PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE JURISPRUDENCIA

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO AL TÍTULO DE ABOGADO

TÍTULO: FILTRACIÓN DE DATOS PERSONALES Y RESPONSABILIDAD PENAL: CASO NOVAESTRAT

NOMBRE: PAULA ALEJANDRA ROMO HIDALGO
DIRECTOR: DR. SANTIAGO ACURIO DEL PINO

Quito, D.M 2023

TABLA DE CONTENIDOS

Resumen:

En el presente proyecto de integración curricular se detalló el fenómeno de la filtración de datos personales, sus causas, consecuencias y conceptualización, para posteriormente, desarrollar los principales mecanismos de protección de datos personales que podrían lidiar con dicho fenómeno y proponer algunos adicionales.

El data breach o filtración de datos personales tuvo lugar en Ecuador con el famoso caso Novaestrat, este al ser un caso de gran magnitud e impacto se analizó la posibilidad de responsabilidad penal por los delitos relacionados a los hechos del caso que son la violación a la intimidad y revelación ilegal de bases de datos en base a ciertos elementos de la teoría del delito.

Palabras clave:

Filtración de datos, protección de datos personales, mecanismos de protección de datos personales, responsabilidad penal, teoría del delito.

Abstract:

In this curricular integration project, the phenomenon of personal data breach, its causes, consequences, and conceptualization were detailed, to later develop the main personal data protection mechanisms that could deal with this phenomenon and propose some additional ones.

The breach of data or leak of personal data took place in Ecuador with the famous Novaestrat case, this being a case of great magnitude and impact, the possibility of criminal responsibility was analyzed for the crimes related to the facts of the case that are the violation of privacy and illegal disclosure of databases based on the elements of the theory of crime.

Key Words:

Data leak, personal data protection, personal data protection mechanisms, criminal liability, theory of crime.

1. Introducción

Para que situaciones como el fenómeno de filtración de datos personales o data breach, se puedan prevenir, proteger, tratar y sancionar, se necesita de una convergencia o unión entre herramientas jurídicas y prácticas. Es decir, de un sistema integral de protección de datos personales. El derecho de protección de datos personales, recogido en el Art.66 numeral 19 de la Constitución ecuatoriana, tan solo ha constituido el peldaño de inicio para el desarrollo paulatino de diversos mecanismos legales. Publicándose recién el 26 de mayo del 2021 la primera Ley de Protección de Datos Personales en el Registro Oficial, acción impulsada por el expresidente Lenin Moreno.

La articulación de todo un sistema eficaz y propicio de protección de datos personales solo se materializa cuando se cumplen al menos ciertos elementos, como el desarrollo de una normativa que garantice su ejercicio, la existencia de una autoridad independiente reguladora la existencia de normas especializadas en protección de los datos (Serrano,2020), implementación de medidas técnicas u organizativas. Actualmente se cumple con únicamente el tercer elemento de esta descripción, siendo per se la existencia de la Ley de Protección de Datos Personales, mientras que los demás elementos aún faltan desarrollo.

Por otro lado, la emergente crisis tecnológica ha generado diversas discusiones frente a las acciones que se podrían tomar para hacer frente a las masivas filtraciones de los datos personales que se dan en el sector empresarial a nivel mundial. Decía Carl Sagan (1994) "vivimos en una sociedad profundamente dependiente de la ciencia y la tecnología y en la que casi nadie sabe nada de estos temas. Ello constituye una fórmula segura para el desastre" (p.1), Dicha afirmación refleja lo sucedido en nuestro país, año 2019, con el famoso caso Novaestrat, la mayor filtración de datos personales en la historia ecuatoriana, del cual únicamente se ha iniciado la investigación previa por parte de Fiscalía y ninguna respuesta adicional.

Gran parte de los ecuatorianos, se encuentran en grave peligro por el mal uso que terceros podrían hacer de sus datos. En este contexto surgen diversas incógnitas como el desarrollo de mecanismos jurídicos eficientes, soluciones que permitan garantizar los derechos y libertades de las personas y la posibilidad de responsabilidad penal en torno al caso Novaestrat.

1.1 Marco conceptual

En este apartado se elabora una revisión bibliográfica, con citas textuales de los conceptos generales a partir de los cuales se sustenta el análisis del tema del presente proyecto de investigación. Los conceptos considerar son el data breach o filtración de datos, los datos personales, los principios de protección en materia de datos personales, la responsabilidad penal y la teoría del delito. Finalizando con los antecedentes teóricos del problema. Dicha información permitirá analizar e interpretar tanto el fenómeno del data breach, los mecanismos de protección y la posibilidad de que se produzca responsabilidad penal en el caso Novaestrat.

Data breach o filtración de datos

Desde el punto de vista de la ciberseguridad, el Data Breach, también conocida como Data Leakage o filtración de datos es la exposición intencional o no intencional de información a terceros (Cheng, Liu, Danfeng, 2017). Dicha circunstancia se produce, según la Comisión Europea (2019), "cuando la información de la que es responsable una organización se ve afectada por un incidente de seguridad que resulta en la infracción de un acuerdo de confidencialidad, disponibilidad o integridad" (p.1).

> Las filtraciones de datos provocan una filtración de información, que es una de las principales ciberamenazas, afectando a una amplia variedad de información comprometida que va desde datos de identificación de carácter personal, datos financieros almacenados en infraestructuras informáticas, hasta datos médicos personales que se guardan en bases de datos. (ENISA, 2020, p.2)

Datos personales

Desde un punto de vista jurídico su conceptualización se ve reflejada por organismos internacionales, así como por la nueva Ley de Protección de Datos personales en el Ecuador.

Concretamente, los datos personales, se definen como: "dato que identifica o hace identificable a una persona natural, directa o indirectamente" (LOPDP, 2021, art.3). Los datos personales incluyen "áreas bastante ampliadas, no solo son los datos personales el nombre, fecha de nacimiento, número verificador o información de contacto, sino también lo son las creencias, opiniones políticas, datos biométricos o genéticos, localización, orientación sexual e incluso actividades laborales, etc." (Catalán, 2022, p.47).

Principios principales de protección de datos

El Comité Jurídico de la a Organización de Estados Americanos, ha desarrollado una serie de principios y conceptos sobre la protección de datos personales que por precepto de convencionalidad son de aplicación directa. Entre los principales, se encuentran los de

seguridad de los datos, los datos personales sensibles, la responsabilidad, el encargado de protección de datos y las autoridades de protección de datos.

Con respecto al principio de seguridad de los datos, se menciona que, los responsables de los Datos:

Deberían establecer y mantener las medidas de carácter administrativo y técnico que sean necesarias para establecer salvaguardias de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los Datos Personales que obren en su poder o bajo su custodia (o de los cuales sean responsables) y cerciorarse de que tales Datos Personales no sean tratados ni divulgados excepto con el consentimiento de la persona o de otra autoridad legítima, ni sean accidentalmente perdidos, destruidos o dañados. (CJI, 2021, p.25)

Este principio nace por el incremento de ataques o intrusiones externas, incluyendo cualquier daño incluso si este es accidental, en todos estos casos "los responsables de los datos deberían notificar a las personas cuyos datos hayan sido (o puedan haber sido) comprometidos, así como a las autoridades penales o civiles relevantes" (CJI,2021, p.25).

Adicionalmente el mismo comité se refiere a los datos personales sensibles, como:

Una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Por ejemplo, datos relacionados con la salud personal, las preferencias o vida sexuales, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños o geolocalización persona (CJI, 2021, p.13).

Los responsables del tratamiento de datos son: "la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización o servicio que (solo o junto con otros) se encarga del Tratamiento y la protección de los Datos Personales en cuestión" (CJI,2021, p.13) . Estos responsables deben proteger los derechos de los titulares al adoptar e implementar medidas técnicas y organizacionales para asegurar y demostrar que el tratamiento se de en concordancia con los principios de protección de datos. Además, deberían asumir la responsabilidad de asegurar que sus requisitos sean observados por terceros a quienes se comuniquen los Datos Personales. Tomando en cuenta la diferenciación con los encargados de

los datos que únicamente prestan sus servicios para llevar a cabo el tratamiento de datos (CJI, 2021, p.36,13).

Con respecto a las autoridades responsables de la protección de datos, se hace una recomendación a los Estados Miembros para que establezcan autoridades supervisoras y órganos independientes que controlen y promuevan la protección de datos personales, es así que el Comité Jurídico Internacional de la OEA indica que la: "legislación nacional de cada Estado debería dotar a dichas autoridades de la capacidad de cooperar internacionalmente entre sí, así como con las autoridades e instituciones públicas y privadas relevantes incluyendo las relacionadas al ámbito penal, financiero, del consumidor, entre otras" (CJI, 2022, p.12,44).

Responsabilidad penal con base a la teoría del delito

La responsabilidad penal alude, según el catedrático Ricardo Vaca al:

> deber social y legal que incumbe al individuo de dar cuenta de lo hecho y de sufrir las consecuencias jurídicas. Es responsable el que acusa de la ejecución de un hecho punible, debe responder por él, ante la sociedad perjudicada. En teoría, ninguna persona puede cometer delitos y pretender luego no responder por lo que hizo. (Vaca, 2005, p.1).

Se deben tomar como base los elementos de la teoría del delito ya que estos permiten determinar la posibilidad de responsabilidad penal, en concordancia, se argumenta:

> el efecto jurídico que se produce cuando concurren todos los requisitos y presupuestos necesarios para hacer a una persona merecedora de sanción, entre los que ha de contarse no sólo el delito mismo, sino también el cumplimiento de las condiciones objetivas de punibilidad y la ausencia de excusas legales absolutorias…compartimos plenamente la opinión de la doctrina en cuanto a que en nuestro país la responsabilidad penal es· el efecto jurídico del delito y no uno de sus elementos. (Fuente, 1989, pp.118-121)

1.2 Antecedentes teóricos

Este apartado presenta un recorrido por ciertas investigaciones que han abordado aspectos del tema de integración curricular desde diversas perspectivas.

La óptica jurídica menciona que el primer paso para prevenir la filtración de datos es la protección de datos personales, ya que de lo contrario tanto personas físicas como jurídicas pueden ser víctimas de la ciberdelincuencia informática. Es así como la Oficina de las Naciones Unidas contra la Droga y el Delito señala que:

> los datos también desempeñan un papel importante en la comisión de muchos delitos cibernéticos, principalmente porque no están protegidos de manera adecuada y se puede acceder a ellos y obtenerlos ilícitamente. Las filtraciones de datos son el resultado de memorias portátiles encriptadas y otros dispositivos de almacenamiento extraviados o robados, una seguridad de sistema y datos deficiente, el acceso no autorizado a una base de datos o el exceso de acceso no autorizado a una base de datos y la divulgación, lanzamiento o publicación accidental de datos (UNODC, 2020, p.2).

Muchas de las conductas delictivas tienden a la utilización de datos personales sin cumplir la normativa de protección de datos. Usualmente se tratan de delitos que castigan el "acceso ilícito a los sistemas informáticos, la permanencia y la interceptación de transmisiones no públicas de datos informáticos, conductas de sabotaje tendentes a la destrucción o deterioro de los datos y programas informáticos; obstaculización del funcionamiento de un sistema informático" (Llul y Blanc, 2018, p.9).

Las conductas penalmente relevantes derivadas de la filtración de datos personales deben considerarse a partir de la interdependencia de la informática y el derecho, siendo menester "determinar si los mismos están ya incorporados a la tipología jurídico penal y en caso negativo proceder a su correspondiente análisis para llevar a cabo su inclusión en el Código penal" (Ruíz, 1996, p.447).

Para proteger los datos personales de posibles abusos y hacer frente a los retos que suponen las nuevas tecnologías más allá de las leyes de protección de datos personales y su reconocimiento a nivel constitucional, se ha redactado el Convenio 108 plus de como un instrumento jurídico internacional vinculante de armonización y convergencia normativa, del cual en Latinoamérica únicamente se han suscrito México, Uruguay y Argentina.

"los países de América Latina están cada vez más implicados en la protección de datos personales y muchos de ellos se dirigen al Consejo de Europa para acceder a su Convenio y participar en sus trabajos o para buscar ayuda en el desarrollo de sus marcos jurídicos en ese importante ámbito". (Consejo de Europa, 2021)

Desde una perspectiva digital, los datos se encuentran registrados en soportes, ficheros o sistemas informáticos complejos. La filtración sucede por incidentes intencionales y no intencionales. Según un informe de Verizon (2022), que involucra el estudio y análisis de las filtraciones de datos a nivel mundial, se han producido del 2008 al 2022 más de 234.638 fugas de datos, sucediendo la mayoría por ataques externos. Adicionalmente y en consonancia con

otros estudios, se dio a conocer que los socios comerciales estuvieron involucrados en el 39 por ciento de las violaciones de datos.

