South American Publishing

SAP Netnography. 2024;2:76
doi: 10.62486/net202476

ORIGINAL

New types of crime and their classification in the Argentine Criminal Code

Nuevas modalidades delictivas y su tipificación en el Código Penal Argentino

Sabrina Ivana Bof[1]

[1] Universidad Siglo XXI, Especialización en cibercrimen. Argentina.

Submitted: 05-01-2024 | Revised: 28-03-2024 | Accepted: 05-08-2024 | Published: 06-08-2024

ABSTRACT

Introduction: the rise of information technology has transformed everyday life, but it has also created fertile ground for the emergence of new crimes. In Argentina, cyber scams are one of the fastest-growing threats, affecting both individuals and public and private institutions. These criminal activities include financial fraud, identity theft, and computer manipulation, which cause significant economic damage and undermine digital trust. This paper analyzed the evolution of cyber scams, current legislation in the country, and its adequacy in the face of current technological challenges. Development: using a mixed approach, legal precedents such as Law 26.388 on computer crimes and adherence to the Budapest Convention were reviewed, in addition to the classification of computer fraud in the Penal Code. It was found that, although these regulations represented progress, they are insufficient in the face of new forms of digital deception. These include phishing, spear phishing, scamming, vishing, and pyramid schemes, which are enhanced by artificial intelligence and social engineering. A comparative study with foreign legislation (US, Japan, European Union) showed that Argentina lags behind in terms of regulations and needs to strengthen international cooperation, training for judicial operators, and public awareness. Conclusion: cyber scams require a comprehensive legal and technological response. The Penal Code needs to be reformed to criminalize specific behaviors such as identity theft and fraudulent use of social media. Only through updated laws, digital education, and inter-institutional coordination will it be possible to reduce the impact of these threats on Argentine society.

Keywords: Cyber Scams; Computer Crimes; Phishing; Argentine Criminal Code; Artificial Intelligence.

RESUMEN

Introducción: el auge de las tecnologías de la información ha transformado la vida cotidiana, pero también ha generado un terreno fértil para la aparición de nuevos delitos. En Argentina, las ciberestafas constituyen una de las amenazas más crecientes, afectando tanto a personas como a instituciones públicas y privadas. Estas conductas delictivas incluyen fraudes financieros, robo de identidad y manipulación informática, que producen daños económicos significativos y socavan la confianza digital. El presente trabajo analizó la evolución de las ciberestafas, la legislación vigente en el país y su adecuación frente a los desafíos tecnológicos actuales. Desarrollo: a partir de un enfoque mixto, se revisaron antecedentes legales como la Ley 26.388 de delitos informáticos y la adhesión al Convenio de Budapest, además de la tipificación del fraude informático en el Código Penal. Se detectó que, si bien estas normas representaron avances, resultan insuficientes ante las nuevas modalidades de engaño digital. Entre ellas destacan el phishing, spear phishing, scamming, vishing y las estafas piramidales, potenciadas por la inteligencia artificial y la ingeniería social. El estudio comparado con legislaciones extranjeras (EE.UU., Japón, Unión Europea) mostró que Argentina presenta rezagos normativos y necesita fortalecer la cooperación internacional, la capacitación de operadores judiciales y la concientización ciudadana. Conclusión: las ciberestafas exigen una respuesta jurídica y tecnológica integral. Es necesario reformar el Código Penal para tipificar conductas específicas como el robo de identidad y el uso fraudulento de redes sociales. Solo mediante leyes actualizadas, educación digital y coordinación interinstitucional será posible reducir el impacto de estas amenazas en la sociedad argentina.

Palabras clave: Ciberestafas; Delitos Informáticos; Phishing; Código Penal Argentino; Inteligencia Artificial.

INTRODUCTION

The advancement of information and communication technologies (ICTs) has brought a series of benefits to society, but it has also created new opportunities for criminals.

In today's digital era, cyber fraud has become an increasingly frequent and sophisticated threat. These criminal modalities, which are carried out through electronic or computer-based means, have a significant impact on victims, both at the individual and economic levels.

This paper will analyze the issue of cyber fraud in Argentina, emphasizing the new criminal modalities that have emerged in recent years. Likewise, it will examine the existing regulations in the Argentine Criminal Code for this type of crime and assess whether they are sufficient to adequately address the complexity of these new forms of criminality.

METHOD

Methodological approach

This work will be based on a qualitative and quantitative approach. The qualitative approach will make it possible to understand the experiences and perspectives of victims of cyber fraud, as well as the opinions of experts in cybersecurity and computer law. The quantitative approach, in turn, will allow for the analysis of statistical data on the incidence of cyber fraud, the most common modalities, and the most affected victims.(1)

Hypothesis

The Argentine Criminal Code has significant limitations for the criminalization of new modalities of cyber fraud, which creates difficulties for the prosecution and punishment of cybercriminals, contributing in turn to the increase in these criminal modalities and to the negative impact on victims. The incorporation of specific criminal offenses into the Argentine Criminal Code, as well as the training of legal practitioners and cooperation between the public and private sectors, are fundamental elements for addressing this challenge.

Regulatory background

In the last decade of the twentieth century, as a consequence of the arrival of electronic commerce, the Argentine Republic found itself immersed in the need for regulatory updating.(2)

Thus, various laws were enacted, among which the following can be mentioned:

Law 24.766 (1996) Confidentiality regarding information and products that are legitimately under the control of one person and are improperly disclosed contrary to honest commercial practices.

Intellectual Property Law 11.723 (1998): which penalizes anyone who reproduces, stores, exhibits, or imports illegitimate copies.

With the arrival of the new century, technological advances, and the emergence of cybercrimes, in the year 2 000, the Personal Data Protection Law (Law 25.326) was enacted for the comprehensive protection of personal data, stored in files, records, and databases. In 2008, Law 26.388 on Computer Crimes, which modified the Argentine Penal Code by incorporating into its articles various criminal offenses arising from the use of new technologies.

In 2013, Law 26.904, which incorporates the offense of grooming into Article 131 of the Criminal Code.

