

## Virtual Screening And Its Legal Structure

NATALIA DOS SANTOS SILVA

Professional Master's Degree in Criminal Law IDP- SGAS Ii St. De Grandes Áreas Sul 607 Módulo 49 - Asa Sul, Brasília – DF, 70200-670

---

### ABSTRACT:

**INTRODUCTION:** The theme of the research addresses scams on the internet, focusing on the analysis of the crime of virtual embezzlement. Cyber-crimes have become an international concern, since countless people are victims of these criminal practices, resulting in real consequences in their lives. The speed with which these crimes are perpetrated and the expertise of the criminals transform the internet, through digital means, into an environment conducive to the occurrence of scams, which previously occurred predominantly in the physical world.

**OBJECTIVE:** The research intends to examine the different types of virtual embezzlement, identifying the techniques used by criminals, the social engineering mechanisms used and the technological resources used to commit these crimes. In addition, it is intended to investigate the factors that contribute to the vulnerability of victims, as well as strategies to prevent and combat this type of crime.

**METHODOLOGY:** Through a methodological approach based on a bibliographical review, analysis of specific cases and statistical data collection, it is expected to obtain an in-depth understanding of the phenomenon of virtual embezzlement. Relevant academic and scientific sources will be consulted, as well as analyzes of real cases of virtual larceny to support the research conclusions. The collection of statistical data will make it possible to identify the dimension and evolution of this type of crime, as well as the characteristics of the victims and the damage caused.

**CONCLUSION:** The research will contribute to the advancement of scientific knowledge in this area, providing subsidies for the implementation of public policies and effective actions to combat cybercrime, aimed at protecting internet users and preserving digital security. By understanding the characteristics, dynamics and impacts of cyber fraud, it will be possible to formulate recommendations to improve cybersecurity at both the individual and institutional levels. With the world increasingly connected, it is essential to face and prevent scams on the internet, minimizing the damage caused to victims and promoting a safe and reliable digital environment.

**Keyword:** Virtual larceny. Virtual crimes. Data protection law. Criminal Law. Criminal responsibility.

---

Date of Submission: 02-06-2023

Date of Acceptance: 12-06-2023

---

### I. INTRODUCTION

Society over the years has been changing more and more. The world has become technological, the internet and the technologies of communication in general have changed from analogue to digital, we live in cyberculture<sup>1</sup>.

The internet went from being limited to a small group to being accessible to the general population, democratizing its use.

Today, in a single device we have access to numerous resources, in addition, the evolution of technologies is beneficial, according to the French sociologist, Lévy, (2012)<sup>2</sup>, new technologies, provide the world with a new way of thinking, expanding knowledge and diversifying culture.

Liquid modernity, named by the theory of the philosopher, Bauman, (2001)<sup>3</sup> is a metaphor referring to the society that ceases to be solid (defined, lasting and stable) and starts to become a liquid society, that is, the liquid just as society is in continuous transformation, its liquid form provides that, be more adaptable to the

---

<sup>1</sup>LÉVY, Pierre, apud, CUNHA, Úrsula Nascimento de Sousa, **cyberculture and liquid identities: reflection on culture in the era of new technologies**, Magazine: Question Points: Languages, identities and literacies - Vol. 2, no. 2, Jul./Dec. 2012 | 163. Available <https://www.revistas.uneb.br/index.php/pontosdeint/article/view/1558>. Accessed January 11, 2023.

<sup>2</sup> The same.

<sup>3</sup> BAUMAN, Zygmunt. **Liquid Modernity**. Translation, Plínio Dentzien. Rio de Janeiro: Jorge Zahar ed., 2001.

changes of modern life asks for change the society solid to liquid, postmodern, peace<sup>4</sup>, the liquidity of society changes refer to politics, technology, media.

Cyberculture is the culture developed in the virtual environment, with its own language, knowledge, providing the communication of several people from countless different connected cultures, its beginning occurs with the birth of technologies.

Digital law is an area of law that arises to meet the high demand for issues involving norms and principles, to protect against possible violations and the influence of the virtual world on society and the legal system. In addition, digital law seeks to regulate and solve problems generated via relationships that occur on the network, according to the words of Pinheiro, (2021), namely:

Digital Law consists of the evolution of Law itself, covering all the fundamental principles and institutes that are in force being applied until today, as well as introducing new institutes and elements for legal thought, in all its areas (Civil Law, Copyright Law, Commercial Law, Contract Law, Economic Law, Financial Law, Tax Law, Criminal Law, International Law, etc.). (PINE, 2021)<sup>5</sup>.

The internet is present in the legal world in online proceedings and hearings, in means of transport, medicine, education and leisure, in the means of communication, among others. These are everyday examples of the use of this technology, the term internet is conceptualized in the Marco Civil da internet, in its art. 5th, because:

I = internet: the system consisting of the set of logical protocols, structured on a worldwide scale for public and unrestricted use, for enable data communication between terminals over different networks. (BRASIL, 2012).

Commerce is another segment that has been radically transformed over the last few decades. Currently, e-commerce (*Ecommerce*), regulated by Decree n. ° 7.962/13, which generated a significant change in the business culture and economy. Transactions take place entirely online: purchase and sale of goods and services, stores that used to be physical stores are now virtual stores, companies begin to reach new customers in various locations.

In short, this type of trade emerges as a horizon of new opportunities, but with the abundance of money and information circulating on the network, criminals perfected their scams, aiming to gain illicit advantage, thus practicing virtual larceny,<sup>6</sup> which has been one of the main crimes committed on the internet, criminals use digital means to commit scams, to deceive, to mislead the victim, and with that they achieve the purpose of obtaining illicit advantage and causing property damage, the victims.

Issues related to data theft, device intrusions and data leaks, and internet scams, are concerns not only for users, but for network entrepreneurs and the State, which, through laws, seeks to prevent and punish those who commit these illicit acts.

Virtual crimes began to be studied as a science not only by Criminal Law, but began to be analyzed as a phenomenon by Cybercriminology, science, which studies and analyzes virtual crime, the criminal, the laws, the victims, that is, everything that takes place in cyberspace.

In this vein, the violation of these rights can be seen from its propagation in a veiled and malicious way through the practice of cyber-crimes, revealing the need for greater inspection, action and civil and criminal accountability in the face of the inappropriate use of digital systems.

It should also be noted that only in 2020, according to a survey carried out by Association Safer net Brazil in partnership with the Public Ministry Federal-MPF —, 156,692 occurrences of crimes committed on the internet were registered at the National Center for the Denouncement of Cyber Crimes = CNDCC, revealing a significant increase in relation to the practice of criminal offenses of this nature compared to the year 2019, whose total number of records of 75,428 occurrences.<sup>7</sup>

In this sense, the Brazilian Yearbook of Public Security -ABSP—, launched in 2022, analyzed the growth in the number of frauds committed electronically, the period of 2018–2021, it was found that there was an increase in the commission of this crime, the analysis is carried out at national and state level, in both the growth doubled, for example, at the level national in this period analyzed the growth of 495%, the Brazilian yearbook is based on

<sup>4</sup> PEACE, E.H. **Liquid Literature: narration in a digital environment. crossings**, Cascavel, v. 11, no. 3, p. 222–234, 2017. Available at: <https://e-revista.unioeste.br/index.php/travessias/article/view/18165>. Accessed on: 11 Jan. 2023.

<sup>5</sup> PINHEIRO, Patricia Peck. **#digital right**. 7. ed. rev., ampl., current São Paulo: Saraiva Jur, 2021. E-book. (1 online resource). ISBN 9786555598438. Available at: <https://integrada.minhabiblioteca.com.br/books/9786555598438>. Accessed on: 10 Jul. 2022, p.26.

<sup>6</sup> GRECO, Rogerio. **Commented Penal Code**. [Type Publisher Location]: GEN Group, 2021. E-book. ISBN 9786559770700. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786559770700/>. Accessed on: 16 Nov. 2022, p.545.

<sup>7</sup> BRAZIL, Safernet, **indicators**. Available at <https://indicadores.safernet.org.br/>. Access 01/20/2023.

reports and statistics from civil police, military police, and federal police, public security secretariats, from all states<sup>8</sup>.

This scenario intensified during the Covid-19 pandemic, which overnight produced a “new normal”, imposing physical and social isolation measures and the use of the computer for everything, from work to daily shopping, up to and bank transactions<sup>9</sup>. The scenario became worrying, to the point that parliamentarians created a law initiative for the creation of a new legal device, thus emerging PL 4554/20<sup>10</sup>, which later became Law No. 14,155/21.

