UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

"LA REVELACIÓN ILEGAL DE BASE DE DATOS EN EL DERECHO COMPARADO"

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA

AUTOR: MADISSON DAYANA CORONEL AÑAZCO

DIRECTOR: AB. FANY QUINTEROS G, Mgtr

Yo me gradué en los 50 años de la Cato!

LA TRONCAL – ECUADOR

2020

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

LA REVELACIÓN ILEGAL DE BASE DE DATOS EN EL DERECHO COMPARADO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA

AUTOR: MADISSON DAYANA CORONEL AÑAZCO

DIRECTOR: AB. FANY QUINTEROS GONZÁLEZ, Mgtr.

AÑO: 2020

Yo me gradué en los 50 años de la Cato!

Universidad Católica de Cuenca

REPÚBLICA DEL ECUADOR

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TITULO: "LA REVELACIÓN ILEGAL DE BASE DE DATOS EN EL DERECHO COMPARADO".

Trabajo de Investigación previo a la obtención del Título de Abogado de los Tribunales de Justicia de la República.

AUTOR: MADISSON DAYANA CORONEL AÑAZCO
Número de cédula: :0942251430

TUTOR: AB. FANY QUINTEROS GONZÁLEZ, Mgtr.

AÑO: 2020

CONTENIDO

ACEPTACIÓN DEL TUTOR

CERTIFICÓ

Que, el presente Trabajo de Investigación realizado por la señorita MADISSON DAYANA CORONEL AÑAZCO de la carrera de Derecho Extensión La Troncal, ha sido orientado, corregido y revisado minuciosamente por lo que declaro APROBADO.

En calidad de tutor de grado, doy fe que dicho trabajo reúne todos los requisitos y méritos suficientes para ser sometido a presentación pública y evaluación por parte del jurado examinador que se designe, dando mi aprobación respectiva para que la señorita MADISSON DAYANA CORONEL AÑAZCO pueda optar por el título de Abogado.

La Troncal, 12 de Marzo de 2021

Ab. xxxxxx, Mg.

DOCENTE TUTOR

DECLARACIÓN DE AUTORÍA

Yo, MADISSON DAYANA CORONEL AÑAZCO declaro bajo juramento que, las ideas, conceptos, procedimientos y resultados del trabajo aquí descrito son de mi autoría, que no han sido previamente procesados para ningún grado ni calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN LA TRONCAL, según lo establecido por la ley de propiedad intelectual, por su reglamento y por la normativa institucional vigente.

MADISSON DAYANA CORONEL AÑAZCO

AUTORA

Dedicatoria

Dedico a mis padres por estar a mi lado apoyándome siempre, por creer en mí y dirigirme para que alcance mi meta.

Gracias por ser la luz que ilumina mi vida, dándome fuerzas para superarme día a día.

A mis Hermanos, tíos gracias por estar siempre a mi lado y por ser la familia que somos.

Agradecimiento

Mi Agradecimiento especial, a mi padre JIMMY CORONEL ORTIZ por su apoyo incondicional.

También a la Universidad Católica de Cuenca `por abrirme sus puertas y darme la oportunidad de superarme profesionalmente.

Resumen

El estudio sobre revelación ilegal de base de datos en el Derecho comparado entre España y Argentina. El estudio tiene como finalidad analizar de manera detallada los delitos informáticos en el Ecuador, en vista de que este delito utiliza una nueva modalidad para cometer delitos que perjudican a la sociedad.

Para lograr este objetivo se analizará el Artículo 229 inciso 2 sobre la Revelación ilegal de base de datos, señalado en el Código Orgánico Integral Penal. Considerando que este tipo de delito se produce cuando el titular o un tercero revelan datos o información registrada en ficheros, archivos, o bases de datos personales que se encuentran en instituciones públicas o privadas

Considerando que este tipo de delitos se dan en todos los países del mundo se realizará un análisis comparativo con Argentina y España, con la finalidad de dar mayor realce al estudio y sobre todo conocer más a profundidad la problemática del estudio.

Palabras clave:

(Revelación ilegal de base de datos – Derecho comparado España – Argentina)

Abstract

The study on illegal disclosure of database in the comparative law between Spain and Argentina. The study aims to analyze in detail the computer crimes in Ecuador, in view of the fact that this crime uses a new modality to commit crimes that harm society.

To achieve this objective, Article 229 paragraph 2 on the Illegal disclosure of database, indicated in the Organic Integral Penal Code, will be analyzed. Whereas this type of crime occurs when the owner or a third party discloses data or information recorded in files, archives, or personal databases held in public or private institutions.

Considering that this type of crime occurs in all countries of the world, a comparative analysis will be made with Argentina and Spain, in order to give more prominence to the study and above all to know more in depth the problems of the study.

Key words:

(Illegal disclosure of database - Comparative law - Spain – Argentina)

INTRODUCCIÓN

El estudio trata sobre la revelación ilegal de base de datos en el Derecho Comparado. El objetivo del estudio es dar a conocer a la ciudadanía la importancia del estudio en vista de que en la actualidad el delito informático se ha expandido debido a los grandes avances tecnológicos, lo cual facilita para que personas con malas intenciones ingresen con sus datos personales para cometer actividades ilícitas.

En este sentido la revelación ilegal de base de datos es un delito se ha expandido en todos los países de América Latina y del mundo provocando graves daños intangibles a los recursos ya sean públicos o privados.

En el Ecuador la revelación ilegal de base de datos no es un caso aislado, ya que se trata de una nueva forma para delinquir, donde personas expertas en el manejo de la tecnología se aprovechan de sus conocimientos para delinquir Es así como en nuestro medio es muy común escuchar que personas inescrupulosas hacen uso de los datos personales de las personas para cometer hechos delincuenciales.

A través del uso de la tecnología los delincuentes pueden cometer un acto ilegal desde cualquier país del mundo. De allí la importancia del estudio sobre la revelación ilegal de base de datos en el Derecho Comparado con países como España y Argentina.

CAPÍTULO I

1. ANTECEDENTES

1.1. Antecedentes

La revelación ilegal de base de datos se refiere a los delitos informáticos, los cuales violan los derechos constitucionales de los ciudadanos. Es importante considerar que usualmente los delitos informáticos se generan por la utilización de las TIC, tecnologías de la información y comunicación, correo electrónico, transacciones financieras, comercio electrónico, y las redes sociales. Lo cual es aprovechado por los ciber-delincuentes para cometer delitos como fraudes informáticos, falsificación de documentos, estafa, sabotaje, robo de identidad, utilización de información no autorizada, entre otros.