Convention on Cybercrime

Known as the Budapest Convention, it was signed in the city that gives it its name on 23 November 2001, and entered into force on 1 July 2004. Promoted by the Council of Europe, it is the first international instrument that specifically addresses cybercrime, as emerges from its preamble, which is based on the need to implement a common criminal policy to protect society from cybercrime, through the adoption of adequate legislation and the improvement of international cooperation. It expresses concern that computer networks and electronic information may be used to commit crimes, recognizing the need to prevent such acts that may endanger the confidentiality, integrity, and availability of data and computer systems, ensuring the criminalization of such acts as crimes.

In its articles, Article No. 1 establishes the meaning: computer system, computer data, service provider, traffic data; then, between Articles 2 and 10, it commits the parties to take legislative or

other measures to criminalize a series of offences, namely: illegal access (Art. 2), deliberate and illegal interception (Art.3), attacks against data integrity (Art. 4), attacks on system security (Art. 5), misuse of devices (Art.6), computer-related forgery (Art. 7), computer-related fraud (Art. 8), child pornography (Art. 9), infringements of intellectual property and related rights (Art. 10). In Article 11 et seq., it commits the parties to adopt legislative or other measures necessary to criminalize in their domestic law any complicity in the commission of the offences provided for above, leaving it to the discretion of the parties to apply them in whole or in part or not to apply them in matters of attempt.

Article 12 commits the Parties to adopt measures to hold legal persons liable for the offences provided for in the Convention, establishing in Article 13 that sanctions must be effective, proportionate and dissuasive, including custodial penalties, and that the imposition of criminal or non-criminal sanctions or measures on legal persons considered responsible must be guaranteed.

Article 15 refers to the conditions and safeguards and establishes: "The Parties shall ensure that the establishment, implementation, and application of the powers and procedures provided for in this section are subject to the conditions and safeguards provided for in their domestic law, which must ensure adequate protection of human rights and freedoms and, in particular, of the rights deriving from various international instruments relating to human rights."

In its Articles 16 to 21, it discusses measures for conservation, dissemination, communication, registration, confiscation, and interception of data, as well as rules concerning jurisdiction, international cooperation, extradition, collaboration, accession to and implementation of the Convention, etc.

Subsequently, the "Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" (the "Protocol") was enacted, and in 2022 the Second Additional Protocol (3) was approved; it aims to strengthen international cooperation and facilitate the obtaining of electronic evidence in order to provide an effective response in criminal investigations against cybercrime. The Argentine Republic participated, among others, in its drafting.

Argentine Penal Code (4)

In 2008, Law 26,388, known as the "Cybercrime Law," was enacted; it incorporates the principles of the Budapest Convention, although our country acceded to that Convention only in 2017 through Law 27,411. Its articles reflect the incorporation of recommendations made by the Council of Europe.

Law 26.388 on Computer Crimes amended the Argentine Criminal Code by incorporating into its articles various criminal offenses related to the use of new technologies.

Thus, in the area of computer crimes against liberty, the law amends Article 153 of the C.P., which in its first paragraph criminalizes accessing, taking possession of, deleting, or diverting an electronic communication that is not addressed to the person. The penalty is greater if the content of the electronic communication is published. In this case, the law protects written communication between persons against undue interference by a third party, whether by accessing it, intercepting it, or diverting it from its purposes.

Article 153, first paragraph, second part, of the C.P. punishes anyone who improperly takes possession of an electronic communication, a letter, a document, a dispatch, or other private paper, even if it is not closed.

The third part of the first paragraph of art. 153 punishes the conduct of anyone who improperly suppresses or diverts from its destination any correspondence or communication not addressed to that person.

The third paragraph of art. 153 of the CP aggravates the penalty if the offender also communicates it to another or publishes the content of the letter, writing, dispatch, or electronic communication.

Likewise, this Law incorporates art. 153 bis, penalizing the conduct of "illegitimately accessing a system or computer data of restricted access." The penalty is aggravated when the access is to the detriment of a system or computer data of a state public body or of a provider of public financial services.

On the other hand, it replaces article 155 of the Criminal Code with the following: "Anyone who, being in possession of correspondence, an electronic communication, a sealed sheet, a telegraphic, telephone or other dispatch not intended for publicity, causes them to be improperly published, if the act causes or may cause damage to third parties shall be punished with a fine of one thousand five hundred pesos ($1,500) to one hundred thousand pesos ($100,000). Anyone who has acted with

the unequivocal purpose of protecting a public interest is exempt from criminal liability."

It also replaces article 157 of the Criminal Code, which is worded as follows: "A public official who reveals facts, actions, documents or data, which by law must be secret, shall be punished with imprisonment of one (1) month to two (2) years and special disqualification from one (1) to four (4) years." The only modification to article 157 is the addition of the word "data". This is how this figure is updated, in which the subject must be a public official who becomes aware of data, actions, facts or documents that by law are secret and that the official also reveals them despite knowing this circumstance.

Article 157 bis- "Anyone who: 1. Knowingly and illegitimately, or in violation of confidentiality and data security systems, accesses, in any way, a personal data bank, shall be punished with imprisonment of one (1) month to two (2) years. 2. Unlawfully provides or discloses to another information recorded in a file or in a personal data bank whose secrecy he is obliged to preserve by law. 3. Unlawfully inserts or causes to be inserted data in a personal data file. When the author is a public official, he shall also suffer a penalty of special disqualification from one (1) to four (4) years.":

The following is incorporated as a second paragraph of Article 183 of the Criminal Code: The same penalty shall be incurred by any person who alters, destroys, or renders useless data, documents, programs, or computer systems; or who sells, distributes, circulates, or introduces into a computer system any program intended to cause damage.

It provides for the replacement of Article 184, Article 197, and Article 255 of the Criminal Code with the following:

Article 184: The penalty shall be 3 (3) months to 4 (4) years of imprisonment if any of the following circumstances is present: 1. committing the act for the purpose of preventing the free exercise of authority or in revenge for its determinations; 2. causing infection or contagion in birds or other domestic animals; 3. using poisonous or corrosive substances; 4. committing the offense in an uninhabited place and as part of a gang; 5. committing it in archives, registries, libraries, museums, or on bridges, roads, promenades, or other property for public use; or in tombs, commemorative signs, monuments, statues, paintings, or other art objects placed in public buildings or places; or in public data, documents, programs, or computer systems; 6. committing it in computer systems intended for the provision of health services, communications, energy supply or transportation, means of transport, or another public service.