Electronic crimes have been growing over the years, = Bank fraud<sup>11</sup>, known for virtual embezzlement, for example, grew by around 165% in 2021 alone, according to data from the Brazilian Federation of Banks (Febraban)<sup>12</sup>. This already high growth intensified during the Covid-19 pandemic, notably in a context in which banking transactions began to be carried out mostly through cell phones, and with the spread of Open Bank,<sup>13</sup> fraudsters use the state difficulty in punishing, and acting; attacks can be individual or in masse, affect individuals or legal entities, are a threat to information security, because:

Cyber-attacks and security breaches in networks, public and private, and especially on the web are a problem of constant concern for the world's leading analysts and information security and web security companies/professionals. (WENDT, 2011)<sup>14</sup>.

How has Brazilian criminal legislation been improving over the last decade to combat, prevent and punish crimes of embezzlement in the virtual environment? During this decade, some laws, criminal and civil, related to data protection, internet regulation, internet principles were elaborated.

However, the present research will analyze the creation of the criminal type referring to the crime of virtual embezzlement, a crime that is recurrent when it comes to internet scams, wondering and how this normative evolution has influenced the fight against and punishment of internet crimes, especially the fight against virtual larceny, in recent years.

## II. METHODOLOGY

The methodology adopted for this study is a bibliographic and documentary approach, with a descriptive dimension. Through this methodology, we intend to analyze the current status of the rules that regulate cybercrime. For this, we will use the hypothetical deductive method, starting from the observation of the current Brazilian norms related to computer crimes, with the objective of understanding its implications for the research problem.

Within the scope of this study, we seek to analyze the legislative evolution of the crime of cyber fraud in Brazilian legislation. In addition, we will examine the concept of internet crimes and the existing legislation in Brazil on this topic. Special attention will be given to the structure of the criminal type of larceny according to article 171 of the Penal Code, together with its specific characteristics. In addition, we will carry out research on the creation of the criminal type of virtual larceny.

<sup>8</sup> BRAZILIAN PUBLIC SAFETY FORUM. **Brazilian Public Security Yearbook: 2022**. São Paulo: FBSP, p.110-111.

<sup>9</sup> COSTA, Taís Barros Trajano Ribeiro da. **The rise of cybercrime during the COVID-19 pandemic**. Faculdade Damas, Recife-PE, 2020. Available at: <https://jus.com.br/> accessed on: May 18, 2020021.

<sup>10</sup> CHAMBER OF DEPUTIES. **Bill No. 4554/20**. Available at: [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1947262&filename=PL%204554/20](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1947262&filename=PL%204554/20). accessed on 01/21/2023.

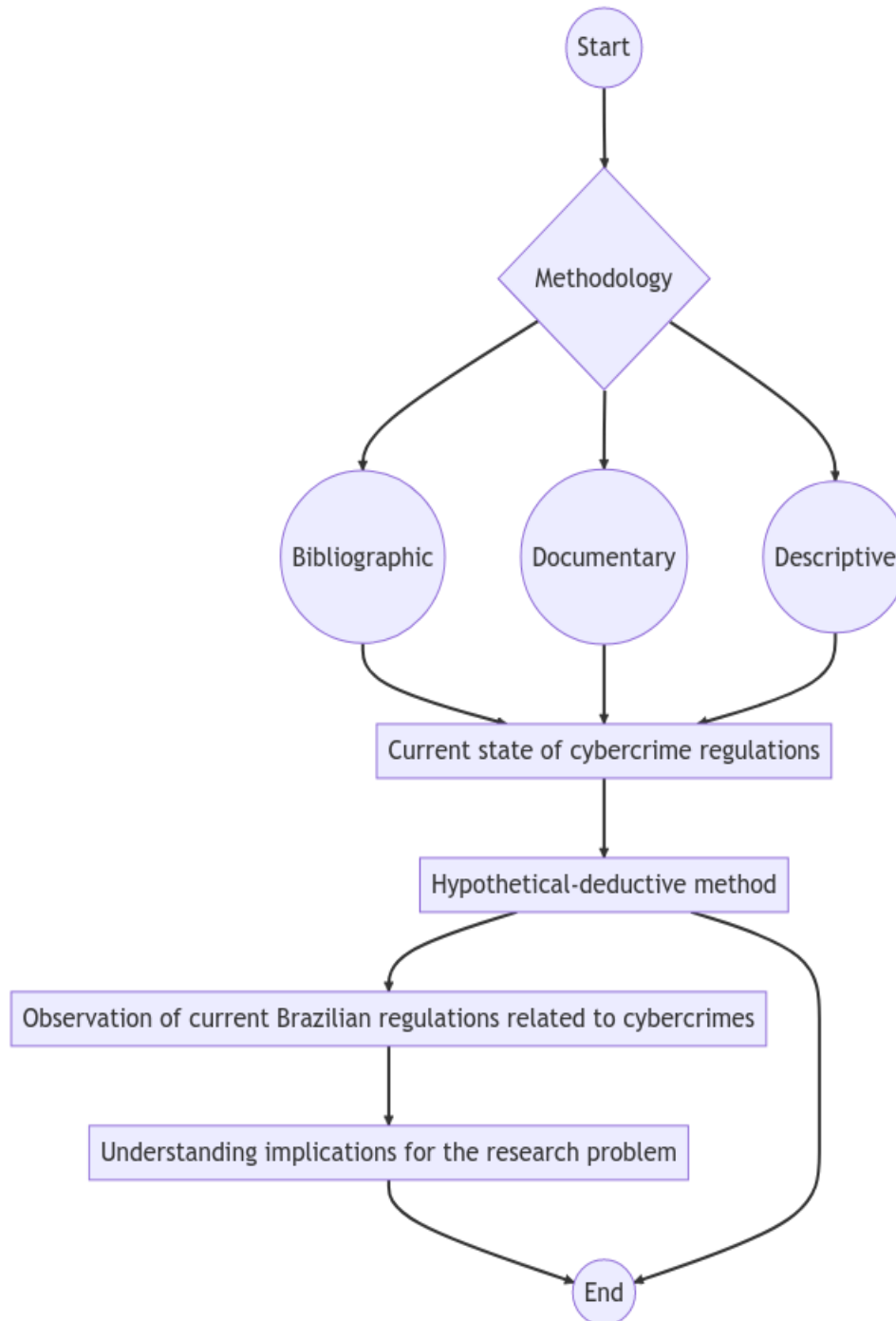
<sup>11</sup> In internet bank transfers by default of the account holders, the agent, with the intention of obtaining an illegitimate asset advantage, harming the account holder, interferes with the result of data processing through the use of bank details without authorization. CORREIA, Pedro Miguel Alves Ribeiro; JESUS Inês Oliveira Andrade - **Combating illegitimate internet bank transfers in Portuguese law: between domestic experiences and global politics conserved**. DIREITO GV MAGAZINE | SAO PAULO | V. 12 No. 2 | 542–563 | NEVER–AUG 2016.

<sup>12</sup> MELLO Danilo: **Fraud against customers grows 65% by e 2021**. Agência Brasil, <https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/fraudes-contras-clientes-de-bancos-crescem-165-em-2021>. São Paulo, publication 10/29/2021. Accessed on 08/28/2022.

<sup>13</sup> LEITE, Luiza; CAMARGO, Matheus. **Open Banking: open innovation in the financial system**. Editora Saraiva, 2022. E-book. ISBN 9786553620353. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786553620353/>. Accessed on: 12 Nov. 2022.

<sup>14</sup> WENDT, E. CYBER WARFARE, CYBER INTELLIGENCE AND VIRTUAL SECURITY: some aspects. **Brazilian Intelligence Magazine**, no. 6, p. 15–26, 1 Apr. 2011.

By using this methodology, we seek to provide an in-depth analysis of Brazilian legislation related to cybercrime, with a focus on virtual larceny. It is hoped that this study will contribute to the understanding of the current legal landscape, as well as to identify gaps and possible improvements in the fight against this type of crime in the digital sphere.