Los delitos informáticos se realizan a través de una computadora, por medio del Internet lo cual facilita para que estos delitos no puedan ser identificados y descubrir a los autores intelectuales, razón por la cual muchos de estos delitos quedan en la impunidad, los cuales son mucho más frecuentes y sobre todo cada vez mucho más sofisticados

En la actualidad existen leyes, cuyo objetivo es proteger integralmente a los sistemas que utilizan tecnologías de información, a fin de prevenir y

sancionar este tipo de delitos. Sin embargo con la finalidad de proteger este derecho de los ecuatorianos la Constitución de la República en el Art. 66 señala el derecho a la protección de datos de carácter personal tiene como influencia el poder del Estado de garantizar y optar por herramientas jurídicas que aseguren la seguridad y la privacidad de los mismos (Constitución de la República del Ecuador, 2008).

De acuerdo a lo anotado anteriormente es responsabilidad del Estado garantizar la seguridad jurídica que proteja y asegure la confidencialidad de los datos de los ciudadanos, mediante la aplicación de leyes y sanciones que permitan la protección de los datos de carácter personal y en el ámbito público.

Igualmente en el Artículo 229 del Código Orgánico Integral Penal, consta la sanción a las personas que revele información registrada, contenida en ficheros, archivos, bases de datos que se encuentren en sistemas electrónicos, informáticos, telemáticos 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. Igualmente señala que si este delito es cometido por un o una servidora pública la sanción privativa será de tres a cinco años (Código Orgánico Integral Penal, 2014)

En el Ecuador de acuerdo a datos proporcionados por la Policía Judicial del Ecuador se han registrado casos de delitos informáticos a partir del 2010, se registraron varias denuncias por la vulneración de páginas de

servicio público, páginas de servicio privado y por estafa utilizando medios informáticos. En el año 2011, la Fiscalía General del Estado reporta 3.662 delitos informáticos (Revelo, 2016).

En el año 2012 se reportó 2721 casos de delitos informáticos en las provincias de Pichincha, Guayas y Santa Elena, de estos 17 tuvieron dictamen acusatorio, 11 dictamen absolutorio, 105 casos fueron de falsificación electrónica esto debido a que los consejos de seguridad que dieron las instituciones del Estado, al igual que en la banca privada para que los ciudadanos se mantengan alertas para evitar que los delincuentes cometan delitos.

En el año 2013, se registraron daños informáticos al servicio privado, daños informáticos al sector público, apropiación ilícita por medios electrónicos. En el año 2014 se reportaron los siguientes casos 136 casos de falsificación electrónica, 1704 casos suplantación de identidad por medios electrónicos. Así mismo se reportaron casos de suplantación de identidad a través de medios informáticos, sobre todo en redes sociales, como Facebook y Twitter. (Fiscalía General del Estado de Ecuador, 2014)

1.2. Revelación ilegal de base de datos

En el Ecuador el delito informático es catalogado como una nueva tendencia para la comisión de delitos en la sociedad, esto es utilizar la informática con ánimo doloso (Iriarte Ahon, 2005)

De acuerdo a esta definición el delito informático puede ser culposo y al mismo tiempo doloso. En vista de que el delito informático o ciberdelito, es considerado como toda acción antijurídica y culpable, que se da aprovechando las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

En este aspecto la revelación ilegal de base de datos tiene que ver con la violación de información confidencial que se encuentra en una base de datos u otro similar. Este delito es un agravante cuando es cometido por un servidor público o colaboradores de instituciones bancarias que realicen intermediación financiera o contratistas, en este caso la pena privativa de libertad es de tres a cinco años. (Código Orgánico Integral Penal, 2014)

Del mismo modo la revelación ilegal de base de datos se encuentra tipificada en el Código Orgánico Integral Penal en la Sección Tercera en los Artículos 229, 230, 231, 232, 233 y 234.

1.3. Sanciones por la revelación ilegal de base de datos

El Código Orgánico Integral Penal sanciona los delitos que se encuentran relacionados con la revelación ilegal de base de datos que se encuentran tipificados en los siguientes artículos:

1.3.1. Artículo 229. Inciso 2 .Revelación ilegal de base de datos (COIP)

En este sentido el Art. 229, trata sobre la revelación ilegal de base de datos este tipo de delito se da cuando 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 (Código Orgánico Integral Penal, 2014).

Este Artículo además aclara que 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.

En este sentido la Constitución de la República del Ecuador en el Art. 66.- Derechos de libertad, señala que se reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (Constitución de la República, 2016).

El sustento legal al derecho a la protección de datos de carácter personal del numeral 19 del Art. 66 de la Constitución de la República, está

en el Art 178 (violación a la intimidad) y 180 (difusión de información de circulación restringida).

1.3.2. Artículo 230. Interceptación ilegal de datos

El Artículo 230, se refiere a la interceptación ilegal de datos, lo cual se puede dar cuando la persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible (Código Orgánico Integral Penal, 2014).

Además aclara que cuando la persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

Por otra parte señala que la persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

Del mismo modo menciona que la persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior, será

sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014).

1.3.3. Artículo 231. Transferencia electrónica de activo patrimonial

Al mismo tiempo el Artículo 231, se refiere a la transferencia electrónica de activo patrimonial, este tipo de delito se puede dar cuando la persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014).

Además será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

1.3.4. Artículo 232. Ataque a la integridad de sistemas informáticos

En este sentido el Artículo 232, que está relacionado con el ataque a la integridad de sistemas informáticos, significa que la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o

de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014).

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

Así mismo se condena a la persona que destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

1.3.5. Artículo 233. Delitos contra la información pública reservada legalmente

En este sentido el Artículo 233, sobre delitos contra la información pública reservada legalmente, señala que la persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionado con pena privativa de libertad de cinco a siete años (Código Orgánico Integral Penal, 2014).

Del mismo modo este artículo aclara que cuando la o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

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

1.3.6. Artículo 234. La persona que sin autorización acceda al sistema informático o sistema telemático o de comunicaciones

Por otra parte el Art. 234, sanciona a la persona que sin autorización acceda ya sea de forma total o parcial a un sistema informático o sistema telemático o de telecomunicaciones, o que se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz, será sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, 2014).