En términos económicos, el International Business Machine Corporation señala que el promedio de costos de una filtración de datos personales "aumentó en USD 0,11 millones a USD 4,35 millones en 2022, el más alto en la historia de este informe" (IBM, 2022, p.9). Más allá de perjuicios jurídicos se generan impacto dentro la economía nacional.

1.3 Identificación del problema

El avance de la tecnología es indetenible, cada día se presentan nuevos retos a nivel jurídico y práctico, por lo que se debe hacer frente a las amenazas que pongan en riesgo o lesionen derechos de las personas. Pero para que un derecho se vea garantizado, no basta únicamente con la emisión de una ley, sino de la configuración de un sistema articulado de protección.

Los datos personales, especialmente, se ven en constante riesgo de sufrir el creciente y perjudicial fenómeno cibernético conocido como Data Breach o filtración de datos. Este se produce debido a que los datos personales, registrados y almacenados, por lo general en plataformas digitales, son susceptibles de ataques e incluso de exposiciones accidentales. A nivel mundial se producen cada vez más filtraciones de datos personales, entre los casos más famosos de encuentran el Data Breach de Yahoo donde se filtraron más de tres billones de cuentas, al igual que en el caso de la red social Facebook con quinientos cuarenta millones de datos y Quora con datos de cien mil millones de personas.

Esto genera consecuencias devastadoras para los titulares de los datos como extorsiones, phishing, fraudes informáticos, suplantación de identidad, secuestros extorsivos, entre otros. Esta situación realmente preocupante obliga a que se desarrollen mecanismos de protección de datos personales que permitan lidiar con las filtraciones de datos.

Es lamentable, pero en Ecuador se produjo la mayor filtración histórica de datos personales, un poco más de diecisiete millones de datos. Esta situación fue conocida como el caso Novaestrat, del cual únicamente se realizó una investigación previa por el delito de violación a la intimidad en Fiscalía y no se ha resuelto nada más hasta el momento. Sería inconcebible que este caso quedare en la impunidad por lo que es necesarísimo analizar la posibilidad de responsabilidad penal en los delitos que se ajusten a la conducta.

1.3.1 Pregunta General de Investigación y objetivos

¿Existen mecanismos extrapenales suficientes en el caso de un data breach para garantizar la protección de datos personales?, ¿La filtración de datos personales en el caso Novaestrat, genera responsabilidad penal frente al delito de violación de la intimidad y revelación ilegal de base de datos?

Los objetivos de esta investigación son:

a) Determinar la existencia de mecanismos suficientes de protección de datos personales en el caso de un data breach.
b) Analizar la posibilidad de responsabilidad penal *en* relación con el delito de intimidad y revelación ilegal de bases de datos en el caso Novaestrat.

Los cuales se desarrollarán en el tema 1 y 2 de este proyecto de integración curricular.

2. Tema 1. Filtración de datos personales y mecanismos extrapenales de protección de datos personales

2.1 Evolución histórica del data breach

El tema tiene sus orígenes en la necesidad humana de registrar la información de otros y de agruparla. Para que existan filtraciones, los datos deben encontrarse almacenados en un espacio físico o digital, conocido como archivo o en dispositivos de almacenamiento respectivamente.

El archivo de datos registrados más antiguo se encontró en Ebla, al oeste de Siria, aproximadamente en el año 3500 a.C, al respecto señalan los historiadores Sagredo y Nuño (1994) que el descubrimiento de Ebla y de su archivo real, fue uno de los más importantes ya que se encontraron multitud de registros íntegros, así como fragmentos textuales casi que incluían información personal. Miles de años pasaron, en los que se siguieron registrando y agrupando datos en lugares como librerías, oficinas gubernamentales, hospitales, empresas, entre otros centros de almacenamiento físico.

Sin embargo, cada vez seguía incrementándose la necesidad de agrupar datos y los espacios físicos resultaban ser ineficaces. Por ende, se produjo uno de los primeros avances en la reducción espacial de los datos, con el uso de cintas magnéticas o casetes y más tarde con el almacenamiento digital en Cd o discos compactos. No es sino hasta el boom de la tecnología computacional en los años sesenta, que fue acuñado por primera vez el término base de datos en un simposio en California, 1963, en el cual se definió a la base de datos como “un conjunto de datos

relacionados que se encuentran agrupados o estructurados en registros y almacenados en un ordenador" (Salcedo, Cardona y Gutiérrez 2018, p.95).

Con el desarrollo de estos espacios de almacenamiento y el uso de las computadoras, se empezaron a recopilar datos a gran escala por parte de empresas estatales y privadas, lo que despertó el interés en los ciberdelincuentes que buscaban beneficiarse económicamente. Ocurriendo en el año 2005 la primera filtración de datos en Estados Unidos, en la cual se filtraron 1.4 millones de cuentas bancarias que incluían números de tarjeta de crédito, el caso de DSW Shoe Warehouse.

2.2 Causas y consecuencias de la filtración de datos personales

La filtración, exposición, data breach de datos personales se pueden producir por dos tipos de incidentes, los primeros son intencionales, se generan por malwares, hacking, virus, troyanos o ingeniería social, ciertas personas que no están autorizadas acceden a los sistemas de almacenamiento de datos e incluso eliminan, modifican o alteran la información personal (Identity Theft, 2022). Los segundos incidentes son inintencionales y se dan por publicaciones accidentales, errores en la configuración, encriptación impropia o pérdida del computador.

Una vez que los datos han sido expuestos , según (Pérez, 2015) "constituyen un bien altamente valorado no solo por las instituciones públicas o privadas que operan legalmente, sino también por los ciberdelincuentes, quienes los usan como insumos para materializar […]delitos cibernéticos" citado por (Rosas y Pila, 2023,p.3) .Es decir se generan diversos tipos de conductas por partes de los cibercriminales, los cuales buscan obtener beneficios económicos a través de la venta ilegal de bases de datos en plataformas como la Dark Web .

Específicamente en la Dark Web se cotizan datos desde los cincuenta centavos, entre los más económicos están los códigos postales o direcciones domiciliarias. También se promocionan cuentas con credenciales de Pay Pal, Facebook, eBay e Instagram con precios mayores, entre quinientos y mil dólares. Es común la oferta de cédulas de identidad, pasaportes, datos financieros, información médica, datos de tarjetas de crédito como Visa, MasterCard y American Express, cuyos precios redondean los veinticinco dólares americanos, incluyendo fechas de nacimiento credenciales de bancos y nombres completos.

El mercado de la venta ilegal de bases de datos cada vez se incrementa más en Ecuador, el negocio de vender datos es incluso más lucrativo que la venta de droga, y no es necesario que

se vendan únicamente en la Dark Web ya que realizando una búsqueda en Google se pueden encontrar bases de datos en plataformas comunes como Mercado Libre o Marketplace.

2.3 Mecanismos extrapenales de protección de datos personales

Los datos merecen de protección desde al ámbito jurídico, es por ello por lo que se procede a analizar los mecanismos extrapenales de protección de datos personales que se han desarrollado para determinar si podrían ser suficientes en caso de un Data Breach.

2.3.1 Protección de datos personales a través de la Ley Orgánica de Protección de Datos Personales

Ecuador a partir del año 2008, incorpora en el art. 66 numeral 19, capítulo de derechos de libertad, el derecho a la protección de datos personales, el cual:

> 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 (Constitución, 2008, art.66).

La protección mencionada en el referido artículo es de "los datos de carácter personal". Para entender cómo funciona la LOPDP como mecanismo de protección, es necesario entender, en primer lugar, que es un dato personal. Este es aquel "dato que identifica o hace identificable a una persona natural, directa o indirectamente" (LOPDP, 2021, art.4), cuando se menciona que identifica a una persona, quiere decir que se distingue a una persona de otras por sus características individuales, y cuando señala que hace identificable significa que el dato podría llegar a identificar a una persona, es decir permite la posibilidad de identificarla en un futuro. De forma directa es que permite la posibilidad de identificarla por sus nombres y apellidos mientras que de forma indirecta significa que la persona puede ser identificada por "un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos edad, empleo, domicilio etc." (Grupo 6,2007, p.14).

Cabe mencionar que hay otros tipos de datos que no entran en el ámbito de protección de dicha esta ley. El dato no personal será aquel que no identifique o haga identificable a una persona natural. Los datos no personales son los metadatos, que, de forma singular, están presentes en diversas actividades, por ejemplo:

> Al sacar una fotografía (hora y fecha de la fotografía, lugar, tamaño de imagen, resolución y dimensiones, etc.), al publicar un tweet en Twitter (hora y fecha del tweet, lugar, cantidad de caracteres, etc.), al enviar un correo electrónico (hora y fecha, destinatario, etc.), al enviar un mensaje en WhatsApp, el buscador utilizado, etc. (Polo, 2021 p.15).

Los datos, metafóricamente, son bloques que brindan o construyen la información, la información es un todo o universo y los datos uno de sus conjuntos, el dato por sí solo tiene protección, ya que de ellos se obtiene información.

A los datos personales se los puede clasificar dependiendo de la legislación del país, de acuerdo con la Ley de Protección de Datos Personales del Ecuador se los puede dividir en dos grandes grupos, los primeros son los datos personales, de forma general y los datos personales sensibles que son datos que indican:

> etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. (LOPDP, 2021, art.4).

Una vez entendidos los datos que se pueden filtrar, es necesario señalar que las filtraciones de datos personales que implican incidentes están en riesgo, por un posible "acceso ilegítimo a los datos personales o riesgos para la confidencialidad, por una modificación no autorizada de los datos, o riesgos para la integridad, e incluso la eliminación no autorizada de datos o riesgos para la disponibilidad" (Atico34, 2022, p.8). Se entiende como confidencialidad que a los datos personales solo pueden acceder personas o sistemas autorizados; por integridad que existe garantía de que no existirá modificación o daño respecto a los datos; y por disponibilidad sé que estos se mantengan disponibles. Sin embargo, estos elementos se protegen a través de la LOPDP, ya que uno de sus objetivos primordiales salvaguardar a través de los denominados responsables o encargados.

Para entender los alcances del responsable o encargado del tratamiento de los datos, es importante saber que tanto personas jurídicas públicas o privadas, sí como personas naturales, recopilan datos personales con objetivos de registro, para su posterior análisis, publicidad o investigación.

Dichas entidades e individuos pueden cumplir dos papeles de acuerdo con la LOPDP. El primer rol llamado "responsable de los datos personales", como su nombre lo dice se responsabiliza por los datos, tomando decisiones respecto al medio a través del cual se tratarán

los datos y determinando los fines por las cuales se los tratará. En palabras sencillas el responsable de los datos decide el "porqué y cómo deberán tratarse los datos personales" (Comisión Europea, s.f, p.1). Mientras que el segundo rol lo cumple el "encargado del tratamiento de datos personales" el cual presta un servicio para el tratamiento de los datos mediante un acuerdo con el "responsable de los datos personales" a través de un acto jurídico como un contrato.

Por consiguiente la Ley Orgánica de Protección de Datos Personales indica que los responsables o encargados del tratamientos de los datos personales identifiquen estos riesgos e implementen principalmente: medidas técnicas y organizativas que permitan que los datos estén seguros así como la respectiva notificación cuando ha ocurrido vulneraciones (incidentes) respecto de los datos personales .De esta forma se prevendría el data breach y en el caso de que llegara a suceder se realizaría la notificación al titular de los datos.

2.3.1.1 Medidas técnicas y organizativas derivadas de la Ley Orgánica de Protección de Datos Personales

La implementación de estas medidas realmente puede evitar incidentes que deriven en una filtración de datos personales. Para que esto sucede es realmente importante, realizar un análisis de riesgos, el cual es un estudio de los escenarios imprevistos, que palabras sencillas implica un "qué hacer en el caso probable de una pérdida", por ejemplo ¿qué hacer en caso de pérdida del sistema del almacenamiento por ataques informáticos?, en casos de cesión de datos, cuando se almacenan los datos en nubes, en casos de filtración, entre otros; implica el desarrollo de una metodología de análisis respecto a la clasificación de los datos, de los sujetos a quienes está dirigido el tratamiento de datos y los fines para los cuales se utilizarán.

