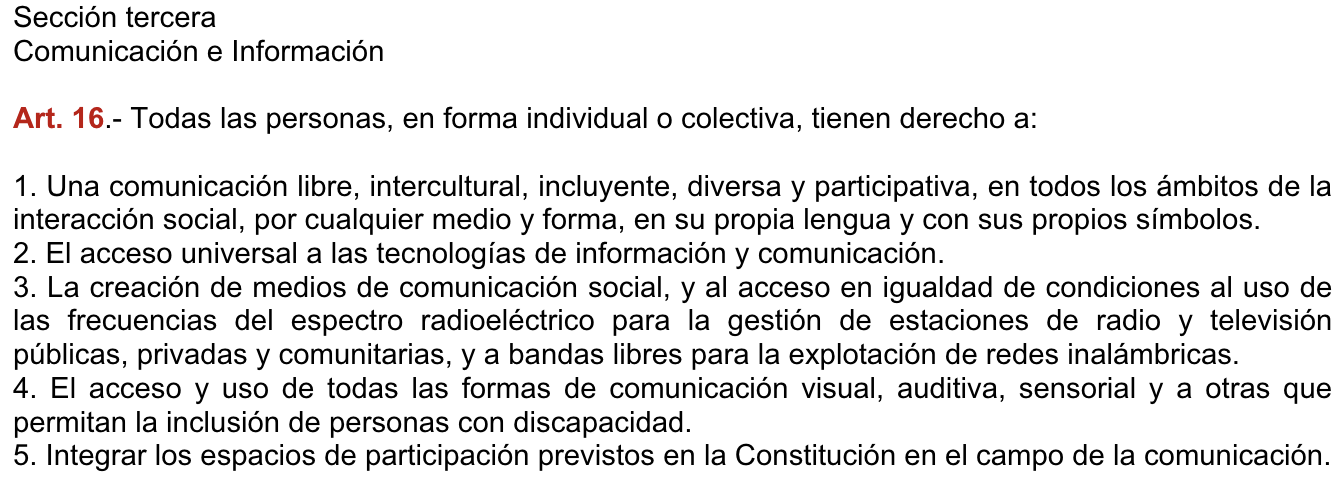
**Homework 4**

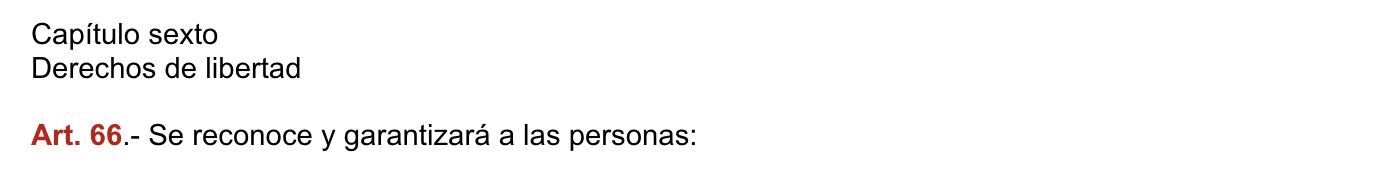
**Name**: Kevin Huertas 213278

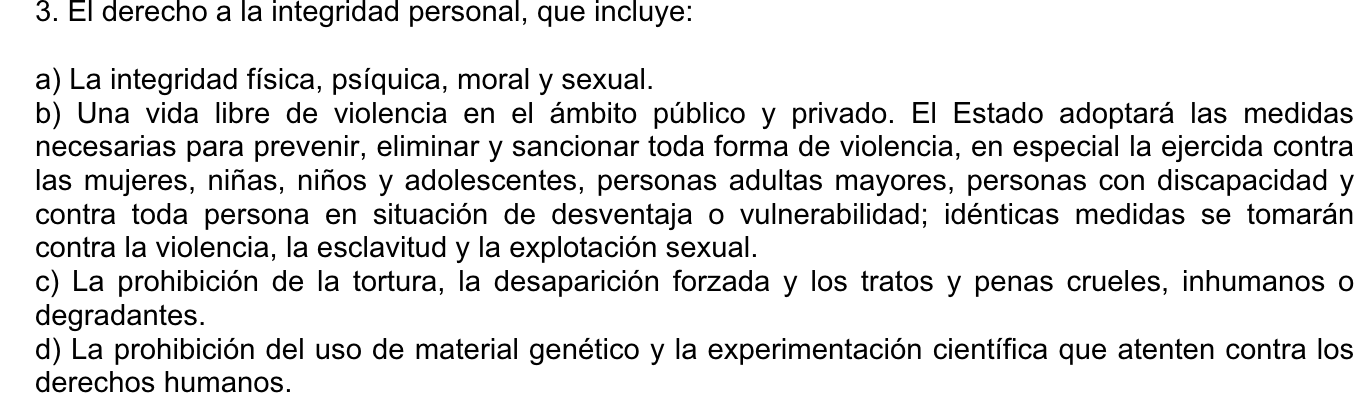
**The goal of this homework is to investigate the Ecuadorian law with respect to information security and privacy.