1.3.7. Artículo 190. Este artículo hace referencia a la apropiación fraudulenta de medios electrónicos.

Igualmente este artículo menciona a los fraudes que realizan los delincuentes informáticos por medios electrónicos, a fin de apropiarse de un bien ajeno, tal es el caso de transferencias de cuentas bancarias no consentidas, este delito es cometido de forma virtual, el cual es sancionado con pena privativa de libertad de hasta tres años (Código Orgánico Integral Penal, 2014).

1.4. Delitos informáticos

En la actualidad la sociedad ha logrado grandes avances gracias a la tecnología, sin embargo los delincuentes también se han beneficiado debido a las grandes facilidades que la tecnología ofrece para cometer delitos desde cualquier parte del planeta los cuales generan grandes pérdidas económicas tanto en la sociedad como en las empresas y los gobiernos.

Telléz Valdes Julio (2019), define al delito informático como aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio. Del mismo modo el profesor chileno Renato Jijena Leiva (2016), menciona que un delito informático es toda acción típica, antijurídica o culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información cometida en un sistema de tratamiento automatizado de la misma.

Para el Dr. Santiago Acurio del Pino (2010), el delito informático es un término que está relacionado con la delincuencia informática para referirse a ellos, indicando que este es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir o manipular cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera.

Existen varios tipos de delitos informáticos los cuales se dan a través de las plataformas informáticas y medios electrónicos, estos son:

- Ataques contra sistemas y datos informáticos
- Usurpación de identidad
- Distribución de imágenes de agresiones sexuales contra menores
- Estafas por medio de Internet
- Intrusión en servicios financieros en línea
- Difusión de virus
- Chantaje informático
- Violación de correo electrónico
- Falsificación de documentos electrónicos (Cuenca Espinosa, 2016).

1.4.1. Fraude informático

De hecho uno de los delitos de mayor frecuencia es el fraude informático, este tipo de delito lo realizan en los cajeros automáticos mediante la

falsificación de instrucciones para el ordenador en la fase de adquisición de datos. Del mismo modo este tipo de delitos se los hace mediante el uso de tarjetas bancarias robadas, al igual que usan equipos y programas de computador especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito (Herrera Avila, 2010)

Del mismo modo el fraude informático lo realizan con la inserción de sistemas informáticos, adaptados a la estructura original de los cajeros automáticos con la finalidad de receptar información de la tarjeta de debido o de crédito alterando el sistema e inutilizando la funcionalidad del legitima del mismo.

1.4.2. Daño Informático

De la misma manera ocurre con el daño de los delitos informáticos los cuales se traducen en la afectación material y real de la información lógica de los sistemas informáticos. Así mismo dañar significa que el delincuente altera el funcionamiento de dichos sistemas lo cual provoca daños severos en el software como en el hardware (Espinoza Jurado, 2019).

1.4.3. Daño informático al software

Tal como ocurre en el año informático, se produce un daño en el software, lo cual ocasiona que los datos se cancelen, se borre toda la información, y se inutilice las conductas que deben ser consideradas como punibles.

De igual forma este delito es considerado como el de mayor gravedad puesto que se puede ver afectado el sistema informático en su parte material física la cual puede ser recuperada, sin embargo existen otros casos en los que se vuelve irreversible el daño del software.

1.4.4. Introducción de datos faltos

De igual modo sucede con el delito de introducción de datos falsos, lo cual altera la modificación de datos constantes en programas de instituciones financieras, públicas, privadas y otras dependencias que contengan información en bases de datos borrando, suprimiendo e introduciendo información falsa.

De hecho la introducción de datos falsos es una manipulación de datos de entrada al ordenador con el fin de producir y lograr movimientos falsos en transacciones de una empresa para solvencia moral y económica a una persona que no la tiene. Este delito también lo cometen para publicar datos reservados de personas, entidades religiosas y políticas.

1.4.5. Caballo de Troya

Del mismo modo este tipo de delito es utilizado por los delincuentes para manipular los sistemas informáticos, lo realizan por medio de rutinas cronológicas predeterminadas que se presentan como acciones no autorizadas por el propietario del sistema.

1.4.6. Recogida de información residual

Asimismo está técnica se caracteriza porque el delincuente se aprovecha de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. De hecho se puede aprovechar de los datos que se encuentran en las papeleras de reciclaje, tomando la información residual que se encuentra en la memoria o en soportes magnéticos.

Usualmente al utilizar esta técnica se puede recabar información que se encuentran en las impresoras, ya que estas registran un historial de datos los cuales pueden ser utilizados con fines delictivos ya que les permite acceder a información de empresas públicas y privadas.

1.4.7. Técnica del salami

De la misma manera esta modalidad de fraude informático es utilizada para introducirse al programa de instituciones públicas o privadas para tener acceso a la determinada cuenta los centavos de muchas cuentas corrientes de los clientes y se aprovechan para recabar cantidades de dinero muy pequeñas se van sacando repetidamente de una cuenta para luego transferir a otra.

1.4.8. Llave no autorizada

Cabe destacar que esta técnica llamada también súperzap o llame maestra es utilizada para tener acceso a los sistemas informáticos, aun cuando se

encuentren con sistemas de seguridad. Al utilizar este programa el delincuente informático puede dañar, alterar y modificar la información que él desee.

1.4.9. Puertas falsas

Sin lugar a dudas está técnica llamada puertas falsas permite introducir irrupciones en los programas para chequear procesos complejos, lo cual permite alterar los comandos de funcionalidad del sistema informático, creando accesos aparentemente legítimos que son imperceptibles por el usuario o propietario del sistema.

1.4.10. Bombas lógicas o cronológicas

Sin lugar a dudas está técnica es la más peligrosa ya que permite que el delincuente informático cometa algunos delitos tradicionales como por ejemplo extorsionar al gerente de una empresa para que le entregue una cierta cantidad de dinero, ya que puede contar con información muy importante de la empresa.

Evidentemente a esta técnica se la conoce como bomba de tiempo debido a que puede ocasionar graves problemas para la empresa en vista de que el delincuente informático puede ocasionar serios daños en el ordenador, distorsionar el funcionamiento del sistema paralizando el mismo. Esta técnica es muy difícil de detectarla antes de que explote (Espinoza Jurado, 2019)

1.4.11. Espionaje informático

Es necesario subrayar que este tipo de delito puede tener acceso directo a los datos más importantes de la empresa sea está pública o privada. Es necesario subrayar que este delito se encuentra tipificado en el Código Orgánico Integral Penal, ya que es considerado como un delito que atenta a la seguridad pública, tal como a las Fuerzas Armadas y la Policía Nacional ya que el servicio de inteligencia manejan información confidencial.

