Paakat
Revista de tecnología y sociedad

Computer crimes in Mexico. Recognition in the criminal laws of the Mexican entities

Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas

http://dx.doi.org/10.32870/Pk.a12n22.667

Miryam Georgina Alcalá Casillas*
Universidad Michoacana de San Nicolás de Hidalgo, México

Miguel Ángel Meléndez Ehrenzweig**
Universidad Autónoma de Baja California, México

Received: June 08, 2022
Accepted: January 26, 2023

ABSTRACT

The global digital transformation has facilitated almost all human activities. The pandemic caused by the SARS-COV-2 virus increased this phenomenon, as commercial, labor, health, educational and social activities moved towards digitalization. In Mexico, this has given rise, among other effects, to computer crimes -such as theft and computer fraud, digital harassment or cyberstalking- which are evolving rapidly and therefore are not on a par with criminal legislation. The purpose of this article is to analyze and assess whether computer crimes are criminalized in the 32 Mexican states. For this purpose, the deductive method and exploratory research were used, in order to observe and confirm whether the entities that recognize digital anti-juridical conducts in their criminal laws contribute to the reporting and investigation, or whether those that do not recognize them promote their ignorance, that the crime is not reported or prosecuted.

Keywords
Cybercrime, computer crimes, cybersecurity; penal systems.

RESUMEN

La transformación digital mundial ha facilitado casi todas las actividades del ser humano y la pandemia originada por el virus SARS-COV-2 aumentó este fenómeno, pues actividades comerciales, laborales, sanitarias, educativas y sociales, transitaron hacia la digitalización. En México, esto ha originado, entre otros efectos, delitos informáticos –como el robo y fraude informático, el hostigamiento digital o ciberacoso– que evolucionan aceleradamente y por tanto no se encuentran a la par en la legislación penal. El objetivo de este artículo es analizar y valorar si los delitos informáticos son tipificados en las 32 entidades mexicanas. Para ello se utilizó el método deductivo y la investigación exploratoria, con el fin de observar y confirmar si las entidades que reconocen las

Palabras clave
Ciberdelincuencia, delitos informáticos, ciberseguridad; ordenamientos penales.

conductas antijurídicas digitales en sus ordenamientos penales contribuyen a la denuncia e investigación, o si aquellas que no las reconocen promueven su desconocimiento, que no se denuncie ni se persiga el delito.

* Professor at the Universidad Michoacana de San Nicolás de Hidalgo, Mexico. Candidate to the National System of Researchers of CONACYT. E-mail: miryam.alcala@umich.mx

** Professor at Universidad Autónoma de Baja California, Mexico. E-mail: melendezm@uabc.edu.mx

INTRODUCTION

Criminal conducts have been present and have evolved in the history of mankind; and in the societies of the 21st century, with the accelerated technological revolution, cybercrimes or computer crimes have emerged and grown exponentially (Acurio del Pino, 2016). Their conceptualization, characteristics and applicable legislation, have been topics of legal debate in recent years, and in Mexico it is a pending issue, so it is considered important to analyze them and determine whether their explicit recognition in criminal law contributes to the reporting, investigation, prosecution, prevention and reduction.

The first computer crimes began in the sixties with the collection of personal information without consent (Morales, 1984, p. 229); but the use of computers in the commercial sector meant that the most common crimes were computer fraud, data manipulation or corporate espionage (Hernández, 2009, p. 229). In the eighties and nineties, the generalization of computers in the population originated massive infringements against intellectual property such as software piracy, in audiovisual products, music and cinema. With the Internet in the 21st century, new forms and methods were created to violate personal privacy, impersonate identity, commit fraud or theft, access and disseminate illicit content or products and services (Hernández, 2009, p. 230).

These crimes have increased due to the confinement brought about by the pandemic originated by covid-19, which forced all activities to transit to digitalization; and in Mexico, according to the report of the Secretariat of Security and Citizen Protection, an increase of 4.1% was reported in crimes related to copyright, intellectual and industrial property, against means of communication and correspondence, falsehood and falsification of information (Government of Mexico, 2021, pp. 70-72). With the above in consideration, the international and national legal framework applicable to computer crimes will be evaluated, the criminal laws of Mexican entities will be analyzed to determine whether they recognize computer crimes, and whether this accreditation contributes to the reporting and investigation.

Cybercrime

The Organization for Economic Cooperation and Development (OECD, 1992) establishes as a computer crime "any unlawful, unethical or unauthorized behavior related to the automatic processing and/or transmission of data". For Téllez Valdés, they are "attitudes contrary to the interests of persons in which computers are used as an

instrument or end, and typical, unlawful and guilty conduct in which computers are used as an instrument or end" (2004, p. 163). From these definitions, it is interpreted that technological devices, such as computers, are perceived as the vehicle, not as the legal good to be protected nor as the active subject.

For Aceytuno, (2022) cybercrimes integrate numerous activities carried out by a variety of agents, includes personal factors, such as ideology, and international phenomena, such as globalization or the expansion of the Internet (p. 225). For other authors they are also cybernetic or electronic crimes because they are related to computers and internet networks (Delgado, 2017, p. 2); because the typical and anti-juridical action is committed through computer mechanisms and/or electronic devices (Tejerina, 2020, p. 48); and because it is carried out using a computer element, or violating rights of the owner of a computer element, whether hardware or software (Davara, 1990, p. 26). Based on this, cybercrime is considered as:

> a set of conducts related to the access, appropriation, exchange and making available of information in telematic networks, which constitute its commissioning environment, perpetrated without the required consent or authorization or using information of illicit content, and may affect diverse legal assets of an individual or supra-individual nature (Romeo, 2006, p. 11).

Cybercrime involves: 1) conducts related to the unlawful processing, treatment and transmission of information without the consent of the owner; 2) the use of the network, electronic devices or media, computer systems or programs, for the transmission, modification or misuse of personal information and data; and 3) affecting personal assets -dignity, privacy, identity- or collective assets -national security, public order- (Tejerina, 2020, p. 49). In computer crimes, subjective and objective elements are distinguished; in the subjective is the willful intent or deliberate will to commit the crime knowing that it is wrong, guilt or preterintention; in the objective, there is the action that affects both the hardware (physical elements) and software (programs or systems) components and the main instruments to perpetrate the crime or consummate the unlawful or anti-juridical act (Delgado, 2017, p. 5).

