Universidad San Francisco

Computer Security

Homework 4 : Information Security and Privacy And Review of Ola Bini's Case

César Cardenás & Edwin Jaramillo & José Contreras

May 6, 2024

The goal of this homework is to investigate the Ecuadorian law with respect to information security and privacy.

1. **Cite the articles of the constitution and COIP that address the topic of information security and information privacy.**

1.1 Constitution of the Republic of Ecuador

a) **Information Privacy as a fundamental right of the people:**

Article 66.- People are recognized and guaranteed:... 19. The right to protection of personal information, including access to and decision about information and data of this nature, as well as its corresponding protection. The gathering, filing, processing, distribution or dissemination of these data or information shall require authorization from the holder or a court order.

b) **Jurisdictional Guarantees: Habeas Data Proceedings:**

Article 92.- All persons, by their own rights or as legitimate representatives for this purpose, shall have the right to know of the existence of and gain access to documents, genetic data, personal data banks or files and reports about themselves or about their assets that appear in public or private entities, whether in hard copy or on electronic media. Likewise, they shall have the right learn about the use made of this information, its end purpose, the origin and destination of the personal information and the time of validity of the data file or bank. The persons responsible for the data banks or files will be able to disseminate the filed information with the authorization of the holder or the law. The person owning the data will be able to request the person in charge to allow access free of charge to the file, as well as update of the data and their correction, deletion or annulment. In the case of sensitive data, whose file must be authorized by law or by the person owning the information, the adoption of the security measures that are needed shall be required. If the petition is not duly answered, the person can resort to a judge. The affected person can file a complaint for damages caused.

a) **Competences of the Constitutional Court in matters of protection of Personal Information:**

Article 436.- The Constitutional Court shall perform the following duties, in addition to those granted to it by the law:... 6. To issue judgments that constitute binding case law with respect to actions of protection, enforcement, habeas corpus, habeas data, access to public information and other constitutional processes, as well as those cases selected by the Court for review.

1.2 Comprehensive Organic Penal Code (COIP)

1.2.1 In the COIP, within the Third Chapter of Crimes against Good Living, in the Third Section, a set of crimes against the security of the assets of information and communication systems are found, typifying the following:

a) **Illegal disclosure of database: Article 229.-** Public servants shall consist of all those persons who in any way or under any category, provide services or hold an office, function, or dignity in the public sector. The rights of public servants cannot be waived. The law shall determine the executive body in charge of human resources and remuneration for the entire public sector and shall regulate admittance, advancement, promotion, incentives, disciplinary system, job security, salary scale and termination of duties of its employees. Public sector employees shall be subject to the Labor Code. Remuneration of public servants shall be fair and equitable, in line with their respective duties, and shall take into account their professional development, training, responsibility, and experience.

b) **Illegal interception of data: Article 230.-** Will be punished with a penalty deprivation of liberty for three to five years: 1. The person who, without prior court order, for his or her own benefit or that of a third party, intercepts, listens to, diverts, records or observes, in any way, computer data at its origin, destination or within a computer system, a signal or a transmission of data or signals. 2. The person who designs, develops, sells, executes, programs or sends messages, security certificates or electronic pages, links or pop ups or modifies the domain name resolution

system of a financial service or electronic payment or other personal site or trusted, in such a way that it induces a person to enter an address or website different from the one they want to access. 3. The person who possesses, sells, distributes or, in any other way, disseminates or introduces into one or more computer systems, electronic devices, programs or other digital content intended to cause what is described in the previous number. 4. The person who, through any means, copies, clones or commercializes information contained in magnetic stripes, chips or other electronic devices supported by credit, debit, payment or similar cards. 5. The person who produces, manufactures, distributes, possesses or provides materials, electronic devices or computer systems intended for the commission of the crime described in the previous section.

c) **Electronic transfer of property assets: Article 231.-** The person who, for profit, alters, manipulates or modifies the operation of a computer or telematic program or system or data message, to procure the non-consensual transfer or appropriation of a property. asset of another person to the detriment of that person or a third party, will be punished with imprisonment of three to five years. The person who facilitates or provides bank account data with the intention of illegitimately obtaining, receiving or capturing a property asset through an electronic transfer resulting from this crime for himself or for another person will be punished with the same penalty.