1.4.12. Sabotaje informático

Es de suma importancia analizar el sabotaje informático puesto que el Articulo 232 del Código Orgánico Integral Penal lo describe como daño, alteración, borrar, suspender, está técnica tiene como finalidad interrumpir y obstaculizar los sistemas informáticos. Es evidente que el sabotaje informático se lo puede realizar por medio de programas maliciosos como virus y gusanos.

1.5. Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales

La Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales, tiene como finalidad proteger el derecho fundamental que tienen todos los ciudadanos de proteger sus datos personales o privados. Es importante resaltar que esta Ley se basa en el

Artículo 17 numeral 1 del Pacto Internacional de Derechos Civiles y Políticos, el cual establece que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y reputación. Por otra parte el numeral 2 señala que toda persona tiene derecho a la protección de la ley.

El propósito de crear la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad, es proteger y garantizar el derecho de todas las personas a la intimidad y privacidad de sus datos personales, que se encuentran en la base de datos de los bancos, ficheros o archivos ya sea de forma física o digital (Asamblea Nacional del Ecuador, 2016).

En nuestro país se encuentran vigentes leyes y reglamentos que protegen los datos personales de los ciudadanos, tales como los siguientes:

Reglamento	Artículo	Descripción
Constitución de la República del Ecuador	Artículo 86 Numeral 19	Toda persona tiene derecho a la protección de sus datos personales Para la recolección, archivo, procesamiento, distribución o difusión de los datos deberán ser autorizados por el titular o por una orden judicial
	Art. 66	La finalidad es garantizar el derecho a

	Numeral 20	la intimidad de los ciudadanos y sus familiares (Constitución de la República del Ecuador, 2008)
Ley Orgánica de Transparencia y Acceso a la Información Pública	Artículo 2 Literal d	Esta Ley tiene como finalidad garantizar la protección de la información personal que se encuentre en poder del sector público o privado (Ley Orgánica de Transparencia y Acceso a la Información Pública , 2014)
Ley del Sistema Nacional de Registro de Datos Públicos	Artículo 6	Esta ley ampara la confidencialidad los datos personales tales como la ideología, la afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y demás datos personales.
Ley de Comercio electrónico, firmas y mensajes de datos	Artículo 9	Esta Ley brinda protección a los datos de transferencias o utilización de bases de datos, los cuales pueden ser publicados solo con la autorización del titular. (Congreso

	Artículo 178	Nacional, 2002) Violación a la intimidad, la persona que acceda, retenga, grave, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video de información confidencial sin la autorización legal , será sancionado con pena privativa de uno a tres años
Código Orgánico Integral Penal	Artículo 229	Revelación ilegal de datos La persona que con intención de aprovecharse revele información, registrada, contenida en ficheros, archivos, bases de datos electrónicos, informáticos o telemáticos violenten los derechos de intimidad y privacidad serán sancionados con pena privativa de uno a tres años. (Código Orgánico Integral Penal, 2014)

Fuente: (Zambrano Rendón, Morales Carrillo, Párraga Ríos, & Loor Vaca, 2019)

Cabe agregar que una vez analizadas estas normativas se puede observar que solamente el Código Orgánico Integral Penal presenta sanciones, mientras que las otras normativas no presentan ninguna sanción para las personas naturales o jurídicas que utilicen la base de datos de los ciudadanos.

1.6. Derecho Comparado entre España y Argentina

1.6.1. España

La legislación de España respecto al delito de revelación ilegal de base de datos, el Código Penal Español ha dividido este delito en tres grupos que son:

1. Suprimir, modificar o falsear datos, lo cual puede tener lugar en distintos momentos tal como el input, la ejecución del programa y en el autput.
2. La obtención y divulgación de secretos industriales, comerciales o personales o la manipulación de sistemas informáticos para producir resultados perjudiciales, su destrucción y la utilización no autorizada de una instalación informática
3. Los referidos a la obtención de programas sin la autorización del propietario (León Moncaleano, 2017).

1.6.2. Argentina

En la legislación Argentina el delito de la revelación ilegal de base de datos las acciones de protección de los datos personales y las sanciones. Se encuentra en:

1. En primer lugar se encuentra contemplado en el delito de grooming, que se refiere al contacto con menores por medios electrónicos con objetivos estrictamente sexuales.
2. El acceso sin el consentimiento a un sistema o dato informático de acceso restringido.
3. El daño de datos, programas o sistemas, la violación de la privacidad en comunicaciones electrónicas, la interrupción de comunicaciones electrónicas, etc.

También se han dictado normas, disposiciones y resoluciones con la finalidad de brindar protección y cuidado a la infraestructura de la información y ciberseguridad (Reyes Velázquez, Servín González, & Suñe Llinás, 2017).

Luego de analizar los delitos informáticos tanto en Ecuador, España y Argentina se puede notar que la tecnología es utilizada para llevar a cabo robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes, entre otros delitos. Sin embargo estos delitos en algunos casos son susceptibles de ser sancionados por el Derecho Penal, debido a la falta de pruebas

Al realizar el Derecho Comparado entre Ecuador, España y Argentina, se pudo notar que en los tres países las sanciones para aquellas personas que cometen el delito de revelación ilegal de base de datos son muy

similares además les exigen el pago de una multa por el daño causado a la víctima.

CAPÍTULO II

2. MARCO SITUACIONAL

En el estudio se utilizó el método bibliográfico, ya que permitió revisar estudios referentes al tema de estudio, además se empleó el método inductivo – deductivo, ya que en base a estos métodos se logró obtener la información necesaria para llevar a cabo el estudio sobre la revelación ilegal de base de datos en el Derecho Comparado, para lo cual se analizará el Artículo 229 del Código Orgánico Integral Penal, además se realizará un estudio comparado entre los países de España y Argentina

Tomando en cuenta que la protección de datos personales tiene como finalidad proteger el derecho privado de las personas, ya que estos tienen información personal, por esta razón son considerados datos sensibles, razón por la cual requieren de la máxima protección posible.

El estudio tiene como finalidad analizar a profundidad el tema de estudio, ya que el Art. 229 se encuentra tipificado en el Código Orgánico Integral Penal, al igual que las sanciones que reciben las personas que revelan información confidencial ya sea de las empresas, instituciones o Seguridad Nacional.