**Figure 1.** Flowchart of the applied methodology. Adapted by the authors:(De Oliveira, 2018).

**CLASSIC SCREENING**

The word embezzlement came from the Latin-*stellionate*, its origin stems from the influence of Roman law, embezzlement refers to the characteristic of the chameleon reptile, an animal that, as one of its characteristics,

changes color depending on the situation.<sup>15</sup> In legal language, it is a criminal type that reflects the way to deceive or acquire things, via fraud, because:

The typified action is to obtain illicit advantage (for oneself or for others), to the detriment of others, inducing or keeping someone in error, through artifice, ruse or any other fraudulent means. The fundamental characteristic of embezzlement is fraud, used by the agent to induce or keep the victim in error, for obtain an illicit financial advantage. (BITENCOURT, 2022).<sup>16</sup>

According to Lessons Loureiro, (2014) in comparative law, the typification of the conduct of embezzlement is based on two models: the German model, which describes the conduct of embezzlement by obtaining undue advantage by deceiving the victim, which generates property damage, this model does not require any type of qualification typical of deceit, embezzlement, therefore, objectivity is sought to be prioritized, namely:

Betrug's German model proscribes the conduct of those who obtain undue advantage from the creation or maintenance of a victim's deception, which causes the disposition of assets induced by error. There is no legal requirement for any specific qualification of this deception, which simply must rest on fact. (LOUREIRO, 2014).<sup>17</sup>

Furthermore, the second model refers to the French model in which embezzlement requires a qualification of the error, which is consolidated in the realization of the fraud, this model observes the subjectivity of the subject's actions, because:

*Scam* it is based on the enumeration of typical situations. The French criminal type requires a qualification of deceit, which will be crystallized in fraudulent maneuvers, use of a false name or quality, or abuse of true quality. (LOUREIRO, 2014).<sup>18</sup>

Furthermore, the crime of embezzlement is listed in the Penal Code of 1940, in its art. 17, caput, as well as following the model adopted by Brazil along the lines of the French concept of embezzlement. In CP, embezzlement is found, in the special part of the code, in title II, of crimes against property, whose purpose is to protect the unfeasibility of property, which may be movable or immovable, and protects individuals or legal entities.<sup>19</sup>

It is noted that the action taken requires the presence of conduct =to obtain for oneself or for others an illicit advantage and harm to others = the binomial illicit advantage and harm to others is essential in the conduct of the agent, since the intended harm or advantage generated can be any nature, it doesn't have to be just economical<sup>20</sup>.

According to Bitencourt, (2019) there is a duplicity of the causal link, that is, it had the double relationship of cause and effect, fraud would be the cause, and deceit would characterize the effect. The Stelionate is, therefore, a double result crime.<sup>21</sup>

The core of the criminal type is described in the verbs: to obtain, for oneself or for others, an illicit advantage, to the detriment of others, inducing or keeping someone in error, through artifice, ruse, or any other fraudulent means.<sup>22</sup>

To induce means to persuade, to instill, to provoke deception or a false perception of reality, the verb to maintain in the crime of embezzlement has the meaning to remain, to persist, in the situation in which one is deceived, persuaded, and finally, the illicit advantage covers any type of benefit.

---

<sup>15</sup> BITENCOURT, Cezar R. **Criminal law treaty: special part: crimes against property up to crimes against religious sentiment and against respect for the dead— arts. 155 a 212.** v.3. [Type Publisher Location]: Editora Saraiva, 2022. E-book. ISBN 9786553622074. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786553622074/>. Accessed on: 13 Jan. 2023, p. 152.

<sup>16</sup> **The same. p. 154**

<sup>17</sup> **Ibidem. LOUREIRO, (2014, p. 16).**

<sup>18</sup>

**Ibid. p. 16.**

<sup>19</sup> BALDAN, Edson Luis. **Fraud. PUC-SP Legal Encyclopedia.** Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga and André Luiz Freire (coords.). Tome: Criminal Law. Christiano Jorge Santos (tome coordinator). 1st ed. São Paulo: Pontifical Catholic University of São Paulo, 2017. Available at: <https://enciclopediajuridica.pucsp.br/verbete/425/edicao-1/estelionato>. Accessed on 10/26/2022

<sup>20</sup> **Ibid. GRECO, (2021, p.536).**

<sup>21</sup> **Idem. BITENCOURT, (2019, p.845).**

<sup>22</sup> **Griffin ours.**

It should be noted that the advantage in the crime of Embezzlement art. 171 of the CP, is an illicit advantage, if the advantage is licit, the crime will not be embezzlement, passing the agent to configure the criminal type of the crime of Arbitrary exercise of the very reasons art. 345 of CP.<sup>23</sup>

### SUBJECTIVE AND OBJECTIVE ELEMENTS OF THE TYPE

The crime of embezzlement has as a subjective element the intention, not having the culpable modality, since the crime in question admits co-authorship and participation, even regarding the characteristics of the crime, it is understood that the active subject can be committed by any person, thus, a common crime, moreover, as far as the taxable person is concerned, any natural or legal person, with or without personality, can be a victim, provided that the victim is determined, and that he suffers financial damage.<sup>24</sup>

It is noted that the victim needs to have the ability to discern to be deceived, if he does not have it, the crime of Abuse of the Disabled, listed in art. 173 of CP. The attempted form of the crime is possible,<sup>25</sup> and the consummation in the crime of embezzlement occurs with obtaining the illicit advantage, that is, it is when the subject achieves economic advantage, causing harm to the victim.

In this sense, the Superior Court of Justice = STJ pacified the understanding about obtaining an advantage in the crime of embezzlement according to the content of informative n.º 663, namely:

If the crime is only consummated with the effective obtaining of the undue advantage by the active agent, it is certain that there is only talk of consummation, in the cases of transfer and deposit, when the amount actually enters the bank account of the beneficiary of the fraud. (BRASIL, 2020).<sup>26</sup>

Given the contributions regarding the identification of embezzlement in its essence for the legal world and its effects on society, in light of the understanding within the scope of the STJ, a brief analysis of some types of embezzlement for the preparation of this study deserves to be highlighted.

### THE REFLECTION OF VIRTUAL CRIMES IN THE FACE OF THE LEGAL VIEW AND IN THE CURRENT CONTEXT

Fraud committed over the internet is one of the most recurrent methods in the current context, given the easiness that many perpetrators employ in their way of reaching victims; many deceive, create fake profiles on social networks, in addition to invading other people's accounts and data with the sole purpose of blackmailing and obtaining illicit advantage.

Therefore, virtual embezzlement is a conduct practiced through electronic means, which seeks to obtain economic advantage for itself or for another, the advantage is obtained in an illicit, fraudulent way, it uses cunning means and artifices virtually, leading the victim to act under deceit and provide or deliver information to criminals, causing economic and property damage to the victim.

It is observed that the consequences of the practice of virtual crimes are destructive, as they reinforce the culture of domination and exploitation of one's own being, as, for example, in the practice of sexual harassment in the remote work environment, in addition to other results, such as the loss assets for the victim acquired through fraud and error.

According to the lessons of Capez, (2022) when analyzing the reflections of the violation of the dignity of the human person in the face of the practice of any type of virtual crime, it states that:

It consists of inducing or keeping someone in error, through the use of artifice, ruse, or any fraudulent means, in order to obtain, for oneself or for others, an illicit advantage to the detriment of others. It is a crime in which, instead of violence or serious threat, the agent employs a stratagem to mislead the victim, leading him to have an erroneous perception of the facts, or to keep him in error, using of maneuvers to prevent her from realizing the mistake she is working on. (CAPEZ, 2022)<sup>27</sup>.

In this regard, the spread of the internet and the greater number of online users, especially during the Covid-19 pandemic, led to the improvement of the crime of embezzlement, bearing in mind that the performance of work, as well as internet purchases, almost doubled. during this period, which facilitated the *mode of operation* of criminals in the virtual environment.

<sup>23</sup> CUNHA, Rogerio Sanches **Penal code for contests: CP.14 ed. rev, current and amp.** Salvador: juspodivm 2021, p.667.

<sup>24</sup> **Ibid.** CUNHA, (2021, p.668).

<sup>25</sup> **The same.** GRECO, (2021, p. 538).

<sup>26</sup> BRAZIL, Superior Court of Justice – STJ. **newsletter n.º 663, February 14, 2020.** CC 169.053-DF, Rapporteur Min. Sebastião Reis Júnior, Third Section, unanimously, judged on 12/11/2019, DJe 12/19/2019. <https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0663.cod.accesso> on 10/13/2022.

<sup>27</sup> **Ibidem.** CAPES, (2022, p.245).

According to the Brazilian Yearbook of Public Security - ABSP - there was a significant growth in the number of complaints in 2022 regarding the practice of fraud committed by electronic means compared to the years between 2018 and 2021, totaling an increase of 495%<sup>28</sup> throughout Brazil, in the practice of this type of virtual crime.

On top of that, the Ministry of Justice and Public Security – MJSP – when carrying out a survey on the practice of virtual crimes, arrived at the result regarding the position occupied by Brazil in the ranking of virtual crimes, this being the 5th country that suffered internet scams in 2021; virtual scams employed by any cunning and fraudulent means from the invasion of electronic devices that aims only at obtaining economic advantage, as already noted<sup>29</sup>.

