Análisis del tipo penal de violación de datos personales en Colombia

Joseph Steven Ibañez Trujillo

Resumen

Este artículo es sobre el delito de violación de datos personales, tiene como objetivo definir y describir el delito de violación de datos personales en Colombia, posteriormente identificar y describir los elementos del delito de violación de datos personales, por último Identificar que técnica se utiliza para indagar e investigar esta conducta ilícita y que dificultades se presentan, se utiliza métodos como el análisis y documental para demostrar que los fiscales, policía judicial y sus colaboradores tienen dificultades para indagar e investigar porque no respetan la rigurosa cadena de custodia y que el tipo penal por ser novedoso en Colombia es escasa la doctrina en la que se identifique los elementos del delito.

Abstract

This article is about the crime of violation of personal data, its objective is to define and describe the crime of violation of personal data in Colombia, subsequently identify and describe the elements of the crime of violation of personal data, finally Identify what technique is used to investigate this illegal conduct and what difficulties arise, methods such as analysis and documentary are used to demonstrate that prosecutors, judicial police and their collaborators have difficulties to investigate because they do not respect the rigorous chain of custody and that the criminal type Because it is novel in Colombia, there is little doctrine in which the elements of the crime are identified.

Introducción

En pleno siglo XXI o cuarta revolución industrial donde el mundo se ha globalizado debido a la conectividad que nos ofrece internet por medio de dispositivos electrónicos, en los cuales podemos interconectarnos, transmitir, acceder y almacenar información por medio de plataformas o páginas web, esto ha traído múltiples beneficios y experiencias positivas a las personas. Aún así, se presenta una problemática la cuales son los delitos informáticos, afirma Portela (2020) “Los delitos informáticos están clasificados en tres grupos así: A. delitos informáticos con sentido económico, B. delitos informáticos sociales, y C. políticos o ideológicos.” (p.23)

En Colombia los motivos de criminalización primaria en los tipos penales contemplados en la ley 1273 de 2009, fue debido a que sujetos con conocimientos y talentos informáticos pretendían sacar provecho para sí mismo u otra persona en perjuicio de sus semejantes, anteriormente estas conductas por ser novedosas no se encontraban tipificadas ni tenían sanción penal por lo que Colombia se quedó atrasado respecto a otros estados, se buscó con esta ley la creación de tipos penales para sancionar conductas ilícitas que utilizaran medios informáticos, por regla general, estos tipos penales son básicos, de verbos alternativos, mera conducta, abiertos, la mayoría son pluriofensivos y dolosos (Grajales, 2021).

Afirma Carmona (2021) que en Facebook, Twitter y otras redes sociales las personas proporcionan irresponsablemente demasiada información personal, teniendo riesgo de que terceros puedan observar, emplear y utilizar esta información en contra del propio propietario de la información, pueden realizar daños informáticos, suplantaciones, captación de datos personales y privados, con estos datos pueden realizar delitos como el hurto, extorsión u otros, y de acuerdo a la constitución y la ley se estaría vulnerando la intimidad entre otros derechos fundamentales.

En Colombia el derecho al olvido no está regulado para redes sociales, pero esta es una herramienta jurídica en otros estados como los de la Unión Europea el cual consiste según De la Vega y Novoa (2019) en el amparo de los datos personales y de identidad, se solicita eliminar información personal de medios sociales y buscadores web, con el fin de prevenir e impedir riesgos y exposición para el dueño de la información. Tener el derecho al olvido es fundamental en el proceso de establecer nuevas y diferentes identidades o personalidades a lo largo de la vida.

Según Rincón (2016) en Colombia hay múltiples instrumentos y mecanismos jurídicos para para proteger el derecho fundamental de habeas data, pueden ser administrativos como el derecho de petición ante la SIC, también acciones constitucionales como la acción de tutela en el caso que vulneren derechos fundamentales, intereses legales perjudicados por el indebido tratamiento por medio de la responsabilidad civil. En materia penal el delito de violación de datos personales protege, la honra, la intimidad y el honor; cuando un sujeto los pone en peligro el acceso sin autorización a los datos personales del titular, para esto no debe haber un contrato que justifique su acceso, esto tiene como fin garantizar los principios.

