimiento Penal) y la Ley N° 9.296, del 24 de julio de 1996, para agravar los delitos de violación de dispositivos informáticos, hurto y fraude cometidos electrónicamente o en internet. Brasilia, DF: Presidencia de la República, 2021. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato20192022/2021/lei/l14155.htm . Consultado el 6 de junio de 2026.

(Asociación de Empresas de Tecnologías de la Información y la Comunicación y de Redes). Brasil **debería invertir R$ 104.600 millones en ciberseguridad para** 2028. São Paulo : Febraban Tech , 2025. Disponible en : https://febrabantech.febraban.org.br/temas/seguranca/brasil-deve-investir-r-104-6-bilhoes-em-ciberseguranca-ate-2028 . Consultado el 7 de junio de 2026 .

CASTELLS, Manuel. **La Sociedad Red** (La Era de la Información: Economía, Sociedad y Cultura - Volumen 1). 19ª edición. São Paulo: Paz e Terra, 2018.

CETIC.BR (Centro Regional de Estudios sobre el Desarrollo de la Sociedad)

Información). **Investigación sobre el uso de las tecnologías de la información y**

Comunicación en los hogares brasileños – Hogares con TIC 2023. São Paulo:

Comité Directivo de Internet en Brasil, 2024. Consultado el 23 de mayo de 2026.

CONTELLI, Éverson Aparecido. Tragedia PIX - Medidas cautelares per saltum : en busca de la efectividad de la persecución penal patrimonial. **Migalhas , 5** de agosto de 2022. Disponible en: https://www.migalhas.com.br/depeso/371148/tragedia-pix-medidas-assecuratorias-per-saltum . Consultado el 12 de junio de 2026 .

FEBRABAN (Federación Brasileña de Bancos). **Se espera que la inversión bancaria en tecnología crezca un 13% en 2025, alcanzando los R$ 47.800 millones** . São Paulo: Portal Febraban, 2025. Disponible en: https://portal.febraban.org.br/noticia/4278/pt-br/ . Consultado el : 7 de junio de 2026.

FEBRABAN (Federación Brasileña de Bancos). **Encuesta sobre Tecnología Bancaria de FEBRABAN 2025** : Volumen 2. São Paulo: Deloitte, 2025. Disponible en: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_2%20%20VF.pdf . Consultado el 7 de junio de 2026 .

FEBRABAN TECH. La inversión en **seguridad de la información debería crecer un 15% en 2025.** São Paulo : Febraban Tech, 2024. Disponible en : https://febrabantech.febraban.org.br/temas/seguranca/investimento-em-seguranca-da-informacao-dev-crescer-15-em-2025 . Consultado el 7 de junio de 2026 .

Instituto Brasileño de Geografía y Estadística (IBGE). Encuesta **Nacional** Continua por Muestreo de Hogares : Acceso a internet y televisión y posesión de teléfonos móviles para uso personal . Río de Janeiro : IBGE , 2025. Disponible en : https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-noticias/noticias/44031-internet-chega-a-74-9-millones-de-domicilios-do-pais-em-2024 . Consultado el 6 de junio de 2026 .

LOPES JR., Aury. **Fundamentos del procedimiento penal** : una introducción crítica. 11.ª ed.

Río de Janeiro: EMERJ/SRV, 2025. Libro electrónico. Disponible en: https://integrada.minhabiblioteca.com.br/reader/books/9788553625611/ . Consultado el: 7 de junio de 2026.

NUCCI, Guilherme de Souza. **Manual de Derecho Penal** . 10.ª ed. revisada, actualizada y ampliada .

Río de Janeiro: Forense, 2014.

PINHEIRO, Patricia Peck. **Derecho Digital** . 7ª edición. Río de Janeiro: Saraiva Jur , 2021.

Libro electrónico. Disponible en: https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/ . Consultado el 6 de junio de 2026.

SOUSA, J. **Brasil encabeza el ranking mundial de víctimas de fraude digital** . Canaltech , [S. l.], 2025. Disponible en: https://canaltech.com.br/seguranca/brasil - esta - no - topo - do - ranking - mundial - de vitimas - de - fraudes - digitais/ . Consultado el: 31 de octubre de 2025.

TRIBUNAL SUPERIOR DE JUSTICIA (Brasil). **Resumen n.° 479.** Las entidades financieras son objetivamente responsables de los daños causados por hechos fortuitos internos relacionados con fraudes y delitos cometidos por terceros en el ámbito de las operaciones bancarias. Brasilia, DF: STJ, [2012]. Disponible en: https://scon.stj.jus.br/SCON/ .
Consultado el 7 de junio de 2026.