The active and passive subject is also observed; the active subject is the one who performs all or part of the criminal action through the management of computer systems or strategic places -it can be people who enter a computer system without criminal intentions, who are just starting in computer science or employees[1]-; and the passive subject or victim is the owner of the legal property on which the conduct of action or omission incurs -it can be individuals, institutions or governments that use automated information systems- (Garrido, 2005).

The United Nations Organization (UNO) recognizes as computer crimes: 1) fraud or economic deception with the intention of obtaining a benefit through computer

[1] The UN Handbook (2015) on Cybercrime Prevention and Control indicates that 90% were executed by employees.

systems; 2) manipulation or theft of data; 3) manipulation or modification of computer programs, insertion of new programs or routines without authorization of the owner; 4) computer forgery, alteration of data of documents stored in computerized form; 5) the instruments as means to commit them, from computers, photocopiers, data storage memories, among others (UNO, 2000).

International and national legal context of cybercrimes

There are international treaties to deal with computer crimes[2] through the harmonization of laws, the improvement of investigation techniques and cooperation among nations; and in recent years, legal assessments of the problems arising from the misuse of information technology have led to changes in the laws of the countries; in addition, the Organization of American States and the Inter-American Development Bank propose the transnational nature of these crimes, mutual aid agreements and the specialization of police forces, prosecutors and judicial officials (OAS and IDB, 2020).

Worldwide, efforts have been made to regulate the new offenses brought by technological progress. El Salvador carried out criminal reforms seeking to update the tools to combat these crimes, and that the authorized authorities consider as evidence for criminal proceedings all digital documents, electronic messages, images, videos or other data stored, received or transmitted through digital channels or electronic devices (Lopez, 2022).

France implemented Law 88-19, on fraudulent access to a data processing system, punishes anyone who accesses, deletes, alters or modifies data contained in or operating the system, anyone who falsifies computerized documents with intent to cause damage, and prosecutes anyone who intentionally and with disregard for the rights of others enters data into an automatic data processing system, The Second Economic Crime Act of 1986 punishes the cancellation, disabling or alteration of data, including attempts to do so, data espionage, computer fraud, falsification of evidentiary data or modifications and falsification of documents (Chawki, 2005).

In 1986, Germany adopted the Second Law against Economic Crime, which punishes data espionage, computer fraud, falsification of evidentiary data or modifications complementary to the rest of documentary falsehoods such as deceit in legal transactions through the elaboration of data, ideological falsehood or use of false documents; it is considered illegal to cancel, disable or alter data even in the form of an attempt; as well as the destruction, deterioration, disabling, elimination or alteration of a data system (Chawki, 2005).

Austria reformed its Criminal Code in 1987, punishing the destruction of personal and non-personal data and programs; it punishes those who maliciously cause financial damage to a third party, by the introduction, cancellation or alteration of data or by acting on the course of data processing (*Das Rechts Informations System des Bundes*, 2020).

[2] Budapest Convention (2001), Rome Statute of the International Criminal Court (1998).

In 2005, Mexico ratified the Rome Statute (UN, 2005), and since 2017 the Senate of the Republic has requested accession to the Budapest Convention (*Secretaría de Gobernación*, 2017); since 2019 at least 15 initiatives have been presented in the H. Congress of the Union to punish computer crimes (Rodríguez, 2022), but there is no law that recognizes them and neither have the necessary reforms been made to implement measures and procedures to punish or mitigate them.

The legal property protected in these crimes is information (messages, images, sounds), the rights that this entails are those that are affected by unlawful conduct carried out through technological resources, either by its dissemination, processing or modification, because it violates human rights, basic legal property - privacy, image, dignity, sexual freedom, intellectual property - and collective legal property - industrial property, market, national security and public order - (Pérez Luño, 2011, p. 430).

Protected legal interest and classification

The OECD Observer analyzed these crimes with a focus on the economic value attributed to information, as the raw material of the new industry and the basis and object of commercial transactions (OECD, 1986). In computer crimes, information is the legal good sought to be protected, because the typical, antijuridical and guilty action falls on the information and attacks its integrity, confidentiality or availability in any of the phases or computer systems linked to its flow or exchange - entry, storage, process, transmission or output - (Meyer, 2017, p. 255).

IT functionality is a presupposition for the performance of IT activities and a set of conditions that make it possible for IT systems to adequately carry out data storage, processing and transfer operations. It constitutes an instrumental legal good of a collective nature, because what is damaged is the information of the human being contained in the instrument, therefore it is necessary to distinguish and classify computer crimes based on the information (Mayer, 2017).

In Mexico, computer crimes are not typified in a specific law, but there are some definitions at federal and local level; for example, the Federal Copyright Law typifies the illegal copy of computer programs (H. Congress of the Union, 2020) and the Federal Law for the Protection of Industrial Property typifies the illegal copy of topographies, such as industrial designs (H. Congress of the Union, 2021).

The Criminal Code for the Federal District (Congress of Mexico City, 2020) punishes espionage[3]; attacks on communication channels, violation of correspondence[4]; communication of sexual content with persons under 18 years of age or who do not have the capacity to understand the meaning of the act or who do not

[3] Articles 127, 128 and 129.

[4] Articles 165-168.

have the capacity to resist it[5]; pornography[6] and violation of sexual intimacy[7] through digital media (H. Congress of the Union, 2021).

Likewise, it punishes crimes related to copyrights[8], illicit access to computer systems and equipment[9], and anyone who deciphers or decodes telecommunications signals, anyone who transmits the ownership, use or enjoyment of devices, instruments or information that allow deciphering or decoding telecommunications signals; anyone who manufactures, commercializes, acquires, installs, carries, uses or operates equipment that blocks, cancels or annuls cellular telephony signals, radio communication or data transmission (H. Congress of the Union, 2021).

After the pandemic there was a growth of computer crimes in Mexico. A study by Grupo Fractalia (2020) indicates that although the Internet was already part of everyday life for various activities, e-commerce grew 108% and the use of digital tools doubled in the first months of the pandemic. In this period, the turnover of online stores increased 60% and cyber threats increased, as by the last quarter of 2020 there were 75% more likely to be a victim of cybercrime compared to 2019.

