RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

Digital Illiteracy as a Vulnerability Factor in Cyber Fraud Crimes

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

El Analfabetismo Digital como Factor de Vulnerabilidad en los Delitos de Estafa Cibernética

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

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, § 2-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 article 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 .

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.

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. Introduction

Human evolution has been cyclically marked by innovations that, at each moment, redefine the fundamental parameters for social coexistence. The arrival of the so-called "technological age" or "information society" represents one of these dividing milestones, in which most of people's lives have become completely connected to and dependent on technology. From an initial point of view, this advancement is undeniably positive, providing the democratization of access to information, the optimization of time, the facilitation of global communication, and the emergence of unprecedented economic and social interaction models. However, collaterally, this acceleration has ended up bringing severe harm and disparities, mainly affecting citizens who are not yet familiar with such advancements.

From this perspective, digital exclusion emerges as a dark side of this progress, creating a new category of social vulnerability. Individuals who lack the minimum skills and technical

knowledge necessary to navigate the online environment—the so-called "digital illiterates"—find themselves on the margins of an increasingly connected society, a factor that makes them drastically more susceptible to cybercrime. This vulnerability is particularly pronounced with regard to personal and property security, transforming this segment of the population into a prime target for organized criminal activities, especially cyber fraud.

The social and practical relevance of this scenario is justified by the fact that Brazil stands out internationally at the top of the *ranking* of nations most affected by digital fraud, victimizing millions of citizens annually. This crime does not affect the social fabric homogeneously; it systematically takes advantage of the good faith and lack of technical skills of certain groups, with particular emphasis on the elderly population. When compelled to interact with complex virtual platforms to carry out everyday banking transactions or to access essential welfare benefits, these individuals face devastating financial losses that often compromise their very subsistence, in addition to suffering profound moral and psychological damage.

Given this situation, an imperative question arises: how can the State develop and implement effective mechanisms to protect the digitally illiterate from fraud and other cybercrimes? The answer to this question is crucial to ensuring that the benefits of the information age are, in fact, universal and safe for all. Traditionally, the State's difficulties in curbing criminal offenses in the virtual environment are investigated in light of provisions such as Law No. 12.965/2014 (Brazilian Internet Bill of Rights). This legislation, while fundamental for regulating rights and guarantees on the internet, may end up limiting the agility and effectiveness of direct State action in repelling electronic fraud in a timely manner.

However, from a theoretical and criminological perspective, a gap is observed in national scientific production, which still focuses mainly on post-crime dogmatic analysis and the sufficiency of criminal prosecution ("afterwards"). It is in this vacuum that the necessary critical doctrine of Aury Lopes Jr. and Nucci on Symbolic Criminal Law is inserted. It is demonstrated that the exclusive focus of the legal system on criminal repression and the mere hardening of penalties—as exemplified by the changes promoted by Law No. 14.155/2021 (Brazil, 2021) in the crime of electronic fraud—functions as an illusory and palliative response from state agencies. The aggravation of the sanction acts belatedly, when the assets of the vulnerable have already been depleted , revealing the urgency of shifting the debate to primary prevention mechanisms and institutional safeguards before the crime is committed.

To guide this investigation, the general objective is to demonstrate and critically verify how digital illiteracy consolidates itself as a factual and legal factor of social and legal hyper-

vulnerability . The aim is to analyze how this condition mitigates the victim's capacity for resistance, facilitating their inducement to error in the crime of cyber fraud (Article 171, § 2-A of the Penal Code), and, simultaneously, to highlight the insufficiency of a purely penal response from the State, proposing preventive mechanisms of a legal and social nature capable of providing effective protection to citizens in the information society.

2. Methodology

To achieve the objectives outlined in this investigation and to resolve the proposed scientific problem—which revolves around the protective effectiveness of the State in the face of the hyper-vulnerability of the digitally illiterate in the crime of cyber fraud—a methodological design of an eminently theoretical and qualitative nature was adopted. The investigative process was guided by the scientific rigor necessary to link classical criminal law doctrine to the factual transformations of the Information Society.