It is noted that the Federal Police, in public-private cooperation with FEBRABAN, proposes the exchange of information between institutions in order to inhibit and punish such electronic fraud. It should be noted that in 2021 alone, according to FEBRABAN, the millionaire loss caused to customers reached BRL two billion reais<sup>30</sup>.

Furthermore, according to the Civil Police of the State of São Paulo, the common electronic frauds are: cloning of WhatsApp, the false bank slip, where the fraudster changes the bar code becoming the beneficiary, false bank attendant the member of the gang that have victim data and ask for account data to gain access.

Another example that can be mentioned is the fake moto boy scam, which occurs when a fraudster calls the victim and reports problems with the card, and informs the user that a moto boy will pick it up, in addition to *phishing* sending emails or malicious links, fake or cloned commerce sites, where the victim, thinking it is a reliable site, makes purchases, but the money goes to the criminal's account and the product never arrives<sup>31</sup>.

In view of this, the State's duty to punish acts to fill legislative gaps and curb the illicit acts that arise, with Criminal Law being the last *ratio*, with a subsidiary character, that is, it only acts when the other branches of law are not effective, in protecting the protected assets. The Portuguese Penal Code contemplates two types of fraud (fraud), computer fraud and telecommunications fraud, both typified in article 221<sup>32</sup> of the Portuguese Penal Code.

With its forerunner legislation, the Portuguese Government, in 1995, proposed a reform through Dec. Law n. ° 48/95 of March 15, which, innovatively, created a law to combat fraud and internet crimes with prison sentences<sup>33</sup>. Despite the current Brazilian legislative scenario, but precisely in view of the repression of virtual crimes, there is still a lot of work to be faced.

Criminal legislation needs to be constantly updated according to the criminal reality of society, in view of the need for laws to be in harmony with the punitive need in the face of situations that arise. There is an effort and concern by the authorities in dealing with security, prevention and inhibition of internet crimes.

<sup>28</sup> **Ibid. Brazilian Public Security Forum, (2022, p.110–111).**

<sup>29</sup> BRAZIL.Ministry of Justice and Public Security. News. <https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos>.

<sup>30</sup> **The same.**

<sup>31</sup> BRAZIL, Civil Police of São Paulo. **Crimes Committed on the Internet, Questions and Answers.** <https://www.policiacivil.sp.gov.br/portal/>

<sup>32</sup> Article 221. **PORTUGUESE CRIMINAL CODE**

Computer and communications fraud:

1 - Whoever, with the intention of obtaining illegitimate enrichment for himself or a third party, causes another person to suffer property damage, by interfering with the result of data processing, incorrect structuring of a computer program, incorrect or incomplete use of data, use of data without authorization or intervention by any other unauthorized mode processing, is punishable with imprisonment for up to 3 years or with a fine.

2 - The same penalty is applicable to anyone who, with the intention of obtaining an illegitimate benefit for himself or a third party, causes property damage to others, using programs, electronic devices or other means that, separately or together, are intended to reduce, alter or prevent, in whole or in part, the normal functioning or exploitation of telecommunications services.

3 - The attempt is punishable.

4 - The criminal procedure depends on the complaint.

5 - If the damage is:

a) Of high value, the agent is punished with imprisonment for up to 5 years or with a fine of up to 600 days;

b) Of considerably high value, the agent is punished with imprisonment from 2 to 8 years.

6 - The provisions of article 206 are correspondingly applicable.

<sup>33</sup> COSTA, Antonio Manuel de A. **A Mockery in the Portuguese Penal Code.** [Type Publisher Location]: Grupo Almedina (Portugal), 2020. E-book. ISBN 9789724084428. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9789724084428/>. Accessed on: 25 Feb. 2023.

Nevertheless, public policies to combat and confront cybercrime are active, we had a CPI = Parliamentary Commission of Inquiry – on cybercrime, known as CPICIBER<sup>34</sup>.

In the Chamber of Deputies, addressing topics on internet crimes, after the CPI, a report was prepared that pointed to the growing increase in internet crimes, which led to the creation of bills:

The CPI on Cyber Crimes, established in August 2015, brought together in more than 35 (thirty-five) meetings different segments of society, from institutions dedicated to the area of Technology and Information Security to investigative bodies, including representatives of social movements and organizations non-governmental organizations, civil society, among other entities. Debates are welcomed in deliberative meetings and public hearings, held in Brasilia, capital of Brazil, in an attempt to equate Digital Law to virtual reality (BRASIL, 2015)<sup>35</sup>.

In addition, Criminal Law is based on the principle of fragmentation, protecting only the most relevant legal assets, which suffer attacks and violations on them, according to the lessons of Reale,<sup>36</sup> it is understood that: “[...] Criminal law, as it is necessarily selective, only incriminating some conducts that are harmful to a certain value, those with a high degree of offensiveness.”

The legislator must observe, in the construction of a criminal type, the constitutional limits on the protection of Fundamental Rights, as well as the scope of Brazilian Criminal Law in which the legislator is bound by the constitutional principle of Proportionality and reasonableness so that no limit is exceeded in view of the *the right to punish* of State.

Canet,<sup>37</sup> unfolds the principle of proportionality in his studies and states that:

By the principle of necessity, the citizen has the right to the least possible disadvantage, and unnecessary limitation of fundamental rights must be avoided, that is, the legislator must adopt the least restrictive effective measure of rights. By the principle of proportionality in the strict sense, it is examined whether “the result obtained with the intervention is proportional to its coercive load” or, in other words, whether or not the means used are disproportionate in relation to the end. It is, therefore, a matter of measure or excess to reach an end. (CANOTILHO, 2020).

It is noted that the Principle of legality is the basis of the Democratic State of Law, since incriminating and punitive norms can only exist in the Brazilian legal system if they are elaborated through laws, considering that no fact can be considered a crime and no penalty can be applied if there is no law prior to the fact that defines it as a crime.

In addition, the principle of legality is provided for in the 1988 Constitution, in its article 5 XXXIX: “[...] there is no crime without a previous law that defines it, nor a penalty without prior legal commission”, in the same sense, begins the Penal Code, in its art. 1, provides that: “[...] There is no crime without a previous law that defines it. There is no penalty without prior legal sanction”.

According to Mendes, (2020), the Principle of legality is the basis of all public law, therefore, for criminal law, its basis is the principle of legality, “*No crime, no punishment without law*”<sup>38</sup> then:

<sup>34</sup> BRASIL, CAMARA. <https://www.camara.leg.br/noticias/487063-parliamentary-commission-of-inquiry-of-cyber-crimes-approves-final-report/>.

<sup>35</sup> PATURY, Fabrício Rabelo, Fernanda Veloso Salgado. **The Criminal Policy of the Nucleus for Combating Cyber Crimes of the Public Prosecutor's Office of the State of Bahia in the face of crimes committed in the digital sphere.** MPBA. Available at [https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a\\_politica\\_criminal\\_do\\_nucleo\\_de\\_combate\\_aos\\_crimes\\_ciberneticos\\_do\\_ministerio\\_publico\\_do\\_estado\\_da\\_bahia\\_-\\_fabricio\\_rabelo\\_patury\\_e\\_fernanda\\_veloso\\_salgado.pdf?download=1](https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a_politica_criminal_do_nucleo_de_combate_aos_crimes_ciberneticos_do_ministerio_publico_do_estado_da_bahia_-_fabricio_rabelo_patury_e_fernanda_veloso_salgado.pdf?download=1). a ceased on 02/13/2023.

<sup>36</sup> JR., Miguel R. *Fundamentals of Criminal Law.* [Type Publisher Location]: GEN Group, 2020. E-book. ISBN 9788530991609. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Accessed on: 11 Feb. 2023.p.9.

<sup>37</sup> CANOTILHO, José Joaquim Gomes, apud REALE, Miguel Junior. **Fundamentals of Criminal Law.** GEN Group, 2020. E-book. ISBN 9788530991609. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Accessed on: 11 Feb. 2023, p.21.

<sup>38</sup> “**No crime, no punishment without law-** Expression in Latin that means: there is no crime or penalty without prior law.



All Law is built on the principle of legality, which constitutes the foundation of modern Public Law. Criminal Law is based on the principle that there is no crime without a previous law, nor a penalty without prior legal commission (article 5, XXXIX). (MENDES, 2020)<sup>39</sup>.

### VIRTUAL SCREENING UNDER THE CRIMINAL Aegis

With the constant transformation of society, new challenges arise in the legal world, for example, with the interaction of the physical world with the virtual world, some crimes migrated and improved to occur in the virtual environment, this is the case of virtual larceny, because:

In Brazil, the crime that stands out in the world of virtual crimes is embezzlement, a crime by which the author of the fact obtains, for himself or for others, an illicit advantage, to the detriment of others, through artifice, ruse or any fraudulent means, provided for in article 171 of the Brazilian Penal Code. This type of crime has increased mainly due to the growing demand for e-commerce, a feature of modern times that has led to the emergence of new forms of execution. (PATURY, 2023)<sup>40</sup>.