Article 197: Whoever interrupts or obstructs telegraphic, telephone, or other communications, or violently resists the restoration of the interrupted communication, shall be punished by imprisonment of 6 (6) months to 2 (2) years.

Article 255: Anyone who removes, alters, conceals, destroys, or renders useless, in whole or in part, objects intended to serve as evidence before the competent authority, records, or documents entrusted to the custody of a public official or another person in the interest of the public service, shall be punished by imprisonment of one (1) month to four (4) years. If the perpetrator is the same depositary, he shall also suffer special disqualification for two years. If the act is committed due to the imprudence or negligence of the depositary, the latter shall be punished with a fine of seven hundred and fifty pesos ($750) to twelve thousand five hundred pesos ($12,500).

The law incorporates the following as subsection 16 of Article 173 of the Criminal Code:

Subsection 16. Any person who defrauds another by means of any computer manipulation technique that alters the normal functioning of a computer system or the transmission of data.

In addition to the articles indicated, although the Argentine Criminal Code does not contain a specific chapter, there are some provisions that may apply to this type of crime. For example:

Article 172: "Anyone who defrauds another with an assumed name, simulated quality, false titles, false influence, breach of trust or by pretending to be goods, credit, commission, company or negotiation or by using any other trick or deception shall be punished with imprisonment of one month to six years."

Art. 173, subsection 15. Whoever commits fraud through the use of a purchase, credit, or debit card, where such card has been forged, adulterated, stolen, taken by robbery, lost, or obtained from the legitimate issuer by trickery or deceit, or through the unauthorized use of its data, even if committed by means of an automated transaction. (Subsection incorporated by art. 1° of Law No. 25.930 B.O. 21/9/2004)

However, these provisions have been criticized for being generic and for failing to consider the particularities of cyber scams.(5)

New Modalities of Cyberfraud

As previously mentioned, new types of crime are appearing daily in which bank account

holders are the victims and in which criminals resort to various criminal maneuvers.(6,7,8)

In particular, credit card fraud offenses have been among those with the greatest growth in recent times. This type of crime, in addition to card theft, encompasses other methods used to capture credit card data. For example, these methods include skimming (the theft of data at ATMs for card cloning) and phishing.(9,10,11)

The passive subjects, the victims of this class of crime, can be individuals, companies, government organizations, etc.

From a recent report presented by CERT.AR (12), it follows that phishing continues to be the main threat, accounting for 75% of incidents reported in 2023, with an evolution observed in the techniques used and more sophisticated attacks via social media.

a) Social engineering: On Interpol's website, one can read that "Fraud based on social engineering encompasses all methods used by criminals to exploit a person's trust in order to obtain money directly or confidential information that allows them to commit a subsequent crime. Social media are the preferred channel for this, although it is not unusual for contact to be made by telephone or in person." (13)

b) Credit card fraud: following the wording of Article 173, paragraph 15 of the C.P., fraud includes purchase, credit or debit cards when they have been forged, adulterated, stolen, robbed, lost or obtained from the legitimate issuer by trickery or deception, or through the unauthorized use of their data, even when carried out by means of an automated operation.

Following Donna,(14) the doctrine has classified frauds committed with credit or debit cards into:

1) Payments by presenting someone else's card (stolen, robbed or lost); 2) Payments by presenting counterfeit cards and 3) use of cards at ATMs.

The offense requires that the card has been: forged (that is, its issuer has never produced it for the person who holds it; this involves passing off as genuine a card that is not genuine); altered (that is, the card has been materially altered, which presupposes that a genuine card exists and that elements that are not genuine have been added to it); stolen, robbed (unlawfully dispossessed), lost (that is, it is outside the sphere of custody or availability of its holder for a cause other than those mentioned, whether because they forgot it, for example, in a store, or misplaced it); lastly, it contemplates that the subject has obtained it from a legitimate issuer by means of trickery or deceit, understanding as issuer the banking or financial entity that issues credit cards, for example by falsifying their identity.

The other case is that fraud has occurred "through the unauthorized use of data"; in this case, the use of the card in physical form does not matter, but rather the data contained in it, which becomes relevant when dealing with remote transactions.

Nowadays it is normal to make purchases online in which the buyer is asked for the debit or credit card numbers and the DNI of the cardholder, with no way to verify that the person making the purchase is the person listed as the cardholder.

Finally, the article mentions "even if it were performed through automatic operations," referring to those operations in which the subject does not deal with another person but with a machine, this being where most doctrinal discussions arise, since "a machine cannot be deceived."

Within this type, we can mention, for example, skimming: these are devices placed on ATMs that fraudulently copy the magnetic stripe in order to later physically clone the card.(15) This maneuver is often accompanied by the use of a camera or device that allows filming or obtaining the card's PIN and then using it to carry out the fraudulent maneuver.

c) Phishing: we can define it as the ability to duplicate a web page in order to make the user believe that they are entering the original web page and thereby obtain sensitive information, such as passwords, usernames, card numbers, etc., as well as the sending of fake emails or text messages that appear to be from a legitimate institution to obtain personal or financial data from the victim.(16,17,18,19)

In short, it is a set of social engineering techniques used by cybercriminals to fraudulently obtain confidential information from one person and thereby assume that individual's identity.

In this case, "the author (phishermen) uses computer means to fraudulently obtain the personal data of the holder of a bank account to access it via home backing".(20,21)

This crime is a complex phenomenon that requires a preparation stage, that is, the use of social engineering, the creation of a website similar to that of the original company, organization, or institution, necessary for the intended purpose, and then the deception begins.

It can be committed by sending emails impersonating a banking entity or an organization or business, so that the recipient accesses the link sent or completes a form and, after this, seizes sensitive information and thereby makes transfers or withdrawals of funds, whether to a single

account, several accounts, or successive transfers.

The active subjects of the crime of phishing, known as phishers, "pretend to belong to banking institutions of recognized prestige and request from internet users credit card data or banking passwords, through a form or an email with a link that leads to a fake web page with an appearance similar to the original website".