The chosen approach to govern scientific reasoning was the **deductive method** . It started from general macrostructural premises—notably the sociological concept of the Network Society and the compulsory transition of financial services to telematic ecosystems—to, through a logical and syllogistic chain of reasoning, arrive at the analysis of the particular and specific phenomenon, namely, the technocognitive vulnerability of the digitally excluded individual in the face of the trickery employed in aggravated fraud through electronic fraud (Article 171, § 2-A of the Penal Code).

Regarding the nature of the research and the objectives pursued, the study qualifies as **exploratory and descriptive** . Exploratory because it delves into a constantly and rapidly changing legal field, whose social repercussions demand new hermeneutical categories; and descriptive because it details the normative elements of the crime of fraud, the contours of objective consumer civil liability, and the statistical data that define the extent of digital exclusion and cybercrime in the contemporary Brazilian scenario.

bibliographic and documentary research was used , operating strictly on secondary sources with reliability and academic/institutional recognition .

- **Bibliographic Research:** This consisted of a systematic and critical review of relevant legal and sociological literature. Established works on criminal law (Guilherme de Souza Nucci and Cezar Roberto Bitencourt), critical criminology and criminal procedure (Aury Lopes Jr.), Digital and Consumer Law (Patrícia Peck Pinheiro), as well as the classical social theory of

Manuel Castells, were examined. The selection of this doctrinal framework followed criteria of thematic relevance and timeliness, ensuring the indispensable theoretical foundation for the critique of Symbolic Criminal Law.

- **Documentary Research:** This involved analyzing the current national legal system, encompassing the 1988 Constitution of the Federative Republic of Brazil, the Brazilian Penal Code (with an analytical focus on the changes introduced by Law No. 14.155/2021), the Marco Civil da Internet (Law No. 12.965/2014), the Consumer Protection Code (Law No. 8.078/1990), and the statement of Precedent No. 479 of the Superior Court of Justice.

Furthermore, the documentary research was enriched by the incorporation of **secondary statistical data of an empirical nature** , extracted from the most recent official reports of government agencies and recognized sectoral class entities. Quantitative indicators from the Continuous National Household Sample Survey (PNAD) of the Brazilian Institute of Geography and Statistics (IBGE), surveys from the Regional Center for Studies on the Development of the Information Society (Cetic.br), and consolidated volumes of the FEBRABAN Banking Technology Survey were amalgamated into the text. The inclusion of this empirical data aimed to contrast the factual reality of digital illiteracy with the normative response given by the State.

Finally, the method of processing and analyzing the collected data was carried out through **critical and explanatory content analysis** . Legal texts, doctrinal constructions, and statistical data were not merely reproduced, but rather subjected to a cross-hermeneutical filter. Legal dogmatics were confronted with factual criminology to demonstrate the inadequacies of the classic punitive model and to substantiate the urgency of a paradigm shift towards primary prevention and proactive civil liability of the financial market.

3. Development

3.1. The Information Society and the Phenomenon of Digital Illiteracy as Social Exclusion

To understand the impact of cyber fraud on vulnerable victims, it is essential to map the structural transformations that culminated in the genesis of the so-called Information Society. According to Castells' sociological thought (2018), the global transition to the "Network Society" has brought about a profound mutation in the matrices of power, economy, and social coexistence. Information and technology have ceased to occupy a merely instrumental function and have become the very infrastructure where civil life takes place. The space of virtual flows

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

has progressively replaced the space of physical places, redefining the dynamics of consumption, leisure, and, fundamentally, access to public and financial services.

However, the advent of this new era did not occur under the mantle of equity. The transition to the hyper-connected ecosystem exposed a severe paradox: while technology shortened distances and democratized formal access to data for a significant portion of the population, it simultaneously deepened pre-existing social divides and structured a new form of segregation: digital exclusion. Castells warns that in the network society, exclusion takes on dramatic proportions, since being disconnected—or being unable to interact autonomously with the network—is equivalent to social invisibility and the loss of the most basic prerogatives of modern citizenship.

technocognitive exclusion is embodied in the phenomenon of digital illiteracy. This concept transcends the mere physical absence of technological devices or connectivity infrastructure; digital illiteracy is characterized by an individual's inability to understand, interpret, and operate safely and critically the virtual tools imposed on them by daily life. It is a digital literacy deficit , in which the user has instrumental surface access (such as turning on a device or launching an application), but lacks the necessary skills to discern risks, validate the legitimacy of virtual interfaces, or identify traps set by third parties.