También se utilizó el método bibliográfico el cual permitió recabar información de varios autores, al igual que de las Constituciones de Ecuador,

España y Argentina, para sustentar el estudio. El método descriptivo permitió evaluar algunas características del tema de estudio lo cual permitirá plantear la propuesta referente al tema sobre la revelación ilegal de base de datos en el Derecho Comparado.

En lo que tiene que ver con el marco contextual de la presente investigación se puede notar que en el Ecuador la revelación ilegal de base de datos es un delito que se encuentra tipificado en el Código Orgánico Integral Penal

Considerando que en la actualidad el uso de la tecnología se ha convertido en una necesidad, ya que a través de esta se puede realizar cualquier tipo de gestión, ya sean estos personales, bancarios, comerciales, etc. Lo cual es visto como una oportunidad para cometer igualmente una gran variedad de delitos que perjudican a muchos ciudadanos, por lo tanto se considera que las sanciones deben ser acordes al cometimiento del tipo de delito que se cometa.

Los delitos informáticos por lo general son cometidos por una o varias personas que tienen conocimientos especializados para el uso de medios informáticos o telemáticos para infiltrarse en áreas electrónicas restringidas para beneficio propio y perjuicio de un tercero. Igualmente se han dados casos que las personas que laboran en instituciones ya sean estas públicas o privadas lo cual es aprovechado para infiltrarse en el sistema informático y adueñarse de los datos de otras personas con el objetivo de causar daño.

Código Orgánico Integral Penal

El Código Orgánico Integral Penal, debido al uso excesivo de sistemas informáticos, lo cual es aprovechado por los delincuentes para cometer delitos llamados informáticos, telemáticos o electrónicos los cuales se encuentran tipificados en los siguientes artículos:

De esta manera el Artículo 190. Trata sobre la apropiación fraudulenta un sistema informático o redes electrónicas y de telecomunicaciones con la finalidad de cometer el delito de apropiarse de bienes, valores o derechos de otras personas para fines personales, alterando, manipulando o modificando archivos que se encuentran en las redes electrónicas, será sancionada con pena privativa de libertad de uno a tres años.

Además aclara que será sancionado con la misma pena la persona que encubra o facilite el descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, violando de esta manera las seguridades electrónicas e informáticas personales de otras personas.

En el Ecuador los delitos informáticos se han incrementado, especialmente en el acceso no consentido a un sistema informático, seguido por el delito de ataque a la integridad de sistemas información, al igual que la interceptación y revelación ilegal de datos.

Derecho comparado

Los delitos informáticos se han incrementado a nivel mundial, ya que los delincuentes se aprovechan de las ventajas que ofrece la tecnología tal como

el Internet, que cuanta con una gran variedad de base de datos a los cuales pueden acceder personas que tienen conocimiento en el manejo de herramientas tecnológicas. Con la finalidad de analizar este tipo de delitos de manera mucho más detallada se ha realizado un análisis comparativo con países tal como España y Argentina.

España

En España los delitos informáticos han crecido de manera acelerada especialmente en las entidades bancarias, lo cual provocan desprestigio y desconfianza de los clientes, las llamadas por este tipo de delitos son muy altas, las denuncias son hechas generalmente por las víctimas sin embargo por la falta de pruebas contra el presunto autor las autoridades poco o nada pueden hacer. Fuente

En este país se calcula que los delitos informáticos ascienden a tres veces más que cualquier otro tipo de delito. En este aspecto el Código Penal Español contiene a los delitos informáticos en los apartados 2 y 3 del Artículo 197 bis.

1. La persona que por cualquier medio o procedimiento vulnere las medidas de seguridad establecidas para impedirlo y sin consentimiento acceda o facilite a otro el acceso a un sistema de información será sancionado con pena de prisión de seis meses a dos años.

2. La persona que utilice instrumentos técnicos y sin autorización intercepte transmisiones no públicas de datos informáticos será castigado con pena de prisión de tres meses a dos años (Codigo Penal Español, 2020)

- **El Art. 197 ter**.

  La persona que sin contar con la debida autorización produzca, adquiera o facilite a otro:, un programa informático, con la finalidad de cometer un delito, al igual que otorgue la contraseña de un ordenador o el código de acceso de datos a otra persona será castigado con pena de prisión de uno a tres años. (Codigo Penal Español, 2020)

  Además el Código Penal Español señala en el Artículo 197 quater. Si los hechos son cometidos en el seno de una organización o grupo criminal, las penas privativas de libertad serán superiores en grado.

Argentina

El Código Penal de Argentina ha incorporado distintas modalidades delictivas vinculadas con la revelación ilegal de base de datos.

- **El Artículo 153.** Señala que será reprimida con prisión de quince días a seis meses la persona que abra o acceda sin permiso a una comunicación electrónica, carta, pliego cerrado, teléfono u otros con la intención de apoderarse de forma indebida dicha información electrónica, será sancionado con pena privativa de un mes a un año, igualmente aclara que la misma pena incurrirá para la persona que indebidamente intercepte o capte comunicaciones ya sean electrónicas o telecomunicaciones provenientes de cualquier sistema sea privado o de acceso restringido.

- **Artículo 153 bis.** Hace referencia a que la persona será reprimida con prisión de quince días a seis meses si se le comprueba que accedió sin la debida autorización a un sistema o dato informático de acceso restringido.

- **El Artículo 155** del Código Penal señala que la persona será reprimida con una multa de mil quinientos pesos a cien mil pesos a la persona que se le halle culpable de la posesión de información electrónica o un pliego cerrado que publique de forma indebida y que esta información perjudique a terceros.

- **Artículo 157**. La persona que sea encontrada culpable de violar sistemas de confidencialidad y seguridad de datos y acceda a datos

personas sin el debido consentimiento será sancionado con pena privativa de un mes a dos años, en los siguientes casos:

1. Cuando se accede a información confidencial
2. Cuando se revele información registrada en archivos o banco de datos personales sin el debido consentimiento
3. Cuando de manera ilegítima inserte archivos en datos personales

- Art- 173, inciso 16. Señala que la persona que defraude o manipule datos informáticos y a la transmisión de datos.

- Art. 183. Este artículo se refiere a que la pena dependerá de los daños causados a los programas o sistemas informáticos, al igual que si vende, destruye o introduce en un sistema informático, con la intención de causar daño. (Código Penal de la República de la Argentina, 2008)

Una vez realizado el derecho comparado se puede dar cuenta que en estos países existe un avance importante en lo que se refiere a la protección de datos. Además se ha podido evidenciar que Argentina ha sido el primer país reconocido por la Unión Europea por contar con normas y leyes adecuadas para brindar protección a los datos personales

de los ciudadanos al igual que España, lamentablemente en nuestro país se las leyes y normas que protegen los datos personales no se encuentran muy claras.