In order to inhibit and rigorously punish these illicit acts, some parliamentarians were asked to legislate and typify the conduct of electronic fraud, thus resulting in Bill No. 4554/20, authored by Senator Izalci Lucas in the Federal District, which in principle, it would only modify art. 155 of the CP, the name of the crime of “combating electronic fraud” would be created, paragraphs 8 and 9 would be added in the referred article<sup>41</sup>.

The justification for the bill is the increase in the number of cases of fraud, the bill sought to intensify the penalty for the crime, theft committed through fraud, however after the bill went to the federal deputies for consideration, it now had a new rapporteur, Federal Deputy Vinicius Carvalho, who proposed the project to expand not only the crime of theft, but the crime of embezzlement<sup>42</sup>.

With the approval of the bills, Law n. ° 14.155/21 was enacted, which created articles 154-A, device invasion, article 155 and its paragraphs 4-B and C, crime of theft through fraud committed by electronic means, with an increase in the penalty for servers located abroad, and modified article 171 of the CP, creating the qualifiers in paragraph 2 -A and B, namely: electronic fraud and using a server abroad to commit fraud<sup>43</sup>.

In addition, the aforementioned law modified article 70, caput, of the Code of Criminal Procedure, relating to jurisdiction in crimes of embezzlement, in the form of bad check or failed payment, now the jurisdiction is the victim's domicile.

### ELEMENTS OF THE CRIMINAL TYPE

*Scamming*, derives from the verb Scam, which in English means to defraud or deceive,<sup>44</sup> is the name given to characterize the fraudulent process, that is, the way of acting in the virtual larceny, that is, the fraud employed through electronic devices, with the intention of deceiving, to obtain an illicit advantage and cause damage to the intended victim's property.<sup>45</sup>

The criminal type is classified as an intentional crime, since all the typified conducts are intentional, since there is no provision for the guilty modality of the crime, as for the legal interest, all practical forms are Impure, since the legal interest reached is the patrimony, the internet is the means used to commit crimes in the form of a ruse and a fraudulent means, so as to the result, the crime is one of damage, as for the agent, the crime does not need any special quality, being therefore a common crime, the crime is unobjective, as there is no provision for a necessary competition, crimes in terms of the result are classified as matters, as the conduct requires an illicit advantage<sup>46</sup>.

Besides, in the procedural part, the crimes committed through electronic means, are not passers-by; it means to be the ones who leave traces<sup>47</sup>. *Oscam*, (fraud) known for *phishing-scam*, are the techniques they use, from fishing on the internet to select their victims, vulnerable and prone to fall into scams<sup>48</sup>.

<sup>39</sup> MENDES, Gilmar F.; BRANCO, Paulo G. IDP Series = Doctrine Line = Constitutional Law Course. Editora Saraiva, 2020. E-book. ISBN 9788553618088. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9788553618088/>. Accessed on: 11 Feb. 2023, p.945.

<sup>40</sup> **Ibid. PATURY, (2020, p.27).**

<sup>41</sup> **Ibid. Bill No. 4554/20.**

<sup>42</sup> **Ibidem. SOUTH, (2022, p.624).**

<sup>43</sup> **The same.**

<sup>44</sup> <https://dictionary.cambridge.org/pt/dicionario/ingles/scam>.

<sup>45</sup> **Ibidem. SOUTH, (2022, p. 612).**

<sup>46</sup> **Ibidem. SOUTH, (2022, p. 624).**

<sup>47</sup> **The same.**

<sup>48</sup> **The same.**

*Scammer* it is the person who commits the crime, and this criminal agent does not act randomly, when using his logical knowledge, and uses his efficient baits, to induce the victim to error; The objective is to steal data, money, deceive, take over social networks, to use this information to impersonate the user to commit crimes as if they were the person, to deceive victims, their contacts, family members or friends.

The qualifier of Embezzlement, under the terms of art. ° 171§ 2° = A, embezzlement through electronic fraud = known as virtual embezzlement, and the qualifier of § 2°-B, use of a server kept outside the national territory, were added by Law n° 14.155, the penalty became severe, then:

§ 2-A. The penalty is imprisonment, from 4 (four) to 8 (eight) years, and a fine, if the fraud is committed with the use of information provided by the victim or by a third party misled through social networks, telephone contacts or sending fraudulent e-mail, or by any other similar fraudulent means. (Included by Law No. 14,155 of 2021);

§ 2-B. The penalty provided for in § 2-A of this article, considering the relevance of the serious result, is increased from 1/3 (one third) to 2/3 (two thirds), if the crime is committed through the use of a server kept outside of the national territory. (Included by Law No. 14,155 of 2021). (BRASIL, 2021).

It is noteworthy that Legislative Decree n. ° 37 of 21, brings the concept of computer fraud, in its article 8, where each Government will adopt measures, in addition to cooperation and create through law-measures that typify and punish the conduct of computer fraud<sup>49</sup>.

In this sense, it is understood that the new law corresponds to =*innovation of the law for the worse* because the qualifier brought a rigid treatment to the crimes of embezzlement practiced in the virtual environment; the new law cannot, therefore, retroact to photos that occurred prior to its publication.

As with the crime of theft, which currently has a qualifier because it is practiced in the digital environment and with the use of a server located abroad, so when the victim or third party is misled through: social networks, telephone contacts, e-mail. mail, or any other fraudulent means, because:

a) Through social networks: currently, advertisements promoted on social networks such as Facebook and Instagram are very common. Not infrequently, they are fraudulent advertisements, cunning maneuvers to attract people who provide their data;

b) by telephone contacts: frauds committed by telephone are also very common. A recurring example involves credit cards. The fraudster calls someone and claims, for example, that the financial institution has detected evidence of fraud with that person's card. Ask her to confirm data and enter the card password. With the password available, the agent makes purchases, makes withdrawals, takes out loans, etc.;

c) by sending fraudulent e-mail: in this case, the victim receives a fraudulent e-mail, often imitating the characters of well-known companies or organizations and, from access through the link provided, the fraudster can obtain personal data and banking information inserted in electronic forms;

d) by any other similar fraudulent means: this analogical formula includes any other fraudulent practices committed by electronic or computer means, such as internet pages, for example, in which the victim is not directly approached by the fraudster, as in the previous modalities, but is misled by various factors (simulation of a regularly constituted commercial establishment; copy of another reputable page, etc.)<sup>50</sup>. (SANCHES, 2021).

The qualifier applies when a third party or the victim is conducted fraudulently through social networks, being social communication structures, where people or organizations are connected, examples are: Facebook, TikTok, YouTube, considering that:

The transmutation of the concept of “community” into “social networks”. This change is mostly due to the explosion of virtual communities in cyberspace, a fact that ended up generating a series of studies not only on this new way of making society, but also on the dynamic structure of communication networks. At the center of this transformation, concepts such as social capital, trust and partial sympathy are invoked in order to think about the new forms of association that regulate human activity in our time. (COSTA, 2005)<sup>51</sup>.

It should be noted that, in order to apply this qualifier of art. 171, § 2 - The capture or obtaining of data, or confidential information, through electronic fraud, must be used by the criminal to achieve illicit advantage and cause property damage<sup>52</sup>. However, if the action taken by criminals is only to collect data in an unauthorized manner, without fraud to obtain information, the crime committed will be the invasion of computer devices, typified in article 154-A of the Penal Code:

<sup>49</sup> **Ibidem. Legislative Decree n.037 of**

<sup>50</sup> SANCHES, Rogério Cunha, apud. GRECO, Rogerio. **Commented Penal Code**: GEN Group, 2021. E-book. ISBN 9786559770700. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786559770700/>. Accessed on: 26 Jan. 2023.

<sup>51</sup> COSTA, R. **For a new concept of community: social networks, personal communities, collective intelligence**. Interface - Comunic..Saúde, Educ., v.9, n.17, p.235-48, Mar/Aug. 2005. Accessed on 02/22/2023.

<sup>52</sup> **Ibidem. JALIL, (2022, p. 58).**

Invading a computer device used by others, connected or not to the computer network, in order to obtain, tamper with or destroy data or information without the express or tacit authorization of the user of the device or to install vulnerabilities to gain an illicit advantage. (BRASIL, 1940).

