Homework 4 Cybersecurity

- Sebastián Navarro 00321588
- Eduardo Guerrero 00326712
- Mateo Pozo 00320780

1. **Cite the articles of the constitution and COIP that address the topic of information security and information privacy**
2. **Describe and summarize such articles, and provide their scope**
3. **What kind of crimes or infractions can a person be judged for using those articles?**

Ecuador Constitution

Art. 66.- Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
20. El derecho a la intimidad personal y familiar.
21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

Description and scope:

Paragraph 19 of Article 66 describes the right that guarantees every person control over their personal data, including access to and the decision on how it is used. It is established that the collection, storage, processing, and distribution of this data can only be carried out with the consent of the data subject or under a legal mandate. This right protects individuals from unauthorized use of their personal information, meaning that any public or private entity that wishes to handle this data must have the explicit authorization of the affected person, unless there is a law justifying the processing of such data. Additionally, it ensures that personal data is handled responsibly and securely to prevent breaches of privacy.

Paragraph 20 of Article 66 describes the right to privacy, which protects individuals from unjustified intrusion into their private and family life, ensuring that their personal and family activities are not exposed. This right protects against undue interference from both public and private entities, and establishes a limit on access to sensitive or private information.

Paragraph 21 of Article 66 describes the right aimed at protecting the confidentiality of communications, whether through any communication medium, such as calls or electronic messages. Only in cases permitted by law, and with judicial authorization, can such communication be accessed. Therefore, any attempt to intercept or access private communications must be legally justified and authorized by a judge. Even in these cases, only matters related to the specific cause will be investigated, protecting any irrelevant information to the case and ensuring the confidentiality of the communication.

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

Description and scope:

Article 92 describes the right that every person has to know the existence of documents or files containing personal information about themselves or their assets, whether in public or private entities. Additionally, it guarantees the right to know how this data is used, its purpose, origin, destination, and the retention period in the files. This right gives individuals the ability to oversee and verify the handling of their personal information in all entities that hold it. Therefore, any individual can request information about what data has been recorded, why, where it comes from, where it is sent, and how long it will be kept, in order to promote transparency in the management of personal data.

Ecuador COIP

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.

Description and scope:

This article penalizes the access, interception, recording, dissemination, or publication of personal data and private communications without the consent of the data subject or legal authorization. In this way, it protects individuals' privacy by prohibiting any form of intrusion into their data or communications without valid permission. This includes both digital and physical means, ensuring that correspondence, personal data, and communications are respected.

Types of crimes or related infractions:

- Entering without permission into databases, electronic devices, or any medium containing private information.
- Listening to, recording, or capturing private communications (such as phone calls, emails, text messages) without the owner's authorization or a court order.
- Storing, retaining, or refusing to return personal data or confidential information that does not belong to the individual without the owner's consent.
- Sharing, reproducing, or disclosing private information, audio or video recordings, or any confidential communication without permission, causing an invasion of privacy.

Art. 179.- Revelación de secreto o información personal de terceros.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación cause daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año. No habrá delito en aquellos casos en que el secreto divulgado verse sobre asuntos de interés público.

Será sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenido digital, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad.

Description and scope:

The article penalizes the unauthorized disclosure of secrets or private information that may cause harm to another person. This improper disclosure can be committed by individuals who, due to their position, profession, or trade, have access to such information. This article protects the confidentiality of information obtained by individuals such as doctors, lawyers, and public officials who have access to sensitive information due to their position, ensuring that the information remains confidential unless the disclosed information is related to matters of public interest. Additionally, it specifies that in specific cases of unauthorized disclosure of messages, images, videos, and other sexual content, the penalty is more severe, reflecting the potential harm it may cause to the private life of the affected individual.

Types of crimes or related infractions:

- When a person, in the exercise of their profession, position, or trade, discloses confidential information that could cause harm to another person, unless it is of public interest, they are sanctioned with a prison sentence of six months to one year.
- The unauthorized disclosure of digital content such as messages, emails, images, audios, videos, especially if they are of a sexual nature. In these cases, the penalty is more severe, with a prison sentence of one to three years.

Art. 186.- Estafa.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.