En el Estado Colombiano, el delito de violación de datos personales fue tipificado a partir de la ley 1273 de 2009 en su artículo 1° que adiciona el Título VII BIS nombrado de la protección de la información y de los datos - artículo 269F al código penal. Esta conducta ilícita vulnera derechos fundamentales, los cuales son el buen nombre, la intimidad personal, habeas data, entre otros. El delito no tiene vínculo con el Convenio de Budapest, pero tiene antecedentes con el artículo 197 del Código Penal de 1995 de España, una diferencia entre ambos estados es que las penas impuestas en España son más blandas las penas aplicadas que en Colombia (Escobar y Jiménez, 2018).

Este tipo penal afirma Torres, (2019) “Se identifica de manera flagrante y directa la afectación de los datos personales de las personas naturales y jurídicas; que con posterioridad

además pueden ser utilizados para la realización de otro punible" (p.48), este tipo penal genera consecuencias en la víctima como pueden ser personales, legales, sociales y laborales.

Por ejemplo, según Hincapié y Ferrer (2019) los casos denunciados ante la Fiscalía Seccional Quibdó, relacionados con la afectación a la intimidad de las personas en los medios sociales por el delito de violación de datos personales durante los años 2017-2018 fueron los siguientes, en el año 2017 estaban en las siguientes etapas procesales: 54 en etapa indagación, 52 en etapa de juicio y 1 querella, para el año 2018 estaban en las siguientes etapas procesales: 87 en indagación, 2 en juicio y ninguna querella.

Toda persona es dueño innato y intrínseco del derecho a la defensa del dato personal, solo dueño está legitimado para autorizar la difusión de sus datos personales referente a su vida privada, pero el fiscal ejerciendo la acción penal puede solicitar a un juez de garantías en audiencia el control de legalidad de actos de indagación e investigación, este debe ponderar realizando una valoración y protección a derechos fundamentales, buscando balancear la mayor protección de un derecho frente al otro. Por ende, los artículos 15 y 29 de la constitución se deben interpretar conjuntamente a derechos sustanciales que regulan actos en las etapas de indagación e investigación donde la fiscalía recolecta material probatorio, el juez de garantías ponderara el derecho a la prueba y el debido proceso serían causal justificante para un eximente de responsabilidad frente a la protección al dato personal por ser una necesidad de probar la comisión de un delito (Mesa, 2015).

Según Aguirre (2020) Se estableció la importancia de renovar la teoría del delito respecto a crímenes informáticos debido a que en la actualidad la imputación objetiva utiliza el nexo causal, este se debe excluir por ser insuficiente y generar inseguridad jurídica porque se entiende que debe haber una conducta física y tangible y un resultado externo para atribuírselo al sujeto, esto no sería aplicable a los delitos informáticos por no ser tangibles si no virtuales y no manifestarse físicamente. Se debe utilizar el nexo lógico para tipos penales como el de

violación de datos personales, dicho de otro modo, es la interacción de un mandamiento emitido y la respuesta del sistema, que conlleva a la manipulación y posteriormente conseguir los datos personales, creando un riesgo jurídicamente desaprobado, esto se llama interacción IN PUT - OUT PUT.

Afirma Sánchez (2016) es necesario realizar cambios en la legislación que permitan a las organizaciones competentes contar con instrumentos científicos, tecnológicos y personal profesional y técnico que tenga la experticia requerida para que la norma no quede en letra muerta, para investigar y detectar a tiempo estas conductas delictivas en medios informáticos.

Las investigaciones acerca de este tipo penal han evidenciado como afecta derechos fundamentales y legales, puede ser utilizado para realizar otras conductas punibles. Sin embargo, se evidencia un vacío respecto a una clara identificación y descripción de los elementos del delito de violación de datos personales y la dificultad que tiene la fiscalía general de la Nación y colaboradores para indagar e investigar esta conducta, porque el ciber delincuente se caracteriza por no dejar rastros u ocultar su actividad, identidad y ubicación, además de que no siempre se respeta la rigurosa cadena de custodia razón por la cual se presentan dificultades probatorias.

No obstante, estos problemas jurídicos es vital investigarlo porque para las partes es necesario tener una definición y descripción clara del delito de violación de datos personales e identificación de los elementos del delito, al momento de afrontar un proceso penal con el fin de evitar que se afecte la teoría del caso, se presenten nulidades o errores en la defensa y acusación. También es pertinente Identificar que técnicas de indagación e investigación que utilizan los fiscales, policía judicial y peritos para conseguir evidencia física, información legalmente obtenida y elementos materiales probatorios y las dificultades tienen para obtenerlos.

