Homework 4

Andres Martinez 00213046 8 - May - 2024

Assingment: 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

The COIP (the penal code) address personal data, privacy of information and information security in these articles

> **Art 12. -** Derechos y garantías de las personas privadas de libertad.- Las personas privadas de libertad gozarán de los derechos y garantías reconocidos en la Constitución de la República y los instrumentos internacionales de derechos humanos: [...]
> Protección de datos de carácter personal: la persona privada de libertad tiene derecho a la
> protección de sus datos de carácter personal, que incluye el acceso y uso de esta información.

> Art. 178. - Violación a la intimidad.- La persona que, sin contar con el consentimiento o la
> autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por

cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles.- La
persona que reprograme o modifique la información de identificación de los equipos terminales
móviles, será sancionada con pena privativa de libertad de uno a tres años.

Art. 192.
- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

> El articulo 190 tambien podria ser mencionado ya que habla de usar sistemas informaticos de forma ilegal para obtener informacion personal

Art. 195.- Infraestructura ilícita.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil,

> será sancionada con pena privativa de libertad de uno a tres años

> Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años [...]

> Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años

> Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los

> proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años

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

1. **Art. 12**: This article protects the personal data of incarcerated individuals, ensuring they have rights to access and control their personal information.
2. **Art. 178**: It criminalizes unauthorized access, interception, retention, recording, reproduction, dissemination, or publication of personal data, private communications, and information on digital media without consent or legal authorization. Exemptions include situations involving personal participation in the recordings or legally defined public information.
3. **Art. 191 and Art. 192**: These articles deal with mobile terminal equipment. Art. 191 penalizes the unauthorized reprogramming or modification of identification information of mobile devices, while Art. 192 addresses the exchange, sale, or purchase of databases containing such identification information.
4. **Art. 195**: It targets the possession of infrastructure or tools that enable the modification of mobile device identification data, aiming to prevent illegal tampering with device identity.
5. **Art. 229**: This article criminalizes the unauthorized revelation of information from databases, files, or electronic systems, infringing on individuals' secrecy, privacy, and intimacy.
6. **Art. 232**: It concerns attacks on the integrity of computer systems. It penalizes acts that destroy, damage, delete, or otherwise harm the data or functioning of information processing systems.
7. **Art. 234**: This final article focuses on unauthorized access to computer, telematic (relating to telecommunications), or telecommunications systems. It covers unauthorized access, web portal modification, data or voice traffic redirection, or unauthorized provision of system services.

The legal framework provided by Ecuador's Comprehensive Organic Penal Code (COIP) addresses the protection of privacy and information against improper access and use. Similarly, Articles 191 and 192, by focusing on mobile devices, reinforce the security of personal

security in a comprehensive manner. The articles mentioned offer a solid legal foundation for preventing and penalizing unauthorized access to personal data, improper manipulation of information, and violations of digital privacy. For example, Article 178 explicitly criminalizes the unauthorized interception or dissemination of private communications and personal data, reflecting a clear effort to protect the confidentiality and integrity of personal information in an era dominated by mobile technology, addressing everything from illegal reprogramming of devices to illegitimate trade of databases. This set of regulations demonstrates a commitment to preserving privacy across various domains, from computer systems to telecommunication communications, and establishes severe penalties for those who violate these norms, thus ensuring that the rights to privacy and information security are respected and effectively protected.

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

Article 178 of the COIP addresses the crime of unauthorized access, interception, or dissemination of personal data and private communications without consent. This provision underscores the legal recognition of the sanctity of personal and private information in the digital realm. This is a very extensive article in reality that has the authorithy in paper to charge a pearson with any missuse of personal data, but the authorithes resposable have not yet decided on the specifics. Articles 191 and 192 are focused on infractions involving mobile devices—specifically the unauthorized alteration of device identification data and the illegal trading of such data. These articles reflect a legal response to the increasing concerns over mobile device security and the unauthorized use of mobile data. Article 229 criminalizes the unauthorized disclosure of information from databases, archives, or electronic systems. This crime pertains to the breach of privacy and confidentiality, highlighting the protective measures enforced to safeguard sensitive information within institutional databases. Article 232 pertains to cyberattacks that compromise the integrity of computer systems. Such infractions include the damaging, altering, or otherwise manipulating data or system functionality, which can severely disrupt organizational operations and security. Finally, Article 234 targets unauthorized access to computer, telecommunications, or telematic systems. This crime involves unauthorized entry into systems for purposes that

might include data redirection or website manipulation, emphasizing the need for stringent security protocols to prevent unauthorized system exploitation.

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

In a case involving alleged violations of information security and privacy laws, prosecutors can utilize a variety of evidences to establish culpability. They could present digital footprints such as IP logs, server access records, and audit trails, which show unauthorized or illegal access to systems. They might also use intercepted communications that indicate malintent or unauthorized data handling, backed by expert testimony on the technical aspects of these actions. Evidence from electronic devices like computers and smartphones, including emails, messages, or files that support allegations of data misuse or unauthorized access, would be crucial. Moreover, testimonies from witnesses or insiders who can describe the accused's actions or intentions might be used to strengthen the case. Forensic analysis results that tie the digital evidence directly to the suspect's devices or accounts would be pivotal, as would any admissions or confessions made by the accused regarding their involvement in the crime.

---

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

Ola Bini, a Swedish programmer and digital rights advocate, became a central figure in a contentious legal saga in Ecuador that underscored tensions between government authorities and digital privacy activists. His case, which unfolded over several years, was fraught with legal irregularities and highlighted the challenges facing those who work at the intersection of technology and human rights.