Description and scope:

This article penalizes the act of obtaining an economic benefit for oneself or for third parties through the simulation of false facts or manipulation of information that distorts or hides the truth to induce the victim into making a mistake that results in economic harm. In this way, the law seeks to protect property and trust in commercial and financial transactions, severely punishing deliberate deception.

Types of crimes or related infractions:

- Use of altered, cloned, duplicated, stolen, or otherwise obtained bank cards without the legitimate consent of the owner.
- Use of devices to alter, modify, clone, or duplicate the originals of an ATM, with the intention of capturing bank card information.
- Providing false certificates about operations or investments made by a legal entity.
- Use of fraudulent practices to influence the buying or selling of securities in the public market.
- Conducting false financial transactions to create the appearance of an economic or financial situation that does not reflect reality.

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. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Description and scope:

This article penalizes the unauthorized disclosure of information contained in files, records, or databases stored or directed in computer systems, to prevent the violation of individuals' privacy for personal gain. The law protects the confidentiality and privacy of digitally stored information, ensuring that individuals cannot disclose sensitive data without authorization. It aims to prevent unauthorized access to databases containing private information, thereby prohibiting its unauthorized use.

Types of crimes or related infractions:

- When a person intentionally discloses information contained in files or databases, violating the confidentiality of individuals and taking advantage of the obtained information. The penalty for this crime is one to three years in prison.
- When the crime is committed by public officials, bank employees, or individuals working in financial institutions of the popular and solidarity economy, the penalty is aggravated to three to five years in prison.

Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.
2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.
3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.
4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Description and scope:

The article penalizes the unauthorized interception of data and the development, distribution, or use of tools intended to commit fraud or computer manipulation, from intercepting data transmissions to altering computer systems with the intent to deceive or redirect information, including cloning electronic devices such as credit cards. In this way, the law protects the privacy of digital information, the integrity of computer systems, and the security of electronic transactions. Furthermore, it establishes clear penalties for those who compromise the confidentiality and security of data through interception or electronic manipulation methods.

Types of crimes or related infractions:

- When a person, without judicial authorization, intercepts, redirects, records, or observes digital content at its origin or destination, or accesses signals or data transmissions.

- Individuals who develop or send fake codes, certificates, links, or pop-ups that lead people to access sites different from the desired one, thus affecting trusted systems such as financial services or personal sites.
- The possession, sale, or distribution of programs or electronic devices that aim to compromise the security of computer systems, such as in cases of phishing or digital attacks.
- The copying, cloning, or commercialization of information contained in magnetic strips or chips of electronic payment devices.
- The manufacturing, distribution, or possession of devices or programs that enable the commission of computer fraud, such as card cloning or altering digital data.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Description and scope:

This article penalizes those who intentionally damage, alter, delete, or interfere with the operation of computer systems, electronic devices, or technological infrastructure necessary for managing information. Furthermore, it penalizes the development and distribution of malicious programs or devices intended to cause harm. The law protects the integrity, availability, and proper operation of computer systems and technological infrastructure that support both private activities and public services. It also establishes a legal framework aimed at maintaining digital security, protecting against malicious actions that could compromise the functioning of critical systems.

Types of crimes or related infractions:

- The destruction, alteration, deterioration, or total or partial deletion of data, or the creation of malfunction in computer systems, electronic devices, or technological infrastructures with the intent to disrupt the normal operation of a computer system, causing significant harm.
- The design, development, distribution, or use of malicious devices or programs such as computer viruses, trojans, or hacking tools.

Art. 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Description and scope:

This article penalizes the destruction or disabling of classified information, the improper obtaining of confidential information by public officials, and the unauthorized disclosure of sensitive data that could compromise state security. The rule seeks to maintain the security and confidentiality of classified state information, especially when its disclosure could have serious consequences for national security, thus preventing unauthorized access, improper manipulation, or destruction of sensitive documents.