Dependiendo del análisis efectuado por parte del responsable y encargado de tratamiento de datos personales, se podrían establecer diversas medidas técnicas. Al respecto y para evitar las filtraciones de datos se sugieren las siguientes:

a) Data masking

Una herramienta poderosa contra la filtración de datos personales es hacer que cualquier información robada sea inutilizable para el atacante. El data masking permite a los usuarios realizar tareas en datos con formato funcional basados en datos auténticos, todo sin requerir o exponer los datos reales. Las técnicas de enmascaramiento de datos incluyen el cifrado, la combinación aleatoria de caracteres y la sustitución de caracteres o palabras. Una de las

técnicas más populares es la tokenización, que sustituye los valores reales con datos ficticios completamente funcionales

b) Encriptación de datos

Si se utiliza un algoritmo criptográfico y claves secretas para garantizar que solo las entidades previstas puedan leer los datos. El cifrado se utiliza para los datos almacenados en una unidad, dentro de una aplicación o en tránsito. Está ampliamente disponible en sistemas operativos, aplicaciones y plataformas en la nube, así como en programas de software independientes. Si l**os** atacantes acceden a los datos cifrados, no se pueden leer y, por lo tanto, los atacantes no obtienen ningún valor de los datos.

c)Softwares de prevención de filtración de datos

Se pueden usar como instrumentos que automatizan el seguimiento de datos, usan regalas para revisar las comunicaciones electrónicas y las transferencias de datos. Adicionalmente evitan que los datos salgan de las redes corporativas o. También se puede utilizar para evitar que los datos corporativos se transfieran a entidades no verificadas o mediante métodos de transferencia ilícitos.

- Softwares de antivirus: permiten escaneos regulares para mantener el estado de salud de su sistema y detectar infecciones como ransomware, si las hay.
- Softwares antispyware: ayuda a protegerse de los espías informáticos que utilizan softwares maliciosos conocidos como spyware, por lo que hay ciertas herramientas que permiten eliminarlos o bloquearlos.
- Bloqueadores de pops ups: permiten bloquear las ventanas emergentes que son programas no deseados que se ejecutan en un sistema y podrían poner en peligro el mismo, es mejor instalar bloqueadores para mantener la información de forma segura.
- Firewall: como su nombre lo indica constituye una barrera, actuando como una especie de pared que previene accesos por parte de terceros a la red, puede filtrar datos, que podrían constituir amenazas. Está destinado a ayudar a prevenir actividades maliciosas y evitar que cualquier persona, dentro o fuera de una red privada, participe en actividades web no autorizadas.

La LOPDP, también menciona que caben medidas organizativas, que no son más que medidas estructurales y de gestión de personal dentro de una entidad, entre las más importantes podrían incorporarse en las empresas:

a) La adecuada capacitación y constante formación al personal.
b) El acceso autorizado solo a los trabajadores de la empresa a través de usuarios, claves personales, reconocimiento facial.
c) Desarrollo de un protocolo o guía que explique claramente, las reglas y las forma en que deben cumplirse las medidas de protección tomadas por una empresa
d) Que se analicen y categoricen los datos a tratar, y que se especifiquen las consecuencias legales.

2.3.1.2 Notificaciones en caso de vulneración a la seguridad

Cuando ha existido un incidente que ponga en peligro los derechos y libertades de los titulares a quienes se les está tratando sus datos, pueda derivar en una filtración de datos personales. Los responsables del tratamiento deben seguir un proceso cuando ha existido vulneraciones a la seguridad. Frente a esta situación se deben tomar tres acciones:

1. La primera se da por parte del responsable: este debe dar notificación a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y control de las Telecomunicaciones en un término de cinco días después de conocer el suceso.
2. La segunda se da por parte del encargado: el cual debe notificar al responsable en un término máximo de dos días después de conocer el suceso.
3. La tercera, también se da por parte del responsable: este debe dar notificación al titular en el término de tres días después de conocer el suceso, salvo que se hayan adoptado medidas de protección que han sido efectivas, que garanticen que el riesgo no sucederá, las cuales la Autoridad de Protección de Datos las calificará de ciertas. En caso de que la notificación incida en múltiples titulares y se requiera un esfuerzo de gran magnitud la notificación se podrá realizar de forma pública.

De esta forma los titulares pueden enterarse de cuando han existido incidentes y tomar acciones legales.

2.3.1.2 Régimen Administrativo Sancionador

En el caso de que se llegasen a incumplir las disposiciones de la Ley Orgánica de Protección de Datos Personales, tanto el responsable o el encargado de protección de datos personales podrán incurrir en infracciones leves o graves que generan sanciones administrativas

Las infracciones leves respecto al responsable de protección de datos personales podrían darse a consecuencia de: la falta de tramitación de solicitudes y quejas del titular, la falta de

implementación de medidas en el diseño de operaciones como el cifrado o la seudonimización, la falta de políticas de protección de datos e incluso que el encargado no esté capacitado o se incumplan medidas de corrección dispuestas por la autoridad competente.

Las infracciones graves respecto al responsable de protección de datos, se generarán si es que entre otras, no se incluyen medidas que garanticen el tratamiento de los datos, si los datos se usan para fines no autorizados, si existe falta de cumplimiento en los procedimientos legales, si no se utilizan métodos para analizar y gestionar los posibles riesgos, si no se da notificación de vulneraciones de seguridad a la autoridad competente, si no se incluyen cláusulas de confidencialidad y tratamiento de datos personales y las demás que señalan la ley de protección de datos personales.

Por otro lado, el encargado de protección de datos incurrirá en infracciones leves si no colaborase con el responsable, no facilitase el acceso a información respecto al cumplimiento de obligaciones, no permitiese inspecciones, auditorías por parte de personas autorizadas o incumpliese medidas correctivas. Las infracciones graves, incluirán entre otras señaladas en la LOPDP, el tratar datos inobservando las disposiciones legales, incumplir el contrato con el responsable, la falta de supresión de datos personales una vez terminado el encargo.

Dependiendo del tipo de infracción y del sujeto activo se establecerán sanciones administrativas, por un lado, si las infracciones son leves y son cometidas por servidores o funcionarios públicos, la multa será de uno a diez salarios básicos unificados. Por otro lado, si son leves y se cometen por un responsable o encargado de una empresa pública o privada la multa será del 0.1% o 0.7% calculada en base al volumen de negocio del ejercicio económico inmediato.

Sin embargo, si las infracciones son graves y el sujeto activo es un servidor o funcionario público la multa será de diez a veinte salarios básicos unificados, mientras que, si es cometida por un responsable, encargado o un tercero es una empresa pública o privada se aplicará la multa de 0.7/ 0 1% en base al volumen de negocios del ejercicio económico inmediato.

2.3.2 Habeas Data

Antes de introducirse a la garantía jurisdiccional del habeas data, para analizar si esta constituye un mecanismo de protección de los datos personales frente a una posible filtración de datos personales. Es importante delimitar su objeto de protección que ha generado confusión en la interpretación con respecto a su diferenciación con la información.

Cabe la siguiente pregunta ¿cuál es el objeto de protección del habeas data?, para responder esta pregunta primero se establecerá cual no es el objeto de protección. En reiteradas ocasiones se han presentado acciones de este tipo para exigir la entrega de documentos físicos, cierto tipo de datos, u otras pretensiones que se alejan del real sentido de esta acción. Respecto a uno de los mencionados, se puede apreciar el caso No.0067-11JD en el que se exigía la entrega física de un documento, que en este caso eran libros físicos de una compañía a través de una acción de habeas data. La Corte Constitucional señala que no es de interés parta el habeas data el soporte donde se encuentre el dato, sea este material o electrónico ni otro tipo de soporte creado por el ser humano. Por consiguiente, en la sentencia No. ° 001-14-PJO-CC emitió la siguiente regla jurisprudencial:

> el hábeas data, como mecanismo de garantía del derecho a la protección de datos personales, no podrá ser incoado como medio para requerir la entrega física del soporte material o electrónico de los documentos en los que se alegue está contenida la información personal del titular sino para conocer su existencia, tener acceso a él y ejercer los actos previstos en el artículo 92 de la Constitución de la República (Corte Constitucional, Sentencia N.º 001-14-PJO-CC, 2014. 20)

Entonces, el objeto de protección del habeas data es la información, pero no cualquier tipo de información sino la "relacionada con "datos personales" y/o "informes sobre una persona" o sobre "sus bienes que reposen en instituciones públicas o privadas, en soporte material o electrónico" (Corte Constitucional, Sentencia No. 1868-13-EP/20, 2020. 5). De lo antedicho la acción de habeas data permite entonces ser un mecanismo de protección de los datos personales al permitir el acceso o conocimiento de estos.

Ahora cabe otra pregunta, ¿la acción de habeas data está encaminada a la protección de datos de carácter personal o a otro tipo de datos?, la respuesta es que la acción de habeas data protege solo a los datos que sean de carácter personal, es decir que permitan identificar o hacer identificable a una persona. Esto se refleja en la sentencia del caso No. 89-19-JD 2021 de la Corte Constitucional, en el cual se presentó una acción de habeas data por parte de una servidora pública para conocer datos que fueron generados de su correo electrónico institucional, del sistema Quipux y de un sistema denominado Agenda Estratégica Presidencial, de los que su acceso, a excepción del correo electrónico, le había sido negados en otras instancias.

Dicha sala consideró que los datos producidos de los sistemas informáticos, así como del correo electrónico respecto a la gestión laboral no eran personales:

> "usando para el efecto inclusive usuarios, claves y contraseñas, aquello no implica que tales datos, por solo ese hecho, sean necesariamente considerados como personales…para la Corte Constitucional se producirá una desnaturalización de la acción de habeas data cuando determinado servidor o exservidor público intenta, mediante dicha garantía, acceder o conocer datos generados por aquel solo por el hecho de que tales datos fueron producidos durante su gestión en forma física o digital. Esto de acuerdo con la Constitución, a la jurisprudencia de esta Magistratura y a la Ley de Datos Personales" (Corte Constitucional, Sentencia No. 89-19-JD/21, 2021. 7)

No se les concedió la acción de habeas data ya que los datos producidos sólo pertenecían al ámbito de gestión laboral, sin embargo, distinto es el caso en el que las personas quieren acceder o conocer a datos que permiten identificarlos o los hacen inidentificables. Por lo que para que proceda la acción de habeas data en base al derecho de protección de datos personales siempre deberá verificarse los tipos de datos a de los que se quiere acceder o conocer en cada caso en concreto.

Dentro del derecho de protección a los datos personales a su vez se encuentra el derecho a la autodeterminación informativa, el cual se recoge en la sentencia No. 1-14-PJP-CC de 2014.

En el caso de la autodeterminación informativa, como parte del derecho a la protección de datos personales, implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder (Corte Constitucional, Sentencia No. 1-14-PJP-CC, 2014 .14).

De lo anterior entonces se concluye que el habeas data constituye una garantía jurisdiccional que permite la protección de datos personales, a través conocimiento, acceso, y pretensiones inherentes la autodeterminación informativa. Es decir, respecto a los datos personales, informes sobre la persona o sus bienes que se encuentren en soportes materiales o electrónicos, como son los bancos o archivos de datos, documentos entre otros. Permite conocer el uso, fin, origen y destino de la información personal, el tiempo de vigencia, así como su actualización, modificación, rectificación, eliminación y anulación. (Constitución, 2008). Sin embargo, en el caso de que se produjese una filtración de datos personales no permitiría prevenirla, notificarla ni sancionar a los responsables, únicamente permite el conocimiento, acceso, actualización, modificación, rectificación y anulación de los datos personales. Siendo necesarios mecanismos de protección de datos personales que puedan hacer frente a este fenómeno, se señalarán otros en los párrafos siguientes.

2.4 Mecanismos adicionales de protección de datos personales

El sistema de protección de datos personales ya inicio, pero aún se encuentra en construcción frente a la filtración de datos personales, para que se genere eficiencia, prevención, protección y sanción se podrían incorporar los siguientes:

2.4.1 Superintendencia de Protección de Datos Personales

El marco jurídico de la protección de datos personales exige tanto a nivel nacional como internacional que se cuente con una autoridad de protección de datos encargada de hacer cumplir la ley. Al respecto la Ley Orgánica de Protección de Datos Personales establece que esta será un Superintendente de Protección de Datos, el cual tiene que cumplir requisitos académicos, pudiendo ser profesionales especializados en sistemas de información comunicación o tecnologías o profesionales en Derecho. Dentro de las funciones que debe cumplir esta autoridad se encuentran las de supervisar la correcta aplicación de la ley, generar resoluciones para proteger los derechos de las personas respecto al tratamiento de sus datos personales, velar por el cumplimiento de reglamentos e imponer sanciones administrativas y garantizar la confidencialidad, integridad y disponibilidad de sistemas informáticos.