Desde que se ha implementado este tipo penal en Colombia, el fiscal, policía judicial y sus colaboradores tienen dificultades para indagar e investigar porque se presentan dificultades para garantizar la cadena de custodia y otros procedimientos, porque los involucrados en ocasiones carecen de conocimientos técnicos informáticos, científicos, experticia o de los medios para conseguir evidencia física o digital, elementos materiales probatorios e información legalmente obtenida para demostrar la violación de datos personales, se tienen dificultades para imputar y demostrar en juicio al juez que no hay duda razonable de que el sujeto activo cometió una comportamiento antijurídico, típico y culpable, por ende es poco probable que se condene. Además, se logra evidenciar que en Colombia el tipo penal de violación de datos personales es nuevo, por lo que es escasa la doctrina en la que se identifique los elementos del delito como la antijuricidad, tipicidad y culpabilidad.

Este artículo científico pretende en principio definir y describir el delito o tipo penal de violación de datos personales en Colombia, posteriormente Identificar y describir los elementos del delito del tipo de violación de datos personales y por último Identificar que técnicas se utilizan para indagar e investigar esta conducta ilícita y establecer que dificultades se presentan, se utilizará métodos como el análisis y documental.

Definición y descripción del tipo penal de violación de datos personales en Colombia.

Delitos informáticos

En esta era en la que existe la conectividad y acceso a información por medio de dispositivos electrónicos y digitales se presenta una problemática la cuales son los delitos informáticos, esta pone en riesgo y vulnera bienes jurídicos a personas naturales y jurídicas y entidades estatales por medio de conductas ilícitas utilizando medios informáticos para obtener un provecho propio o de un tercero. A continuación, se recopila por medio de autores definiciones de delitos informáticos.

Delitos o crímenes informáticos son aquellas acciones u omisiones típica, antijurídica y culpable contra entidades estatales, personas jurídicas o naturales, usando un sistema de tratamiento de la información, que producen un perjuicio en la víctima ocasionando lesiones o poniendo en peligro bienes jurídicos para conseguir un beneficio propio o de un tercero, sea o no de carácter patrimonial o personal y con o sin ánimo de lucro (Huerta; Libano, 1998 citado en Acurio Del Pino, 2016).

> Delincuencia informática 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 (Acurio Del Pino, 2016, p.14).

Otra definición de delitos informáticos es los autores Ojeda et al. (2010) en la que indican lo sigueinte:

> Es toda conducta ilícita, ya sea por acción u omisión, que realiza una persona mediante el uso de cualquier recurso informático y que, como consecuencia, afecta un bien informático jurídico y/o material que se encuentra legalmente protegido, haciéndose penalmente responsable por tal hecho. (p.51)

Teniendo en cuenta las definiciones anteriores se da el siguiente concepto de lo que se entiende por delitos informáticos, como aquéllas conductas punibles realizadas por omisión u acción, que es antijurídico típico y culpable, que ejecuta un sujeto activo con conocimientos técnicos y científicos en informática y telemática u otros, por medio del uso indebido de cualquier medio informático dirigido a modificar, socavar, destruir, o manipular, obtener, divulgar, sustraer, interceptar entre otros verbos, algún sistema informático o una cierto

componente e información, para conseguir un provecho propio o de un tercero, el cual lesiona o pone en peligro uno o más bienes jurídicos y/o material protegidos del sujeto pasivo.

Violación de datos personales

En el estado colombiano se incorporó el tipo de violación de datos personales por medio del artículo 269F del Código Penal, adicionado por la Ley1273 de 2009. (2009, 5 de enero). Congreso de la República. Diario oficial 47.223. establece lo siguiente:

> El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Datos personales

Empezaremos por definir que son los datos personales, la Ley Estatutaria 1266 DE 2008. (2008, 31 diciembre). Congreso de la República. Diario Oficial No. 47.219. artículo 3 literales e, f, g, h nos define lo siguiente:

> e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.
>
> f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquéllos que no sean semiprivados o privados,

> de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;
>
> g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.
>
> h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

El decreto 1377 de 2013 (2013, 27 junio) Presidente de la República de Colombia. Diario Oficial No. 48834. artículo 3, numeral 3 nos define:

> **Datos sensibles:** aquéllos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquéllos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Códigos personales

Los códigos personales son los códigos, contraseñas y claves, los cuales pueden ser una combinación de números, letras y símbolos; empleado por el titular o titulares para acceder

y proteger un archivo, fichero, sistema de información, base de datos o semejantes, estos contienen datos personales, información confidencial o sensible.