The numbers of these crimes from 2019 to 2021 went from 300.3 million in 2019 to 120 billion in 2021, an increase of almost 400 times, and are social engineering attacks the most frequent, particularly phishing and malware, attacks on end-user networks of which, and more than 60% were directed to online banking (Calderon, 2022). In this sense, regarding cybersecurity in Mexico, experts consider that:

> The movement restrictions imposed by the coronavirus pandemic triggered cybercrime, a large, diversified, for-profit industry, with individuals or groups often performing specific functions, with a division of labor, in their own illicit market readily available to drive activity in other illicit markets (Réyez, 2021).

Some Mexican institutions have also had their computer systems breached, such as the Ministry of Public Function, the National Commission for the Protection and Defense of Financial Services Users, the Bank of Mexico or the Tax Administration Service (Riquelme, 2021). In addition to this, the National Guard has detected thousands of websites pretending to be from the federal government or for marketing purposes, in which fraud, malicious code downloads or theft of sensitive information are committed (*Centro Nacional de Respuesta a Incidentes Cibernéticos*, (National Cyber Incident Response Center) 2022). Therefore, policy, technological and strategic measures aimed at cybersecurity are necessary (Réyez, 2021).

[5] Title VII, Chapter I.
[6] Article 202.
[7] Article 199
[8] Article 424-429.
[9] Article 211.

Telecommunications reforms and the National Digital Strategy have prioritized the digitization of government activities and public services, without addressing cybersecurity (Arreola, 2018); and according to the OAS and IDB Cybersecurity Report 2020, the country faces the challenge of strengthening the State's capacities to guarantee security in cyberspace based on a comprehensive strategy and generate appropriate technological and human resources for the new cybersecurity conditions.

In order to analyze cybercrime in Mexican entities, the Budapest Convention and the Federal Criminal Code are taken as a reference. The former distinguishes crimes in four categories: those against the confidentiality, integrity or availability of information; those that use technology as a medium; those related to content; and those related to intellectual property infringements. The second covers crimes against the privacy of sexual information, against the free development of the personality and against persons in their patrimony, in addition to dealing with the disclosure of secrets and illicit access to computer systems and equipment.

With this consideration and given that there is no specific definition of computer crimes in the Federal Criminal Code (H. Congress of the Union, 2023), a common concept and characteristics are proposed to interpret them, classifying them in four criminal types protecting the affected legal assets: 1) Of confidentiality, privacy and identity: disclosure of secrets, violation of correspondence, improper computer access, impersonation and violation of privacy; 2) of sexual freedom and security, free development of the personality: harassment, cyberstalking, child pornography or of incapable persons; 3) of patrimony: fraud, theft and extortion; 4) of public faith: forgery and improper use of documents, seals, passwords and others (see Table 1).

Table 1. Characteristics of computer crimes

Revelation of secrets	• - Disseminating or disclosing confidential information or private communication without consent and with prejudice, and disclosing scientific, industrial or commercial information from the source that generated it.
Correspondence violence	• Opening, intercepting or fraudulently intercepting private communication (written, electronic, magnetic, optical or computer) • Disclose, divulge or misuse information or images intercepted without consent.

Improper computer access	• - Accessing information on a data processing or storage device or interfering with the operation of a computer system, program, database or file, without permission • - Accessing images or videos concerning genitalia or sexual acts, without permission of the owner • - Accessing, modifying, destroying, copying or causing loss of information contained in video surveillance systems that enable the protection, viewing, transmission, recording and storage of information. Locate, install, use and operate video surveillance systems to record or capture images in places, equipment, furniture, roads or public space, without authorization, or notice to the competent authorities. • - Attacking, destroying, stealing, physically and intentionally sabotaging any video surveillance equipment and its structure belonging to police, public security and law enforcement institutions.
Impersonation	• - Usurp or substitute another person by any means, using without consent his or her personal data for illicit or lucrative purposes. • - Assuming, appropriating or using the identity of a natural or legal person • - Transferring, possessing or using another person's identification data with the intention of committing, attempting or favoring any unlawful activity • - Taking advantage of homonymity, physical resemblance or voice similarity
Violation of privacy privacy	• - Disclose, share, distribute, commercialize or threaten to publish personal, private or confidential information of a person, images, audios or videos of intimate, erotic or sexual content, printed or digital. • - Condition the blocking of the dissemination of the content or seek to obtain an economic benefit with the publication or dissemination of the material.
Harassment	• - Capturing images or audiovisual recordings of another person's body or any part thereof without consent and of a sexually erotic nature
Cyber harassment	• - Harass, threaten or send unsolicited content on one or more occasions through any digital space and cause personal harm.

Child Pronography	• - Photographing, videotaping, posting, printing, displaying, observing, marketing, distributing, disseminating, storing, possessing or offering acts of indecent exposure by a person or persons under 18 years of age, or persons who do not have the capacity to understand or resist such an act
Computer fraud	• - Unlawfully obtaining a thing or obtaining an undue advantage, by deceiving or taking advantage of error or ignorance; by any digital means
Theft computer	• - Taking advantage of electric power, telephone, Internet or television image services without consent. Acquiring, marketing or possessing one or more electronic devices capable of connecting to the Internet wirelessly.
Extortion	• - To obtain a profit by causing a patrimonial damage to the victim, by forcing him, through the use of physical or moral force, to do, tolerate or cease to do something.
Falsification	• - To supplant, alter, alienate, destroy or ocularize any kind of official or private seals, marks, keys, tickets, passwords, stamps or stamps or unauthorized use thereof • - Altering a public or private document, or any electronic device in the form of a plastic card, or imitating the originals, obtaining a benefit or causing damage.

Source: own elaboration.

Methodology

Research was conducted on the computer crimes provided for in the ordinances of the Mexican entities (see annex) and crime incidence indicators for years 2019, 2020 and 2021. Instruments for the Registration, Classification and Reporting of Crimes and Victims CNSP/38/15 (Executive Secretariat of the National Public Security System, 2022) were used, which provide the figures from January to December of the occurrence of alleged crimes recorded in investigation files initiated in the Public Prosecutor's Offices and reported by the Attorney General's Offices and Prosecutor General's Offices of the 32 states.

Many of the conducts reviewed have not been legislated as criminal offenses in some of the country's states; what is a crime in one state is not in another; in addition, the penalties are diverse, some are very light in comparison with the damage they cause to the protected legal right (see annex), but the legal right or material object is not identified in a specific criminal offense, that is to say, the means by which a theft or computer harassment is committed (computer, telephone or other computer material object) is not identified and considered, since there may continue to exist means or new means or material objects to commit conducts already contained in our criminal legislation.