After the information is obtained, the cybercriminal can either use the data to carry out, for example, an online purchase by providing the card numbers, passwords, username, etc., that were provided by the victim, or make a transfer of funds to other accounts that the criminal may have.

Spear Phishing: This is a type of phishing attack directed at a specific individual. The target is usually someone with privileged access to confidential data or with certain authority that can be exploited by the scammer, such as a chief financial officer, a treasurer, etc., individuals who can move money from a company's accounts.(22)

The cybercriminal uses social engineering, conducts a study of the target in order to gather the necessary information to impersonate or pass themselves off as one person or entity that the target really trusts (a friend, a boss, a colleague, a supplier, or one trusted financial institution). Much of this information is obtained from social media, or professional pages where people congratulate or greet their colleagues or promote their suppliers and tend to share too much.

These cybercriminals use their research to craft messages with specific personal details, thereby making them appear highly credible to the target.

d) Pharming: although it has the same purpose as Phishing, in Pharming there is no bait with which to lure the user to a website where their data will be stolen; rather, Pharming attacks the user directly, accessing their computer (either the host or the DNS server) and sending them directly to the website where the information will be stolen from them (instead of giving them the option to click, or not, on a link).

It is a cyberattack whose objective is the theft of sensitive information. In these cases, cybercriminals carry out a DNS attack by which they manage to redirect users to a fake website, which has the official domain name, for the purpose of stealing their private information.

The following can be read on Banco Santander's website in this regard: "Imagine for a moment that you are in a car driving along a road toward a country house to enjoy a few days of vacation. You follow all the signs along the way, including a sign that makes you turn right and that, without you noticing, diverts you from your destination. Then, instead of reaching the original house, you end up somewhere else without knowing why, how it happened, or where the failure was. In the same way, but in the virtual world, pharming operates, a fraud that consists of altering legitimate web pages or servers to redirect users to pages that impersonate the originals in order to steal their personal data or money".(23)

e) Vishing: fraud in which the criminal clones the victim's voice and uses it to send messages via WhatsApp requesting money or to carry out another type of fraudulent maneuver.

f) Scamming: This is among the greatest risks faced by internet users.(24)

These are scams committed through the internet or by electronic means, generally through fraudulent websites, emails, social media, dating app profiles, telephones, etc.

Unlike other cybercrimes, in this case the scammer does not need to be a hacker or have extensive computer knowledge, because they generally use social engineering to deceive potential victims.

The objective of cybercriminals is to deceive the user to achieve an end, generally to obtain money from their victim under the pretext of offering a greater reward. They generally offer opportunities for travel, prizes, loans, donations, lotteries, offers, courses, promotions, and scholarships, thereby convincing the user to provide their personal data, account numbers, etc.(15)

There are different types of scamming, among the most common of which are the following:

g) Romance scam: This occurs through dating websites. In this case, the scammer impersonates a fictitious person and establishes a trusting relationship with another person – the victim – until making the latter develop romantic feelings. After obtaining the victim's emotional dependence, the scammer asks the victim for money, for example, to buy tickets to travel to the country and meet in person, or claiming to have financial problems. This is one of the most dangerous scams because, since the victim is emotionally attached, the victim does not realize that she has been scammed until she has handed over large sums of money.

This type of cybercrime is not recent; it has been developing since the emergence of the Internet. At first, scammers operated through chat rooms or forums, or through emails, with the aim of getting a victim to hand over money. The methods have now evolved, involving large fraudulent organizations, complex techniques, fake profiles, retouched photographs, or the collection of information relevant to the victim, making the use of social engineering a key element in com-

mitting this type of crime.

h) Job offers: Here the offender exploits the victim's desperation for a source of income by offering a fake job and, in exchange, asking the victim to deposit money in order to purchase, for example, work materials, or even to deposit a small sum in order to be able to join the "company".

i) Real estate rental: The approach is similar to that of the fake job offer, but here the offender posts a property for rent; when contacting the victim, the offender sends photographs of the dwelling, directions to the location, etc., and, in exchange for the reservation, asks the victim for a money deposit. Then, when the victim arrives at the location, the victim does not find the dwelling and cannot locate the supposed landlord.

j) Nigerian scam or Nigerian fraud: This is very common; in these cases, the victim is called by telephone or sent an email and told that they have a large sum of money to collect, for example from an inheritance or by a court ruling, and that in order to receive it, they must pay an advance.

Use of Artificial Intelligence to Commit Scams through Social Engineering

With the advancement of AI, the techniques used by cybercriminals have become more sophisticated in order to manipulate people and make them reveal confidential information, with effective results. In these scenarios, the following can be mentioned:

Phishing: This is how AI can analyze social media data and create highly convincing phishing emails targeted at specific individuals.

Likewise, generative artificial intelligence tools can also be used to create phishing messages. These tools allow the creation or generation of personalized text messages or emails that lack grammatical errors or any other warning or suspicion sign customary in cases of identity impersonation.

In turn, generative AI can also help scammers expand their operations. According to IBM's X-Force Threat Intelligence Index, a scammer takes 16 hours to manually create a phishing email. With AI, scammers can create even more convincing messages in only 5 minutes.

Scammers also use image generators and voice synthesizers to make their scams more credible. For example, in 2019, attackers used AI to clone the voice of the CEO of an energy company and defraud a bank director of 243 000 dollars.(25)

Deepfakes and identity impersonation: Deepfakes are videos, images, and/or voice files that are manipulated with artificial intelligence software to appear real and authentic; cybercriminals use them to extort or manipulate victims or to commit fraud.

Malicious chatbots: these interact with victims in such a way as to obtain sensitive data.

Exploration of vulnerabilities, since AI can quickly detect flaws in software and networks that attackers can exploit before they are fixed.

Theft, usurpation, or identity impersonation

These are acts in which criminals use personal data to impersonate another person whose identity they have stolen.

These thefts, together with the anonymity of online transactions, are used to commit different types of crimes, from fraud to terrorist acts; among the most important and current, the following can be mentioned: bank fraud, online extortion, and money laundering.(26)

This crime can be committed through the theft, loss, or photocopying of the DNI, or even through the acquisition of personal data obtained from different places.