Another criminal type that needs to be differentiated is Theft through fraud by electronic or computer device, typified in art. 14.155/21, theft receives the qualifier for being committed by electronic or computer means, connected or not to the internet:

155 § 4º-B. The penalty is imprisonment, from 4 (four) to 8 (eight) years, and a fine, if the theft through fraud is committed by means of an electronic or computer device, connected or not to the computer network, with or without violating a security mechanism, or the use of a malicious program, or by any other similar fraudulent means. (BRASIL, 1940).

However, in electronic fraud, fraud is committed using information or data provided by the victim himself or by a third party, through deception, by the delinquent agent; electronic means are the means used to obtain fraud, which can be through social networks, fraudulent or false emails, telephone contacts, or any similar fraudulent means, the legislator chose to leave the broad interpretation:

171§ 2-A. The penalty is imprisonment, from 4 (four) to 8 (eight) years, and a fine, if the fraud is committed with the use of information provided by the victim or by a third party misled through social networks, telephone contacts or sending fraudulent electronic mail, or by any other similar fraudulent means (BRASIL, 2021).

In addition, STJ bulletin No. 135 deserves to be highlighted in recognizing the constitutive elements of theft through fraud and larceny, namely:

Theft through fraud cannot be confused with embezzlement. In theft, fraud is used to circumvent the victim's vigilance, to draw attention away from him. In larceny, fraud aims to obtain consent from the victim, tricking her into voluntarily handing over the good. (BRAZIL, 2021)<sup>53</sup>.

The penalty provided for in article 171 § 2 - A, considers the serious result to be extremely important, thus increasing from 1/3 (one third) to 2/3 (two thirds), if electronic fraud has been used for its commission, server located abroad. In addition, the penalty for electronic fraud is imprisonment from 04 (four) years to 08 (eight) years, and a fine, if the fraud is committed with the use of information provided by the victim or by a third party induced to error, by through social networks, telephone contacts, or sending fraudulent e-mail (electronic mail), or by any other analogous means<sup>54</sup>.

The penalty imposed in the abstract, for the crime of electronic fraud, makes it impossible to grant the decriminalized benefit of Sursis (conditional suspension of the procedure), provided for in art. 89 of Law No. 9,099/95, the benefit can be applied to crimes where the minimum sentence imposed is equal to or less than one year<sup>55</sup>. In addition, it is not possible by law, to the benefit of the Agreement of non-criminal prosecution, art. 28-A of the CPP, added by Law No. 13,964 of 2019, which provides for the granting of the benefit for crimes with a sentence of less than 04 (four) years<sup>56</sup>.

It should also be noted that the practice of "electronic gluing" does not constitute virtual embezzlement, it does not fit into any type of embezzlement, as before Law No. 12,550/11 came into force, this conduct was considered atypical. In this context, it is mentioned that the STF, in Judgment n. ° 1.145 deciding that the conduct of fraud, since there is no legal provision, should not be used, in order to avoid analogy in part, in this understanding, the STJ, in its Newsletter No. 506: "[...] The "electronic glue", before the enactment of Law No. 12,550/2011, was an atypical conduct, not constituting the crime of embezzlement"<sup>57</sup>.

After the enactment of Law No. 12,550/11, the crime of fraud in public interest events, introduced in the Penal Code in art. 311-A, which punishes the conduct of using or disclosing content improperly, with the aim of benefiting oneself or others, which compromises the credibility of the event.

In this sense, electronic fraud is not considered to be the conduct of a crime involving the use of virtual assets, securities and financial assets. Conduct typified as a crime under Law No. 14,478 of December 21, 2022,

---

<sup>53</sup> **Ibid. STJ, Bulletin No. 315.**

<sup>54</sup> **BRAZIL, Criminal Code of 1940 = Art.171§ 2-A.**

<sup>55</sup> **BRAZIL, Lei n.º 9,099/95.** Art. 89: Nos crimes where the minimum penalty imposed is equal to or less than one year, covered or not by this Law, the Public Prosecutor's Office, when offering the complaint, may propose the suspension of the process, for two to four years, provided that the accused is not being prosecuted or has not been convicted of another crime, the other requirements that would authorize the conditional suspension of the sentence are present."

<sup>56</sup> **BRAZIL, Criminal Procedure Code - Art. 28-A of the CPP.** "Not being a case of filing and having the investigated formally and circumstantially confessed to the commission of a criminal offense without violence or serious threat and with a minimum penalty of less than 4 (four) years..."

<sup>57</sup> **Ibid., STJ Information STJ, n.º 506. HC 245.039-CE.**

being a kind of Embezzlement, specific to electronic asset transactions, the new law found in the *Exemption Law* (180) days to start its term.

In addition, the aforementioned law regulates providers of virtual assets<sup>58</sup>, inserting a new article in the Penal Code, namely: art. 171-A, with the following wording:

Art. 171-A. Organizing, managing, offering or distributing portfolios or intermediating operations involving virtual assets, securities or any financial assets in order to obtain an illicit advantage, to the detriment of others, inducing or keeping someone in error, through artifice, ruse or any other fraudulent means.

Penalty - imprisonment, from 04 (four) to 08 (eight) years, and fine. (BRASIL, 2022).

### **The reason for the increase in article 171, §2— “b”**

The reason for increasing the penalty in the second paragraph, item “b”, of article 171, is an exclusive cause for increasing the sentence, in article 171, § 2º-A, although other types of larceny can be practiced using electronic devices, when creating the new law n. ° 14.155/21, which amended article 171, creating the criminal type of virtual larceny.

The legislator chose to use this cause of increase only in fraud, where the criminal misleads the third party or the victim to provide data or information through social networks, as well as through telephone contacts or by receiving fraudulent electronic mail, or by any similar fraudulent means<sup>59</sup>.

An internet provider, according to Sydow lessons, (2022) is defined as: “[...] being a software or device that provides a service to another software, its users are the clients, the Data Center, the server is a physical device on which a program is executed”<sup>60</sup>.

In this sense, Legislative Decree No. 37 of 2021, known as the Convention on Cyber Crimes, in its first article, classifies servers by:

Service provider: (I) any entity public or private that allows its users to communicate through a computer system, (ii) any other entity that performs the processing or storage of computer data on behalf of these communication servers or their users. (BRASIL, 2021).

It should be noted that the reason for increasing the penalty is always applied to those who commit the offense of virtual larceny, since the social network servers and email managers are located abroad, even if large companies have representation in Brazil, its headquarters and servers are hosted abroad<sup>61</sup>, then:

The penalty is increased if the server from which attacks on other people's devices are hosted in territory outside Brazil, as it makes investigation and discovery of authorship very difficult. The increase should be based on the degree of difficulty of investigating the case. (SYDOW, 2022)<sup>62</sup>.

Another point found is about the difficulty in providing data and tracking them as proof in identifying crimes committed on the internet, as the servers, for the most part, are located abroad, their privacy is protected narrowly, as well as being private companies, protect the privacy of their customers who are not subject to the laws Brazilian.

It is noted that even though Brazil is part of the Budapest Convention in cooperation between countries in the prevention and punishment of virtual crimes, as well as it does not practice obtaining information that proves the authorship and materiality in the crimes in question, it is not so simple, either by bureaucracy, or delay, which makes punishment even more difficult and often leads to statute of limitations for crimes.

On that occasion, Law n. ° 14.155/21 added to article 171 the 4th paragraph, which provides for an increase in the penalty for larceny committed against the elderly or vulnerable person, namely: “[...]§ 4 The penalty is increased by 1/3 (one third) to double, if the crime is committed against the elderly or vulnerable, considering the relevance of the serious result”.

---

<sup>58</sup> **Art. 3 of Law No. 14,478/22.**

“For the purposes of this Law, a digital representation of value that can be traded or transferred by electronic means and used to make payments or for investment purposes is considered a virtual asset, not including:

I - national currency and foreign currencies;

II - electronic currency, pursuant to Law No. 12,865, of October 9, 2013;

III - instruments that provide their holder with access to specified products or services or to benefits arising from these products or services, such as points and rewards from loyalty programs; It is

IV - representations of assets whose issuance, bookkeeping, negotiation or settlement is provided for by law or regulation, such as securities and financial assets.”

<sup>59</sup> **Ibidem. SOUTH, (2022, p. 635).**

<sup>60</sup> **Ibidem. SOUTH, (2022, p. 636).**

<sup>61</sup> **The same.**

<sup>62</sup> **Ibid. NUCCI, (2022, p.456).**

The degree of increase in the penalty is related to the serious result generated by the victim, considering that the greater the damage caused to the victim, the greater the fraction applied to the penalty, the cause of the increase in the penalty is applied, with an elderly victim, or vulnerable, in accordance with Law No. 10,741/03, art. 1, caput Statute of the Elderly Person.