**

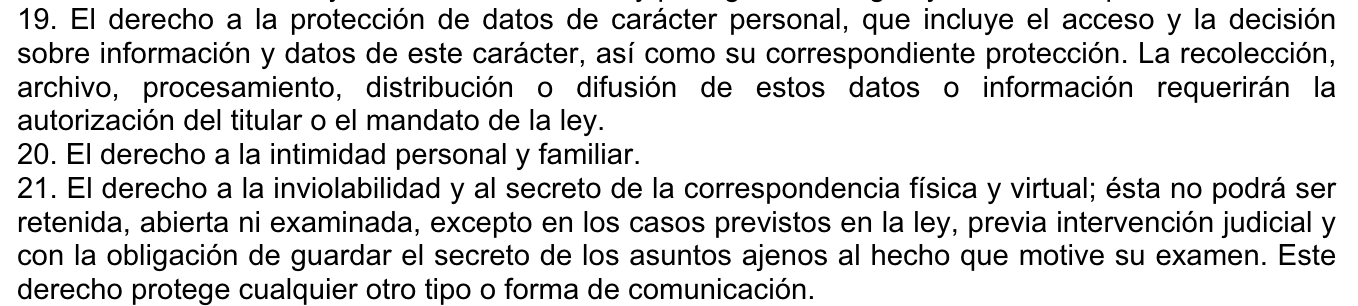
1. Cite the articles of the constitution and COIP that address the topic of information security and information privacy

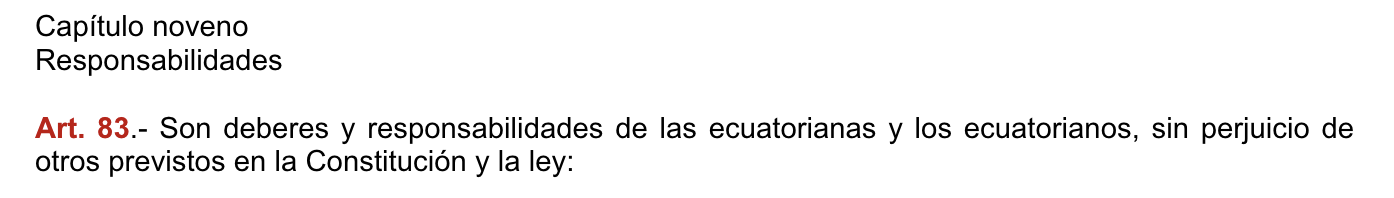
Constitution: <https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf>