Analysis and discussion of results

When reviewing the crime of disclosure of secrets, the penalties in the entities range from six months to five years of imprisonment, and fines ranging from five dues to 500 UMAs. Baja California Sur, Guerrero and Querétaro, also enforce community work; Campeche, Guanajuato, Jalisco and Sonora order suspension of a profession, position or employment; Aguascalientes requires the reparation of damage and Coahuila manages supervised freedom. In contrast, the State of Mexico and San Luis Potosí do not include this crime in their legislation.

Regarding the violation of correspondence and private communications, we find penalties ranging from three days to five years in prison, and fines from five dues to 1,500 days. In addition, some states require reparation of damages (Aguascalientes), others impose community service (Sonora, Tabasco and Yucatán) and supervised release (Coahuila).

Undue computer access or illicit access to computer systems is not contemplated in Coahuila, Mexico City, Guerrero, Hidalgo, Michoacán, Estado de México, San Luis Potosí, Sinaloa, Sonora and Tlaxcala. In the rest of the states, penalties ranging from two months to two years imprisonment and fines of 50 to 1,000 quotas are established. In this regard, Aguascalientes, once again, considers the reparation of damages.

It was found that impersonation is not regulated in Puebla, Querétaro, Veracruz and Yucatán, and in Guerrero only impersonation of civil status or filiation is considered. In the other states the penalties range from six months to twelve years imprisonment, fines from 400 to 2,000 UMAs and from 400 to 900 days of salary. Aguascalientes contemplates as an aggravating circumstance when the offender takes advantage of his position or employment to impersonate the identity of the person, adding up to one half more to the penalty, while in Morelos the reparation of the damage is indicated.

As for the violation of personal privacy, this crime is not found as such in the regulations of Colima, Guerrero, Jalisco, State of Mexico, Oaxaca, San Luis Potosí and Tamaulipas; in the other entities it is punishable from six months to eight years in prison, and has fines ranging from 100 to 2,000 UMA. Aguascalientes provides for reparation of damages and Chihuahua from 90 to 180 days of community service. At this point, it is worth mentioning the Penal Code of Baja California which, in addition to the penalties provided, orders the company providing digital or computer services (Internet server, social network, administrator or owner of the digital platform) to immediately remove the publication and the unauthorized intimate content from the media or any other where it is located.

The crime of digital harassment is not regulated in Mexico City, Hidalgo, Querétaro, Sinaloa and Veracruz; in the other entities, the penalties range from six months to eight years in prison and fines from 50 to 500 days of salary or from 100 to 600 UMA. In addition, Aguascalientes establishes as an aggravating circumstance when the harassment is committed by relatives or public servants, adding one half more to the penalty; Baja California and Baja California Sur consider as an aggravating circumstance when the offended party is under fourteen years of age, punishing with two

to three years in prison and two to four years, respectively; Tabasco adds as punishment the dismissal from the position, employment or public service.

Digital harassment is not regulated in Aguascalientes, Baja California, Campeche, Chihuahua, Colima, Guanajuato, Guerrero, Michoacán, Nayarit, Nuevo León, Oaxaca, Querétaro, San Luis Potosí, Sinaloa, Sonora, Tabasco, Tamaulipas, Tlaxcala and Veracruz. While Baja California Sur, Chiapas, Coahuila, Mexico City, Durango, Hidalgo, Jalisco, Morelos, Estado de México, Puebla, Quintana Roo, Yucatán and Zacatecas, establish penalties ranging from five months to eight years in prison, fines from 100 to 600 days or from 36 to 1,000 UMA. Coahuila also adds disqualification from public or professional office, employment or service.

In the penal codes of Chihuahua, Jalisco and Querétaro, the articles that contemplated the crime of pornography were repealed, and this crime is not mentioned in that of San Luis Potosí. In the other states, the penalties range from two to 18 years in prison, fines from 300 to 5,000 days and from 1,500 to 12,000 UMA. A similar situation occurs with the crime of extortion, repealed in the codes of Chihuahua and Puebla; in the rest of the states the penalties range from four to 15 years of imprisonment, fines from 50 to 4,000 days of salary, or from 100 to 1,500 UMA; and again, Aguascalientes adds the reparation of damages.

Fraud is found in the codes of all 32 states, with penalties ranging from six months to twelve years of imprisonment, fines from fifteen to 1,200 days of salary or from 100 to 1,000 UMA. Theft is also found in all states, with penalties ranging from six months to fourteen years of imprisonment, depending on the value of the stolen goods, and fines from 100 to 1,500 days of salary or from 36 to 1,200 UMA; in addition, Aguascalientes requires payment for the repair of damages.

Finally, the forgery and misuse of documents, seals, marks, keys, tickets, passwords, official or private stamps or stamps, public or private documents, or plastic cards, carries penalties ranging from three months to ten years in prison, fines ranging from 25 to 500 days of salary and from 18 to 700 UMA. Chihuahua adds community service, Coahuila supervised release, and Aguascalientes reparation of damages.

It was found that, in the total annual figures of registered crimes, only the following crimes are reported: harassment, harassment, fraud, theft, extortion and falsification of codes, seals and documents. It should be noted that these instruments add sections indicating: other crimes against life and bodily integrity; other crimes against personal liberty; other crimes against sexual liberty and security; other crimes against property; other crimes against society; and other crimes against other affected legal assets. In spite of this, no section of the instrument specifies which crimes are referred to, what these types of crimes consist of or what elements are being considered for them to be highlighted as "other crimes".

In addition, they do not include the disclosure of secrets, violation of correspondence, improper computer access, identity theft, cyberstalking, harassment, violation of privacy and pornography, even though these are regulated in the Criminal Codes of the states. In addition, the crimes that are registered in the instruments do not

specify how many were carried out through digital media, which led to an investigation on the website of the State Prosecutor's Offices to find whether or not computer crimes are reported in the reports submitted to the Ministry of Public Security and the National Information Center.

As a result of the investigation, it was found that in almost all the websites of the Prosecutor's Offices, there are no reports on the incidence of computer crimes, only homicide, robbery, rape, threats, extortion and fraud are reported in their different modalities, all of which are divided into violent and non-violent crimes. The exception to the above is the case of Zacatecas, which does report the numbers of crimes shown in Table 2 (Attorney General's Office of the State of Zacatecas, 2019, 2020, 2021).