In addition, the legislator does not conceptualize the figure of the person considered objectively vulnerable, but equates it to a situation of difficulty or impossibility of defense as a result of induction into error, fraud or any situation that reduces their ability to offer resistance, according to the criminal classification carved in the conduct of the crime of rape of vulnerable, under the terms of art. 217 — A, of the Penal Code of 1940.

In the aforementioned article, minors under 14 years of age are considered venerable; someone who is in illness or mental illness, and does not have the discernment, in the practice of the act, or anyone who in some way cannot offer resistance. In this vein, by analogy, the same characteristics of the vulnerable victims of article 217-A are used, in the application of the cause of increase in the penalty of art. ° 171, §4° and of article 155, §4°, item II<sup>63</sup>.

Therefore, it is understood that the virtual environment has been the *mode of operation* of countless criminals in Brazil and in the world, given its breadth of facilitation regarding access to sensitive data or financial information of thousands of users who want to have the dimension of how the lack of security and protection of its use properly can cause great damage.

It is necessary that not only the legislation be updated with the objective of confronting virtual crimes, nor with regard to the increase of penalty as the only solution for a possible criminal responsibility, but it is understood that the confrontation with the persistence in this modality of crime is encouraged by empowering users to use technology appropriately.

### III. CONCLUSION

It was found, the occurrence of the criminal type of virtual larceny, although this specific type of larceny was not written in the Penal Code, its practice occurred, it intensified, mainly during the Covid-19 Pandemic, however, its practice was not punished for not there was a typification of the type, during social isolation, there was an increase in online users and consequently there were crimes.

It was found throughout the research an excessive increase in the number of crimes of embezzlement committed by electronic means, according to the Brazilian Yearbook of Public Security (ABSP), published in the year 2022, there was an increase in the number of embezzlements committed through electronic means. electronics, the period from the years of 2018–2021.

It was also verified that there was a very high increase in the commission of this crime, the analysis was carried out with statistics at the national and state level, in both scenarios, the growth was doubled, for example, at the national level the period studied, the growth of 495 %, the Brazilian Yearbook is carried out, according to information, in reports and statistics, collected from the civil police, military police, and federal police, Public Security Secretariats of all Brazilian states<sup>64</sup>.

It is also understood that, over the years, the criminal figure of embezzlement has been modernized and started to be practiced in the virtual environment, we have noticed a high number of growths of this practice, which has brought harm to commerce, this has encouraged Congress to create a law that typified such conduct, which resulted in publication in Law 14.155/21.

The Stelionate has been one of the crimes that has changed in the last 5 years (2018–2022), they were: law n. ° 13.964/19, which changed the criminal action, which started to proceed upon complaint of the victim, the change of competence, where it is fixed in the place of domicile of the victim, with the exception of the victims of § 5, that is, direct and indirect administration, children or adolescents, people with mental disabilities or people over 70 years of age.

In addition, other changes occurred after the enactment of Law n.° 14.155/21, which included article 171 of the Penal Code, larceny, §2°-A and B, and §4°. Electronic fraud added to the crime of embezzlement, §2— A, has a prison sentence of 04 (four) to 08 (eight) years and a fine, if the fraud is committed with the use of information provided by the victim or a third party, which were induced by error, using social networks, telephone means, false e-mails, or any other electronic means, the legislator left open, the extensive interpretation, being able to reach new forms, or other fraudulent means.

During the study, it was also observed that the increase in the penalty of §2°-B, which applies to the crime when it is committed with the use of a server kept outside the national territory, but this increase will always be calculated, that is, every criminal who committing Electronic Fraud will receive an instant increase in penalty,

---

<sup>63</sup> **Ibidem. SOUTH, (2022, p. 640).**

<sup>64</sup> **Ibid. Brazilian Public Security Forum, (2022, p.112–113).**

as all servers are located abroad, even if they have a company representation in Brazil, processing and storage are outside Brazilian territory<sup>65</sup>.

In the light of all the analyzes carried out in the elaboration of the present study, it is concluded that the new modality of virtual larceny is a crime that is in constant movement, at every moment new forms of scams or ruses appear, it is necessary that the punitive public power of the State, continue to act in the prevention of these illicit acts, popular participation in denouncing the crimes and forwarding the authorities, ensures that there is an adequate investigation and punishment.

## REFERENCES

- [1]. BALDAN, Edson Luis. Fraud. PUC-SP Legal Encyclopedia. Celso Fernandes Campilongo, Álvaro de Azevedo Gonzaga and André Luiz Freire (coords.). Tome: Criminal Law. Christiano Jorge Santos (tome coordinator). 1st ed. São Paulo: Pontifical Catholic University of São Paulo, 2017. Available at: <https://enciclopediajuridica.pucsp.br/verbete/> Accessed on 26. Oct. 2022.
- [2]. BAUMAN, Zygmunt. Liquid Modernity. Translation: Pliny Dentzien. Rio de Janeiro: Jorge Zahar Ed., 2001.
- [3]. BIOLCATI, Fernando Henrique DeO. Internet, Fake News and Liability of Social Networks. (Advanced Civil Law Collection). [Type Publisher Location]: Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276410. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786556276410/>. Accessed on: 08 Oct. 2022.
- [4]. BITENCOURT, Cezar R. commented penal code. Editora Saraiva, 2019. E-book. ISBN 9788553615704. Available at: <https://integrada.minhabiblioteca.com.br/#/books>. Accessed on: 12 Oct. 2022.
- [5]. BITENCOURT, Cezar Roberto. Criminal law treaty: special part: crimes against property up to crimes against religious sentiment and against respect for the dead - arts. 155 to 212. v.3: Editora Saraiva, 2022. E-book. ISBN 9786553622074. Available at: <https://integrada.minhabiblioteca.com.br/#/books> Accessed on: 15 Oct. 2022.
- [6]. BITTENCOURT, Rodolfo Pacheco Paula. Anonymity, freedom, publicity and electronic law, 2016. Available in: [HTTPS://rodolfoppb.jusbrasil.com.br/artigos/](https://rodolfoppb.jusbrasil.com.br/artigos/). Accessed on: May 18. 2021.
- [7]. BRASIL, INPUTEC. Marco civil da internet: what do you need to know and what is your relationship with Igpdp?bahia— BA, 2020. Available at: <https://www.inputec.com.br/marco-civil>. Accessed on: 12. May. 2021.
- [8]. BRAZIL, Chamber of Deputies. Bill No. 4554/20. It combats the practice of electronic fraud, modifies art. 155 of the Decree-Law n.º 2,848, of December 7, 1940 - Penal Code and presents aggravating hypotheses. Available at: <https://www25.senado.leg.br/>. Accessed on: 21. Jan. 2023.
- [9]. BRAZIL, Chamber of Deputies. bill n.º 6444 of 2019. Amends art. 171 of the Decree-Law n.º 2,848, of December 7, 1940, Penal Code, to deal with sentimental embezzlement. Available at: <https://www.camara.leg.br/>. Accessed on: 26. Oct. 2022.
- [10]. BRAZIL, Dec. Law n.º 3689 of October 3, 1941. Criminal Procedure Code. Available at: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Accessed on: 01. Nov. 2022.
- [11]. BRAZIL, Decree n.º 7962 of March 15, 2013. regulates the law n.º 8,078, of September 11, 1990, to provide for hiring in electronic commerce. Available at: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/) Accessed at: 11. Ago. 2022.
- [12]. BRAZIL, Federal Senate. Legislative Decree n.º December 37, 16, 2021. Approves the text of the Convention on Cybercrime, concluded in Budapest on 23 November 2001. Available at: <https://legis.senado.leg.br/>. Accessed on: 08. Jan. 2023.
- [13]. BRAZIL, Law No. 13,853 of July 8, 2019. Amends Law No. 13,709, of August 14, 2018, to provide for the protection of personal data and to create the National Data Protection Authority; and take other measures. Available in: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Accessed on: 19. May. 2021.
- [14]. BRAZIL, Law No. 14,155 of May 27, 2021. Amends Decree-Law No. 2,848, of December 7, 1940 (Criminal Code), to make more serious crimes of violation of a computer device, theft and larceny committed electronically or over the internet; and Decree-Law No. 3,689, of October 3 of 1941 (Criminal Procedure Code), to define competence in.
- [15]. BRAZIL, Law n.º 12,965 of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. Available in: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Accessed on: 19. May. 2021.
- [16]. BRAZIL, Law n.º 12737 of November 30, 2012. Provides for the criminal classification of computer crimes; amends the Decree-Law n.º 2,848, of December 7, 1940— Penal Code; and takes other measures. Available in: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Accessed on: 19. May. 2021.
- [17]. BRAZIL, Law n.º 8072 of July 25, 1990. Provides for heinous crimes, pursuant to art. 5, item XLIII, of the Federal Constitution, and determines other measures. Available at: [https://www.planalto.gov.br/ccivil\\_03](https://www.planalto.gov.br/ccivil_03). Accessed on: 16. Oct. 2022.
- [18]. BRAZIL, Law n.º 8078 of September 11, 1990. Provides for consumer protection and other measures. Available in: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Accessed on: 11. Ago. 2022.
- [19]. BRAZIL, PORTAL G1. Reports of crimes committed over the internet more than double in 2020. Available at: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09>. Accessed on 21. Sep. 22.
- [20]. BRAZIL, Safernet, indicators. Available at <https://indicadores.safernet.org.br/>. Access 01/20/2023.
- [21]. BRAZIL, Constitution of the Federative Republic of Brazil of 1988. Available in: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Accessed on: 19. May. 2021.
- [22]. BRAZIL, Law No. 12,550/11 of December 15, 2011. Authorizes the Executive Branch to create the public company named Empresa Brasileira de Serviços Hospitalares — EBSERH; adds provisions to Decree-Law No. 2,848, of December 7, 1940 — Penal Code; and takes other measures. Available at: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Accessed on: 16. Oct. 2022.
- [23]. BRAZIL, Law No. 14,478 of December 21, 2022. Provides for guidelines to be observed in the provision of virtual asset services and in the regulation of virtual asset service providers; amends Decree-Law No. 2,848, of December 7, 1940 (Criminal Code), to provide for the crime of fraud with the use of virtual assets, securities or financial assets; and amends Law No. 7,492, of June 16, 1986, which defines crimes against the national financial system, and Law No. 9,613, of March 3, 1998, which provides for money laundering, to include the virtual asset service providers in the list of its provisions. Available at: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Accessed on: 11. Jan. 2023.
- [24]. BRAZILIAN PUBLIC SAFETY FORUM. Brazilian Public Security Yearbook: 2022. São Paulo: FBSP, p.110-111.