d) **Attack on the integrity of computer systems: Article 232.-** The person who destroys, damages, deletes, deteriorates, alters, suspends, blocks, causes malfunctions, unwanted behavior or totally or partially deletes digital content, computer systems, systems of information and communication technologies, electronic devices or technological infrastructure necessary for the transmission, reception or processing of general information, with the purpose of seriously, deliberately and illegitimately hindering the operation of a computer system, will be punished with a custodial sentence of imprisonment. freedom from three to five years. The person who designs, develops, programs, acquires, sends, introduces, executes, sells or distributes in any way, will be punished with the same penalty. Machine Translated by Google devices, programs or computer systems that are malicious or intended to cause the effects indicated in the first paragraph of this article. If the violation is committed on computer assets intended for the provision of a public service or linked to citizen security, the penalty will be five to seven years of deprivation of liberty.

e) **Crimes against legally reserved public information: Article 233.-** Crimes against legally reserved public information, The person who destroys or disables classified information in accordance with the Law will be punished with imprisonment of five to seven years. The public servant who, using any electronic or computer means, obtains this type of information, will be punished with imprisonment of three to five years. In the case of confidential information, the disclosure of which could seriously compromise the security of the State, the public servant in charge of the custody or legitimate use of the information who, without the corresponding authorization, reveals said information, will be punished with imprisonment of seven years. to ten years and disqualification from holding a public office or function for six months, provided that no other more serious infraction is established.

f) **Non-consensual access to a computer, telematic or telecommunications system: Article 234.-1** The person who, without authorization, accesses all or part of a computer system or telematic or telecommunications system or remains within it against of the will of whoever has the legitimate right over said system, will be punished with a custodial sentence of three to five years. 2. If the person who accesses the system does so to illegitimately exploit the access achieved, modify a web portal, divert or redirect data or voice traffic or offer services that these systems provide to third parties, without paying them to the service providers. legitimate services, will be punished with imprisonment of three to five years.

g) **The crime of computer falsification is incorporated: Article 234.1; 234.2.-** the aggravation of penalties and in 234.3 the responsibility of legal entities in these cases, in accordance with the provisions of articles 49 and 71 of the same code.

h) Also added in the last COIP reform is article 234.4 in which they list definitions:

a. Digital content - Digital content is any computer data that represents facts, information or concepts of reality, stored, processed or transmitted by any technological means or communication

channel that lends itself to computer processing, including programs designed for isolated technological equipment. , interconnector related to each other. **b. Traffic data** -Digital content related to a communication carried out through a computer system or communication channel, generated by this system as an element of a communication chain, indicating its origin, destination, route, time, date, size, the duration or type of underlying service. **c. Service provider** -Any entity, public or private, national or international, that provides users of its services with the ability to communicate through a computer system, or any of the information and communication technologies, as well as any other entity that processes or store digital content in the name and on behalf of that providing entity or its users. **d. Computer system** -Any device or set of interconnected or associated devices, in which one or more of them develops, executing a program, the automated processing of digital content.

1.2.2 Additionally, the COIP establishes other crimes that are related to the information security and protection of personal data:

a) Protection of people considered part of the most vulnerable groups, who require special attention, within the catalog of rights and guarantees recognized in the Constitution of the Republic and international instruments of human rights of deprived persons is found in article 12 of the COIP, Rights and guarantees of persons deprived of liberty, 6. Protection of personal data: the person deprived of liberty has the right to the protection of his or her personal data, which includes access and use of this information.
b) In accordance with the reform published in the Official Registry No. 526 to the COIP, article 154.2 is incorporated into the section dedicated to crimes against personal integrity, in which Harassment is classified as a crime , in the following sense : natural or legal person who, by themselves or through third parties or through any technological or digital means, persistently or repeatedly annoys, disturbs or distresses another, will be punished with imprisonment of six months to one year, provided that The active subject of the offense seeks proximity to the victim in order to cause harm to his or her physical or sexual integrity. The same article incorporates aggravating factors in the sanction for cases in which the victim is a minor or with some type of disability that prevents him or her from understanding the magnitude of the action. Likewise, the penalty becomes more burdensome in cases where the aggressor is a family member, has had family or dating ties, and other cases, with the victim.
c) Article 179 of the COIP establishes the crime of revealing secrets or personal information of third parties, punishing with imprisonment the action of any person who, having knowledge due to his or her status or trade, employment, profession or art, of a secret whose disclosure causes harm to another person and reveals it, except in those cases where the disclosed secret relates to matters of public interest.