Archivo o fichero

Los archivos o ficheros son estructuras que abarcan información de manera ordenada y secuencial, estos están almacenados en un dispositivo (Lazo, 2018).

Base de datos

Acurio (2016) “Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios” (p.59).

Definición de violación de datos personales

Teniendo en cuenta lo anteriormente mencionado se define y describe como violación de datos personales como: comportamientos punibles, que es antijurídico, típico y culpable, la cual ejecuta o realiza el sujeto activo sin consentimiento del titular, a través de cualquier medio informático, telemático o dispositivos, compile, modifique, intercepte, obtenga, ofrezca, emplee, sustraiga, venda, envié, intercambie, compre y divulgue archivos, ficheros, base de datos o semejantes que contienen datos personales, semi privado, públicos, sensibles y privados; o códigos personales respecto de los cuales son una combinación de números, letras y símbolos que utiliza el titular para proteger y acceder a estos; el objetivo del sujeto activo es sacar provecho propio o de un tercero, además de lesionar el interés jurídico de la protección de la información y de los datos puede lesionar uno o más bienes jurídicos y/o material protegidos del sujeto pasivo. Por esta conducta se incurre en condena de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Identificación y descripción de los elementos del delito del tipo penal de violación de datos personales.

En este capítulo tiene como objetivo identificar y describir los elementos del delito del tipo penal de violación de datos personales, porque es vital para las partes en el proceso establecer la estructura del tipo penal de violación de datos personales con el fin de evitar que se afecte la teoría del caso, nulidades o errores en la defensa o acusación. se considera pertinente identificar y describir elementos del delito como la tipo objetivo y subjetivo, antijuricidad, culpabilidad.

Según Vega (2016) “los tipos penales son una serie de oraciones gramaticales contenidas en normas penales, que están ubicadas en la parte especial del Código Penal en la cual se hace la abstracta descripción objetiva y subjetiva de comportamientos vulneradores de bienes jurídicos” (p.56).

En Colombia el código penal exige que la adecuación típica debe realizarse de forma objetiva y subjetiva a esto se le denomina el tipo penal complejo, el tipo objetivo es definido como lo que puede ser percibido por los sentidos y ocurre por fuera de la psique del sujeto y el tipo subjetivo se comprende como lo que ocurre dentro de la psique del sujeto, es decir el nexo que hay entre la psique del sujeto y la realización de la conducta (Vega, 2016).

Tipo objetivo.

Sujeto activo y pasivo.

El sujeto activo.

Es la persona natural o jurídica que incurre en el tipo penal descrito en la norma, en el presente caso el sujeto que incurre en la conducta (acción u omisión) de los verbos rectores descritos en el tipo penal de violación de datos personales. Este tipo es mono subjetivo debido

a que solo se requiere para su conformación un solo sujeto activo, sin embargo, este no excluye la posibilidad de ser realizado por dos o más sujetos activos. El sujeto activo es indeterminado porque no requiere una calidad especial para realizar el tipo penal, pero existe una circunstancia de agravación punitiva si el sujeto activo es un funcionario público en funciones, este agravante se encuentra en el artículo 269H numeral 2.

Sujeto pasivo.

Es uno o más sujetos jurídicos o naturales contra la que incurre el tipo penal, vulnerando así su bien jurídico tutelado, es decir es la persona que recibe la ofensa por parte del sujeto activo. En el delito de violación de datos personales, el sujeto pasivo es indeterminado, este puede ser el Estado Colombiano (sociedad), persona jurídicas y particulares.

Objeto.

Objeto jurídico.

Objeto o interés jurídico es el bien jurídico protegido por el código penal, este se define según Chanjan et al. (2020) es el "objeto de protección de cada delito, el cual consiste en los intereses sociales, principios o derechos que se quieren tutelar en cada delito" (p.12). Este bien jurídico protegido tiene como nombre de la protección de la información y de los datos. Este tipo penal básico puede ser pluriofensivo porque podría afectar más de un interés jurídico como el derecho a la intimidad, entre otros. Es un tipo penal resultado de lesión porque al realizar la acción de alguno de los verbos rectores menoscaba o daña el bien jurídico tutelado.

Objeto material.

El objeto material de este tipo penal es fenomenológico o inmaterial, considera Vega (2016) "que el objeto material es fenomenológico cuando la conducta descrita en el tipo recae sobre un fenómeno jurídico distinto a una cosa o una persona" (p.61). en el caso del tipo de

violación de datos personales recae sobre datos personales y códigos contenidos en archivos, ficheros, bases de datos o medios semejantes.