The empirical dimension of this problem is evidenced by official statistical data. According to consolidated reports from the Continuous National Household Sample Survey (PNAD Contínua), published by the Brazilian Institute of Geography and Statistics (IBGE), although the formal digital inclusion of the elderly population has jumped from 44.8% to 69.4%, the contingent that remains on the margins of the network reveals the core of the exclusion. Among the millions of Brazilians aged 60 or older who declare that they do not access the internet, **66%** explicitly point to "not knowing how to use technology" as the determining reason for their digital isolation (IBGE, 2025).

Complementing this diagnosis, the national **ICT Households survey** , conducted by the Regional Center for Studies on the Development of the Information Society (Cetic.br), demonstrates that the majority of non-internet users in Brazil are concentrated in the age group over 60 years old, totaling more than 16 million individuals completely detached from basic digital skills. Concomitantly, the meteoric advance of instant transaction tools, spearheaded by the mass adoption of Pix, has caused access to banking channels and financial institutions via the internet to jump to **71.2% of users** (IBGE, 2025).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

This rapid, forced, and sometimes pedagogically unguided migration to digital environments has created a scenario of extreme vulnerability, as Patricia Peck Pinheiro points out when discussing security and education in the digital age:

> "Technological evolution without proper digital acculturation and preventive education creates a society exposed to immeasurable risks. Digital Law demands that inclusion be accompanied by literacy, because simply handing over complex technological tools to vulnerable individuals, without teaching them security safeguards, is equivalent to placing them in an arena of danger without any defense mechanism." (PINHEIRO, 2021).

It is therefore evident that the confluence between mandatory digital banking—intensified by the dematerialization of physical branches—and chronic digital illiteracy paves the way for mass victimization. Individuals lacking technological discernment are forcibly inserted into a market of complex digital transactions, operating under the constant risk of interacting with fraudulent social engineering.

In this context, digital illiteracy ceases to be merely a matter of social isolation and takes on the contours of genuine **legal hyper-vulnerability** , transforming the elderly and the technically disadvantaged into the preferred targets of criminal organizations specialized in exploiting the technological cognitive vacuum, as will be detailed in the subsequent dogmatic and criminological sections of this study.

3.2. Cyber Fraud: Dogmatic Analysis, the Medium Fraudulent and creation of the Qualifying Circumstance (Law No. 14.155/2021)

The study of the victimization of the digitally illiterate invariably requires a dogmatic dissection of the crime of fraud, as defined in Article 171 of the Brazilian Penal Code. Considered by traditional doctrine as the quintessential fraudulent property crime, fraud is not committed through the use of violence or serious threat, but rather through a vitiation of consent induced in the victim. The perpetrator induces or maintains the victim in error so that the latter, voluntarily but deceived, makes the harmful financial transfer.

For the basic type of crime to be established, criminal doctrine requires the concurrence of four fundamental elements, which are linked in a double causal nexus: the use of fraudulent means; the inducement or maintenance of the victim in error; the obtaining of an illicit

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

advantage; and the consequent harm to another. According to the precise lesson of Guilherme de Souza Nucci (2014), the core of the criminal type lies in the deceptive conduct:

> *"The act of fraud consists of obtaining an illicit advantage, to the detriment of another, by inducing or maintaining someone in error, through artifice, trickery, or any other fraudulent means. Artifice is material fraud (e.g. , the use of a false document); trickery is moral or intellectual fraud (e.g. , deceptive conversation, cunning). The fraudulent means is the generic formula (deceptive procedure of any other nature)."* (Nucci, 2014).