CAPÍTULO III

1. PRESENTACIÓN DE LA PROPUESTA

Luego de haber investigado de manera minuciosa el tema de estudio sobre la revelación ilegal de base de datos en el derecho comparado, para lo cual se realizará un análisis exhaustivo del Artículo 229. del Código Orgánico Integral Penal, respecto a la revelación ilegal de base de datos, el cual señala que toda persona que saque provecho de un tercero, revelando información registrada en bases de datos o sistema electrónico informáticos.

De igual manera aclara que si un servidor público o empleado bancario o de instituciones de economía popular sean intermediarios para la revelación de datos personales también serán sancionados de acuerdo a la ley.

En lo que se refiere a la Constitución de la República en el Artículo 86, literal 19, manifiesta que toda persona tiene derecho a la protección de sus datos personales. Cómo se puede notar todos los ciudadanos tenemos derecho a la protección de nuestros datos personales ya que son considerados como un derecho a la privacidad e intimidad.

Sin embargo pese a que en el Ecuador existe esta Norma Suprema y algunos artículos que brindan protección a los datos personales, se puede notar que no existe una ley exclusiva para su protección, al igual que

sanciones drásticas, para aquellas personas empresas o instituciones que utilizan los datos personales de los ciudadanos sin su previo consentimiento.

Uno de los casos donde se puede evidenciar claramente la violación de los derechos personales es cuando las instituciones bancarias utilizan la base de datos de los cuenta ahorristas sin su consentimiento para acosar con llamadas telefónica y ofrecer prestaciones y servicios tales como las tarjetas de crédito, préstamos, variedad de seguros, entre otros servicios.

Otro ejemplo son las compañías telefónicas que hacen uso indebido de base de datos de los clientes, los cuales son aprovechados para ofrecer su servicio o promociones de planes para celulares en post pago y pre-pago. Por todo esto los ciudadanos se ven amenazados a que sus datos personales o vida privada sean divulgados debido a que sus bases de datos se encuentran tanto en empresas públicas como en privadas y no les brindan la protección que deberían.

En este sentido la Ley Orgánica de Telecomunicaciones, en el Artículo 22 menciona que los datos personales que son entregados a la empresa que presta un servicio deben ser protegidos de acuerdo a como lo dispone la ley. Sin embargo no se cumple debido a que esta ley no es clara, lo cual es aprovechado por terceras personas para hacer uso de estos datos personales para fines de su propio interés.

En cuanto a los delitos informáticos, el Ecuador no cuenta con una estadística cierta puesto que no existe la cultura de la denuncia, muchos ciudadanos no denuncian por desconfianza en las autoridades o por no

contar ni con el tiempo ni recursos para los trámites pertinentes para denunciar este tipo de delitos.

Cabe agregar que hoy en día personas especializadas en el manejo de medios electrónicos pueden tener acceso a cualquier plataforma electrónica, claro está sin el consentimiento de sus titulares, lo cual de acuerdo a la ley es considerado como una vulneración a la protección de datos personales, por lo que es necesario tipificar los delitos que violan los derechos de los datos personales de los ciudadanos, en vista de su utilización es ilegal.

En nuestro país los delitos informáticos está tipificados en el Código Orgánico Integral Penal (COIP), entre los delitos informáticos más frecuentes se encuentra: la apropiación de datos por medios electrónicos, inhabilitación de alarmas, descifrado de claves para la apropiación de medios electrónicos, acceso a sistemas informáticos o de comunicaciones, ataque a sistemas informáticos, apropiación de transferencias electrónicas, apropiación de bases de datos, revelación ilegal de bases de datos, uso de la cuenta bancaria para recibir de forma ilegítima las transferencias, desarrollar sistemas informáticos que permitan acatar, introducir, ejecutar o vender otros dispositivos y revelar información pública reservada.

De esta manera las autoridades competentes deben ser quiénes se encarguen de hacer cumplir los derechos de los ciudadanos tal como se encuentra establecido en la Constitución de la República y Tratados Internacionales que permitan garantizar el cumplimiento de este derecho.

Por lo tanto se considera que si la Constitución de la República reconoce y garantiza el derecho a la protección de base de datos, cuyo responsable de garantizar este derecho es el Estado ya que todos los ecuatorianos tenemos derecho a que se respete nuestra privacidad o vida íntima, además de proteger nuestros bienes patrimoniales.

CONCLUSIÓN

El Artículo 229. Revelación ilegal de base de datos del Código Orgánico Integral Penal, menciona que quién revele información registrada, contenida en ficheros, archivos, bases de datos o medios electrónicos, informático o telemáticos, que violen ya sea de forma voluntaria o involuntaria la intimidad y privacidad de las personas.

En este sentido la Carta Magna garantiza el cumplimiento de este derecho a través de la sanción y tipificación que se encuentra descrito en el Código Orgánico Integral Penal. Sin embargo en la práctica esto no sucede ya que el Estado no brinda una protección eficiente a través de un organismo especializado que se encargue específicamente de vigilar y proteger este tipo de delitos y dar la protección que se requiere a los derechos de los titulares de los datos.

En el Ecuador los delitos más comunes referentes a la revelación ilegal de base de datos son los delitos informáticos entre ellos el robo de contraseñas y clonación de tarjetas de débito y crédito, ataque a páginas web, al igual que falsificación o fraude informático, en las entidades bancarias. Además se encuentran otros tipos de delitos tales como la revelación de datos sin el consentimiento de su titular.

Los delitos informáticos son una modalidad de estafa, ya que se aprovechan de los datos personales de los usuarios de las cuentas

bancarias, de sus claves personales, para luego perjudicar al titular de la cuenta, apropiando de los activos patrimoniales de una persona.

Con la finalidad de dar solución a este tipo de delitos el Código Orgánico Integral Penal (COIP), sanciona los delitos de revelación ilegal de base de datos, al igual que la apropiación ilegal de datos, transferencias electrónicas de dinero, que se obtengan de manera ilegal, afectando a los titulares de los datos personales, en vista de que vulneran sus derechos de intimidad y privacidad para lucrarse de forma ilegal.

Bibliografía

Acurio del Pino, S. (2010). Derecho y Nuevas Tecnologías. 1ª Edición. *Corporación de Estudios y Publicaciones*, 180.