In digital contexts, digital identity theft, whether on the Internet or on social media, occurs either by impersonating the digital identity of an Internet and social media user, or by stealing their passwords and credentials to access them, generally for criminal purposes.(27)

Identity theft is not defined in our legal system as a specific crime, so it is necessary to resort to the general offense of fraud. However, various bills have been introduced in the National Congress.

Identity is the set of traits proper to an individual that characterizes that individual in relation to others, with digital identity understood as a manifestation of identity in virtual life in cyberspace.

Consequently, the legally protected interest in this type of crime is identity and, therefore, dignity and privacy.

Digital identity theft can occur in various ways, although its basic elements and purpose are the same: obtaining personal information to cause some type of harm.

Identity impersonation and identity usurpation share the improper manipulation of one person's identity without their consent, and the fact that the offender seeks some type of benefit through deception, with victims potentially suffering financial and emotional harm and even harm to their reputation. However, there are some differences between them.(28,29)

The main difference is that impersonation focuses on superficial imitation, such as using

someone's name or image online, whereas in usurpation, there is a complete and continued appropriation of identity, making its planning and execution more complex.

This behavior is usually the prelude or the first link for the commission of certain illicit activities that are indeed criminally punished, as is the case with fraud and crimes against sexual integrity such as grooming.

However, that conduct per se does not constitute a crime, insofar as it would be a preparatory act for another crime.

Pyramid Scheme and Ponzi Scheme

Pyramid scams and Ponzi schemes have points in common, and also some differences. In both cases, it is about recruiting more and more participants to achieve the profits they promise.

They originate from a criminal act that took place in the United States in the decade of 1920, in which an Italian named Carlo Ponzi started a company that promised its clients a 50 % return within a period of 45 days, or 100 % within 90 days. What was interesting about the proposal was that these profits were obtained by the simple act of buying discontinued postal coupons in other countries and redeeming them at face value in the United States.

This scheme devised by Carlo Ponzi did not really depend, as he claimed, on coupon trading; rather, the returns for the first investors were paid with the money of new investors.(30)

With this proposal of high returns, Ponzi attracted many investors, since the better known he became, the greater the number of people who invested, and the more the fraud spread.

Ponzi attracted thousands of people with the promise of extraordinary returns, and the more people invested, the more his fraud spread.

At first everything worked, or at least seemed to work normally; however, as more people joined the fraud, payment obligations increased, so more money was required in order to fulfill the promises made.

Finally, in 1920, the scheme collapsed and Ponzi ended up being arrested, tried and convicted of fraud.

In 2013, with the emergence of cryptocurrencies, in the USA, the Securities and Exchange Commission (S.E.C.) filed the first civil lawsuit against Trendon T. Shavers, also known as "Pirateat40," and his company Bitcoin Savings and Trust.

Shavers' scheme is known as the first Ponzi scheme in the crypto world. What he did was promise investors large profits, of up to 7% weekly, by buying bitcoin at a low price and selling it at a higher price on the market. Obviously, this attracted many investors.

However, he did not invest that money, nor did he carry out the bitcoin business activities he promised; instead, he used the money from new investors to pay the old ones. When he could no longer pay everyone, the scam collapsed, leaving estimated losses of more than 700 000 bitcoins. This case marked the beginning of a series of similar frauds in the crypto world and throughout the world.

What does a pyramid scheme consist of? It is a business scheme that is presented as an opportunity to obtain a large economic return; people are led to believe that they will be part of an attractive business model, in which they will double or triple their investments in a short time. To take part, they must make a monetary investment and are encouraged to recruit new investors who want to be part of this network.

The issue centers on the fact that the business is a front; in reality, no such business exists, and with the money that comes in from new participants, older investors are paid, making them believe that everything is working perfectly. It is called "pyramidal" because few receive money, while those at the base of the pyramid are the ones who are harmed.

Some of these scams are known by names such as the "Flower of Abundance", "Prosperity Mandala", "Loom of Dreams", "Friendship Wheels", among others. All of them promise quick and high income in exchange for an initial contribution.

This model is related to the "Ponzi scheme," which is another fraudulent system that differs only in a sole detail: that something is indeed invested in.

As far as our country is concerned, in 2022 the Grupo Zoe began to gain media coverage, as it was presented as an entity that combined coaching, education, and financial services, and another in which they reported the group's great growth to the point of launching the cryptocurrency Zoe Chash, the NGO BITCOIN ARGENTINA filed the complaint against the CEO of Generación Zoe, Leonardo Positorto, for the crimes of fraud, unauthorized financial intermediation, and illegal fundraising.

The Group's maneuver consisted of:

1. They promoted the cryptocurrency Zoe Cash as an investment that was backed by gold, which was not true.
2. They offered coaching programs with promises of exorbitant profits, thereby attracting a large number of investors with false expectations.
3. They promoted investments through a trust that did not have authorization from either the Central Bank or the National Securities Commission.
4. They used the logo of the National Securities Commission, making it appear that they had the backing or authorization of the agency.
5. They issued misleading publications in media outlets and social media promoting Zoe Cash as a high-yield investment.
6. It operated as a Ponzi scheme, because the money received was used not to invest but to pay old investors

Both pyramid fraud and the Ponzi scheme system are crimes that are classified in Articles 309 and 310 of the Criminal Code, which punishes the crime of unauthorized financial intermediation.

Legal Framework

Upon establishing the criminal modality of these new behaviors, it remains to define under which criminal offense the facts would be classified and, in the absence of specific legislation, when the time comes, a choice must be made between the offenses of theft or fraud.

In this regard, voices are raised both in favor and against.

Thus, if we take into account a classic phishing maneuver in which one person, using another person's data, makes a purchase through Mercado Libre, for example, where the data are recorded by a machine, here there is no fraud, inasmuch as the machine cannot be deceived; or in cases in which home banking is accessed with another person's data, here there is likewise no error, deception, or disposition of assets.

Now then, with the reform of Law 26.388, art. 173 inc. 16 of the C.P. was included as one special case of fraud, contemplating the scenario when the maneuver is carried out "through any computer manipulation technique that alters the normal functioning of a computer system or data transmission."

For the purposes of analyzing the offense type, we must refer to the basic figure provided for in art. 172 of the C.P., that is, deceit or deception, error, act of detrimental disposition of property. However, it is noted that, in the first place, for the configuration of the criminal offense type, the provision requires the alteration of the normal functioning of a computer system or data transmission system.