Contar con un Superintendente de Protección de Datos personales resulta urgente y necesario para la aplicación eficaz de la Ley de Protección de Datos Personales, la propia disposición transitoria primera de la ley establece que el régimen sancionatorio entrará en vigor en un plazo de dos años a partir de la publicación de la ley en el registro oficial. Dicha fecha tuvo lugar el 26 de mayo del 2021 por lo que el plazo para que entidades públicas y privadas se ajusten a la Ley de Datos es el 26 de mayo del 2023, y mientras no se designe a esta autoridad no se podrá aplicar la ley.

2.4.2 Convenio 108 +

El Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal conocido como convenio 108, se firmó el 28 de enero de 1981 en Estrasburgo, día en el que actualmente se celebra a nivel internacional el día de la protección de datos personales. Fue el primer instrumento legal de unión internacional en el ámbito de protección de datos personales, siendo la organización internacional del Consejo de Europa quien lo desarrolló. Más tarde este convenio se amplió en el convenio 108 + el cual incluyó salvaguardas adicionales para atacar a los desafíos frente a la protección de datos personales debido al avance de nuevas tecnologías y prácticas.

Este es un convenio abierto que permite que cualquier país en el mundo con una legislación de protección de datos personales acceda a través de solicitud. Su objeto y finalidad se estipulan en el art.1 que reza:

> el fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»). (Consejo de Europa, 1981, art.1)

Únicamente en Latinoamérica se han adherido México, Uruguay y Argentina. Ecuador podría ser uno más de los países que se una a dicho convenio debido a tres razones principales que le permitirían mejorar, mantenerse actualizado y reforzar la protección de datos personales, la primera es que este convenio promueve un estándar universal, preserva de una forma general y flexible la práctica de la aplicación de las leyes de protección de datos personales. La segunda razón es que se obliga a los países miembros a entre muchas otras:

a) declarar y notificar las filtraciones de datos
b) mayor responsabilidad en los encargados y responsables del tratamiento de datos aplicación del principio de "diseño de privacidad"
c) reforzamiento de poderes respecto de las autoridades de protección de datos y mejorar la base legal para la cooperación internacional.
d) principios que se enfocan en la seguridad de los datos y en los derechos del sujeto afectado
e) principios enfocados en promover la advertencia pública frente a las filtraciones de datos personales.
f) cooperación entre autoridades de los países miembros respecto a dudas en el ejercicio de sus poderes particularmente: asistencia mutua, coordinación de investigaciones o conductas conexas, suministro de información o documentación respecto a la aplicación práctica de la protección de datos personales, todo ello dándose a través de una red de comunicaciones, sin costos u honorarios a excepción de los expertos o intérpretes dado el caso.
g) asistencia a víctimas de las filtraciones de datos por parte de todos los miembros a través de solicitud expresa. (Consejo de Europa, 2018)

2.4. 3 Centros especializados de respuesta y prevención de incidentes

Centro de respuesta a incidentes informáticos

Como se analizó anteriormente existe el deber de notificar, como parte del principio de seguridad y protección de la confidencialidad, integridad y disponibilidad de los datos. Tanto a la Autoridad de Protección de Datos Personales que aún no se posesiona y a la Agencia de Regulación y Control de las Telecomunicaciones. En Ecuador existen entidades adscritas al Ministerio de Telecomunicaciones y de la Sociedad de la Información, como por ejemplo con la Arcotel, Agencia de Regulación y Control de las Telecomunicaciones, cuyo ámbito de protección son las telecomunicaciones, uso de redes privadas y el espectro radioeléctrico, en concordancia con la Ley Orgánica de Telecomunicaciones.

El centro de respuestas a incidentes informáticos del Arcotel es el EcuCERT, este organismo adscrito que contribuye a la seguridad de las redes de telecomunicaciones del Ecuador. Actualmente es tan solo un centro de respuesta a incidentes sectorial del tema de telecomunicaciones, "se entiende por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, textos, vídeo, imágenes, sonidos o informaciones de cualquier naturaleza, por sistemas alámbricos, ópticos o inalámbricos, inventados o por inventarse" (Ley Orgánica de Telecomunicaciones, 2022, art.5).

Sin embargo la protección de datos personales va más allá que solo las telecomunicaciones por lo que podría crear un Cerf, Centro de Respuesta a Incidentes de nivel Nacional que se enfoque en la confidencialidad, integridad, disponibilidad de datos personales que responda frente a una emergencia cibernética para manejar incidentes de ciberseguridad, investigando causas, alcance de daño, secuencias de eventos y haciendo uso de herramientas forenses para determinar cómo, cuándo y dónde se produjo la filtración de datos personales.

Centro de operaciones de ciberseguridad

Con respecto al manejo interno de cada organización, la doctrina señala que se puede incorporar un centro de Operaciones de Ciberseguridad o SOC, el cual es un equipo interno que opera de las organizaciones privadas, con ingenieros, analistas, y expertos brindando sus servicios. Estos protegen bases de datos, servicios en la nube y monitorean espacios de almacenamiento activos digitales de las organizaciones para detectar anomalías o riesgos antes de que se incurra en una filtración de datos, es decir ayudan a prevenir ataques masivos y posibles exposiciones o filtraciones de bases de datos. Cumpliendo con actividades de mantenimiento, planificación y pruebas de vulnerabilidad, manejando una infraestructura de tecnología de gama alta, con inversiones en hardware y software (Edx, 2020).

3. Tema 2. Filtración de datos personales en el derecho penal y posibilidad de responsabilidad penal en el caso Novaestrat

3.1 Tipos penales relacionados a la filtración de datos personales

Se argumenta que estos delitos están directamente relacionados a la filtración de datos personales porque implican el fenómeno per-sé que es la exposición intencional de la información.

Por un lado, en el delito de violación a la intimidad en sus verbos rectores, acceder, publicar y difundir datos personales constituye las causas y consecuencias de la filtración de datos personales. En referencia a la revelación ilegal de bases de datos la persona en provecho propio o de un tercero revela información almacenada en medios como bases de datos, implica la exposición de los datos personales que es justamente la conceptualización de data breach y el provecho ya que la mayoría de las veces este fenómeno se da para obtener beneficios económicos, ya que existe un mercado de datos como en párrafos anteriores se detalló.

Con respecto a su incidencia a nivel penal, en Ecuador, se quiso dar una visión general de cómo se encuentra la situación general, reciente a delitos relacionados al data breach, por lo que se ha solicitado a la Fiscalía Provincial de Pichincha el número de denuncias desde el año 2019 al año 2022 a nivel nacional, las cuales se detallan a continuación:

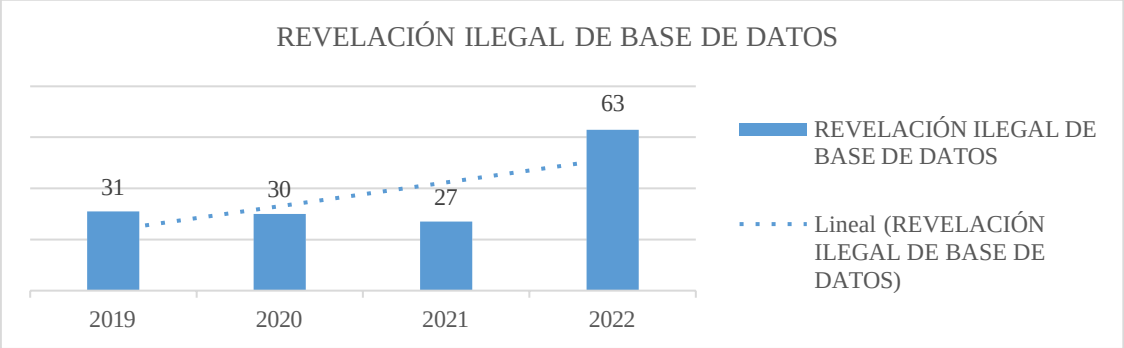

Gráfico 1
Fuente: Fiscalía Provincial de Pichincha
Elaboración: Paula Romo, 2023

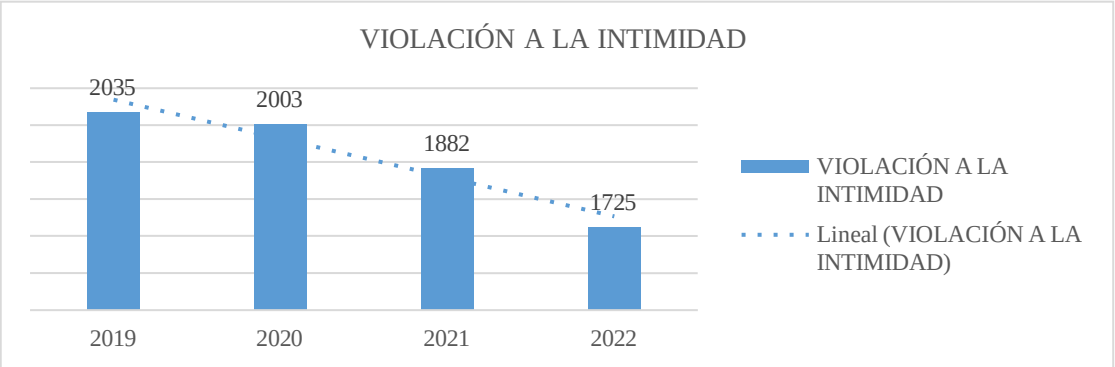

Gráfico 2
Fuente: Fiscalía Provincial de Pichincha
Elaboración: Paula Romo, 2023

Como se puede observar en los gráficos elaborados, la revelación ilegal de bases de datos ha incrementado drásticamente del año 2019 al año 2022, lo que podría denotar que el fenómeno de data breach se podría está incrementado. Si bien se puede asegurar ello con total seguridad podrían encontrase varios datos personales revelados.

Lo antedicho se relaciona ya que detrás del bien jurídico que busca proteger de la seguridad de los activos de los sistemas de la información y la comunicación se encuentra la confianza que el titular de los datos deposito respecto al almacenamiento y tratamiento de sus datos personales.

Por consiguiente, cabe mencionar que, si bien este tipo se efectúa "materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas" (COIP,2023, art.229). Se podría contemplar esta posibilidad de que se aluda también a la protección de datos personales, lo cual se puede establecer, modificando la norma a través de una reforma al Coip y podría añadir: "materializando voluntaria e intencionalmente la violación de secreto, la intimidad, privacidad de las personas **y la violación a los datos de carácter personal**".

3.2 Caso Novaestrat

3.2.1 Antecedentes del caso

Novaestrat es el nombre de una compañía de responsabilidad limitada, fundada el 16 de noviembre del 2017, manejada por Agustín M, Gerente General, Rocío A, Presidente de la compañía y William R, Gerente saliente de la compañía. Esta persona jurídica se definía así misma como "una empresa ecuatoriana dedicada a reinventar tu empresa en base a los datos procesados, para tomar decisiones acertadas con el menor impacto posible" (Novaestrat, 2019),

la cual brindaba servicios de segmentación de mercado, asesoría en decisiones financieras, y además "sería la propietaria de un servidor, alojado en Miami, Estados Unidos", (Fiscalía General del Estado,2019, p. 2) , dicho servidor estaba indexado al motor de búsqueda conocido como ElasticSearch.

El servidor aparentemente manejaba una base de datos con información de más 20 millones de ecuatorianos, información que se llegó a conocer gracias al sitio web de revisión de vpn, más grande del mundo y equipo de ciberseguridad denominado vpnMentor. Este afirmaba que gracias a uno de sus diagnósticos de red pudieron hallar "una gran filtración de datos que podría impactar a millones de individuos en Ecuador. La filtración de la base de datos incluía más de 20 millones de sujetos". (vpnMentor, 2019, p.1). El equipo presentó un informe y notificó del hallazgo vía correo electrónico a los funcionarios del Centro de Respuesta a Incidentes Informáticos del Ecuador EcuCERT el 7 de septiembre del 2019.

En respuesta a lo sucedido, EcuCERT ejecuto diversas acciones que produjeron resultados favorecedores:

El 11 de septiembre del 2019 se obtuvo como resultado la "mitigación final de la vulnerabilidad a través de la cual se encontraba expuesta una base de datos en el extranjero, alojada en un servidor privado, que contenía datos personales de ciudadanos ecuatorianos, todo esto en procura del aseguramiento de esta" (Comisión de Soberanía, Integración y Seguridad Integral, 2020, p.5).

A pesar de estas acciones, la preocupación persistía ya que una vez que la data ha sido filtrada ya no es posible deshacerse los perjuicios ni las consecuencias de su exposición, tal como señala el equipo de vpnMentor (2019) "La base de datos ahora está cerrada, pero la información, ya podría encontrarse en manos de terceros malintencionados" (p.4).