Types of crimes or related infractions:

- The destruction or disabling of any type of classified information according to legal regulations. This type of crime affects the integrity and availability of protected data.
- Public officials who obtain classified information using electronic or computer means without proper authorization will be penalized.
- The most severe penalty applies to public officials who, while in legitimate custody of reserved information, disclose it without authorization, when such disclosure could severely compromise the security of the state.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

1. 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 sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.
2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Description and scope:

This article penalizes unauthorized access to computer systems, telematics, or telecommunications systems, whether partial or total. It also establishes penalties for those who illegally exploit access to these systems by modifying content, redirecting data or service traffic, or using resources without authorization. In this way, it seeks to prevent unauthorized access to technological systems, protecting both the ownership of computer systems and the data and services they manage. Additionally, it focuses on the exploitation of illegal access, ensuring that data and service traffic is not redirected or exploited fraudulently.

Types of crimes or related infractions:

- When a person accesses, either partially or fully, a computer system, telematics, or telecommunications system without the consent of the legitimate owner of the system. This includes unauthorized intrusion into networks, devices, or electronic platforms.
- When, after accessing without authorization, the person uses the gained access to modify a website, redirect data or voice traffic, or provide services without paying the legitimate service providers.

Art. 234.1.- Falsificación informática:

1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.
2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena.

Description and scope:

The article penalizes the manipulation of digital content with the intent to deceive the parties involved in legal relationships, either to cause harm or obtain illicit benefits. The falsification of digital content includes the alteration of documents or data, which can have serious consequences, such as the creation of false information or documents that appear legitimate. The article seeks to punish any action that alters digital data in order to cause deception, any action that illegitimately interferes with the processing of information, and the creation of counterfeit documents that, when presented in transactions or legal relationships, deceive the parties involved.

Types of crimes or related infractions:

- The person who, with the intent to deceive, alters or creates false digital documents to modify the processing of data. These acts may involve anything from altering simple files to creating false legal or financial documents to cause harm.
- The person who uses documents that have been falsified through the manipulation of digital content, such as invoices, contracts, or reports, with the intent to cause harm or obtain an illicit benefit.

Art. 234.2.- Agravación de las penas.- La práctica de los hechos que se describen en los artículos 232, 234 y 234.1 será sancionada con pena agravada en un tercio de su pena máxima si logra perturbar de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, como cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los servicios públicos.

Description and scope:

This article establishes the aggravation of penalties for the offenses described in Articles 232, 234, and 234.1 (Attack on the Integrity of Computer Systems, Unauthorized Access to Computer Systems, and Computer Forgery), specifying that if these offenses severely impact computer systems that support critical social functions, the corresponding penalties will be increased. The article specifically refers to the grave or lasting disruption of computer systems involved in the management of public services and critical functions that directly affect the safety, well-being, and economy of individuals, such as: computer systems related to the distribution of essential products, management in hospitals, clinics, and other healthcare centers, payment processing, transfers, and other services in financial and banking systems, and infrastructures that facilitate access to basic services.

Types of crimes or related infractions:

- When a computer system supporting critical social functions is seriously or durably disrupted. This includes, for example, a cyberattack that severely affects healthcare systems, security, or the operation of essential public services.
- If the damage to the computer system affects a function that is vital for public well-being, such as the supply of essential products, the management of public health emergencies, or the infrastructure of basic public services.

4. 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?

Constitution of Ecuador: Data Protection Rights

Article 66 of the Constitution of the Republic of Ecuador establishes fundamental guarantees for the protection of personal data, closely related to the right to privacy and respect for communication:

Clause 19:

- The right to the protection of personal data, including access to and decision over the collected information.
- The collection, storage, processing, or dissemination of such data requires the explicit authorization of the owner or a legal mandate.

Clause 20:

- Right to personal and family privacy, protecting individuals' private lives in their closest environment.

Clause 21:

- Right to the inviolability and secrecy of physical and virtual correspondence.
- Communications can only be examined in cases provided by law, with a judicial order, and with an obligation to respect unrelated content.

Organic Law on Data Protection (LOPDPP)

The LOPDPP, in force since 2021, reinforces these guarantees by setting specific requirements for handling personal data, requiring companies operating in Ecuador to adhere to high standards of transparency and protection.

Consent Requirements (Article 8)

The consent for data processing must be:

1. Free: Without coercion or flaws in consent.
2. Specific: Detailing the means and purposes of processing.
3. Informed: Providing clear and transparent information to the owner.
4. Unequivocal: Without doubts about the scope of the authorization.