In the cyber ecosystem, the traditional concepts of artifice and trickery take on complex technological forms. *Artifice* materializes through malicious software engineering, such as cloned websites of legitimate banking institutions, fraudulent applications, and deceptive hyperlinks (*phishing*). *Trickery* , in turn, manifests itself through social engineering, in which the criminal, taking advantage of the anonymity of the network, adopts a false identity (fake bank security support employees, simulated relatives in messaging applications) to ensnare the victim in a highly believable fictional narrative.

In this vein, Cezar Roberto Bitencourt (2020) emphasizes that, for the crime of fraud to be classified as such, the fraudulent means adopted by the perpetrator must be suitable and have the concrete capacity to deceive the average person. There must be a direct causal relationship between the fraud and the error:

> *"Between fraud and error there must be a cause-and-effect relationship, that is, the error must be the direct consequence of the fraud. If the error stems from a cause other than the fraudulent conduct of the perpetrator, there will be no crime of fraud. It is required that the means employed be suitable to deceive, induce or maintain someone in error, depriving them of the accurate perception of reality."* (Bitencourt, 2020).

It is precisely at this dogmatic junction that the present investigation locates the breaking point in relation to the digitally illiterate. The concept of "average man" or "suitable fraudulent means" becomes diffuse and insufficient when confronted with technological exclusion. An electronic fraud that appears manifestly crude or easily detectable to a digitally native or technologically literate user takes on contours of absolute reliability for the individual affected by digital illiteracy.

The lack of literacy prevents the identification of basic warning signs, such as URL deviations, lack of digital security certificates, or atypical requests for master passwords over

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

the phone. Consequently, the suitability of the fraudulent means must be assessed concretely, considering the hyper-vulnerability of the victim's technical skills.

Aware of the massive proliferation of these behaviors in the online environment, the federal legislature enacted Law No. 14,155/2021, which added the aggravating circumstance of electronic fraud to § 2-A of Article 171 of the Penal Code. The provision stipulates that the penalty will be imprisonment for 4 to 8 years, and a fine, if the fraud is committed:

> *"[...] using information provided by the victim or by a third party misled through social networks, telephone contacts or sending fraudulent emails, or by any other similar fraudulent means."* (BRAZIL, 2021).

The creation of this aggravating circumstance shifted the focus from common fraud to the devaluation of digital conduct, recognizing that the use of automated telematic systems exponentially expands the scope of the damage and the speed of asset dissipation.

3.3. The Punitive Response and the Protective Illusion: Penal Populism in the Light of Aury Lopes Jr.

The enactment of Law No. 14,155/2021, as analyzed in the previous section, introduced more severe dogmatic constraints on the crime of electronic fraud, significantly raising the abstract penal boundaries. (BRAZIL, 2021) However, from the perspective of contemporary critical criminology, this incessant legislative activity of increasing penal severity reveals a symptomatic facet of the modern State. Instead of addressing the structural causes of cybercrime—which are rooted in technological exclusion—the public authorities resort to expanding the right to punish as a palliative mechanism to satisfy public opinion.

(LOPES JR., 2025).

This dynamic fits perfectly into the concept that Aury Lopes Jr. (2025) coins as **penal populism** or **symbolic criminal law** . In his work **Fundamentos do Processo Penal* (Fundamentals of Criminal Procedure*), the author warns that the Brazilian legislator suffers from a chronic "legislative neurosis," operating under the false premise that the mere creation of qualified offenses or the increase in penalties has the magical power to stop the phenomenon of crime. This produces a symbolic law: a quick response with strong media appeal that generates an illusory sense of legal security and state efficiency, while the factual vulnerability of the citizen remains untouched.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

In the context of crimes committed against the digitally illiterate, the selectivity and ineffectiveness of this symbolic model become blatant. The increase in punishment with the creation of paragraph 2-A of article 171 of the Penal Code is based on the classic logic of negative general prevention, that is, on the belief that the severity of the sanction will dissuade the criminal from committing the crime. However, the criminological lesson of Lopes Jr. brings the debate back to empirical reality, demonstrating the methodological error of this premise:

> *"The criminal does not calculate the sentence with the Penal Code in hand. The real deterrent factor is not the quantum of the sentence prescribed in the abstract, but rather the certainty of punishment, the effectiveness of the investigative apparatus, and the real probability of capture. When the investigative system is ineffective, increasing the sentence only functions as a legislative pyrotechnic spectacle that calms social anxieties, but does not intimidate the offender." (LOPES JR., 2025).*

Translating this lesson to the virtual environment, it is observed that the cyber fraudster operates under the cloak of telematic anonymity, making use of virtual private networks (VPNs), servers hosted in other countries, data encryption, and the use of third-party data ("front men") to conceal the proceeds of the crime. (PINHEIRO, 2021) The criminal agent acts with the full conviction of impunity, aware that the state police and investigative apparatus lacks the technological structure and specialized personnel to track large-scale offenses in cyberspace. (LOPES JR., 2025).

the prediction of a prison sentence of four to eight years becomes meaningless ; the devaluation of the abstract law is lost in the face of the factual certainty of impunity.

Furthermore, the intervention of Criminal Law and, consequently, of Criminal Procedure, is characterized by its essentially retrospective and repressive nature. The punitive apparatus is designed to act *ex post facto* , that is, only after the violation of the protected legal right. It is at this point that Aury Lopes Jr.'s critical lens defines criminal procedure as a **"late ritual** ." It is a bureaucratic, slow, and ritualistic mechanism that begins when the harm to the individual's property and dignity has already been fully consolidated in reality.

For those affected by digital illiteracy—often elderly, retired, and low-income individuals—the belated nature of criminal law takes on devastating proportions. By the time a police investigation is initiated or criminal proceedings are filed, the financial assets stolen through Pix (Brazil's instant payment system) or fraudulent payroll loans have already been dispersed into an endless chain of phantom bank accounts, making civil redress virtually

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

impossible (CONTELLI, 2022). The highly vulnerable elderly , lacking the technical discernment to repel electronic fraud at the time of its execution, witness the depletion of their subsistence savings while the State belatedly offers them the symbolic promise of punishing a defendant who is often unreachable.

In conclusion, based on the doctrine of Lopes Jr. (2025), the obsession with punitivism and the abandonment of primary prevention policies represent a structural flaw in the legal system. The exclusive focus on post-crime penal repression masks the state's omission in preventively protecting the technically vulnerable in the Information Society. It is therefore imperative to remove Criminal Law from the center of solutions and shift the axis of legal debate to the field of preventive responsibility, requiring the State and private institutions to implement mechanisms of technological protection and digital literacy that prevent the consummation of deception before the "belated ritual" of sanction becomes necessary.

3.4. Primary Prevention Mechanisms: Digital Education and the Strict Liability of Financial Institutions

The observation that the State's repressive apparatus acts in a retrospective and eminently symbolic manner—as per the forceful criticisms of Aury Lopes Jr. (2025) analyzed in the preceding section—requires a shift in the center of gravity of the legal debate. Beyond the protective illusion of penal punitivism, it becomes imperative to devise primary prevention mechanisms that neutralize cyber fraud before its factual consummation.

This preventive engineering is structured on two inseparable pillars: public policies for digital literacy aimed at the hyper-vulnerable population and the objective civil liability of the banking sector, whose business model has driven the compulsory financial digitization of society. (PINHEIRO, 2021).

The first pillar is based on the need to mitigate the *deficit.* Cognitive impairment generated by digital illiteracy can be addressed through public and inclusive education. If fraudulent electronic means acquire the appearance of absolute trustworthiness for individuals lacking technical literacy, the most effective response lies in providing these individuals with the conceptual tools to decode virtual deception. Governmental financial and digital education campaigns should abandon generic communication and focus on specific behavioral guidelines for the elderly and vulnerable, teaching them to identify systemic anomalies such as URL distortion, atypical telephone requests for confidential data, and the irreversible nature of instant transactions. (PINHEIRO, 2021).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

The fact is that the transfer of governance of economic transactions to cyberspace did not result from a deliberate choice by citizens, but rather from a strategic choice for corporate efficiency by large banking corporations.