But if we take into account the maneuver deployed by the active subjects of these crimes, that is, the sending of an email impersonating a company, banking institution, etc. that leads the victim into error, who provides sensitive data, which will later be used by the offender for the purpose of seizing the victim's money, here there is no alteration of the normal operation of a computer system, and the victim did not even make a patrimonial disposition, because it is the active subject himself who uses the credentials to subsequently obtain the money, so that for this special type of fraud to be constituted, only 3 typical elements would suffice: trickery or deception, error, and detrimental patrimonial disposition.

The situation differs in the case of phishing through malware, in which the active subject implants a virus or a Trojan on the victim's system in order to be able to extract information or obtain access credentials.

Digital identity theft is another activity that is currently not criminalized under Argentine law, despite various bills pending parliamentary consideration.

These are behaviors in which a first and last name, photographs, or images are used to create a profile, whether on a social network or a website, in order to impersonate the person claimed to be or whose image is displayed.

Such conduct may pursue different purposes, whether in cases of grooming, or in cases of fraud such as romance scams – among others – or even to commit slander and libel; however, until it can be determined what the purpose is, the offender's act will remain a preparatory act.

At the national level, none of these behaviors is penalized as an autonomous offense. Only in the Autonomous City of Buenos Aires are they regulated in the Contraventional Code:

- Art. 64 CC: Supply of pornographic material to minors through computer media.
- 71 bis CC: Unauthorized dissemination of intimate images or recordings. The victim may have consented to the obtaining of such images in a private space, but NOT to their mass distribution.

- 71 quinquies CC: Digital identity impersonation. These are cases in which the cyberaggressor creates a false digital profile by impersonating the victim and, through it, commits other crimes in another person's name.

Cyber Mules: Participants, Accessories, or Victims

In this victim-offender relationship, the figure of the cyber mule is added. These are people who, often unknowingly, provide their bank account so that deposits are made into it or transfers are carried out with money obtained from cyber fraud.

In several cases, these people are contacted through a job offer, in which they are "hired" to perform commercial intermediation tasks, and for which they must have a bank account into which transfers will be made and from which they will make transfers or withdraw funds in order to deliver them to the phisher; that is, these are simple tasks in exchange for a sum of money.

However, from a legal standpoint, the question arises as to whether we are dealing with an accessory after the fact or a participant.

Those who maintain that the conduct of cyber mules falls within the offense set forth in art. 277 inc. 1 ap. C, of the C.P., consider that it constitutes subsequent assistance to the perpetrators of the fraud.

For others, by contrast, the mule receives money derived from a criminal offense and gives it the appearance of lawful origin, with their conduct falling within the scope of money laundering (art. 303 of the C.P.).

Most legal doctrine holds that in reality these are necessary participants in the fraud, since their conduct facilitates the commission of the offense, which could not have been carried out or consummated without their participation.

This was held by Chamber 7 of the National Chamber of Appeals in Criminal and Correctional Matters of the Autonomous City of Buenos Aires, in its ruling of 2/11/22, which confirmed the indictment of the defendant for the crime of fraud, accused of providing his bank account to receive money of fraudulent origin, in order to transfer it immediately to other accounts, given that the provision of a bank account as an intermediate or final destination for the transfer of electronic money obtained through any form of fraud serves the material completion of the criminal offense. (Judges: Mariano A. Scotto - Juan Esteban Cicciaro - Id SAIJ: FA22060033)

Comparative Law

Some of the countries that have been pioneers in combating cyber fraud and have robust legislation include:

United States

With a highly digitalized economy, the United States has numerous federal and state laws to combat cybercrime.

Thus, in 1988 it passed the Identity Theft Act, providing for up to 15 years in prison for the conduct of any individual who illegally uses another person's means of identification to carry out any illegal activity. Such conduct is considered a federal crime.

Also, its Computer Fraud and Abuse Act (CFAA) punishes a wide range of computer crimes, including cyber fraud, and was pioneering in this area.

Particular attention should be paid to the so-called "Anti Phishing Act" of the State of New York, which penalizes any person who, using electronic means, requests, solicits, or collects personal information in order to deceptively represent a company or government agency, without due authorization to do so.

Japan

With a strong tradition of privacy protection, it has implemented specific laws to combat cyber scams.

In 2000, the Law on the Prohibition of Illegal Access Acts was passed, consisting of 14 articles, establishing in art. 1 its objective of preventing cybercrime and maintaining order in telecommunications.

This Law refers to unauthorized access to another person's computer, focusing on identity impersonation; likewise, it prohibits the act of illegally obtaining, storing, or requesting another person's identification codes (ID, password).(31)

European Union Countries

The EU has adopted a series of directives and regulations to harmonize the national laws of its member states in matters of cybersecurity and cybercrime. In 2023, the European Union's new Digital Services Act (32) (DSA) came into force, under which the 19 largest digital platforms

operating in European territory—including Facebook, Instagram, TikTok, or X (formerly Twitter), but also commercial intermediary giants such as Amazon, Zalando, or AliExpress—must have systems that enable them to flag and remove illegal content more quickly. They must also have mechanisms allowing users to report illegal content and may be sanctioned with large fines in case of non-compliance.(33)

In this way, the European Union became the first region in the world to regulate the activity of online platforms and, as of February 2024, applied these principles to all other online platforms, regardless of their size.

In Spain, within the European Community, the reform of the Criminal Code effected by Organic Law 14/2022 of 22 December criminalizes common frauds separately from cyberfraud conduct that requires the manipulation of a computer system or the use of a debit and/or credit card, which it regards as offenses of own activity.

Within Spanish criminal law, phishing is a novel crime, classified under various criminal offenses depending on the circumstances and the damage caused.(34)

Phishing is considered a form of fraud and is regulated in Article 249 of the Spanish Penal Code. It is punishable by prison sentences ranging from 6 months to 3 years, depending on the manner of commission, for those who: manipulate computer systems or data to obtain unauthorized transfers; fraudulently use cards, traveler's checks, or other payment instruments; or manufacture, possess, or distribute tools to commit fraud or illegally acquire checks or cards.(35)

If phishing involves the improper use of another person's identity, it could fall under the crime of identity usurpation, which is punishable by 6 months to 3 years of imprisonment.