Table 2. Incidence of crime in Zacatecas (2019, 2020, 2021)

Crime incidence	2019	2020	2021
Extortion through digital media	1 077	360	486
Fraud	21	1 008	1 243
sexual harassment	97	19	22
sexual molestation	46	93	121
Attacks on communication routes	0	11	8
Attacks on the integrity of persons	48	0	0
Corruption of minors	0	0	0
Offenses committed in the custody of documents	3	0	1
Crimes against sexual privacy		80	132
Crimes against computer media security	28	20	22
Defamation	0	0	0

Falsification of certifications	1	1	2
Falsification of documents in general	111	61	83
Falsification of seals, marks, keys and dies.	1	1	1
Falsification of securities, documents or electronic device	13	6	8
Falsification and identity theft	66	51	99
Revelation of secrets	2	1	3
Variation of name, nationality or domicile	0	0	0
Violation of seals	6	5	4
Violation or retention of correspondence	0	0	4

Source: Transparency Unit of the Jalisco State Prosecutor's Office, 2022.

It was found on the website of the Prosecutor's Office of Jalisco that the Cyber Police (2022), in order to detect, through patrolling the network, sites, processes and those responsible for criminal conduct that can be committed against and making use of computer and electronic media, provides guidance to citizens regarding filing a complaint in case of being a victim of a crime committed through information technology; However, despite the search, the steps to file a complaint were not found, only security recommendations were identified for online shopping, for false job offers that arrive by e-mail, for users of dating or chat rooms, to avoid being a victim of fraud, phishing or ransomware.

As a consequence of the lack of data regarding the incidence of computer crimes, it was considered necessary to make requests for information to the state prosecutors' offices, to the executive secretariats of the public security secretariats and to the guarantor bodies of access to information, in order to locate these indicators and check whether these agencies record them in a special way in the investigation files or whether these crimes are those referred to as "others".

After making requests for information on crime incidence data for the years 2019, 2020 and 2021, most of the guarantor bodies of access to information declared themselves incompetent to provide the information, the secretariats of public security indicated that they did not have the data and that it was up to the prosecutors' offices to provide it, Most

of them did not provide the numbers of these crimes registered in investigation files, nor did they clarify what they meant by "other crimes", with the exception of the Prosecutor's Offices of Quintana Roo (Table 3) and Guanajuato (Table 4). When analyzing the data from these entities, it is observed that the crimes with the highest number of complaints are: identity theft, violation of privacy, harassment and stalking.

Table 3. Incidence of crime in Quintana Roo (2019, 2020, 2021)

Crime incidence	2019	2020	2021
Revelation of secrets	4	5	6
Violation of correspondence/private communication	0	0	1
Identity theft	137	142	233
Violation of privacy	117	184	171
Cyberbullying	2	12	23
Pornography	16	15	25
Corruption of minors	53	72	91

Source: Ramirez S. M (2022). Response FGE/QR/DFG/CHE/UT/1045/2022

Table 4. Crime Incidence Guanajuato (2019, 2020, 2021)

Crime incidence	2019	2020	2021
Stalking	86	257	335
Affectation of privacy	99	228	423
Recruitment of minors	3	3	4
Computer crimes	0	0	11

Sexual harassment	44	39	47
Revelation of secrets	12	6	6
Identity theft	374	375	520
Violation of correspondence	13	16	8
Corruption of minors	21	20	4
Child pornography	2	2	4

Source: Ángeles Salazar, G. A. (2022). Response to request for information, oficio No. 431/2022. Prosecutor's Office of Guanajuato.

On the other hand, the Transparency Unit of the Attorney General's Office of Mexico City (2022), through the Coordination of Proactive Transparency of Criminal Information, criminal policy body, statistics and transparency unit, attended our request for information and integrated in the response document the breakdown of crimes, forming a total of 670 127 rows that describe the date and time of filing the complaints, the type of crime impact, the crime reported, the modality, date, time, streets, neighborhood and delegation of the facts. Since the information was not provided as requested, it was necessary to filter the data provided, resulting in an interesting description of the crimes (Table 5).

When comparing the data, Mexico City has a high rate of complaints for crimes committed through digital and electronic media, similar to what happens in Quintana Roo and Guanajuato. Among the main crimes are: identity theft; production, printing, alienation, distribution, alteration or falsification of bearer securities, public credit documents or exchange vouchers; crimes against sexual intimacy; falsification or alteration and misuse of documents; attacks to the means of communication, disclosure of secrets; pornography; and to a lesser extent, violation of correspondence.

After reviewing the data, it is concluded that the prosecutors' offices are responsible for promoting the culture of reporting and investigation of criminal acts, but if there is no intense dissemination of the possibility of reporting crimes committed by digital media, and if they are not reported as such, it will not be possible to promote the culture of prevention, investigation and application of justice to them.

Table 5. Incidence of crime in Mexico City (2019, 2020, 2021)

Incidencia delictiva[10]	2019-2021
Falsification or alteration and misuse of documents	3052
Production, printing, sale, distribution, alteration or counterfeiting of bearer securities, documents or redemption vouchers	10 341
Identity theft	10 439
Against sexual privacy	4 632
Attack on communication routes	2 141
Violation of correspondence	116
Revelation of secrets	808
Pornography	777
Internet crimes (sexual harassment and abuse, fraud, pornography and corruption of minors, violation of privacy, threats, extortion, robbery).	48
Crimes committed through Facebook	110
Crimes committed through Twitter	10
Crimes committed through Instagram	21
Crimes committed through messages	48
Crimes committed by means of telephone calls	10

[10] For more information and complete statistics, it is recommended to visit the transparency website of the Government of Mexico.

Crimes committed through WhatsApp	64
Crimes committed via e-mail	14
Crimes committed through social media	472
Trata de personas a través de WhatsApp	1
Against sexual intimacy via Telegram	1
Identity theft through YouTube	1

Source: Saucedo M. M. (2022). Response to request for information FGJCDMX/110/3848/2022-05. Mexico City Attorney General's Office.