Asamblea Nacional del Ecuador. (2016). *Ley Orgánica de Protección de Datos Personales*. Obtenido de https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.*

Código Penal de la República de la Argentina. (2008). *Código Penal de la República de la Argentina*. Obtenido de https://www.oas.org/juridico/PDFs/arg_ley26388.pdf

Codigo Penal Español. (2020). *Código Pena Comentado*. Obtenido de https://adefinitivas.com/arbol-del-derecho/penal/articulo-197-bis-codigo-penal/

Congreso Nacional. (2002). *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador.*

Cuenca Espinosa, H. A. (2016). *El delito informático: su evolución, punibilidad y proceso penal en el Ecuador.*

Espinoza Jurado, S. F. (2019). *Tratamiento jurídico de los delitos informáticos en el Ecuador.*

Fiscalía General del Estado de Ecuador. (2014). *Dirección de Gestión Procesal Penal – SINAEP. "Reporte de Delitos Informáticos 2009 – 2013".*

Herrera Avila, C. (2010). *Hacia una correcta hermeneutica penal: delitos informáticos vs. delitos electrónicos*. Obtenido de https://dspace.ucuenca.edu.ec/bitstream/123456789/2673/1/tm4391.pdf

Iriarte Ahon, E. (2005). *Sociedad de la información: Políticas y Regulación en América Latina y el Caribe ¿Hacia dónde vamos?*

Jijena Leiva, R. (2016). *Chile, La protección penal a la Intimidad y el Delito Informático.* Santiago.

León Moncaleano, W. (2017). *De la comunicación a la informática: Jurídica Penal Bancaria.* Colombia: Ediciones Doctrina y Ley Ltda.

Revelo, H. (2016). *Estadísticas 2010, Delitos Informáticos en el Ecuador.*

Reyes Velázquez, A., Servín González, O., & Suñe Llinás, E. (2017). *Derecho Informático e Informática Jurídica. Primera Edición.* México: Porrúa Editorial.

Téllez Valdés, J. A. (2019). Gobierno electrónico y cómputo en la nube. *Actualidad administrativa*, 7-8.

Zambrano Rendón, A. D., Morales Carrillo, J. J., Párraga Ríos, J. M., & Loor Vaca, S. (2019). *La protección de datos personales: análisis de las leyes en el Ecuador*. Obtenido de http://sigloxxi.espam.edu.ec/Ponencias/VIII/II%20CIDEIT/SIMPOSIO3/TPES-001-2019.pdf

Universidad Católica de Cuenca

PARA SUBIR AL REPOSITORIO INSTITUCIONAL

Yo, Coronel Añazco Madisson Dayana**,** portador (a) de la cédula de ciudadanía Nro. 0942251430, en calidad de autor y titular de los derechos patrimoniales del trabajo de titulación: **"La revelación illegal de base de datos en el Derecho Comparado",** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de Los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos, Así mismo; autorizo a la Universidad para que realice la publicación de éste trabajo de titulación en Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

La Troncal, 23 de febrero de 2021

Madisson Coronel Añazco

ESTUDIANTE

Universidad Católica de Cuenca

ANEXOS

CENTRO DE IDIOMAS

ABSTRACT

The current research on unlawful disclosure of personal data in comparative law between Spain and Argentina aims to analyze the importance of protecting users' database who are in public or private institutions since these can be used by others not having proprietor's consent.

In order to achieve this objective, Article 229 paragraph 2 on Unlawful Disclosure of Personal Data within the Comprehensive Organic Penal Code was analyzed, considering that this type of crime occurs when data or information registered into files, archives, or sensitive personal data is revealed. It should be noted that this type of crime must be punished given the citizens' privacy rights are infringed.

In our country, although there are constitutional and penal laws that intend to protect citizens' data, they do not really give the necessary protection, so laws must be created to provide adequate custody of users' databases since these cannot be disclosed without prior consent of their owners.

Keywords: unlawful disclosure, database, comparative law

La Troncal, 11 de marzo del 2021

EL CENTRO DE IDIOMAS DE LA UNIVERSIDAD CATÓLICA DE CUENCA, CERTIFICA QUE EL DOCUMENTO QUE ANTECEDE FUE TRADUCIDO POR PERSONAL DEL CENTRO PARA LO CUAL DOY FE Y SUSCRIBO

LIC. NANCY PAOLA ORELLANA PARRA
Documento certificado digitalmente por Emergencia Sanitaria en Ecuador por COVID-19
La Troncal - Ecuador
2021-03-11 11:14-05:00

Lic. Nancy Orellana de Cabrera, MSc.
COORDINADORA CENTRO DE IDIOMAS LA TRONCAL

“LA REVELACIÓN ILEGAL DE BASE DE DATOS EN EL DERECHO COMPARADO”

INFORME DE ORIGINALIDAD

7%	6%	1%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	cornare.gov.co Fuente de Internet	<1%
2	www.blogespierre.com Fuente de Internet	<1%
3	clubderevistasgruposaludmental.blogspot.com Fuente de Internet	<1%
4	Submitted to Universidad Politecnica Salesiana del Ecuado Trabajo del estudiante	<1%
5	Submitted to Instituto Madrileno de Formacion Trabajo del estudiante	<1%
6	eprints.rclis.org Fuente de Internet	<1%
7	www.politicaspublicas.net Fuente de Internet	<1%
8	www.eltiemponeworleans.com Fuente de Internet	<1%

9	www.ecuadorencifras.gob.ec Fuente de Internet	<1%
10	ecotec.edu.ec Fuente de Internet	<1%
11	www.pj.gob.pe Fuente de Internet	<1%
12	www.uoc.edu Fuente de Internet	<1%
13	Ökonomische Prinzipien im argentinischen Bundesstrafprozess, 2012. Publicación	<1%
14	repositorio.unan.edu.ni Fuente de Internet	<1%
15	repositorio.umch.edu.pe Fuente de Internet	<1%
16	adefinitivas.com Fuente de Internet	<1%
17	www.ezone.net Fuente de Internet	<1%
18	mixtli8.spaces.live.com Fuente de Internet	<1%
19	200.13.202.26 Fuente de Internet	<1%
	dspace.udla.edu.ec	