Empirical data published by the Brazilian Federation of Banks (FEBRABAN) highlight the magnitude of this migration. According to the second volume of the FEBRABAN Banking Technology Survey (2025), transactions carried out through physical channels (bank branches and ATMs) are showing continuous declines, while transactions via *mobile banking are increasing.* They have become absolutely consolidated. The Pix ecosystem, in isolation, showed a dizzying growth of 41% compared to the previous period, reaching the historic mark of almost **25 billion operations** concentrated mainly in digital channels of mobile devices (FEBRABAN, 2025).

This hyperconnectivity and acceleration of electronic transactions, while generating billions in operational optimization for credit institutions, has exponentially expanded the attack surface for cybercrime, making the digitally illiterate the preferred target of online fraud. Sectoral studies reported by the FEBRABAN Tech platform itself (2024) indicate that approximately **15.8% of users** surveyed have already been direct victims of scams or financial fraud perpetrated through the internet or mobile devices.

Given this scenario, the banking industry has systematically increased its technological investments. The first volume of the FEBRABAN Banking Technology Survey (2025) reveals that projections for total bank investments in innovation and technology should reach the historic figure of **R$ 47.8 billion** , of which it is estimated that around **R$ 5 billion annually** (approximately 10% of the sector's technological budget) will be specifically allocated to the development of information technology systems focused on security and cybersecurity (FEBRABAN, 2025; BRASSCOM, 2025).

Despite substantial investments in *software* and information security tools, the persistence and sophistication of fraud—which victimizes nearly one-sixth of the country's digital users—indicate that the corporate apparatus still fails to protect the highly vulnerable consumer at the time of transaction. It is precisely in this vacuum that the legal system calls upon the norms of Civil Law and Consumer Law to balance the technical asymmetry. (BRAZIL, 1990).

The second pillar of prevention, designed to address this asymmetry, is consolidated in the legal attribution of responsibility to financial institutions. This responsibility is based on the Theory of Enterprise Risk, enshrined in Article 14 of Law No. 8,078/1990 (Consumer Protection Code). The legal instrument stipulates that the service provider is objectively

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 10/06/2026 | Accepted: 13/06/2026 | Publication: 16/06/2026

liable—that is, regardless of proof of fault—for repairing damages caused to consumers by defects related to the provision of services, as well as for insufficient or inadequate information about their use and risks (BRAZIL, 1990).

A defect in electronic banking services occurs when the institution's security system fails to prevent manifestly atypical, disproportionate, and incompatible financial transactions with the socioeconomic profile of a vulnerable or elderly client, allowing the immediate dispersal of assets stolen through social engineering. This dogmatic interpretation has been consolidated nationally through the issuance of **Precedent No. 479 of the Superior Court of Justice (STJ)** , whose text settles the matter by stating:

> *"Financial institutions are objectively liable for damages caused by internal fortuitous events related to fraud and crimes committed by third parties within the scope of banking operations." (STJ, 2012).*

The fundamental concept coined by the Summary rests on the distinction between external and internal fortuitous events. While external fortuitous events break the causal link because they are events completely unrelated to the activity (such as a force of nature), internal fortuitous events encompass all the risks inherent in the organization and economic exploitation of the business itself.

Data leaks that enable fraudulent approaches, the opening of fictitious current accounts by fraudsters ("dummy accounts") used to receive the proceeds of fraud, and the fragility of real-time fraud detection algorithms are all inherent risks in modern banking.

Therefore, imputing objective and full civil liability to financial institutions for fraud affecting the digitally illiterate acts as the most powerful mechanism for economic inducement to prevention. By transferring the financial burden of the loss from the most vulnerable link in the chain (the digitally excluded individual) to the economic agent who profits from digitalization, the law forces the financial market to design proactive technological barriers, double human validation systems, and cognitive security safeguards capable of preventing the consolidation of the vulnerable party's error, definitively overcoming the retrospective ineffectiveness of criminal sanctions. (BRAZIL, 1990; SUPERIOR COURT OF JUSTICE, 2012).