Según el informe una variedad de datos se filtró. Con fines académicos se los procede a categorizar o clasificar como como datos personales generales o sensibles, entre otros según criterios de la ley de protección de datos personales, aún no vigente a la fecha de los sucesos:

Por un lado, se encontraron datos personales generales, los cuales señalaban que eran del Registro Civil e incluían bloques de: números de cédula, nombres completos, fecha y lugar de nacimiento, dirección personal, números de teléfono del trabajo, de la casa y personales, dirección empresarial, estado civil, fecha de matrimonio, fecha de muerte, nivel de educación, profesión, de cada persona. Asimismo, se encontraron datos personales sensibles crediticios,

del Banco del Instituto Ecuatoriano de Seguridad Social incluyendo: estado de cuenta, saldo actualizado de la cuenta, créditos, ubicación y salario. VpnMentor en colaboración con Zdnet señalaron que lo más preocupante fue la información detallada sobre los familiares de las personas, donde existía una gran cantidad de información acerca de familiares, niños, género, localización, que vendrían a ser datos personales sensibles.

Una de las preguntas que surgen es ¿cómo Novaestrat podría tener en su poder esta información?, en relación con ello, Santacruz y Vergara señalan que "solo existen dos vías legales para la obtención de los datos: la primera bajo el conocimiento del titular y la segunda, cuando exista una autorización mediante una ley. Si no viene por ninguna de estas vías, es un tratamiento ilegal" (Comisión de Soberanía, Integración y Seguridad Integral, 2020, p.3). Esto quiere decir que para que se logre obtener ilícitamente información, pudo haber existido una presunta venta por parte de alguna compañía, institución pública o privada, o por otro lado un presunto uso no autorizado de ciertas bases de datos. Incluso Andrés Michelena, ministro de Telecomunicaciones, argumentó que "no hubo hackeo sino una posible venta de las bases de datos conectadas con SNI" (PlanV, 2019, p.4).

Por su parte la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional, presentó un informe en respuesta a la resolución que le disponía iniciar una investigación respecto a la filtración de datos personales. Concluyendo que:

> los dueños de la empresa NOVAESTRAT, exfuncionarios públicos, aparentemente tuvieron acceso a información de instituciones públicas, como: BIESS, SENPLADES, CFN, produciéndose así la supuesta filtración de datos de más de 17 millones de ecuatorianos, ya que no existió un control y seguimiento suficiente de la regularización de los datos personales de los ciudadanos. (Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral, 2020, p.25)

La inquietante noticia alertó y causó indignación en diversos medios de nivel internacional como CNN, Forbes, BBC, New York Times, El Tiempo entre otros. Por lo que posterior al escándalo, se tomaron dos acciones principales: la primera se dio el 16 de septiembre del 2019; gracias a múltiples denuncias y a información mediática. La Fiscalía General del Estado ejecutó un allanamiento para recabar elementos sobre el presunto delito de violación a la intimidad; la segunda acción tuvo lugar el 17 de septiembre del mismo año, fecha en la que se tomaron las versiones de Agustín M, presidente de Novaestrat y William R dentro de la fase de investigación previa.

Toda esta situación condujo a que el presidente Lenin Moreno ordene, el 16 de septiembre del 2019, en un plazo no mayor a 72 horas, la emisión de la Ley de Protección de Datos Personales, por lo cual el 19 de septiembre de 2019 se presentó el proyecto de Ley de Protección de Datos personales, que una vez aprobado se publicó en el Registro Oficial el 26 de mayo del 2021.

Cabe una pregunta ¿si el hecho se cometió en Miami, Estados Unidos, ¿por qué se está llevando a cabo una investigación previa en Ecuador?, si cabe por principio de extraterritorialidad se puede juzgar en Ecuador. La extraterritorialidad encuentra varios ámbitos de aplicación de la ley penal uno de ellos es el ámbito espacial personal de validez, el cual no es más que determinar la zona geográfica en donde se aplicará norma. La legislación ecuatoriana permite aplicar las normas del Coip, cuando la infracción produzca efectos en Ecuador, también cuando la infracción se cometa en territorio extranjero, entre otros casos, en concordancia al Art.14 del Coip. Dicho principio tuvo sus primeros matices en la sentencia del caso Lotus, en la ex Corte Permanente de Justicia Internacional argumentaba que "aunque es cierto que en todos los sistemas legales es fundamental el carácter territorial del Derecho penal, no es menos cierto que todos o casi todos estos sistemas extienden su jurisdicción a delitos cometidos más allá del territorio del Estado" (Collantes s.f, p.68)

Procedimiento ordinario

En este apartado se analizará únicamente el procedimiento que se ha llevado a cabo en torno al caso Novaestrat hasta el presente.

Procedimiento de acción pública en el Caso Novaestrat

La responsabilidad penal "sólo puede establecerse a través del proceso penal, que es el procedimiento establecido para garantizar los derechos fundamentales de todas las partes" (Muñoz, 2014, p.108). Por lo que se señalarán las fases del proceso penal que hasta el momento se han realizado en el caso Novaestrat.

A. Conocimiento del delito

"La noticia criminis es el conocimiento que se tiene de la posible existencia de un delito o falta y que justifica el inicio de una investigación" (Silvestri,2012, p.108). En el caso de análisis el conocimiento del delito provino tanto por medios de comunicación social, así como por denuncias escritas de la Dirección General de Registro Civil, Identificación y cedulación; de la

Agencia de Regulación y Control de Telecomunicaciones y de la Dirección Nacional de Registro de Datos Públicos.

B. Fase pre procesal del procedimiento ordinario

La noticia criminis mereció de una investigación previa, la cual según Vivanco (2015) "tiene como finalidad la recolección de elementos de convicción para determinar si existen indicios de la comisión de un delito" (p.755).

En esta pre fase el Fiscal, como titular del ejercicio de la acción pública, recaba información útil, pertinente, conducente para el esclarecimiento del hecho y la responsabilidad. Toma en cuenta elementos de cargo y de descargo en favor del sospechoso, solicita la detención para la investigación en caso de ser procedente, asegura el derecho de defensa del sospecho y de la víctima y recopila "elementos de convicción, huellas, instrumentos, vestigios conducentes para el esclarecimiento del hecho" (Fiscalía General del Estado, 2014, p.32), profundizando los actos de investigación siguiendo una teoría del caso

Como en párrafos anteriores se mencionó , la investigación se apertura el 16 de septiembre del 2019 , mismo día en el que se realizó un acto urgente, el cual consistió de un allanamiento, en el domicilio de uno de los representantes legales de Novaestrat, y que según la Fiscalía General del Estado (2019) "se efectuó para recabar elementos sobre un presunto delito de violación a la intimidad […]se incautaron equipos electrónicos, computadores y dispositivos de almacenamiento, además de documentación, entre otros elementos"(p.1). Al día siguiente el 17 de septiembre del 2019 se tomaron las versiones del representante y presidente legal de Novaestrat en la que se recabó información sobre procesos, relaciones y cuestiones dependientes del giro del negocio de esta.

Es menester señalar que la duración de la investigación previa contada desde la fecha de inicio no puede superar los plazos expresos en el artículo 585 del Coip, el cual señala que "en los delitos sancionados con pena privativa de libertad de hasta cinco años durará hasta un año" (COIP, 2019, art.585). En consecuencia, si la investigación previa inició el 16 de septiembre del 2019 y la pena de libertad por el delito de violación a la intimidad que versa en el art. 178 es de uno a tres años, el plazo para la investigación terminó el 16 de septiembre del 2020.

Lamentablemente, el caso hasta el momento no ha producido sentencia alguna, y de la información brindada por Fiscalía únicamente se conoce que se realizó la investigación previa. Esta situación es preocupante ya que independientemente de si se continuó con el archivo, se reapertura la investigación previa o se inició con el proceso de la causa, falta tan solo un año

para la prescripción por el presunto delito de violación a la intimidad. Por lo que se analizará la posibilidad de responsabilidad penal en el Caso Novaestrat en base al delito de violación a la intimidad y sus posibles adecuaciones a otros tipos penales.

3.2.3 Análisis de responsabilidad penal en el caso Novaestrat con base en la teoría del delito

Para analizar la posibilidad de responsabilidad penal (*ex ante)* en el caso Novaestrat, se tomará en cuenta:

a) conceptualización y requisitos para su determinación, por lo que se usará, la teoría del delito considerando por doctrina penal.
b) las disposiciones legales del Código Orgánico Integral Penal vigente en septiembre de 2019, fecha en la que se apertura la investigación previa. En concordancia a la regla del *tempus regit actum*, tiempo rige el acto, que "ordena la aplicación de la norma en vigor en el momento del hecho" (RAE,2023, p.1) en concordancia a lo estipulado en el artículo 16 que determina que "toda infracción será juzgada y sancionada con las leyes vigentes al momento de su comisión" (COIP, 2019, art.16).
c) en concordancia a lo mencionado en el párrafo anterior, no se analizarán errores de tipo ni de prohibición ya que estos fueron incorporados recién por Ley Orgánica reformatoria al Código Orgánico Integral Penal, publicada en Registro Oficial Suplemento 107 el 24 de diciembre del 2019.

Grosso modo, la responsabilidad penal, se puede definir como la obligación que tiene todo individuo que comete un delito de soportar las consecuencias jurídicas que derivan de su conducta ilícita, las cuales se configuran en la imposición de una pena. Criterio comparte la doctrina al señalar que:

> en suma, la responsabilidad penal ha de ser concebida como la consecuencia jurídica de la comisión de un delito, que se traduce en el estado de sometimiento a que queda sujeto un individuo frente a la potestad sancionatoria estatal y que se materializa en la imposición de una pena (Rodríguez, 2011, p.2).

Sin embargo, no existe responsabilidad penal sin ciertas condiciones o requisitos, por lo que en la misma línea de ideas, Muñoz y García (2010) argumentan que para que exista responsabilidad penal es necesario que concurran los siguientes requisitos: a) la existencia de

un hecho típico, antijurídico y culpable; b) que el autor del hecho sea imputable c) que no concurra ninguna causa de justificación, u otras que se considere el ordenamiento. Dichos elementos se analizarán en esta sección en base a las actuaciones de Fiscalía hasta el momento. Por lo que se hará uso de la teoría del delito para identificar los elementos comunes a todas las conductas delictivas y verificar que lo que se está constatando es un delito y que merece pasar a la punibilidad o responsabilidad penal (Araujo 2020).

En conclusión, la responsabilidad penal es la obligación jurídica que experimenta el sujeto activo de un delito, de soportar las consecuencias jurídicas que las normas determinen. Misma que se producirá siempre que se demuestre en su totalidad los requisitos propios de responsabilidad penal, los cuales implican una conducta típica, antijurídico, imputable y culpable, en concordancia y cumplimiento del proceso penal.

3.2.1.1 Delito de violación a la intimidad

Los requisitos establecidos en párrafos anteriores se desglosarán de acuerdo con el delito de violación a la intimidad, que es por el cual Fiscalía inició la investigación previa. Todo ello, con el objetivo de verificar si pudiera generarse responsabilidad penal o no. "Con la constatación positiva de estos elementos, tipicidad, antijuridicidad y culpabilidad, se puede decir que existe delito y su autor puede ser castigado con la pena que se asigne en cada caso concreto al delito en la ley". (Muñoz, 1999, p.4)

El Código Orgánico Integral Penal, en relación con la infracción de violación a la intimidad, reza en su art. 178 lo siguiente:

> 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 (COIP, 2019, art.178)

a.1 La conducta típica

La existencia de una conducta en la realidad permite la valoración negativa de las misma por parte de un ordenamiento, a pesar de ello no todos los comportamientos socialmente

inaceptables tienen relevancia penal, son solo aquellos que se expresan en un acto externo. Dichos actos pueden ser acciones u omisiones y para tener relevancia penal deben enmarcarse en una conducta descrita en un tipo penal. Es decir, la conducta del mundo real tiene que verse descrita y coincidir en una infracción penal para que puedan entrar en consideración de ver la posibilidad de que se incurra en responsabilidad penal.

Así mismo la conducta típica está formada de elementos subjetivos y objetivos, los primeros analizan la voluntad e intención, mientras que los segundos se enfocan en la descripción externa de la conducta. Dentro de elementos subjetivos de la conducta típica se encuentran el dolo o la culpa, es decir la intención positiva de hacer daño o la intencionalidad. En particular el delito de violación a la intimidad refleja dolo.

En lo que respecta a elementos subjetivos se identifican ciertos verbos. Los verbos rectores gramaticalmente que hablan describen la conducta que se busca sancionar, "rigen la oración gramatical llamada tipo" (Vega, 2016, p.62). Cuando el tipo penal tiene un solo verbo se le denomina elemental, mientras que si tiene varios compuestos.