20	Fuente de Internet	<1%
21	www.transparency.org Fuente de Internet	<1%
22	www.hipertext.net Fuente de Internet	<1%
23	englishforeverybody2010.blogspot.com Fuente de Internet	<1%
24	www.bopcadiz.org Fuente de Internet	<1%
25	media.timetoast.com Fuente de Internet	<1%
26	repository.unab.edu.co Fuente de Internet	<1%
27	generosocongeneres.blogspot.com Fuente de Internet	<1%
28	bdigital.uexternado.edu.co Fuente de Internet	<1%
29	e-archivo.uc3m.es Fuente de Internet	<1%
30	www.lexisnexis.cl Fuente de Internet	<1%
31	comercioelectronico-vgcs.blogspot.com Fuente de Internet	<1%

32	php.programacion.net Fuente de Internet	<1%
33	www.netmio.com Fuente de Internet	<1%
34	www.ricsh.org.mx Fuente de Internet	<1%
35	cristianoronaldo.wordpress.com Fuente de Internet	<1%
36	www.cintel.org.co Fuente de Internet	<1%
37	mylatinlady.com Fuente de Internet	<1%
38	www.senado.gob.mx Fuente de Internet	<1%
39	sipiapa.org Fuente de Internet	<1%
40	sanjosedepayamino.gob.ec Fuente de Internet	<1%
41	www.nva.org Fuente de Internet	<1%
42	revistaacademica-istcre.edu.ec Fuente de Internet	<1%
43	www.sic.gov.co	

	Fuente de Internet	<1%
44	www.cfnavarra.es Fuente de Internet	<1%
45	administracionelectronica.gob.es Fuente de Internet	<1%
46	www.conadeh.hn Fuente de Internet	<1%
47	www.iustelecom.com Fuente de Internet	<1%
48	bioetica.org Fuente de Internet	<1%
49	Leydy Soraya Ruiz-Ramón, Cecilia Ivonne Narváez-Zurita, Juan Carlos Erazo-Álvarez, Camilo Emanuel Pinos-Jaén. "Limitación del derecho a la defensa por el plazo establecido en el procedimiento directo", IUSTITIA SOCIALIS, 2020 Publicación	<1%
50	Carla Huerta Ochoa. "El carácter administrativo del derecho a la información", Boletín Mexicano de Derecho Comparado, 2015 Publicación	<1%
51	www.dspace.uce.edu.ec Fuente de Internet	<1%

52	tngconsultores.com Fuente de Internet	<1%
53	www.amnistiainternacional.org Fuente de Internet	<1%
54	www.pulsorock.com Fuente de Internet	<1%
55	www.unihost.org Fuente de Internet	<1%
56	Manaces Esaud Gaspar-Santos, Rously Eedyah Atencio-González, Johanna Emperatriz Coronel-Piloso, Julio César Arrias-Añez. "Publicidad engañosa en actividades turística y hotelera", IUSTITIA SOCIALIS, 2020 Publicación	<1%
57	grad.uprm.edu Fuente de Internet	<1%
58	edudistancia2001.wikispaces.com Fuente de Internet	<1%
59	booksnow1.scholarsportal.info Fuente de Internet	<1%
60	fliphtml5.com Fuente de Internet	<1%
61	www.opsecu.org Fuente de Internet	<1%

62	www.cenda.usb.ve Fuente de Internet	<1%
63	bcnmontjuic.com Fuente de Internet	<1%
64	www.ulacit.ac.cr Fuente de Internet	<1%
65	Red Televisiva Megavision Publicación	<1%
66	www.diarioelsur.cl Fuente de Internet	<1%
67	Eugenia Novoa. "El derecho a la protección de datos de personales en la prestación de servicios de cloud computing.", Revista de Derecho, 2020 Publicación	<1%
68	derechoinformaticouna.blogspot.com Fuente de Internet	<1%
69	translate.evernote.com Fuente de Internet	<1%
70	phersublog.wordpress.com Fuente de Internet	<1%
71	www.adultedreg.com Fuente de Internet	<1%
	www.rosarionet.com.ar	

72	Fuente de Internet	<1%
73	isavbi.wordpress.com Fuente de Internet	<1%
74	barcelonaspain.loan Fuente de Internet	<1%
75	www.ripred.org Fuente de Internet	<1%
76	José Patricio Bermejo-Camas, Cecilia Ivonne Narváez-Zurita, Juan Carlos Erazo-Álvarez, Diego Fernando Trelles-Vicuña. "Ius puniendi y la pena de prisión por la no afiliación a la seguridad social", IUSTITIA SOCIALIS, 2020 Publicación	<1%
77	Tannia Cecilia Mayorga Jácome, Ronald Fernando Coloma Andagoya, Marianela Edith López Veloz, Juan Alberto Toro Álava. "Chapter 46 Method for Implementation of Preventive Technological Tools for Control and Monitoring of Fraud and Corruption", Springer Science and Business Media LLC, 2021 Publicación	<1%
78	eumed.net Fuente de Internet	<1%
79	www.delitosinformaticos.com Fuente de Internet	<1%

80	future.inese.es Fuente de Internet	<1%
81	www.espanol.ashoka.org Fuente de Internet	<1%
82	www.uninotas.net Fuente de Internet	<1%
83	forenceecuador.blogspot.com Fuente de Internet	<1%
84	Carlos Affonso Souza, Caio César de Oliveira, Christian Perrone, Giovana Carneiro. "From privacy to data protection: the road ahead for the Inter-American System of human rights", The International Journal of Human Rights, 2020 Publicación	<1%
85	revistas.juridicas.unam.mx Fuente de Internet	<1%
86	onlinebooks.library.upenn.edu Fuente de Internet	<1%
87	spanishrevolution.org Fuente de Internet	<1%
88	Daniel Wiegant, Manuel Peralvo, Pieter van Oel, Art Dewulf. "Five scale challenges in Ecuadorian forest and landscape restoration governance", Land Use Policy, 2020	<1%

Publicación

89	galolima.blogspot.com Fuente de Internet	<1%

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado		

El Bibliotecario de la Unidad Académica de Ciencias Sociales.

De la Extensión San Pablo de La Troncal

CERTIFICA:

Que la estudiante: CORONEL AÑAZCO MADISSON DAYANA

Con cedula de ciudadanía N° 0942251430, de la carrera de DERECHO

No adeuda libros, a esta fecha.

La Troncal, 16 de Marzo de 2021

Atentamente,

Ing. Stefania Alvarado Ortega
Bibliotecaria

UNIDAD ACADEMICA "SAN PABLO" DE LA TRONCAL
ucacue
COMUNIDAD EDUCATIVA AL SERVICIO DEL PUEBLO
BIBLIOTECA