<sup>65</sup> **Ibidem. SOUTH, (2022, p.638).**

- [25]. CANOTILHO, José Joaquim Gomes, apud REALE, Miguel Junior. *Fundamentals of Criminal Law*. GEN Group, 2020. E-book. ISBN 9788530991609. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Accessed on: 11 Feb. 2023, p.21
- [26]. CORREIA, Pedro Miguel Alves Ribeiro; JESUS Inês Oliveira Andrade - Combating illegitimate bank transfers over the Internet in Portuguese law: between domestic experiences and concerted global policies. *DIREITO GV MAGAZINE | SAO PAULO | V. 12 No. 2 | 542-563 | MAY-AUG 2016*.
- [27]. COSTA, Antonio Manuel de A.A Mockery in the Portuguese Penal Code. [Type Publisher Location]: Grupo Almedina (Portugal), 2020. E-book. ISBN 9789724084428. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9789724084428/>. Accessed on: 25 Feb. 2023
- [28]. COSTA, Taís Barros Trajano Ribeiro da The rise of cybercrime during the COVID-19 pandemic. Faculdade Damas, Recife-PE, 2020. Available at: <https://jus.com.br/> accessed on: May 18, 2021.
- [29]. CUNHA, Rogerio Sanches Penal code for contests: CP.14 ed. rev, current and amp. Salvador: juspodivm 2021, p.667.
- [30]. De Oliveira, M., Lima, V. M., Yamashita, S. M. A., Alves, P. S., & Portella, A. C. (2018). Experimental planning factorial: a brief review. *International Journal of Advanced Engineering Research and Science*, 5(6), 264164.
- [31]. GRECO, Rogerio. Commented Penal Code. [Type Publisher Location]: GEN Group, 2021. E-book. ISBN 9786559770700. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786559770700/>. Accessed on: 16 Nov. 2022, p.545.
- [32]. JAISHANKAR, k. space transition theory of cyber-crimes in crimes of the internet. pearson prentice hall. new jersey, 2008, p. 286.
- [33]. JR., Miguel R. *Fundamentals of Criminal Law*. [Type Publisher Location]: GEN Group, 2020. E-book. ISBN 9788530991609. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Accessed on: 11 Feb. 2023, p.9.
- [34]. LEITE, Luiza; CAMARGO, Matheus. Open Banking: open innovation in the financial system. Editora Saraiva, 2022. E-book. ISBN 9786553620353. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9786553620353/>. Accessed on: 12 Nov. 2022.
- [35]. LÉVY, Pierre, apud, CUNHA, Úrsula Nascimento de Sousa, cyberculture and liquid identities: reflection on culture in the era of new technologies, Magazine: Question Points: Languages, identities and literacies - Vol. 2, no. 2, Jul./Dec. 2012 | 163. Available <https://www.revistas.uneb.br/index.php/pontosdeint/article/view/1558>. Accessed January 11, 2023.
- [36]. LOSSIO, Claudio Joel Brito. *Easy Digital Law Manual: guide for Law and Technology Professionals-2*. Current ed. rev. Ampl- São Paulo: publisher JusPodivm, 2021.
- [37]. MELLO Danilo: Fraud against customers grows 65% by e 2021. Agency Brazil, <https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/fraudes-contra-clientes-de-bancos-crescem-165-em-2021>. São Paulo, publication 10/29/2021. Accessed on 08/28/2022.
- [38]. MENDES, Gilmar F.; BRANCO, Paulo G. *IDP Series - Doctrine Line— Constitutional law course*. Editora Saraiva, 2020. E-book. ISBN 9788553618088. Available at: <https://integrada.minhabiblioteca.com.br/#/books/9788553618088/>. Accessed on: 11 Feb. 2023, p.945.
- [39]. NUCCI, Guilherme de Souza. *Code of Criminal Procedure commented*. 20. ed. rev., current., ampl Rio de Janeiro: Forense, 2021. E-book. (1 online resource). ISBN 9788530993474. Available at: <https://integrada.minhabiblioteca.com.br/>. Accessed on: 10 Jul. 2022.
- [40]. PATURY, Fabrício Rabelo, Fernanda Veloso Salgado. The Criminal Policy of the Nucleus for Combating Cyber Crimes of the Public Prosecutor's Office of the State of Bahia in the face of crimes committed in the digital sphere. MPBA. Available at [https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a\\_politica\\_criminal\\_do\\_nucleo\\_de\\_combate\\_aos\\_crimenes\\_ciberneticos\\_do\\_ministerio\\_publico\\_do\\_estado\\_da\\_bahia.\\_-\\_fabricio\\_rabelo\\_patury\\_e\\_fernanda\\_veloso\\_salgado.pdf?download=1](https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a_politica_criminal_do_nucleo_de_combate_aos_crimenes_ciberneticos_do_ministerio_publico_do_estado_da_bahia._-_fabricio_rabelo_patury_e_fernanda_veloso_salgado.pdf?download=1). a ceased on 02/13/2023.
- [41]. PEACE, E.H. Liquid Literature: narration in a digital environment. *crossings*, Cascavel, v. 11, no. 3, p. 222–234, 2017. Available at: <https://e-revista.unioeste.br/index.php/travessias/article/view/18165>. Accessed on: 11 Jan. 2023.
- [42]. PINHEIRO, Patricia Peck. #digital law. 7. ed. rev., ampl., current São Paulo: Saraiva Jur, 2021. E-book. (1 online resource). ISBN 9786555598438. Available at: <https://integrada.minhabiblioteca.com.br/books/9786555598438>. Accessed on: 10 Jul. 2022, p.26.
- [43]. PORTUGAL. Portuguese penal code. Available in: <https://www.codigopenal.pt/>. Accessed on 25. Feb. 2023.
- [44]. SYDOW, Spencer Toth. *Computer crimes and their victims*. 2nd ed. São Paulo: Saraiva Jur, 2015. E-book. (1 online resource). (Monographic knowledge). ISBN 9788502229488. Available at: <https://integrada.minhabiblioteca.com.br/>. Accessed on: 2 Oct. 2022.
- [45]. SYDOW, Spencer Toth. *Computer Criminal Law Course, general and special part*. 3rd ed. rev. e. current. Salvador: Editora JusPodivm, 2022.
- [46]. VIANA, Eduardo-criminology, 9. Ed. rev. Current. And ampl-Salvador: Juspodivm, 2021.
- [47]. WENDT, E. CYBER WARFARE, CYBER INTELLIGENCE AND VIRTUAL SECURITY: some aspects. *Brazilian Intelligence Magazine*, no. 6, p. 15–26, 1 Apr. 2011.