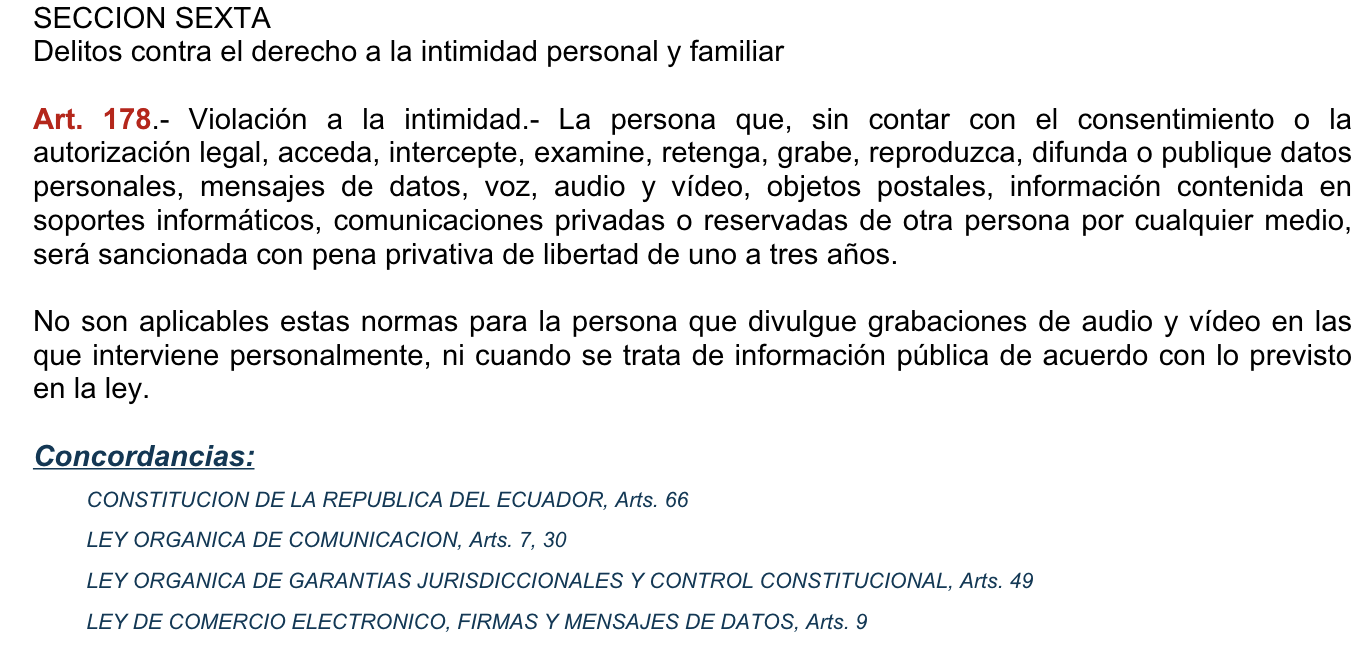


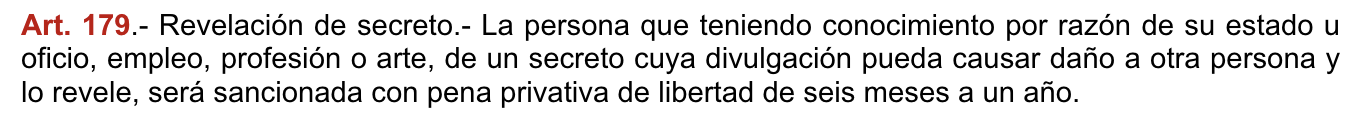


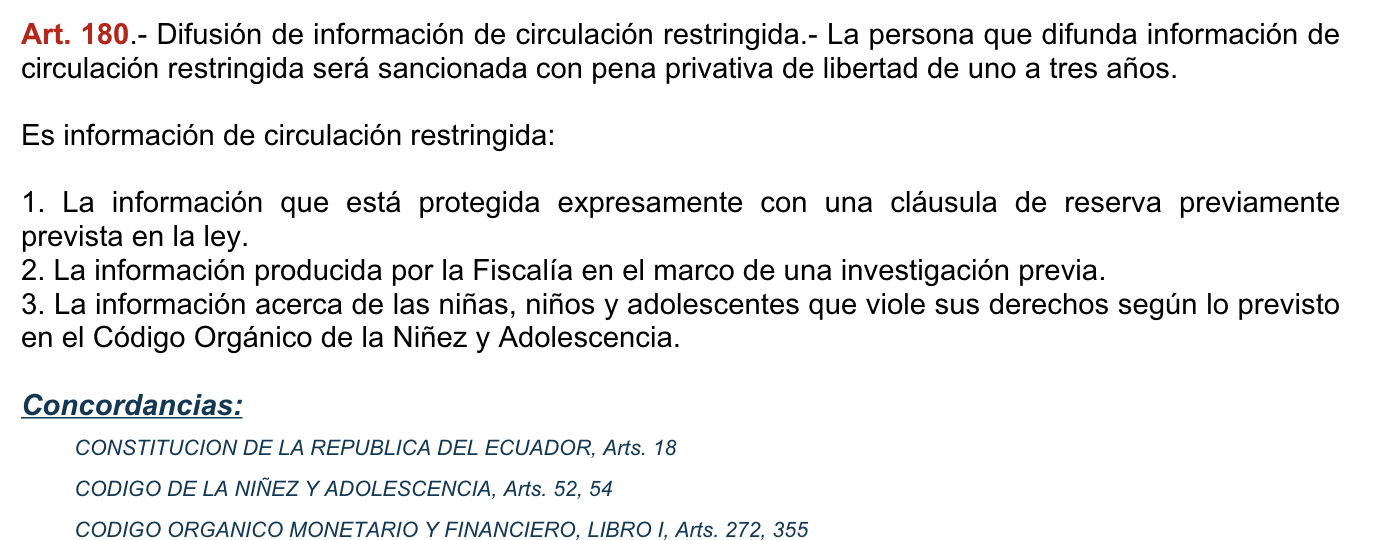


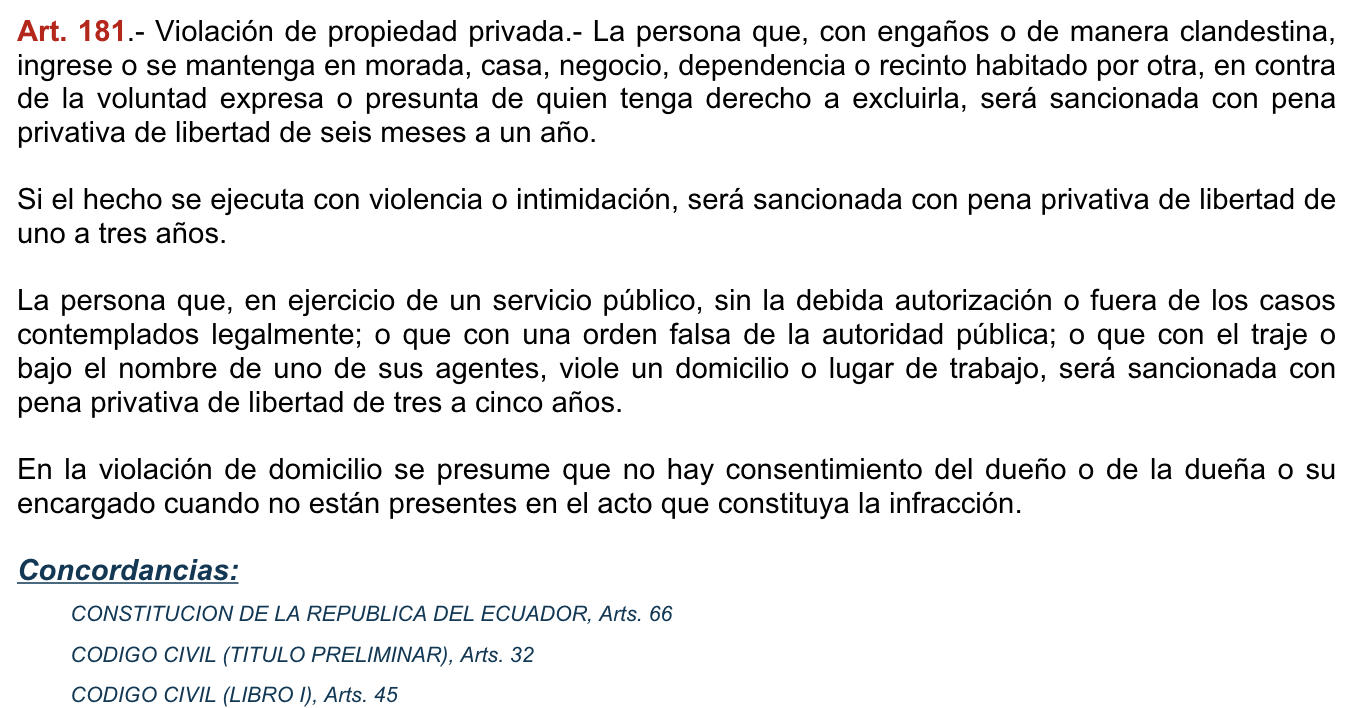