4. Final considerations

This article aimed to analyze digital illiteracy not only as a phenomenon of social exclusion, but also as a factual and legal vector of hyper-vulnerability within the scope of contemporary Criminal Law, with a special focus on the crime of cyber fraud. At the end of this academic journey, it is evident that the abrupt and compulsory transition of civil and economic relations to the telematic environment—driven by the pursuit of efficiency and optimization by financial institutions—has generated a contingent of marginalized citizens whose lack of technological literacy makes them prime targets for cybercrime.

In response to the inflationary influx of cybercrimes, the Brazilian State enacted Law No. 14,155/2021, introducing the aggravating circumstance of electronic fraud (§ 2A of Article 171 of the Penal Code). However, the dogmatic and criminological analysis undertaken revealed the inadequacy of this model. The traditional interpretation that anchors the typicality of fraud in the abstract figure of the "average person" falters in the face of technological exclusion; cybernetic artifices and tricks that appear evident or rudimentary to a digitally literate user take on contours of insurmountable reliability for the digitally illiterate. Consequently, the imperative need for the suitability of the fraudulent means to be assessed concretely, weighing the technocognitive vulnerability of the victim, was demonstrated .

Furthermore, relying on the critical lens of Aury Lopes Jr., it was found that the hardening of abstract penal guidelines conforms to the phenomenon of legislative penal populism. This is a merely symbolic response from the State, aimed at appeasing social outcry and mitigating the feeling of legal insecurity, but which structurally fails in its deterrent function. As cybercriminals operate under the guarantee of telematic anonymity and are aware of the structural shortcomings of criminal investigation bodies, the increase in penalties becomes... innocuous . Criminal law and the legal process thus manifest themselves as a "belated ritual": a slow bureaucracy that intervenes in a purely retrospective way, when the assets and livelihood of the vulnerable have already been irrevocably pulverized in cyberspace.

Faced with this diagnosis of repressive ineffectiveness, this work addresses its central problem by proposing a shift in the legal focus from post-crime penal repression to primary prevention mechanisms. Effective protection of the digitally illiterate will not be achieved through sterile punitive expansionism, but rather through a public pedagogy of digital literacy combined with the mobilization of civil and consumer protection tools.

In this context, it can be concluded that the strict liability of financial institutions, based on the Theory of Enterprise Risk and enshrined in Precedent No. 479 of the Superior Court of Justice, emerges as the most powerful mechanism for preventive deterrence. By imputing the financial burden arising from electronic fraud and social engineering to the banking sector—

which profits billions from the dematerialization of service channels and the instantaneous flow of transactions such as Pix—the legal system compels the market to invest in the creation of cognitive safeguards, predictive artificial intelligence for detecting atypical situations, and proactive information security systems.

Ultimately, safeguarding the digitally illiterate in the cyber ecosystem is an imperative of human dignity and social justice. Technological progress cannot proceed dissociated from the inclusion and security of the vulnerable. It is hoped that this work can contribute to the academic and jurisprudential debate, demonstrating that the role of Law in the Information Society should not be that of a belated spectator armed with ineffective sanctions, but rather that of an agent inducing an ethical, protective, and truly democratic digital environment.

References

BITENCOURT, Cezar Roberto. **Treatise on criminal law** : crimes against property. 20th ed. São Paulo: Saraiva Educação, 2020. v. 3.

BRAZIL. [Consumer Protection Code]. **Law No. 8.078, of September 11, 1990.** Provides for consumer protection and other measures. Brasília, DF: Presidency of the Republic, 1990. Available at: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm . Accessed on: June 7, 2026.

BRAZIL. **Law No. 12,965, of April 23, 2014.** Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. Official Gazette of the Union, Brasília, DF, Apr. 2014. (Marco Civil da Internet). Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Accessed on: Nov. 3, 2025 .