Los verbos rectores en el tipo penal de violación a la intimidad son seis, por ende, el tipo penal es compuesto. El primero de ellos es acceder, que en palabras ordinarias significa entrar a, tener acceso. El Tribunal Supremo Español en la STS 803/2014 concluye que acceder es la acción del sujeto activa que ocurre "tan pronto los conoce y tiene a su disposición, pues sólo con eso se ha quebrantado la reserva que los cubre" (Sanz et al., 2021, p. 379).

El segundo verbo es interceptar del latín interceptus, inter (entre), ceptus (capturado) , se define doctrinariamente según el tipo de interceptación, debiendo usarse el concepto de interceptación de indiscreción, la cual se define como : ciertas acciones para interferir una comunicación con el fin de tomar conocimiento de algo, no debiendo este concepto confundirse con la interceptación de obstrucción que implica acciones para impedir, detener o interrumpir la comunicación (Sanz et al. , 2021) , ya que la simple obstrucción no supone la violación a la intimidad.

Continuando con el análisis de verbos rectores, el verbo examinar por su lado refleja su definición lingüística en la acción de, "investigar o escrudiñar con diligencia y cuidado algo" (RAE, 2023, p.1); retener del latín retinere re (atrás) tenere (dominar) quiere decir no entregar

lo que se tiene. Grabar, es captar cualquier dato auditivo o visual a través de un soporte que permita almacenamiento. Reproducir, se entiende como volver a producir algo, es decir previamente ya existe información o un dato personal; que se vuelve a producir, valga la redundancia.

Finalmente, difundir según la definición del Tribunal Supremo Español en la STS 1219/2004 indica que: "difundir comporta una mayor publicidad cual es la de propagar, divulgar o esparcir un hecho" (Sanz et al,2021, p.338) haciendo uso de medios de comunicación; mientras que publicar se diferencia del anterior verbo ya que este último consiste en la acción de hacer pública información o datos, pero no implica el objetivo de expansión como si está inmerso en la difusión.

Los verbos rectores, desde la perspectiva de la gramática penal, tienen la función de describir las acciones u omisiones dentro de algunos tipos penales y sirven para determinar si la conducta podría configurar o no en un delito. Por lo tanto, forman parte del proceso de interpretación, siendo importante identificarlos y entenderlos para ver si se podría generar responsabilidad penal en este caso particular.

Existen causas de exclusión de la conducta, que, si bien ocurren en algunos delitos, en el delito de violación a la intimidad y revelación ilegal de bases de datos es casi nula su ocurrencia, sin embargo, se clasifican en la doctrina, como fuerza irresistible, movimientos reflejos y estados de inconsciencia, lo cual casi concuerda a la perfección con el art.24 del Coip. Por lo que se los explicará escuetamente.

La primera implica que aquella fuerza externa, sea natural o de un tercero, impacte de forma absoluta al receptor de manera que este quede imposibilitado de resistirla anulando su voluntad.

Los movimientos reflejos por su parte implican un movimiento de carácter involuntario en el que usualmente a causa enfermedades como epilepsia, síndrome de Tourette que producen movimientos incontrolables y dañinos, los cuales no se deben confundir con movimientos producidos por la ira ya que si bien pueden llegar a ser violentos el elemento de la voluntad aún existe.

Finalmente, los estados de inconsciencia como el sueño no son incluidos en el Coip, sino aquellos de plena o total inconsciencia es decir no baste con el sueño sino un estado de NREM 2 que sería la fase más profunda del sueño en donde expertos mencionan que la voluntad ya no

existe. Se exceptúan de esta última parte cuando el sujeto de forma voluntaria se ha puesto en ciertos estados para cometer infracciones, las llamadas actiones liberae in causa (Muñoz y García, 2010, pp.217,218)

b.1 .1 Los sujetos

Un sujeto es una persona natural o jurídica, la doctrina jurídica clasifica usualmente a los sujetos en activos y pasivos. El sujeto activo en el análisis de tipicidad se entiende como aquel individuo que realiza la acción, aquel que adecua su conducta e la infracción penal.

El sujeto activo a su vez se podrá clasificar dependiendo de si es un delito común o un delito propio. La característica del delito común es que puede ser cometido por cualquier persona, mientras el propio debe cumplir requisitos específicos. Específicamente el art.178 estipula un delito común ya que el sujeto únicamente cumple la característica de ser cometido por cualquier persona, esto se expresa en el inicio del tipo penal, la frase: la persona que.

El sujeto pasivo este es el titular del bien jurídico protegido también conocido como víctima. Evidentemente esto dependerá del tipo de delito, en el caso de violación a la intimidad será el titular de la intimidad personal o familiar.

b.1 .2 Los objetos

Los objetos dentro del tipo penal se clasifican en materiales y jurídicos, los materiales son "la persona o cosa sobre la que materialmente recaen los resultados de la acción delictiva, puede ser el propio sujeto pasivo, y las cosas animadas o inanimadas que se afectan con la acción del sujeto activo." (Kim, 2017 p.2)

El objeto material de la violación a la intimidad es la persona o cosa que sobre la conducta delictiva recae y que se ven afectados por la conducta, se identifican los siguientes:

a) datos personales: son aquellos datos que permitan identificar o hacer identificable a una persona física de manera directa o indirecta.

b) mensajes de datos, voz, audio y video: la Ley de Comercio Electrónico Firmas y Mensajes de datos señala que el mensaje de datos

> "es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su

> definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos" (Ley de Comercio Electrónico, Firmas y Mensajes de Datos, 2023, disposición general novena).

c) objetos postales: en la resolución 18-DE-ANP-2013, la Agencia Nacional Postal señala que objetos postales:

> "se entiende por las cartas, tarjetas postales, aerogramas, facturas, extractos de cuentas, recibos de toda clase, impresos, periódicos, envíos publicitarios, ecogramas, muestras de mercaderías, pequeños paquetes y los demás objetos que cursen por las redes postales del servicio de correos y del servicio de mensajería expresa" (ANP, 2013, 18-DE-ANP-2013).

d) información contenida en soportes informáticos, la información es un género amplio dónde pueden entrar datos de diversos tipos que conforman la información ahora bien esta información es la que está contenida en soportes informáticos, es decir en medios de almacenamiento informáticos como CD, cintas magnéticas, tarjetas de memoria, unidades USB, en ordenadores, tabletas o celulares, entre otros

e) comunicaciones privadas o reservadas, las comunicaciones privadas son aquellas conversaciones orales o escritas en las que el emisor escoge a los destinatarios con el fin de que la información se recibida solo y únicamente a ellos.

El objeto jurídico, o bien jurídico de forma general no es más que "todo objeto que la ley u concretamente la ley penal en los respectivos tipos considera digno de protección jurídica" (Bernate, 2007, p.23)

Cabe recalcar que los bienes jurídicos no son creados por el derecho penal, sino por el derecho constitucional e internacional "el derecho penal no crea bienes jurídicos, sino que se limita a sancionar con una pena a ciertas conductas que lesionan ciertos bienes" Kierszenbaum (2009, p.189). Se determina entonces que, el derecho penal tiene como objeto la protección de bienes jurídicos que se encuentran dentro de los códigos penales, los cuales han sido creados por el derecho constitucional pero incorporados al código, con el objetivo de que se sancionen conductas que los lesionen. En el derecho ecuatoriano el COIP sanciona aquellas conductas

típicas, antijurídicas y culpables que lesionen ciertos bienes jurídicos protegidos que se encuentran a lo largo de las secciones incorporadas.

Específicamente, en delito de violación a la intimidad, el bien jurídico protegido, señalado en el Código Orgánico Integral Penal es, la intimidad personal y familiar.

Este se refleja como derecho reconocido en el artículo 16 numeral 20 de la Constitución ecuatoriana, así como en diversos tratados internacionales como la Declaración Universal de los Derechos Humanos al mencionar que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su hora o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Asamblea General de las Naciones Unidas, 1948, art.12), así como otros que recogen la misma que entre los principales se encuentran la Convención Americana de derechos y deberes del hombre y el Pacto de Internacional de Derechos Civiles y Políticos.

El bien de la intimidad se encuentra catalogado doctrinariamente, dentro de los denominados bienes jurídicos individuales, los cuales son bienes jurídicos que se refieren a los intereses y derechos de las personas en particular, posicionándose así la intimidad como un bien personalísimo e individual.

b. 2 Conducta antijurídica

> Una vez subsumido, el caso de la realidad en el supuesto de hecho de una norma penal, el siguiente paso, en orden a la averiguación de si ese caso puede engendrar responsabilidad penal, es la determinación de la antijuridicidad, es decir, la constatación de que el hecho producido es contrario a derecho, injusto o ilícito (Conde, 1999 p.75).

La antijuridicidad no solo se aplica al derecho penal sino a todas sus ramas, por lo que específicamente en derecho penal debe basarse en la tipicidad para contradecir a los tipos penales que recogen cada uno de los comportamientos antijurídicos. En este sentido. Conde (1999) señala que: "el derecho penal no crea la antijuridicidad, sino que selecciona, por medio de la tipicidad, una parte de los comportamientos" (p.75)

La antijuridicidad se conforma de dos partes, la formal y la material, la primera es el simple ejercicio de oponer la acción con la norma, de contradecirla, la cual no agota la antijuridicidad.

Mientras que, la antijuridicidad material se refleja en la ofensa al bien jurídico protegido. La antijuridicidad está ligada al principio de lesividad, ya que para que exista antijuridicidad se necesita una lesión o puesta en peligro del bien jurídico protegido, no basta con una simple contradicción, es decir no basta con la antijuridicidad formal.

Cabe recalcar que no todos los hechos típicos son antijurídicos para verificar que efectivamente ese hecho típico es contrario al ordenamiento jurídico específico, se deberá desvirtuar "la concurrencia de una causa de justificación" (Conde, 1999, p.75). Las causas de justificación convierten el hecho o conducta en lícita, por lo que impiden aplicar cualquier sanción, impiden derivar en responsabilidad penal y culpabilidad. Las causas de justificación son taxativas en el Código Integral Penal siendo estas, la legítima defensa, el estado de necesidad, el cumplimiento de una orden de autoridad competente y el cumplimiento de un deber legal.

De la búsqueda en la jurisprudencia ecuatoriana, no se han encontrado casos con causas de justificación relacionadas con la conducta del art .178 la violación a la intimidad. Sin embargo, se podría darse por ejemplo cuando Las causas de justificación más comunes serían las del cumplimiento de un deber legal y cumplimiento de orden legítima y expresa de autoridad competente. Un ejemplo de ello puede se puede dar cuando un juez ordena la interceptación de comunicaciones en cumplimiento de sus deberes legales y el policía lo cumple por orden expresa de dicha autoridad. En concordancia a ello:

> desde el punto de vista de RODRÍGUEZ LAINZ, queda muy clara la causa de justificación. Que posibilitan al juez acordar la detención de la correspondencia privada, intervención de las comunicaciones telefónicas del procesado o la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal" (Menéndez, 2017, p.77).

Es muy poco probable que legítima defensa con respecto a la violación a la intimidad, por lo que se podría recaer en casos de exceso en la causa de justificación como sucedió en el caso 11001650019220170608O-01 del Tribunal Superior del Distrito Judicial de Bogotá el cual precisa que:

> "la sala considera que el imputado obró en legítima protección de un bien jurídico tutelado con rango de derecho fundamental –la intimidad-, ante el riesgo inminente de vulneración por parte de su excompañera sentimental, quien, de forma abusiva, sin autorización del titular. Toma el teléfono celular con la finalidad de revisar su correspondencia privada…si bien actuó

> de forma jurídicamente permitida en defensa de uno de sus derechos, la sala considera que bien pudo haber logrado recuperar su teléfono por otros medios persuasivos, como el dialogo, o haber solicitado el apoyo del hijo que se encontraba presente en la vivienda, antes de acudir al uso de la fuerza física, razón por la cual, se derivará responsabilidad penal al haber obrado en exceso," (Tribunal Superior del Distrito Judicial de Bogotá, 2021, p.11).

Culpabilidad

a) conducta culpable

La culpabilidad o juicio de reproche que se emite sobre la conducta típica y antijurídica de una persona, cuando ésta ha actuado con capacidad de entender y de querer, y no concurre ninguna causa de exclusión de esta. Los requisitos de la culpabilidad son tres el primero la capacidad de culpabilidad o imputabilidad, el segundo el conocimiento de la antijuridicidad relacionada con los errores de prohibición y por último la no exigibilidad de otra conducta. (Conde, 1999)

a) La capacidad de culpabilidad o imputabilidad

Se refiere a la madurez mental y a la habilidad el individuo para realizar el hecho típico y antijurídico con motivación. Se necesitan de ciertas capacidades mentales para que se dé una motivación racional, ya que sin ciertas habilidades no se puede atribuir culpabilidad.