Bini was arrested on April 11, 2019, just hours after Ecuador revoked Julian Assange's asylum. He was apprehended at Quito's airport without a warrant and under dubious circumstances, including not being informed of his charges in his native language, which signaled potential due process violations from the outset (Singh, 2024)

The charges against Bini centered around alleged unauthorized access to computer systems, specifically targeting the National Telecommunications

Corporation (CNT) of Ecuador with the aim of trying to obtain information from the digital content of the platforms of the oil company Petroecuador and the former National Intelligence Secretariat (EFFE, 2024). The prove that they presented was an image of a Telnet session. The case against him was primarily built on his association with Julian Assange and his use of privacy-focused tools like Tor, which prosecutors pointed to as evidence of suspicious activity. However, these actions are generally recognized as part of lawful privacy protection practices (Alimonti, 2023).

Throughout the judicial process, Bini faced several legal setbacks, including his initial 70-day detention, which was later ruled illegal. His trial saw numerous delays and procedural irregularities, raising significant concerns about the integrity of Ecuador's judicial processes in his case. After an initial acquittal due to lack of evidence, a reversal occurred when an appeal court sentenced him to a year in prison, citing his technical expertise as a potential tool for committing crimes (Flores, 2022).

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

Emilia

I support the government's efforts to secure its digital infrastructure and protect against potential cyber threats, recognizing that this is essential for national security. It's plausible that Ola Bini may have crossed legal boundaries in this context. This case importantly highlights the ongoing debate about how nations should balance national security with individual freedoms, especially in the digital and cyber realms where legal and ethical boundaries are still being defined. However, I am critical of the manner in which the authorities handled the case. The use of unlawful arrest and other procedural irregularities

Andres

while I think its important for a country to have legislation dedicated to convering cybercrime widely so to cover the scope of problems yet to come, this kind of legislation can also be abused as blanket legislation to justify arrest with polical intent behind, as it was the case for Ola Bini in Ecuador. Bini's arrest, which occurred under the pretext of cybersecurity violations, raised significant concerns about the potential misuse of broad cybercrime laws. Such laws, while essential for protecting against real threats, can be weaponized for political purposes, undermining the principles of justice

undermines the legal process, suggesting a disregard for the principles of justice and due process. These actions not only damage the integrity of this specific case but also potentially erode public trust in how digital laws are enforced.

and due process. In Bini's case, the use of digital privacy tools, which are commonly used for legitimate protection of personal information, was portrayed suspiciously, illustrating how cybersecurity laws can be selectively interpreted or enforced to target individuals. This situation highlights the critical need for clear, precise legal frameworks that not only address the complexity of cybercrimes but also safeguard against their misuse, ensuring that the rights to privacy and free expression are not compromised under the guise of national security or legal enforcement.

7. How do the terms of services of applications like Whatsapp and TikTok align with the privacy laws in Ecuador? What kind of protections Ecuadorian citizens are guaranteed under the law?

WhatsApp and TikTok have to comply with Ecuador's data protection law which means ensuring that any processing of personal data from Ecuadorian users aligns with these requirements. This involves securing valid consent where necessary, especially for sensitive data, and respecting users rights as laid out by the law. Additionally, these applications must adhere to principles such as data minimization and ensuring transparency about data use, particularly when it comes to cross-border data transfers

The protections Ecuadorian citizens are guaranteed under the law are:

1. Consent requirements:TikTok and WhatsApp must obtain clear and explicit consent from users before collecting and processing their data. This

consent must be freely given, specific, informed, and unambiguous, particularly for sensitive personal data (Legal500, 2024)

2. Sensitive personal data: the law defines sensitive personal data very broadly, including characteristics such as ethnicity, health data, biometric data, and political opinions, among others. The processing of such data is generally prohibited unless explicit consent is provided to the applications (DLA, 2023)
3. Data portability: Ecuadorian users can request a copy of their data in a structured, commonly used format, which they can then transfer to another service provider, enhancing their control over their personal data (Flor, 2024)
4. Rights of individuals: users have the right to access their personal data stored by these platforms, rectify, or delete them when it is no longer necessary for the purpose it was collected. Also users can object to certain types of data processing, like for marketing purposes, and request that their data processing be restricted under specific circumstances (Andrews, 2021)
5. Security measures: TikTok and WhatsApp are required to implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage (Andrews, 2021)

Bibliography

Singh, T. (2024). Activist Ola Bini sentenced to one year in prison after Ecuadorian court overturns acquittal. Retrieved from https://peoplesdispatch.org/2024/04/08/activist-ola-bini-sentenced-to-one-year-in-prison-after-ecuadorian-court-overturns-acquittal/

Alimonti, V. (2023). The Aftermath of Ola Bini's Unanimous Acquittal by Ecuadorian Court. Retrieved from https://www.eff.org/deeplinks/2023/03/aftermath-ola-binis-unanimous-acquittal-ecuadorian-court

Flores, C. (2022). Ola Bini, the cyberactivist who causes panic in Ecuador. Retrieved from https://globalvoices.org/2022/10/21/ola-bini-the-cyberactivist-who-causes-panic-in-ecuador/

EFFE. (2024). Ola Bini: ¿Por qué fue condenado a un año de prisión en Ecuador?. Retrieved from https://www.expreso.ec/actualidad/ola-bini-condenado-ano-prision-ecuador-195812.html

Flor, M. (2024). Ecuador – Data Protection Overview. Retrieved from https://www.dataguidance.com/notes/ecuador-data-protection-overview

Legal500. (2024). Ecuador: Data protection and cybersecurity. Retrieved from https://www.legal500.com/guides/chapter/ecuador-data-protection-cybersecurity/

DLA. (2023). Law in Ecuador. Retrieved from https://www.dlapiperdataprotection.com/index.html?t=law&c=EC

Andrews, H. (2021). Ecuador approves data protection law. Retrieved from https://natlawreview.com/article/ecuador-approves-data-protection-law