Conclusions

Cybercrime is an international phenomenon that integrates activities carried out through the Internet and digital technologies as unlawful conduct related to the unlawful processing, use, treatment and transmission of data through the network, systems or computer programs, in which the legal property affected is information. The unlawful conducts that make use of technological resources or mass media affect the data of an individual (messages, images, sounds, etc.), either by their dissemination, processing, misuse or modification, infringe basic legal rights, goods and interests, such as privacy, image, dignity, honor, sexual freedom, intellectual property, privacy of personal and sensitive data.

For this reason, it was considered necessary to classify computer crimes according to the information, since, in Mexico, although there are definitions at the federal level and some others in the local legislation of the entities, these crimes are not typified as such in a specific law. Likewise, the penalties contemplated in the laws are diverse or very light in comparison with the harm to the protected legal right.

The investigation of crime incidence indicators, both at federal and state level, for the years 2019, 2020 and 2021, showed that the level of cybercrime in Mexico has been increasing since 2020, including several federal institutions have been violated. It was also found that, in the total annual figures of registered crimes, only the following are reported: harassment, harassment, fraud, theft, extortion and falsification of passwords, seals and documents, and do not include the disclosure of secrets, violation of correspondence, improper computer access, identity theft, cyberbullying, harassment, violation of privacy and pornography, despite the fact that these crimes are regulated in the Criminal Codes of the entities.

In addition, the crimes that are registered in the instruments do not specify how many were committed through digital media. When delving into the websites of the state prosecutors' offices, it was found that, with the exception of Zacatecas, almost all of them do not report computer crimes.

In view of the lack of data on the incidence of computer crimes, requests for information were made to the state prosecutors' offices; however, the data obtained from these requests were scarce. The exceptions were the prosecutors' offices of Quintana Roo, Guanajuato and Mexico City, where it was found that the crimes with the highest number of complaints are: identity theft, violation of privacy and stalking or harassment.

For these reasons it is concluded that Mexico must implement political, technological and strategic measures to ensure cybersecurity, likewise, it is important to note that Prosecutor's Offices are responsible for promoting the culture of reporting and investigation of criminal acts, but if there is no intense dissemination of the possibility of reporting crimes committed through digital media, and also not reported as such, it will not be possible then to promote the culture of prevention, proper investigation and enforcement of justice to them.

REFERENCES

Aceytuno, M. T. (8 de febrero de 2022). La ciberdelincuencia es un reto económico global. The Conversation. https://theconversation.com/la-ciberdelincuencia-es-un-reto-economico-global-175970

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades. Organización de los Estados Americanos. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arreola García, A. (5 de septiembre de 2018). Ciberseguridad Nacional en México y sus desafíos. Documentos de Análisis 48/18. Instituto de investigaciones estratégicas de la armada de México. https://cesnav.uninav.edu.mx/cesnav/ININVESTAM/docs/docs_analisis/da_48-18.pdf

Calderón, C. (9 de junio de 2022). México 'clientazo' de los ciberataques: crecen 42% amenazas por internet. *El Financiero*. https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

Centro Nacional de Respuesta a Incidentes Cibernéticos. (26 de octubre de 2022). Virus informáticos. Gobierno de México. https://www.gob.mx/gncertmx/articulos/105221

Chawki, M. (2005). A critical look at the regulation of cybercrime. The ICFAI Journal of Cyberlaw, IV(4). https://www.crime-research.org/articles/Critical

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Serie de Tratados Europeos, (185). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Congreso de la Ciudad de México. (2020). Código Penal para el Distrito Federal. Gaceta Oficial del Distrito Federal. https://www.congresocdmx.gob.mx/media/documentos/9cd0cdef5d5adba1c8e25b34751cccfdcca80e2c.pdf

Cuervo, J. (5 de enero de 1988). Legislación Informática de Francia. Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique. Informática Jurídica. https://www.informatica-juridica.com/anexos/legislacion-informatica-de-francia-loi-no-88-19-du-5-janvier-1988-relative-a-la-fraude-informatique /

Consejo de Europa. (23 de noviembre de 2001). Convenio no. 185 del Consejo de Europa, sobre la ciberdelincuencia (Convenio de Budapest). https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20810/5/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20(Convenio%20de%20Budapest).pdf

Das Rechts informations system des Bundes. (5 de febrero de 2020). Austria, Criminal codes. Legislationline. https://www.oesterreich.gv.at/lexicon/R/rechtsinformationssystem.html

Davara, R. M. (1990). Análisis de la Ley de Fraude Informático. Revista de Derecho de UNAM.

Delgado, G. M. (2017). Delitos Informáticos Delitos Electrónicos. Orden Jurídico Nacional. http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

Fiscalía del Estado de Jalisco. (17 de enero de 2022). Prevención y platicas informativas. Fiscalía del Estado. https://fiscalia.jalisco.gob.mx/policia-cibernetica/prevencion

Fiscalía General de Justicia del Estado de Zacatecas. (2019). Denuncias ante agencias del ministerio público. https://www.fiscaliazacatecas.gob.mx/wp-content/uploads/2020/05/snsp_2019.pdf

Fiscalía General de Justicia del Estado de Zacatecas. (2020). Denuncias ante agencias del ministerio público. https://www.fiscaliazacatecas.gob.mx/wp-content/uploads/2021/01/S_N_S_P-2020-FIN.pdf

Fiscalía General de Justicia del Estado de Zacatecas. (2021). Denuncias ante agencias del ministerio público. https://www.fiscaliazacatecas.gob.mx/wp-content/uploads/2022/02/snsp_2021.pdf

Garrido Montt, M. (2005). Derecho Penal. Vol. Tomo III. Parte Especial. Editorial Jurídica de Chile.