2. **Describe and summarize such articles and provide their scope.**

   The articles of the COIP are intended to safeguard and protect personal integrity, as well as guarantee the enjoyment of the good life constitutionally enshrined and which is part of the rights of people. Likewise, special protection is sought for those people who are most vulnerable, that is, children and adolescents, people deprived of liberty, older adults and disabled people.The provisions of the COIP largely seek to address the countless cases that may occur of violation of rights in the use of social networks and other technological applications, which aggressors use to defraud people's trust. These are crimes that can be carried out in cyberspace, or that are planned there and materialize in other places, but which have as a common element the presence or use of technology, and which can cause direct damage to specific people and in In other cases, they can affect groups. The scope of these rights is both the protection of the integrity of the person and their data, in order to protect their honor and reputation, and computer assets.

3. **What kind of crimes or infractions can a person be judged for using those articles?**

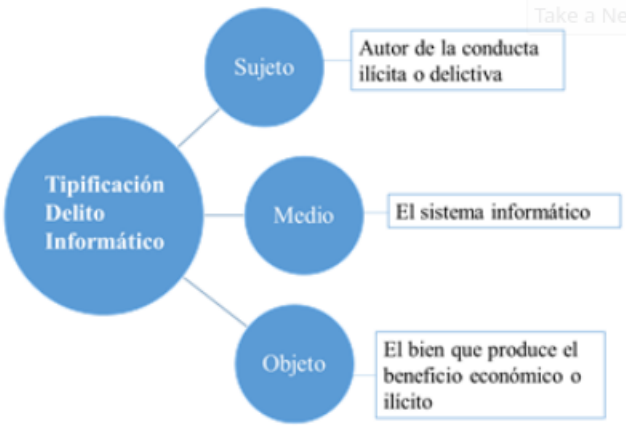

Figura 1: Cyber Crime Definition
(Saltos, M., Robalino, J., y Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343-351. Recuperado de: https://scielo.sld.cu /scielo.php?script=sci$_a rttextpid = S1990 - 86442021000100343lng = estlng = es.$)

As indicated previously, the Third Chapter of Crimes against Good Living, in the Third Section a set of crimes against the security of the assets of the information and communication systems. Now, according to the consulted doctrine (Santos et al. 2021), the behaviors or actions that the United Nations considers as computer crimes are the following:

• Fraud committed through computer manipulation: this type of computer fraud, also known as data theft, represents the most common computer crime.

• Program manipulation; This crime consists of modifying existing programs in the computer system or inserting new programs that have specialized knowledge in computer programming.

• Manipulation of output data; It is carried out by setting an objective to the operation of the computer system, the most common example being the fraud that targets ATMs through the falsification of instructions for the computer in the data acquisition phase.

• Fraud carried out by computer manipulation of computing processes.

• Computer falsifications; when data in documents stored in computerized form is altered.

• As instruments; Computers can also be used to carry out falsification of documents for commercial use.

• Computer Sabotage; is the act of deleting, deleting or modifying without authorization computer functions or data with the intention of hindering the normal functioning of the system.

• Viruses; It is a series of programmatic keys that can attach to legitimate programs and spread to other computer programs.

• The Worms; which are analogous to the virus with a view to infiltrating legitimate data processing programs or to modify or destroy data, but is different from the virus because it cannot regenerate.

• The Logic or Chronological Bomb; which requires specialized knowledge, since it requires the programming of the destruction or modification of data at a given time in the future.

• Unauthorized access to computer services or systems; This is for various reasons, from simple curiosity, as in the case of many hackers, to sabotage or computer espionage.

• Computer Pirates or Hackers; This access is often made from a external location, located in the telecommunications network.

• Unauthorized reproduction of legal protection computer programs; which brings a substantial economic loss to the legitimate owners.

4. **What kind of evidence could the persecutors use to incriminate someone with this kind of crime?**