However, those amendments would seem insufficient for prevention purposes. Thus, on 10/3/24, the Spanish newspaper El País published that more than half of Spanish citizens had reportedly been victims of these crimes, with the most frequent being "romantic or investment" scams, which constitute the second most reported crime after theft (36).

Germany: In that country, cybercriminal conduct is regulated in different legal instruments.

Thus, the Criminal Code criminalizes several offenses, including espionage and interception of data (art. 202a-c StGB), computer fraud (art. 263a StGB), computer sabotage (art. 303b StGB), and data modification (art. 303a StGB). Preparatory acts are also penalized, such as the production or acquisition of computer programs intended for the commission of computer fraud (art. 202c StGB). Careless handling of passwords can also lead to the initiation of preliminary proceedings.

Hacking constitutes a criminal offense under sections 202a and 202b of the Criminal Code, referred to as data espionage and data interception (phishing), respectively. With regard to preparatory conduct for the crimes of data espionage and phishing, Article 202c CP penalizes the manufacture, sale, and acquisition for the purpose of using, distributing, or otherwise making available a device, including computer programs, designed or prepared primarily for the purpose of committing certain cyberattacks.

Identity theft may give rise to various criminal offenses, depending on how the offender gains access to the data information. If it occurs through phishing methods, it falls under Article 202b CP, already mentioned. If it involves the use of such identity data for fraudulent purposes, it could give rise to the crimes of fraud or computer fraud, with penalties of between 5 and 10 years of imprisonment in serious cases. The use of another person's identity may give rise to the crimes of document forgery or falsification of data with probative value.

In addition, Germany has the Federal Data Protection Act, the Copyright Act, the Art Copyright Act, the German Telemedia Act, and the Act Against Unfair Competition (UWG).(37)

CONCLUSIONS

The analysis of new forms of cyber scams in Argentina reveals a concerning reality: current legislation is not fully prepared to address these modern challenges. Although the Argentine Penal Code provides for computer crimes, the rapid evolution of online fraud techniques often outpaces existing preventive and punitive measures. Cybercriminals exploit artificial intelligence tools and other advanced technologies to carry out sophisticated scams.

Throughout this work, it has been possible to demonstrate the harm that this class of crimes causes not only to victims but also to companies, institutions, and even the State; therefore, it is imperative to criminalize not only phishing but also identity theft and the collection of personal information by processing the various bills presented in Congress.

It is necessary to be able to propose a deep and serious reform of the Criminal Code regarding the issue of digital platforms, cryptocurrencies, and cybercrimes in order to implement it in procee-

dings and investigations, whether through the creation of specific offenses or the incorporation, as an aggravating factor, of the "use of social networks" for the commission of certain classes of crimes.

The inclusion of a general clause in the Criminal Code establishing an aggravating circumstance for all crimes when social media are used to commit them would allow greater flexibility and adaptability to new forms of crime.

On the other hand, the need to expand the protection of computer systems and personal data is also evident through the criminalization of cyberattacks, identity theft, and cyber extortion.

As has been seen, cyber frauds carry minimal penalties compared with the harm they cause to people's lives as well as to institutions.

However, modifying laws alone, although a major step, is not enough. It is important to train those who address these crimes so that they have the necessary tools to combat them.

The implementation of these reforms poses various challenges, among which the following stand out:

- It is necessary to strike a balance between protecting freedom of expression and the need to combat crimes committed through social media.
- Information technologies evolve rapidly, so criminal law provisions must be flexible enough to adapt to these changes.
- It is essential to guarantee the protection of the personal data of internet users, while allowing the investigation of crimes.
- Close collaboration is required among the Judiciary, the Legislative Branch, security forces, and technology companies to combat cybercrime.

In conclusion, the classification of aggravating circumstances in crimes committed through social networks is a complex issue that requires in-depth analysis and broad debate.

Cyber fraud is a growing threat that affects individuals, businesses, and states. To combat it effectively, a multidisciplinary approach is necessary, involving governments, businesses, civil society organizations, and each of us as citizens.