Rights of Data Owners

Articles 14 through 19 of the LOPDPP grant citizens fundamental rights over their data:

1. Right to Rectification (Article 14): Modify inaccurate or incomplete data.
2. Right to Erasure (Article 15): Delete data when:
   - Processing is improper or unnecessary.
   - Data has fulfilled its purpose.
   - Consent has been revoked.
3. Right to Object (Article 16): Refuse processing in cases of direct marketing or unjustified legitimate interest.
4. Right to Data Portability (Article 17): Request data in compatible and transferable formats.
5. Right to Suspend Processing (Article 19): Temporarily restrict data use under specific conditions.

International Data Transfers (Article 57)

Transferring data outside Ecuador requires adequate guarantees, such as:

1. Compliance with protection standards equivalent to or higher than Ecuadorian laws.
2. Access to administrative or judicial remedies in case of violations.
3. Right to full reparation if privacy is infringed.

Applications like WhatsApp and TikTok Under Ecuadorian Law

Applications such as WhatsApp and TikTok operate globally but must adhere to Ecuador's specific privacy laws, which provide robust data protection rights under the Constitution of Ecuador and the Ley Orgánica de Protección de Datos Personales (LOPDP). Below is an evaluation of how their terms of service align with Ecuadorian legal standards:

WhatsApp

WhatsApp is known for its focus on secure communication, including end-to-end encryption, which aligns with Ecuador's guarantees for inviolability and secrecy of communication under Clause 21 of Article 66 in the Constitution. However, concerns arise in the following areas:

- Explicit Consent (LOPDP, Article 8): WhatsApp requires users to accept broad data collection practices, including metadata and information shared with its parent company, Meta. While users must accept these terms to use the app, the extent of their freedom to reject specific processing purposes is

limited. The sharing of user data with Meta for advertising or analytics may conflict with Ecuadorian requirements for specific and informed consent.

- Data Minimization and Purpose Limitation (LOPDP, Articles 6 and 8): Ecuadorian law mandates that personal data be collected only for specific, explicit, and lawful purposes. WhatsApp's policy of collecting a wide range of user data (e.g., device info, contacts) may exceed the purposes necessary for providing its messaging service.
- International Transfers (LOPDP, Article 57): WhatsApp processes and stores user data outside Ecuador, primarily in the U.S. This requires the company to ensure that equivalent data protection standards are in place, which may not always be transparent or verifiable under its current terms.

TikTok

TikTok, a social media platform with extensive data collection practices, presents unique challenges under Ecuadorian privacy laws:

- Explicit Consent and Transparency (LOPDP, Article 8): TikTok collects a wide range of data, including location, browsing behavior, and device information, often used for content personalization and targeted advertising. The platform's consent mechanisms may not clearly explain the purposes or scope of this processing, potentially failing to meet the unequivocal and informed consent standard required in Ecuador.
- Data Minimization and Specificity (LOPDP, Articles 6 and 8): The volume and types of data collected by TikTok might exceed what is necessary for its stated purposes, violating Ecuadorian requirements for data minimization and lawful purposes.
- International Transfers (LOPDP, Article 57): TikTok's potential transfer of data to jurisdictions like China raises questions about compliance with Ecuador's strict rules on adequate protection for international data transfers. The absence of detailed guarantees in its terms may conflict with the need for administrative or judicial remedies in case of privacy violations.

Protection for Citizens Under Ecuadorian Law

Ecuadorians have robust legal protection against privacy violations:

- They can demand information about how their data is used and request its correction or deletion.
- The law imposes administrative and criminal penalties for the misuse of personal data.
- Companies must respond to data owners within reasonable timeframes and avoid opaque practices.

References:

Constitución de la República del Ecuador. (2008). Constitución de la República del Ecuador. Recuperado de https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-CONSTITUCION_DE_LA_REPUBLICA_DEL_ECUADOR

Código Orgánico Integral Penal (COIP). (2014). Código Orgánico Integral Penal. Recuperado de https://app.lexis.com.ec/sistema/visualizador-norma/PENAL-CODIGO_ORGANICO_INTEGRAL_PENAL_COIP

Ley Orgánica de Protección de Datos Personales. (2021). Ley Orgánica de Protección de Datos Personales. Recuperado de https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-LEY_ORGANICA_DE_PROTECCION_DE_DATOS_PERSONALES