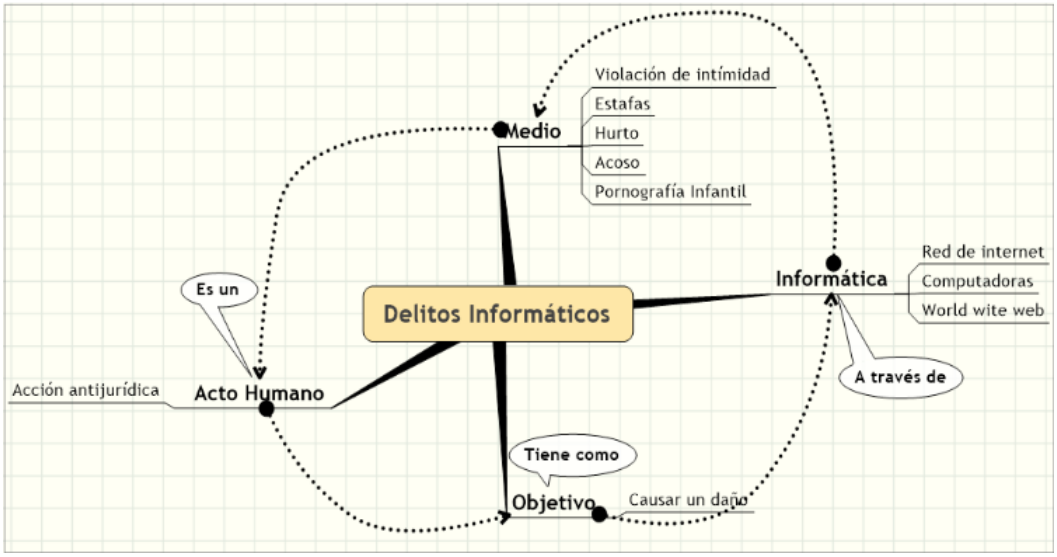

Figura 2: Evidence in CiberCrime Paradygm
((Saltos, M., Robalino, J., y Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343-351. Recuperado de: https://scielo.sld.cu /scielo.php?script=sci$_a rttextpid = S1990 - 86442021000100343lng = estlng = es.$)

The evidence of computer crimes continues to be a topic of observation and discussion, given the difficulty of obtaining it in each specific case. However, it has been advanced that these are elements obtained through forensic expert examination techniques, with the participation of experts in the different computer and IT areas, who, keeping the necessary aspects of the chain of custody and others established by law, can be brought to trial, as described by Ochoa (2018), who refers to the need for a methodical series of techniques and procedures to collect evidence, from computer equipment and various storage devices and digital media, which can be presented in a court of law in a coherent and meaningful format. The evidence that serves as elements of conviction to prove the commission of computer crimes, particularly when it comes to non-consensual access to a computer system, must seek to prove that the person who is being identified as the author of the crime actually had access. and it is not found that this is an action and that it would have been done illegally to a computer or telecommunications system, as the case may be.

5. **Provide a summary of Ola Bini's case and present the main arguments and crimes of which he was accused.**

Figura 3: Ola Bini and his local lawyer Carlos Soria
(Notimundo (13 de abril de 2022). Los procesos legales que enfrenta el sueco Ola Bini son producto de una persecución que se inició hace 3 años, dice su abogado. Notimundo. Recuperado de: https://notimundo.com.ec/los-procesos-legales-que-enfrenta-el-sueco-ola-bini-son-producto-de-una-persecucion-que-se-inicio-hace-3-anos-dice-su-abogado/)

The case of Ola Bini, who has been identified as a computer expert and has been identified as the perpetrator of the crime of non-consensual access to a computer system, specifically for having accessed the system of the National Telecommunications Corporation (CNT) without authorization or consent. with the objective of obtaining information from the digital content of the Petroecuador Public Company and the then National Intelligence Secretariat (SNAI). However, the Prosecutor's Office initially prosecuted him for an alleged attack on computer systems and then reformulated charges for the alleged crime of non-consensual access to a computer, telematics or telecommunications system. After almost four years of trial, the Criminal Guarantee Court has declared him innocent. Within the allegations given by the parties to the case, it is stated that the crime of attacks on computer systems is a serious crime of national connotation, in which it has been implicated even by the violation of a computer nature, a crime that would even entail other crimes that They will be investigated. Additionally, since the accusation is a foreign person as the author, there has been the incentive of danger of flight, even more so due to his immigration details that he was even on the verge of leaving the country, that is, he could obtain the means to evade state action. Regarding the evidence presented by the Prosecutor's Office in this case, it has consisted of computer forensic and audio and video expert reports; as well as the international criminal assistance required from the United States, through which information was extracted from one of the defendant's devices; In addition to versions, letters from the Ministry of Foreign Affairs, the Financial and Economic Analysis Unit (UAFE) and other public and private entities.