Gobierno de México. (2021). Tercer Informe de Gobierno 2020-2021. Gobierno de México. https://framework-gb.cdn.gob.mx/informe/5b8e7a983a893dfcbd02a8e444abfb44.pdf

Gobierno de México. (2022). Incidencia Fuero Común CDMX 2019-2021. Transparencia Sitio web del Gobierno de México. https://transparencia.cdmx.gob.mx/storage/app/uploads/public/628/ebf/20c/628ebf20c4a48681755383.xlsx

Gobierno del Estado de Guerrero. (2008). Código Penal para el Estado Libre y Soberano de Guerrero, número 499. Poder Judicial del Estado de Guerrero: http://tsj-guerrero.gob.mx/transparencia/instituto_mejoramiento_judicial/2017/Octubre/Codigo_Penal_para_el_Estado_de_Libre_y_Soberano_de_Guerrero.pdf

Gobierno del Estado de Nayarit. (2020). Código Penal para el Estado de Nayarit. Gobierno del Estado de Nayarit. https://www.nayarit.gob.mx/transparenciafiscal/marcoregulatorio/ordenamientos/c%C3%B3digo%20penal%20para%20el%20estado%20de%20nayarit.htm

Gobierno del Estado de Tamaulipas. (2020). Código Penal para el Estado de Tamaulipas. Periódico Oficial del Estado. http://po.tamaulipas.gob.mx/wp-content/uploads/2020/08/Codigo_Penal.pdf

Grupo Fractalia. (2020). El ciberdelito en tiempos de COVID en México. https://fractaliasystems.com/los-ataques-ciberneticos-aumentan-40-en-mexico-durante-la-pandemia/

H. Congreso de la Unión. (2020). Ley Federal del Derecho de Autor. *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf

H. Congreso de la Unión. (2021). Ley Federal de Protección a la Propiedad Industrial. *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPPI_010720.pdf

H. Congreso de la Unión. (2023). Código Penal Federal. *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf

H. Congreso del Estado de Aguascalientes. (2013). Código Penal para el Estado de Aguascalientes. *Periódico Oficial del Estado.* https://eservicios2.aguascalientes.gob.mx/NormatecaAdministrador/archivos/EDO-4-11.pdf

H. Congreso del Estado de Baja California. (2021). Código Penal para el Estado de Baja California. *Periódico Oficial*. https://www.congresobc.gob.mx/Documentos/ProcesoParlamentario/Leyes/TOMO_V/20210226_CODPENAL.PDF

H. Congreso del Estado de Baja California Sur. (2014). Código Penal para el Estado Libre y Soberano de Estado de Baja California Sur. Periódico Oficial. https://www.cbcs.gob.mx/index.php/cmply/1488-codigo-penal-para-el-estado-libre-y-soberano-de-estado-de-baja-california-sur

H. Congreso del Estado de Chiapas. (2020). Código Penal para el Estado de Chiapas. *Periódico Oficial*. https://www.congresochiapas.gob.mx/new/Info-Parlamentaria/LEY_0012.pdf

H. Congreso del Estado de Chihuahua. (2017). Código Penal del Estado de Chihuahua. *Periódico Oficial*. http://www.congresochihuahua2.gob.mx/biblioteca/codigos/archivosCodigos/64.pdf

Congreso del Estado de Coahuila. (2017). Código Penal de Coahuila de Zaragoza. *Periódico Oficial*. Congreso del Estado de Coahuila: https://congresocoahuila.gob.mx/transparencia/03/Leyes_Coahuila/coa08_Nuevo_Codigo.pdf

H. Congreso del Estado de Colima. (2020). Código Penal para el Estado de Colima. Periódico Oficial "El Estado de Colima". https://congresocol.gob.mx/web/Sistema/uploads/LegislacionEstatal/Codigos/codigo_penal_02mayo2020.pdf

H. Congreso del Estado de Durango. (2009). Código Penal para el Estado Libre y Soberano de Durango. *Periódico Oficial* no. 48. http://congresodurango.gob.mx/Archivos/legislacion/CODIGO%20PENAL%20(NUEVO).pdf

H. Congreso del Estado de Guanajuato. (2020). Código Penal del Estado de Guanajuato. *Periódico Oficial.* https://idea.guanajuato.gob.mx/wp-content/uploads/2021/03/C%C3%B3digo-Penal-del-Estado-de-Guanajuato.pdf

H. Congreso del Estado de Hidalgo. (2021). Código Penal para el Estado de Hidalgo. *Periódico Oficial.* http://www.congreso-hidalgo.gob.mx/biblioteca_legislativa/leyes_cintillo/Codigo%20Penal%20para%20el%20Estado%20de%20Hidalgo.pdf

H. Congreso del Estado de Jalisco. (2022). Código Penal para el Estado Libre y Soberano de Jalisco. Periódico Oficial. https://legislacion.scjn.gob.mx/Buscador/Paginas/wfArticuladoFast.aspx?q=lOyqDofbFLGDAD4UXA/alLagMW1wQoxLFuNL8H0akZi87LEkSEL6HoKF3xMTGo2zAWr/IxuktRcK30VX61kKCQ

H. Congreso del Estado de Michoacán. (2022). Código Penal para el Estado de Michoacán de Ocampo. *Periódico Oficial del Estado*. http://congresomich.gob.mx/file/CODIGO-PENAL-REF-29-DE-AGOSTO-DE-2022.pdf

H. Congreso del Estado de Morelos. (2021). Suprema Corte de Justicia de la Nación. *Periódico Oficial*. https://legislacion.scjn.gob.mx/Buscador/Paginas/wfArticuladoFast.aspx?q=sGiNPMW3FcBkLTcl6r0z02WoNGsQRUMNQh2Ix0EMw9UqvR4T2DYZKsSXx59NhGpXx0GIBIO8l3svQd5HnnDlf

H. Congreso del Estado de Nuevo León. (2022). Código Penal para el Estado de Nuevo León. *Periódico Oficial.* http://www.hcnl.gob.mx/trabajo_legislativo/leyes/codigos/codigo_penal_para_el_estado_de_nuevo_leon/

H. Congreso del Estado de Puebla. (1986). Código Penal para el Estado Libre y Soberano de Puebla. https://www.congresopuebla.gob.mx/index.php?option=com_docman&task=doc_download&gid=5928&Itemid=

H. Congreso del Estado de Quintana Roo. (2018). Código Penal para el Estado Libre y Soberano de Quintana Roo. *Periódico Oficial del Estado*. http://documentos.congresoqroo.gob.mx/codigos/C6-XV-20180427-157.pdf

H. Congreso del Estado de San Luis Potosí. (2021). Código Penal del Estado de San Luis Potosí. *Periódico Oficial del Estado*. https://www.teeslp.gob.mx/wp-content/uploads/2021/10/Codigo_Penal_Estado_de_San_Luis_Potosi_13_Sept_2021_PARTE_I.pdf

H. Congreso del Estado de Sinaloa. (2016). Código Penal para el Estado de Sinaloa. *Periódico Oficial*. http://www.congresosinaloa.gob.mx/images/congreso/leyes/zip/codigo_penal_28-dic-2016.pdf