BRAZIL. **Law No. 14,155, of May 27, 2021.** Amends Decree-Law No. 2,848, of December 7, 1940 (Penal Code), Decree-Law No. 3,689, of October 3, 1941 (Code of Criminal Procedure), and Law No. 9,296, of July 24, 1996, to make the crimes of violation of computer devices, theft, and fraud committed electronically or on the internet more serious. Brasília, DF: Presidency of the Republic, 2021. Available at: http://www.planalto.gov.br/ccivil_03/_ato20192022/2021/lei/l14155.htm . Accessed on: June 6, 2026.

(Association of Information and Communication Technology and Network Technologies Companies). Brazil **should invest R$ 104.6 billion in cybersecurity by** 2028. São Paulo : Febraban Tech , 2025. Available at : https://febrabantech.febraban.org.br/temas/seguranca/brasil-deve-investir-r-104-6-bilhoes-em-ciberseguranca-ate-2028 . Accessed on : June 7 , 2026 .

CASTELLS, Manuel. **The Network Society** (The Information Age: Economy, Society and Culture - Volume 1). 19th ed. São Paulo: Paz e Terra, 2018.

CETIC.BR (Regional Center for Studies on the Development of Society)

Information). **Research on the Use of Information Technologies and**

Communication in Brazilian Households – ICT Households 2023. São Paulo:

Internet Steering Committee in Brazil, 2024. Accessed on: May 23, 2026.

CONTELLI, Éverson Aparecido. PIX Tragedy - Precautionary Measures per saltum : in search of the effectiveness of patrimonial criminal prosecution. **Migalhas ,** August 5, 2022. Available at: https://www.migalhas.com.br/depeso/371148/tragedia-pix-medidas-assecuratorias-per-saltum . Accessed on : June 12 , 2026 .

FEBRABAN (Brazilian Federation of Banks). **Bank investment in technology is expected to grow 13% in 2025, reaching R$ 47.8 billion** . São Paulo:
Febraban Portal, 2025. Available at: https://portal.febraban.org.br/noticia/4278/pt-br/ . Accessed on : June 7, 2026.

FEBRABAN (Brazilian Federation of Banks). **FEBRABAN Banking Technology Survey 2025** : Volume 2. São Paulo: Deloitte, 2025. Available at: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_2%20%20VF.pdf . Accessed on: June 7 , 2026 .

FEBRABAN TECH. Investment in **information security should grow 15% in 2025.** São Paulo : Febraban Tech, 2024. Available at : https://febrabantech.febraban.org.br/temas/seguranca/investimento-em-seguranca-da-informacao-dev-crescer-15-em-2025 . Accessed on : June 7 , 2026 .

Brazilian Institute of Geography and Statistics (IBGE). Continuous **National Household Sample Survey** : Access to the internet and television and possession of mobile phones for personal use . Rio de Janeiro : IBGE , 2025. Available at : https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-noticias/noticias/44031-internet-chega-a-74-9-milliones-de-domicilios-do-pais-em-2024 . Accessed on : June 6 , 2026 .

LOPES JR., Aury. **Fundamentals of Criminal Procedure** : A Critical Introduction. 11th ed.

Rio de Janeiro: EMERJ/SRV, 2025. E-book. Available at: https://integrada.minhabiblioteca.com.br/reader/books/9788553625611/ . Accessed on: June 7, 2026.

NUCCI, Guilherme de Souza. **Manual of Criminal Law** . 10th ed. rev., updated and expanded .

Rio de Janeiro: Forense, 2014.

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

E-book. Available at: https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/ . Accessed on: June 6, 2026.

SOUSA, J. **Brazil is at the top of the world ranking of victims of digital fraud** . Canaltech , [S. l.], 2025. Available at: https://canaltech.com.br/seguranca/brasil - esta - no - topo - do - ranking - mundial - de vitimas - de - fraudes - digitais/ . Accessed on: October 31, 2025.

SUPERIOR COURT OF JUSTICE (Brazil). **Summary No. 479.** Financial institutions are objectively liable for damages caused by internal fortuitous events related to fraud and crimes committed by third parties within the scope of banking operations. Brasília, DF: STJ, [2012]. Available at: https://scon.stj.jus.br/SCON/ .
Accessed on: June 7, 2026.