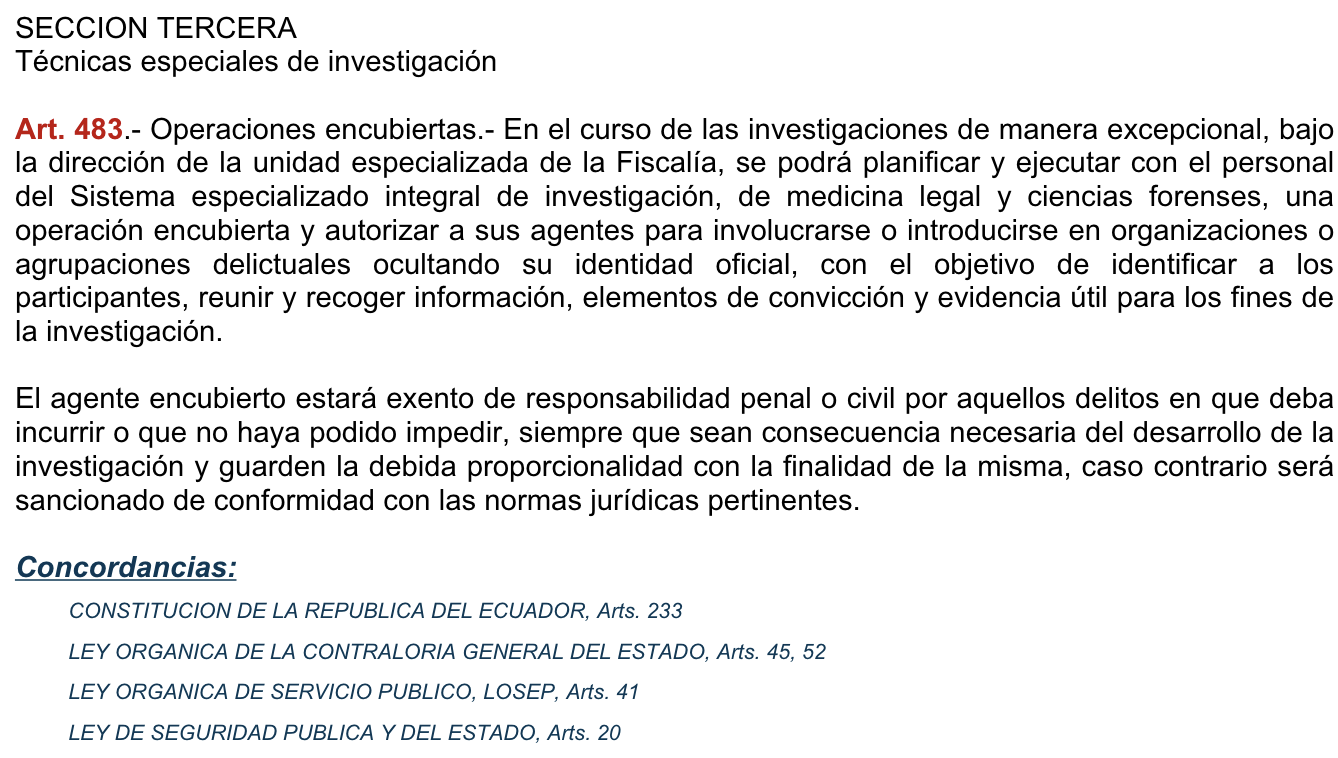
COIP:<https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf>











1. **Describe and summarize such articles, and provide their scope**

**Article 16:**

Ensures the right to free and inclusive communication, access to technology, and media diversity. It also promotes participation in communication spaces outlined in the Constitution.