En el derecho penal ecuatoriano se la puede excluir:

a.1 Cuando los sujetos son niños niñas y adolescentes se aplica el Código Orgánico de la Niñez y Adolescencia, no se genera impunidad, sino que se da a través de un procedimiento diferente.

a.2 Cuando existe trastorno mental total, "al momento de la infracción el sujeto padece de una alteración psíquica grave, por ende, no comprende lo que hizo" (Santillán y Bayardo, 2020, p.2). Cuando se alegue esto cual se necesitará un informe pericial que confirme el trastorno, por ejemplo, que presente psicosis, oligofrenias, psicopatías, neurosis entre otras afecciones psiquiátricas que al momento de cometer la infracción se encuentre presente, posterior a ello se dictan medidas de seguridad "la medida de seguridad es una consecuencia jurídica aplicada a una persona física en función de la peligrosidad de su hecho. No se imponen en función de la culpabilidad, pues es precisamente ésta la que les falta para responder penalmente" (Fernández, Vallejo y Perrino, 2017, p.)

a.3 Cuando existe trastorno mental con disminución en la capacidad de compresión:

"La imputabilidad disminuida es un caso particular de menor culpabilidad que sirve de regla para la cuantificación de la pena" (Sierra, y Salvador, 2005, p.263) El Coip en concordancia a lo citada señala que de darse este caso se aplica un tercio de la pena mínima.

a.4 Cuando la persona está ebria o intoxicada, es decir ha consumido alcohol o drogas, será eximida de culpabilidad siempre que, según el COIP (2019) se ha privado del conocimiento al sujeto y se produce como consecuencia de caso fortuito. Si por otra parte solo se demuestra que se ha privado tan solo una parte del conocimiento, pero no en su totalidad se aplica un tercio de la pena mínima.

b) El conocimiento de la antijuridicidad en el contexto de los errores de prohibición

Para atribuir la responsabilidad penal a alguien es necesario que este conozca que su hacer está prohibido en la norma penal. Quiere decir que el individuo debe saber, tener conciencia o conocer que conductas están prohibidas. En la legislación ecuatoriana, se ha incorporado la teoría del error, existiendo errores de tipo que se incorporan en la sección de tipicidad y errores de hecho o también llamados errores de prohibición que se incorporan en la sección de culpabilidad. Sin embargo, no se detendrá a profundizar en este tema, ya que el Coip 2019 del cual se está analizando el caso Novaestrat aún no mantenía vigentes dichas modificaciones.

c) Cuando existen excusas legales absolutorias

Son condiciones que de suceder liberan de responsabilidad a una persona, en estas no hay pena, por ende, no existirá responsabilidad penal, se encuentran especificadas en cada tipo penal, con frases como, no habrá lugar a la responsabilidad, no serán aplicables estas normas, no será punible, entre otras. De cumplir las condiciones, la excusa legal absolutoria deja sin castigo o pena al sujeto que realice la acción u omisión. En este caso el art. 178 prevé que "no serán aplicables estas normas" cuando las personas que divulguen grabaciones de audio y video intervengan de forma personal, ni cuando se trata de información pública.

3.2.1.1 Revelación ilegal de bases de datos

Aunque la Fiscalía no inicio la investigación previa por este delito se considera que la conducta también se relaciona a este tipo penal. Para ver si podría surgir responsabilidad penal en este tipo y ya que en párrafos anteriores se han analizado los requisitos anteriormente explicados, de manera escueta se procede a indicarlos:

El art. 229 reza:

> 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 (COIP,2019, art.229)

a) Conducta típica

Dentro de los elementos subjetivos, dolo o culpa, de este tipo penal se determina que existe dolo, reflejando explícitamente en la frase "materializando voluntaria e intencionalmente". Este tipo penal elemental, establece un solo verbo rector, el cual es revelar, su significado es "descubrir o manifestar lo ignorado o secreto" (RAE,2023, p.1)

Respecto a los sujetos este delito es mixto al englobar en su primer párrafo un delito común y en su segundo un delito propio. Por consiguiente, puede ser cometido por una persona cualquiera, así como por un servidor público, empleado bancario, empleado de instituciones de economía popular y solidaria que realicen intermediación financiera, o contratistas, la diferencia está en la pena.

Con respecto al objeto material, los resultados recaen en la información que esté registrada.

Por otro lado, no deben confundirse el objeto material de las circunstancias en las que puede encontrarse registrada esa información:

a) por un lado, la información puede estar contenida en cualquier medio de almacenamiento, como ficheros, bases de datos o similares
b) a su vez transportarse o fluir (a través o dirigida) en sistemas electrónicos. usan electrones; sistemas informáticos, programas o sistemas operativos; un sistema telemático, telecomunicaciones e informática; un sistema de telecomunicaciones que es un sistema que "incluye servicios de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros" (Consejo de Europa, 2007, p.6)

El objeto jurídico, recae en el bien jurídico protegido es estos delitos es la seguridad de los activos de los sistemas de información y comunicación, un activo puede ser los datos personales, por lo que se busca brindar protección frente a la revelación de la información registrada, que conexamente busca proteger la confidencialidad e intimidad de los datos. Adicionalmente es un bien jurídico supraindivual o colectivo ya que no sirve únicamente a intereses individuales sino a intereses comunitarios.

b) conducta antijurídica

Con respecto a la antijuridicidad formal, y considerando la conducta de Novaestrat se puede deducir que se contradeciría con la conducta expresamente prohibida el art.229 del Coip.

Por otro lado, en relación con la antijuridicidad material se determina si ha lesionado o puesto en peligro un bien jurídico protegido, en este tipo de antijuridicidad se debe materializar en una ofensa. En este caso la acción de Novaestrat debería causar una lesión a la seguridad de activos de los sistemas de información y comunicación incluso causaría lesión a otros bienes jurídicos conexos como la intimidad. Por ende, al existiría armonía entre la material y la formal sí se podría llegar a dar este requisito.

Con respecto a las causas de justificación la doctrina menciona que es muy poco probable que se den en este tipo de delitos por lo que no se ha encontrado jurisprudencia extranjera ni nacional respecto a las mismas.

c) conducta culpable

En primer lugar, con respecto a la capacidad de culpabilidad o imputabilidad de la información conocida, los representantes legales de Novaestrat son mayores de dieciocho años, deberá verificarse si presentaron trastorno mental total o transitorio al momento del cometimiento de los hechos, o si se encontraban ebrios o intoxicados de acuerdo con los requisitos legales establecidos en el COIP.

Concurso ideal de infracciones

En este proyecto de integración curricular no se busca analizar el ex post, sin embargo, cabe mencionar la posibilidad de un concurso ideal de infracciones que ejemplifique la posibilidad de sancionar y que el caso Novaestrat no quede en la impunidad.

Tanto el delito de violación a la intimidad como el de revelación ilegal de bases de datos son delitos de resultado, ya que implican una consecuencia de la actividad, en el primero la

violación a la intimidad y en el segundo la violación a la intimidad, secreto y privacidad. En este tipo de delitos debe "mediar una relación de causalidad entre la acción y el resultado, es decir, una relación que permita, ya en el ámbito objetivo, la imputación del resultado producido al autor de la conducta" (Muñoz y García, 2010, p.226).

Cuando un solo hecho, por un solo hecho se entiende un único, compacto, consolidado, una sola manifestación de la voluntad, de como resultado la comisión de varios tipos penales se conoce como concurso ideal de infracciones. Ya que los fines de esa manifestación de voluntad pueden ser varios.

Por consiguiente, si se determinase que efectivamente se ha llegado a infringir tanto el tipo penal de violación a la intimidad, así como el tipo penal de revelación ilegal de base de datos, y que el autor tenía al mismo tiempo el fin de acceder, publicar los datos y al mismo tiempo revelar la información. En este caso el hecho único del Data Breach o filtración de datos personales que ocurre en Novaestrat, que se hubiese dado con fines de acceder, publicar (etc.) los datos y revelar la información registrada, constituiría tanto una violación a la intimidad como una revelación de base de datos, dándose ambos tipos penales a causa de un solo hecho, e imponiéndose tal como señala el COIP, la pena de la infracción más grave en este caso cinco años.

Conclusiones y recomendaciones

En el caso de que ocurra una filtración de datos o data breach provocada por un incidente o falta de medidas de protección, la Ley Orgánica de Protección de Datos Personales es un mecanismo jurídico eficiente que establece lineamientos claros que el responsable y encargado de protección de datos personales deben cumplir, así como un régimen administrativo sancionador frente a las vulneraciones de datos, y la disposición de aplicar diversos tipos de medidas técnicas y organizativas para prevenir incidentes de seguridad.

Si bien el habeas data, desde el punto de vista de la protección de datos personales, permite ser es un mecanismo efectivo de protección de estos al permitir su acceso, conocer su uso o destino, así como pedir la respectiva modificación, eliminación, anulación o actualización de los datos personales a las instituciones públicas o privadas donde se almacenen. En el caso de un Data Breach, este mecanismo de protección no permite prevenir, notificar o sancionar a los responsables, no permite enfrentarse o prevenir los incidentes informáticos por lo que su campo de acción se centraría únicamente en los datos personales antes de la ocurrencia del fenómeno informático.

Para que se pueda hacer efectiva le Ley de Protección de Datos Personales y se pueda garantizar el principio de seguridad de la información, la confidencialidad, integridad y disponibilidad de los datos personales, y hacer frente a un Data Breach o filtración de datos personales y que se sancione a los responsables y encargados, es necesario que se designe a la Autoridad de Protección de Datos personales, en este caso al Superintendente de Protección de Datos Personales.

Para que se protejan los datos personales de forma integral y así evitar filtraciones de datos se necesita de un sistema de protección integral de datos personales por lo que son necesarios mecanismos adicionales como la Convención 108+ del Consejo de Europa que permita la cooperación internacional y aplicación de medidas de acción, tanto en la prevención, como asistencia, y seguridad de los datos frente al Data Breach.

Se podría crear un centro especializado que permita salvaguardar la confidencialidad, integridad y disponibilidad de datos personales, responder frente a emergencias cibernéticas, investigar causas, consecuencias y el origen de las filtraciones de datos personales. Adicionalmente dentro de cada empresa privada se podría contar con un SOC es decir un centro de operaciones de ciberseguridad para mantener, planificar, manejar el almacenamiento en bases de datos, servicios en la nube entre otros, con un equipo multidisciplinario y así lidiar con las filtraciones de datos personales y prevenir sanciones.

El caso Novaestrat, sí podría derivar en responsabilidad penal por el delito de violación a la intimidad o revelación ilegal de bases de datos, si se cumplen con los elementos descritos en el segundo tema de esta tesis, es decir que la conducta sea típica, antijurídica y culpable, además de desvirtuar causas de justificación y de exclusión de la culpabilidad. El caso Novaestrat puede dar lugar a un concurso ideal de infracciones por los delitos los delitos de violación a la intimidad y revelación ilegal de bases de datos. Se recomienda que se prosiga con el procedimiento en el caso Novaestrat ya que tan solo falta un año para la prescripción de la acción en el delito por el cual se estuvo siguiendo la investigación previa que es el delito de violación a la intimidad.

Referencias bibliográficas

Araujo, P. (2020). *La Teoría del Delito, elementos de todos los delitos y su importancia.* CONDUCTA DE RELEVANCIA PENAL. Recuperado de https://www.youtube.com/watch?v=0VaCR_V5a7Q

Agencia Nacional Postal ANP. (2013). *No. 18-DE-ANP-2013*. Recuperado de https://regulacion.mintel.gob.ec/wp-content/uploads/2013/07/REFORMA-AL-REGLAMENTO-DE-ENVIO-DE-INFORMACION-DE-OPERADORES-POSTALES-PARA-EL-REGISTRO-ESTADISTICO-NACIONAL-REFERENTE-AL-MERCADO-POSTAL.pdf

Novaestrat. (2019). *Novaestrat, Información, Análisis y Tecnología*. Archive Today. Recuperado de https://archive.is/K61ZH#selection-1029.1-1029.1649

Asamblea General de las Naciones Unidas. (1948). *La Declaración Universal de Derechos Humanos*. Recuperado de https://www.un.org/es/about-us/universal-declaration-of-human-rights#:~:text=Art%C3%ADculo%2012,contra%20tales%20injerencias%20o%20ataques.