H. Congreso del Estado de Sonora. (2022). Código Penal para el Estado de Sonora. *Periódico Oficial.* http://www.congresoson.gob.mx:81/Content/Doc_leyes/doc_443.pdf

H. Congreso del Estado de Tabasco. (2021). Código Penal para el Estado de Tabasco. *Periódico Oficial.* https://tsj-tabasco.gob.mx/resources/pdf/biblioteca/codigo_penal.pdf

H. Congreso del Estado de Tlaxcala. (2016). Código Penal para el Estado Libre y Soberano de Tlaxcala. Periódico Oficial. http://tsjtlaxcala.gob.mx/transparencia/Fracciones_a63/I/codigos/codigopenaltlaxcala.pdf

H. Congreso del Estado de Veracruz. (2015). Código Penal para el Estado Libre y Soberano Veracruz Ignacio de la Llave. *Gaceta Oficial*. https://www.legisver.gob.mx/leyes/LeyesPDF/PENAL270115.pdf

H. Congreso del Estado de Zacatecas. (2022). Código Penal para el Estado de Zacatecas. *Suplemento al Periódico Oficial del Estado de Zacatecas*. https://www.congresozac.gob.mx/63/ley&cual=103

H. Congreso del Estado Libre y Soberano de Oaxaca. (2018). Código Penal para el Estado Libre y Soberano de Oaxaca. *Periódico Oficial del Estado de Oaxaca*. https://sspo.gob.mx/wp-content/uploads/2018/09/C%C3%B3digo-Penal-para-el-Estado-Libre-y-Soberano-de-Oaxaca.pdf

Hernández, D. L. (2009). El delito informático. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, (227), 227-243. https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

López, J. (1 de febrero de 2022). El Salvador reforma código penal para atajar delitos informáticos; temen espionaje. *El Economista*. https://www.eleconomista.com.mx/internacionales/El-Salvador-reforma-codigo-penal-para-atajar-delitos-informaticos-temen-espionaje-20220201-0069.html

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho*, *44*(1), 235-260. http://dx.doi.org/10.4067/S0718-34372017000100011

Morales, P. F. (1984). *La tutela penal de la intimidad: privacy e informática*. Destino.

Naciones Unidas. (1998). Estatuto de Roma de la Corte Penal Internacional. https://www.un.org/spanish/law/icc/statute/spanish/rome_statute(s).pdf

Organización para la Cooperación y el Desarrollo Económicos (OECD). (1986). The OECD Observer, (142). https://doi.org/10.1787/observer-v1986-5-en

Organización para la Cooperación y el Desarrollo Económico. (1992). OECD Guidelines for the Security of Information Systems, 1992. https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

Organización de las Naciones Unidas (ONU). (2000). Lucha contra la delincuencia en la Internet. X Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml

Organización de las Naciones Unidas (ONU). (2005). México se convierte en el centésimo país en ratificar el Estatuto de Roma. Noticias ONU. https://news.un.org/es/story/2005/10/1066761

Organización de las Naciones Unidas (ONU). (2015). Delito cibernético. 13° Congreso sobre Prevención del Delito y Justicia Penal. https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

Organización de los Estados Americanos y Banco Interamericano de Desarrollo (OEA y BID). (2020). Reporte Ciberseguridad 2020. Riesgos, avances y el camino a seguir en América Latina y el Caribe. BID. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Pérez Luño, A. E. (2011). Internet y los derechos humanos. *Anuario de Derechos Humanos, 12*, 287-330. http://dx.doi.org/10.5209/rev_ANDH.2011.v12.38107

Poder Judicial Yucatán. (2021). Código Penal del Estado de Yucatán. https://www.poderjudicialyucatan.gob.mx/digestum/marcoLegal/03/2012/DIGESTUM03002.pdf

Poder Legislativo del Estado de Campeche. (2021). Código Penal del Estado de Campeche. *Periódico Oficial del Estado*. https://legislacion.congresocam.gob.mx/index.php/leyes-focalizadas/anticorrupcion/6-codigo-penal-del-estado-de-campeche

Poder Legislativo del Estado de Querétaro. (2015). Código Penal para el Estado de Querétaro. http://legislaturaqueretaro.gob.mx/app/uploads/2016/01/COD004.pdf

Ramírez Sánchez, M. (2022). Respuesta a solicitud de acceso a la información. FGEQR. Mérida.

Réyez, J. (2021). México, el auge del mercado de la ciberdelincuencia. *Contralínea*. https://contralinea.com.mx/mexico-el-auge-del-mercado-de-la-ciberdelincuencia/

Riquelme, R. (2 de enero de 2021). 2020, en 12 hackeos o incidentes de seguridad en México. *El Economista*. https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

Rodríguez, L. C. (1 de octubre de 2022). Congeladas, 15 iniciativas contra delitos informáticos. *El Universal.* https://www.eluniversal.com.mx/nacion/congeladas-15-iniciativas-contra-delitos-informaticos

Romeo, C. C. (2006). De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal, en C. M. Montalvo, *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales* (1-43). Comares.

Saucedo Martínez, M. d. (26 de mayo de 2022). Respuesta FGJCDMX/110/3848/2022-05.

Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. (2022). Incidencia delictiva del Fuero Común, nueva metodología. Gobierno de México.

https://www.gob.mx/sesnsp/acciones-y-programas/incidencia-delictiva-del-fuero-comun-nueva-metodologia

Sistema de Información Legislativa de la Secretaría de Gobernación. (2017). Proposición con punto de acuerdo por el que se exhorta a la Secretaría de Relaciones Exteriores para que inicie los trabajos necesarios para la adhesión al Convenio de Budapest. Gaceta Parlamentaria. http://sil.gobernacion.gob.mx/Archivos/Documentos/2017/05/asun_3543563_20170530_1496162027.pdf

Tejerina, O. (2020). *Aspectos jurídicos de la ciberseguridad*. Ra-ma.

Téllez Valdés, J. A. (2004). *Derecho Informático* (3ª ed.). Mc Graw Hill.

Unidad de Transparencia de la Fiscalía del Estado de Jalisco. (2022). Resolución Oficio FE/UT/3837/2022. Exp. Admvo. Int, LTAIPJ/FE/1239/2022.