REFERENCES

1. Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión 2023. Disponible en: https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-senalo-un-alza-continua-de-los-delitos-informaticos-en-su-informe-de-gestion-2023
2. Bekerman U. Ciberseguridad en Argentina: la protección de las infraestructuras críticas. En: Sistema Penal e Informática. Tomo 4. Buenos Aires: Hammurabi; 2021. p. 35–50.
3. Ministerio de Seguridad de la Nación. Ciberdelito: aprobación del Segundo Protocolo Adicional del Convenio de Budapest. Disponible en: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest
4. Código Penal Argentino. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/texto
5. Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires. Delitos y contravenciones en el mundo digital: las normas que nos amparan. 2024 may. Disponible en: https://buenosaires.gob.ar/sites/default/files/2024-05/B4_Delitos%20y%20contravenciones%20en%20el%20mundo%20digital.pdf
6. Roibón MM. La estafa informática en el Código Penal. 2019. Disponible en: https://www.pensamientopenal.com.ar/system/files/2019/01/doctrina47322.pdf
7. Peña M, Lofeudo I. Fraudes: cuáles son las modalidades de ciberdelitos más habituales. Infobae. 2023 sep 21. Disponible en: https://www.infobae.com/opinion/2023/09/21/fraudes/
8. Ministerio de Seguridad de la Provincia de Buenos Aires. Cibercrimen y delitos informáticos: guía de estudio 2. 2021. Disponible en: https://www.mseg.gba.gov.ar/areas/Vucetich/GUIAS%20DE%20MATERIAS%202021/2%20Cibercrimen.pdf
9. Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Delitos informáticos. 2018 mar 9. Disponible en: https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos
10. Ministerio de Justicia de la Nación. Qué es el ciberdelito. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito
11. Brodowski D, Linares MB. Los delitos informáticos en el Código Penal Argentino. En: Cibercrimen y protección de la seguridad informática. Buenos Aires: Ad-Hoc; 2021. p. 155–91.
12. CERT.ar. Incidentes informáticos. Informe anual de incidentes de seguridad registrados en 2023. Dirección Nacional de Ciberseguridad; 2024. Disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-7
13. Interpol. Fraudes basados en la ingeniería social. Disponible en: https://www.interpol.int/es/Delitos/Delincuencia-financiera/Fraudes-basados-en-la-ingenieria-social
14. Donna EA. Derecho penal: parte especial. Tomo II-B. 2ª ed. Santa Fe: Rubinzal-Culzoni; 2012.
15. Martínez M. Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico: implicancias y consecuencias en materia penal y de responsabilidad civil. En: Cibercrimen y delitos informáticos. Buenos Aires: Errepar; 2018. p. 33–47.
16. Petrone D, Basso M, Emiliozzi A. Phishing attacks: problemáticas de su recepción en el ordenamiento local y nuevos desafíos. En: Cibercrimen: aspectos del derecho penal y procesal penal. Buenos Aires: IBdeJF; 2017.
17. Luján S. El problema de phishing en Argentina. Infobae. 2024 jul 1. Disponible en: https://www.infobae.com/opinion/2024/07/01/el-problema-de-phishing-en-argentina/
18. Departamento de Ciberdelitos y Tecnologías Aplicadas de la SPC. Ciberseguridad, phishing y estafas digitales. Disponible en: https://www.mpba.gov.ar/phishing
19. Bisquert SO. La figura del “phishing” como modalidad delictiva: problemática en cuanto a su encuadre jurídico. 2006. Disponible en: http://www.saij.gob.ar/doctrina/dacf060096-bisquertfiguraphishingcomomodalidad.htm
20. Aboso G. Cibercriminalidad y delitos contra la propiedad. En: Sistema Penal e Informática. Tomo 4. Buenos Aires: Hammurabi; 2021. p. 241–305.
21. Aboso G. Ciberdelitos: análisis doctrinario y jurisprudencial. Buenos Aires: elDial Libros; 2022.
22. Instituto Nacional de Ciberseguridad (INCIBE). Spear-phishing. Disponible en: https://www.incibe.es/aprendeciberseguridad/spear-phishing
23. Santander. “Pharming”: otro motivo para detenerse y pensar antes de hacer clic. 2022 sep 12. Disponible en: https://www.santander.com/es/stories/pharming
24. Grupo Ático 34. El scamming o los peligros de las estafas por internet. Disponible en: https://proteccion-datos-lopd.com/empresas/scamming/
25. IBM. ¿Qué es el phishing? Disponible en: https://www.ibm.com/es-es/topics/phishing
26. Saij. G. R. M. s/ Procesamiento. Estafa. Disponible en: http://www.saij.gob.ar/camara-nacional-apelaciones-criminal-correccional-nacional-ciudad-autonoma-buenos-aires--procesamiento-estafa-fa22060033-2022-1102
27. Secretaría de Innovación Tecnológica del Sector Público. Delitos informáticos en Argentina: modalidades detectadas durante la pandemia COVID-19. Recomendaciones preventivas para los ciudadanos. 2022. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf
28. Defensa del Consumidor. Cuadernillos COFEDEC. Disponible en: https://www.argentina.gob.ar/produccion/defensadelconsumidor/cuadernilloscofedec
29. Departamento de Delitos Tecnológicos de la Policía Federal Argentina. Denunciar un delito informático. Disponible en: https://www.argentina.gob.ar/servicio/denunciar-un-delito-informatico

30. Ámbito Financiero. Quién fue Carlo Ponzi, uno de los estafadores más famosos de la historia. 2024 oct 12. Disponible en: https://www.ambito.com/economia/quien-fue-carlo-ponzi-unolos-estafadores-mas-famosos-la-historia-n6069767
31. Toki K. Acciones prohibidas bajo la Ley Japonesa de Prohibición de Acceso No Autorizado. 2024 mar 21. Disponible en: https://monolith.law/es/it/unauthorized-computer-access
32. Centro Europeo del Consumidor de España. Noticias: Ley de Servicios Digitales. 2023 ago 25. Disponible en: https://cec.consumo.gob.es/CEC/comunicacion/noticias/2023/NI_Ley_De_Servicios_Digitales_25_08_2023.htm
33. Ayuso S. La UE pone coto a las grandes plataformas: empieza a aplicarse la nueva Ley de Servicios Digitales. El País. 2023 ago 25. Disponible en: https://elpais.com/economia/2023-08-25/la-ue-pone-coto-a-las-grandes-plataformas-empieza-a-aplicarse-la-nueva-ley-de-servicios-digitales.html
34. Sunkel & Paz. Phishing en España: ¿qué es y cómo se castiga este delito en el derecho penal?. 2024. Disponible en: https://www.sunkel-paz.es/post/phishing-en-espana-que-es-como-se-castiga
35. Abogacía Española, Consejo General. Delitos en internet: ciberestafas. Disponible en: https://www.abogacia.es/actualidad/opinion-y-analisis/delitos-en-internet-ciberestafas/
36. Pérez-Colomé J. Las ciberestafas ya son el segundo delito más denunciado: nadie está a salvo de caer en la trampa. El País. 2024 mar 10. Disponible en: https://elpais.com/tecnologia/2024-03-10/las-ciberestafas-ya-son-el-segundo-delito-mas-denunciado-nadie-esta-a-salvo-de-caer-en-la-trampa.html
37. Weidenslaufer C, Juan Pablo, Cifuentes P. Jurisdicción y ciber-delitos. Biblioteca Nacional del Congreso de Chile; 2022 nov. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33744/1/BCN_jurisdiccion_ciber_delitos_CW_JPC_PC_2022.pdf

FUNDING

The authors received no funding for the development of this research.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHORSHIP CONTRIBUTIONS

Conceptualization: Sabrina Ivana Bof.
Data curation: Sabrina Ivana Bof.
Formal analysis: Sabrina Ivana Bof.
Investigation: Sabrina Ivana Bof.
Methodology: Sabrina Ivana Bof.
Project administration: Sabrina Ivana Bof.
Software: Sabrina Ivana Bof.
Supervision: Sabrina Ivana Bof.
Validation: Sabrina Ivana Bof.
Visualization: Sabrina Ivana Bof.
Writing – original draft: Sabrina Ivana Bof.
Writing – review and editing: Sabrina Ivana Bof.