**Scope**: Protects freedom of communication and access to information, ensuring inclusion and participation in public discourse.

**Article 66:**

Recognizes and ensures various aspects of personal integrity, including protection against violence in all spheres, prohibition of torture and forced disappearances, and safeguarding against inhumane treatment. It also establishes the right to personal data protection, privacy, and the confidentiality of physical and virtual correspondence, subject to lawful exceptions.

**Scope**: Safeguards personal integrity, privacy, and confidentiality, while setting standards for data protectionWhat kind of crimes or infractions can a person be judged for using those articles?

**Article 83:**

Outlines the duties and responsibilities of Ecuadorian citizens, with the understanding that additional responsibilities may be outlined in the Constitution and laws.

**Scope**: Defines the obligations and responsibilities of Ecuadorian citizens within the legal framework of the country.

COIP:

**Article 178** prohibits unauthorized access, interception, or dissemination of personal data and communications, punishable by one to three years of imprisonment. Article 179 addresses disclosing secrets and carries a penalty of six months to one year in prison.

**Article 180** deals with disseminating restricted information, punishable by one to three years in prison. These articles aim to protect privacy, prevent harm from disclosure of secrets, and restrict dissemination of sensitive information, particularly concerning children and adolescents.

**Article 181**: Prohibits unauthorized entry into inhabited premises, penalizing it with six months to one year imprisonment, escalating to one to three years if done with violence. Unauthorized entry by public servants carries a penalty of three to five years. The absence of the owner or their representative implies lack of consent.

**Article 483**: Allows for undercover operations by specialized units of the Public Prosecutor's Office to infiltrate criminal organizations. Agents are exempt from liability for offenses committed during investigations if necessary and proportionate to the investigation's purpose.

**Scope**: These articles establish legal provisions to protect privacy rights, prevent unauthorized entry into private property, and facilitate law enforcement through undercover operations. They aim to deter privacy violations, safeguard individuals' rights to security and privacy, and provide a framework for conducting covert operations while ensuring accountability and proportionality.

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

In general, individuals can be judged for a variety of crimes:

Violations of freedom of communication, access to technology, and media diversity, such as censorship, restriction of access to information, or interference with communication channels.

Offenses related to personal integrity, privacy, and confidentiality, including unauthorized access to personal data, interception of communications, dissemination of private information without consent, and violation of privacy rights in physical and virtual spaces.

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

Persecutors could use digital records like intercepted communications or digital footprints, witness testimony, surveillance footage, official documents, forensic analysis, expert testimony, and confessions to incriminate someone with crimes related to communication rights, personal integrity, privacy, and citizen responsibilities.

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

**Case:**

Ola Bini, a Swedish software developer and privacy advocate, was arrested in Ecuador in April 2019, accused of involvement in a plot to destabilize the government. He was initially accused of hacking into Ecuadorian government computer systems, a charge he vehemently denied. Bini's arrest sparked international attention, with many human rights and digital privacy organizations advocating for his release and expressing concerns about the fairness of the legal proceedings.

Bini and his supporters vehemently denied these accusations, asserting that his arrest was politically motivated and lacked substantial evidence.

**Accused of:**

Ola Bini was accused of alleged involvement in cyber-related criminal activities, including hacking, unauthorized access to computer systems, and association with WikiLeaks. he was detained on suspicion of being involved in a purported plot to destabilize the Ecuadorian government.

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

The case of Ola Bini seems to show that cybercrime laws are being used for political reasons. There isn't much clear evidence, and it seems like he was arrested more because of his friendships than for actually doing something wrong. This raises doubts about justice and the protection of digital rights in Ecuador.

1. **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?**

Applications like WhatsApp and TikTok align their terms of service with Ecuador's Organic Law on Personal Data Protection (LOPD). The LOPD guarantees Ecuadorian citizens rights regarding their personal data, including consent for data collection, control over information, and limitations on data transfer. It also imposes obligations on companies to ensure data security and confidentiality, with penalties for non-compliance. Therefore, these apps' terms of service are designed to comply with LOPD provisions, protecting Ecuadorian users' privacy rights.