Asamblea Nacional del Ecuador. Ley 67. Ley de comercio electrónico, firmas y mensajes de datos. (29 de abril de 2013). R.O. 16 de mayo de 2013

Asamblea Nacional del Ecuador. Código Orgánico Integral Penal (COIP). (septiembre 2019). R.O. 3 de febrero del 2014

Asamblea Nacional del Ecuador. Código Orgánico Integral Penal (COIP). (marzo 2023). R.O. 3 de febrero del 2014

Asamblea Nacional del Ecuador. Constitución de la República del Ecuador (CE). (26 de enero del 2021). R.O 25 de julio del 2008

Asamblea Nacional del Ecuador. Ley Orgánica de Protección de Datos Personales (LOPDP). (21 de mayo de 2021). R.O. 459 de 26 de mayo de 2021.

Asamblea Nacional del Ecuador. Ley Orgánica de Telecomunicaciones (LOT). (diciembre 2022). R.O.10 de febrero del 2015

Atico34, G. (2022). *Análisis de Riesgos en la Protección de Datos*. Recuperado de https://protecciondatos-lopd.com/empresas/analisis-riesgos/#Que_es_un_analisis_de_riesgos_en_proteccion_de_datos

Bernate, F. (2007). *Delitos de falsedad en estados financieros*. Recuperado de https://www.google.com.ec/books/edition/Delitos_de_falsedad_en_estados_financier/1kVfDRIHvrgC?hl=es-419&gbpv=0

Catalán, F. (2022). *Comparativa entre la normativa de Protección de Datos Personales en Chile y el Reglamento General de Datos de la Unión Europea* (Tesis). Universidad Alberto Hurtado. Recuperado de https://repositorio.uahurtado.cl/bitstream/handle/11242/26617/ADM_Catal%c3%a1n.pdf?sequence=1&isAllowed=y

Cheng, L., Liu F., y Dafeng D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowlege Discovery*, volumen 7 (5) (p. 1). DOI: 10.1002/widm.1211

Collantes, L. (s.f). *Crímenes de derecho internacional y la justicia penal de los Estados.* Recuperado de https://vlex.puce.elogim.com/#/search/jurisdiction:EC/principio+de+extraterritorialidad/vid/crimenes-derecho-internacional-penal-382226890

Comisión Especializada Permanente de Soberanía, Integración Relaciones Internacionales y Seguridad Integral. (2021). *Informe para dar cumplimiento a la resolución del pleno de la Asamblea Nacional de 17 de septiembre de 2019.* Quito. Asamblea Nacional

Comision Europea. (2019). What is a data breach and what do we have to do in case of a data breach? *Obligaciones* .Recuperado de https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en

Comisión Europea. (s.f). *¿Qué es un responsable o encargado del tratamiento?* Recuperado de https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_es

Comité Jurídico Interamericano (CJI). (2021). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. *Departamento de Derecho Internacional.* Recuperado de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Consejo de Europa. (2007). *Proyecto sobre criminalidad.* Recuperado de https://rm.coe.int/16803042f3

Consejo de Europa. (1981). *Convenio Para La Protección De Las Personas Con Respecto Al Tratamiento Automatizado De Datos De Carácter Personal*. No.108. Recuperado de https://rm.coe.int/16806c1abd

Consejo de Europa. (2018). Convención 108+. Convención para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. Recuperado de https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Consejo de Europa. (2021). *El Convenio 108 + para proteger los datos personales también en América Latina.* Recuperado de https://www.coe.int/es/web/data-protection/-/convention-108-to-protect-personal-data-also-in-latin-america

Corte Constitucional .(7 de julio del 2021) *Sentencia No. 89-19-JD/21* [MP Agustín Grijalva] Recuperado de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic2MWI1ZDhiMy1iYmE1LTRhN2UtOWZjNS02NzM1ZWFiMzVlNTYucGRmJ30

Corte Constitucional .(23 de abril de 2014*) Sentencia No.001-14-PJO-CC* [MP Patricio Pazmiño] Recuperado de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J2FsZnJlc2NvJywgdXVpZDonYmU3ZGE3NjMtZjQ1OC00ZmVmLWFhYzYtOWZhODg2NjUxYjU2LnBkZid9

Corte Constitucional. (8 de julio del 2020) *Sentencia No. 1868-13-EP/20* [MP Kala Andrade] Recuperado de (http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOicyNzE4ZjljZC1hZjU4LTQxMTItYjBkYi01MjVlYmUwNDU2ZjgucGRmJ30

Edx. (2020). Gobierno Digital. *Ciberseguridad: el rol gubernamental*. Recuperado de https://courses.edx.org/assets/courseware/v1/3d031ea7c44e4f6c44bb52afe5112400/asset-v1:IDBx+IDB31x+1T2020+type@asset+block/2.4.2_Ciberseguridad_el_rol_gubernamental.pdf

European Union Agencie for Cybersecuity ENISA. (2020). Filtración de información. *Panorama de Amenazas de la ENISA.* Recuperado de https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-information-leakage-ebook-en-es.pdf

Fernández, E., Vallejo, M., y Pérez, P. (2017). Penas, medidas y otras consecuencias jurídicas del delito (1.a ed.). Dykinson, S.L. DOI: https://doi.org/10.2307/j.ctt1zgwjd8

Fiscalía General del Estado. (2019). *Fiscalía lidera operativo por presunta violación a la intimidad.* Boletín de Prensa FGE No. 381-DC-2019 Recuperado de https://www.fiscalia.gob.ec/fiscalia-lidera-operativo-por-presunta-violacion-a-la-intimidad/

Fiscalía General del Estado. (2019). *Fiscalía realizó la toma de versión de directivos de Novaestrat.* Boletín de Prensa FGE No.383-DC-2019.Recuperado de https://www.fiscalia.gob.ec/fiscalia-realizo-la-toma-de-version-de-directivos-de-novaestrat/

Fiscalía General del Estado. (2014). *Guía para Actuaciones del Fiscal dentro del Código Orgánico Integral Penal.* Recuperado de https://www.fiscalia.gob.ec/pdf/escuela-fiscales/GUIA-COIP.pdf

Fuente, F. (1989). Revista de Derecho de la Universidad Católica de Valparaíso. Sobre el concepto de responsabilidad criminal en nuestro código penal, 2 (13), (pp.118-121). Recuperado de http://www.rdpucv.cl/index.php/rderecho/article/download/234/215.

Grupo 6. (2007). *Dictamen 4/2007 sobre el concepto de datos personales.* Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Identity Theft. (2022). *Data Breach Report.* Recuperado de https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

International Business Machine Corporation IBM. (2022). *Cost of a Data Breach Report.* Recuperado de https://www.ibm.com/downloads/cas/3R8N1DZJ

Kierszenbaum, M. (2009). *El bien jurídico en el derecho penal. Algunas nociones básicas desde la óptica de la discusión actual.* Recuperado de http://www.derecho.uba.ar/publicaciones/lye/revistas/86/07-ensayo-kierszenbaum.pdf

Kim, P. (2017). *Sujetos y Objetos de delito.* Recuperado de https://gc.scalahed.com/recursos/files/r161r/w19856w/sujetos_objetos_delito.pdf

Mas, M y Blanc, C. (2018). *La responsabilidad legal frente al ciberataque.* Recuperado de https://www.garrigues.com/sites/default/files/documents/20180517-la-responsabilidad-legal-frente-al-ciberataque-palma.pdf

Menéndez, N. (2017). *El descubrimiento y la revelación de secretos* (Tesis de grado). Universidad de León. Recuperado de https://buleria.unileon.es/bitstream/handle/10612/9895/Men%E9ndez%20P%E9rez,%20Noelia.pdf;jsessionid=8151F8BE6F2BB4359C3E40BE182F3ABE?sequence=1

Muñoz, C. (1999). *Teoría General del Delito*. Recuperado de https://www.sijufor.org/uploads/1/2/0/5/120589378/06_mu%C3%91oz_conde_t_del_delito.pdf

Muñoz, C. (2014). *Derecho Penal: Parte General*. 8va edición. Valencia, España Editorial Tirant lo Blanch

Muñoz, C y García, A. (2010). *Derecho Penal Parte General.* Recuperado de https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2020). *Serie de Módulos Universitarios: Delitos Cibernéticos.* Módulo 10: Privacidad y Protección de Datos. Recuperado de **https://www.unodc.org/e4j/es/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html**

PLAN, V (2019). *La peor filtración de datos en la historia del Ecuador al descubierto.* Recuperado de https://www.planv.com.ec/historias/sociedad/la-peor-filtracion-datos-la-historia-del-ecuador-al-descubierto

Polo, A. (2021). *Datos, Datos, Datos: El Dato Personal, El Dato No Personal, El Dato Personal Compuesto, La Anonimización, La Pertenencia del Dato y otras cuestiones sobre datos.* Recuperado de https://revista-estudios.revistas.deusto.es/article/view/2149/2594

Real Academia de la Lengua Española (RAE). (2023). *Diccionario de la lengua española.* Recuperado de http://dle.rae.es/retener

Real Academia de la Lengua Española (RAE). (2023). *Diccionario de la lengua española.* Recuperado de https://dpej.rae.es/lema/tempus-regit-actum

Real Academia de la Lengua Española (RAE). (2023). *Diccionario de la lengua española.* Recuperado de https://dle.rae.es/revelar?m=form

Rodríguez, L. (2011). Naturaleza y fundamento de las circunstancias modificatorias de la responsabilidad criminal. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, volumen 36* (p.2). DOI: http://dx.doi.org/10.4067/S0718-68512011000100011

Rosas, G. y Pila, G. (2023). La protección de datos personales en Ecuador. *Una revisión histórica-normativa de este derecho fundamental en el país suramericano*, volumen 10 (4568). DOI: https://doi.org/10.37467/revvisual.v10.4568

Ruiz, E. (1996). *Responsabilidad Penal en Materia de Informática.* Recuperado de https://dialnet.unirioja.es/descarga/articulo/248765.pdf.

Sagan, C (1994). 25 Years Ago: Carl Sagan Warns of the Risks of Scientific Ignorance. *Words of Wisdom*. Recuperado de https://bigthink.com/words-of-wisdom/carl-sagan-warned-us-about-the-risks-of-scientific-ignorance-25-years-ago/

Sagredo, F. y Nuño, V. (1994). En los orígenes de la Biblioteconomía y Documentación: Ebla. Recuperado de https://revistas.ucm.es/index.php/DCIN/article/viewFile/DCIN9494110123A/20046

Salcedo, M., Cardona, S., Gutiérrez, M. (2010). *La calidad del dato en los sistemas de información.* Recuperado de https://bibliotecadigital.univalle.edu.co/bitstream/handle/10893/18907/La_calidad_del_dato.pdf?sequence=1

Santillán, F. y Bayardo, H. (2020). La imputabilidad por trastorno mental en el Código Orgánico Integral Penal. *Axioma.* (23) DOI: https://doi.org/10.26621/XVI23.2020.12.A05.PUCESI.2550.6684 Recuperado de http://axioma.pucesi.edu.ec/index.php/axioma/article/view/624/554

Sanz, E et al. (2021). *Tratado de Delincuencia Cibernética,* Navarra, país: España: Aranzadi

Serrano, R. (2020). Análisis del Proyecto de Ley de Protección de Datos Personales. *Conferencia de la Cámara de Comercio Ecuatoriano Americana.* Guayaquil, Ecuador. Recuperado de https://revistas.usfq.edu.ec/index.php/lawreview/article/view/2184/3026

Sierra, M. y Salvador, A. (2005) Lecciones de Derecho penal: parte general. Bahía Blanca: Univ. Nacional del Sur: Ediuns

Silvestri, J. (2012). *Derecho procesal penal.* Buenos Aires, Argentina. Editorial Abeledo-Perrrot

Tribunal Superior del Distrito Judicial de Bogotá (13 de abril del 2021) Sentencia *No. 11001650019220170608O-01 1* [MP Jaime Velasco] Recuperado de https://www.bmoabogados.com/wp-content/uploads/2021/04/Sentencia-Legi%CC%81tima-Defensa-Violencia-Intrafamiliar.pdf

Vaca, R. (2005). La responsabilidad penal. *Derecho Ecuador*. Recuperado de https://derechoecuador.com/la-responsabilidad-penal/

Vega, H. (2016). El análisis gramatical del tipo penal. *Justicia*, 29, (53) DOI: http://dx.doi.org/10.17081/just.21.29.1233

Verizon. (2022). *Data breach investigations Report*. Recuperado de https://www.verizon.com/business/resources/Tff8/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Vivanco, P. (2015). *"La investigación previa y el principio de oportunidad en el Código Orgánico de la Función Judicial"*. Anuario de Derecho Penal y Ciencias Penales, 68(2), pp. 755

vpnMentor. (2019). *Report: Ecuadorian Breach Reveals Sensitive Personal Data*. Recuperado de https://www.vpnmentor.com/blog/report-ecuador-leak/#How-and-Why-We-Discovered-the-Breach