6. **What is your opinion on the case in general and its outcome?**

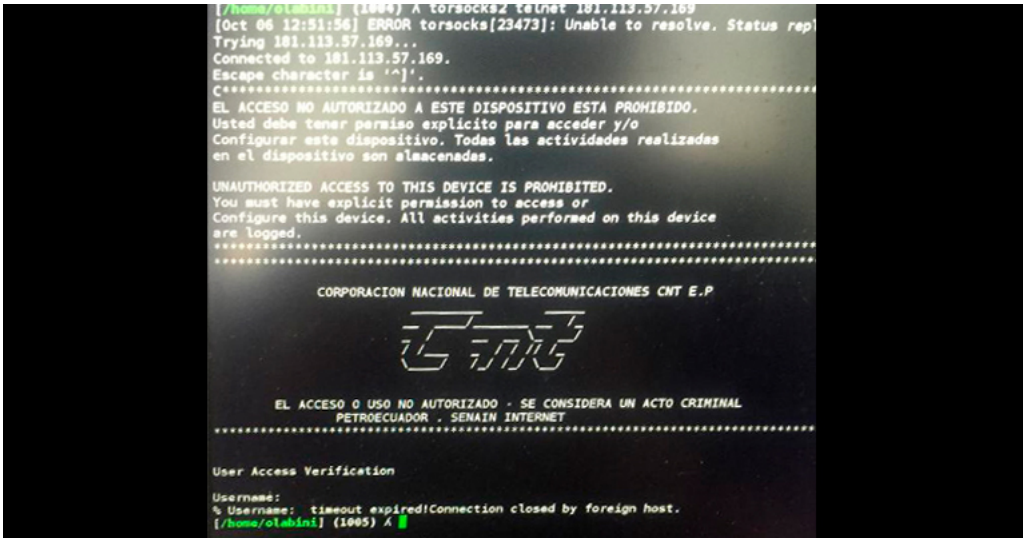

Figura 4: Phothograph of Ola Bini's shell with evidence of the alleged attack-intromission to CNT systmes (Primicias (2021) Fotografía hallada en el celular de Ola Bini que, según la Fiscalía, prueba el intento de vulnerar el sistema informático de la CNT, en 2015. Primicias. Recuperado de: https://www.primicias.ec/noticias/en-exclusiva/ola-bini-eencriptador-desencriptado-politica-ecuador/)

From the criminal procedural perspective, the case of Ola Bini reveals the difficulties of both determining which type of crime the action classified as computer crime fits, such as access without consent, as well as other crimes that are classified in criminal legislation; but there are also evidentiary difficulties, which allow the judge to be provided with the necessary elements of conviction to declare the person guilty or innocent, as the case may be, since the evidence, in the actions of the Prosecutor's Office as the institution in charge of criminal action, must seek the truth of the case, whether it leads to the innocence or guilt of the person identified as the author of the act. It cannot be overstated that this specific case serves as an example of the problems involved in the relationship between politics and the administration of justice, especially in cases of national and international connotation, and given the implications of the use of technology. Likewise, it has highlighted the delay in criminal justice, since Ola Bini's case was prosecuted in 2019 and reached a sentence in 2023, that is, four years later.

7. **How do the terms of services of apps like Whatsapp and TikTok align with privacy laws in Ecuador? What type of protections does the law guarantee to Ecuadorian citizens?**

Within the criminal types indicated above (see answer to question 1), attention is sought for the integrity of people and their good living. However, in accordance with the constitution, the protection of personal data must be guaranteed, so reference must be made to the Organic Law on the Protection of Personal Data, published in the Official Registry Supplement 459 of May 26, 2021, in accordance with the which seeks to guarantee the exercise of the right to protection of personal data, which includes access and decision on information and data of this nature, as well as its corresponding protection; and through which principles, rights, obligations and protection mechanisms are regulated, provided for and developed. On the other hand, regarding social networks and other applications such as Whatsapp and TikTok, there is no express provision that regulates privacy and guarantees the protection of Ecuadorian citizens. However, in 2019, a draft "Organic Law on the responsible use of social networks" was presented to the National Assembly, which was later withdrawn, but whose objective was to "regulate the responsible use of social networks with thein order to guarantee a new form of responsible communication, since networks are not only a source of information but also a means of disseminating content, and can contribute to the strengthening of the institution and the interaction with all citizens of the country and the entire world."

Referencias

[1] Ochoa, P. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. Revista Economía y Política, 28, 35-44. Recuperado de: https://www.redalyc.org/journal/5711/571167817003/html/

[2] Saltos, M., Robalino, J., y Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343-351. Recuperado de: http://scielo.sld.cu/scielo.php?script=sci$_a rttextpid = S1990 - 86442021000100343 lng = estlng = es$.

[3] Notimundo (13 de abril de 2022). Los procesos legales que enfrenta el sueco Ola Bini son producto de una persecución que se inició hace 3 años, dice su abogado. Notimundo

[4] Primicias (2021) Fotografía hallada en el celular de Ola Bini que, según la Fiscalía, prueba el intento de vulnerar el sistema informático de la CNT, en 2015. Primicias. Recuperado de: https://www.primicias.ec/noticias/en-exclusiva/ola-bini-eencriptador-desencriptado-politica-ecuador/