Verbos rectores.

Este tipo penal tiene verbos rectores compuestos - alternativos o disyuntivos debido a que cualquier verbo consuma el delito, además que los verbos rectores están apartados por (,) o por la letra (o). en el presente tipo de violación de datos personales (artículo 269F) los verbos rectores de mera conduta son los siguientes: comprar, ofrecer, compilar, emplear, intercambiar, vender, divulgar y enviar. de resultado son los siguientes: obtener, sustraer, interceptar y modificar.

Circunstancias específicas de agravación punitiva.

El tipo de violación de datos personales se presentan circunstancias de agravación punitiva, estas están descritas en el artículo 269H - Ley 599 de 2000 (2000,24 julio) Congreso de la República. Diario Oficial No. 44.097, 2000:

> **Artículo 269H. circunstancias de agravación punitiva.** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
>
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
>
> 2. Por servidor público en ejercicio de sus funciones.
>
> 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
>
> 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Resultado.

El resultado es un cambio fenomenológico en el mundo exterior; pero para este caso es el mundo virtual, para esto debe haber una causalidad, que es la acción del sujeto de realizar alguno de los verbos rectores del artículo 269F, teniendo que haber un nexo con el resultado que es el cambio fenomenológico de violar códigos y/o datos personales privados, semiprivados o sensibles contenidos en archivos, ficheros, bases de datos o medios semejantes. El tipo penal de violación de datos personales es de resultado permanente para algunos verbos rectores porque el sujeto activo puede permanecer lesionando en el tiempo el bien jurídico tutelado conforme su voluntad, es decir el sujeto activo puede mantenerse en el tiempo realizando los verbos rectores del artículo 269F como el de obtener, sustraer, intercepte, y modificar códigos personales, datos personales. También existe verbos rectores de mera actividad o conducta como: ofrecer, Compilar, vender, comprar, emplear, intercambiar, divulgar y enviar, estos no admiten tentativa.

Imputación objetiva

Según la imputación objetiva no pueden ser considerados prohibidos aquellos comportamientos o conductas que están permitidos socialmente como el uso de sistemas

informáticos y dispositivos electrónicos, pero cuando el sujeto activo transgrede la esfera de lo aprobado socialmente, creando con su conducta un riesgo jurídico desaprobado contra el dueño de los datos personales y códigos, el titular no debe haber facultado al sujeto activo para que exista un riesgo jurídicamente desaprobado. Existe causalidad cuando se incurre en el tipo penal a través de los verbos rectores de mera conducta como emplear, ofrecer, intercambiar, vender, enviar, comprar, divulgar y compilar o de resultado como obtener, sustraer, interceptar y modificar; el vínculo causal surge cuando mediante acción u omisión de los verbos rectores tienen un nexo causal o incidencia con el resultado de violar códigos y/o datos personales privados, semiprivados o sensibles contenidos en archivos, ficheros, bases de datos o medios semejantes.

Sin embargo según Aguirre (2020) se estableció la importancia de renovar la teoría del delito respecto a los delitos o crímenes informáticos debido a que en la actualidad la imputación objetiva utiliza el nexo causal, este se debe excluir por ser insuficiente y generar inseguridad jurídica porque se entiende que debe haber una conducta física y tangible y un resultado externo para atribuírselo al sujeto, esto no sería aplicable a los delitos informáticos por no ser tangibles si no virtuales y no manifestarse físicamente. Se debe utilizar el nexo lógico para tipos penales como el de violación de datos personales, es decir la interacción de un mandamiento emitido y la respuesta del sistema, que conlleva a la manipulación y posteriormente conseguir los datos personales, creando un riesgo jurídicamente desaprobado, esto se llama interacción IN PUT - OUT PUT.

Tipo subjetivo

En el tipo subjetivo, el tipo de violación de datos personales solo se puede cometer por medio de la modalidad de la conducta dolosa, debido a que en el código penal no tipifica expresamente las modalidades de la conducta como la culpa o la preterintencion para el delito de violación de datos personales, esto con base en el artículo 21 del código penal. Para que

exista dolo en este delito el sujeto activo debe tener conocimiento, entendimiento o dominio de los hechos constitutivos y quiere realizarlo o ha previsto como probable o posible y su no producción del tipo se deja librada al azar, en el presente delito no existen elementos adicionales al dolo como el ánimo, la finalidad o el propósito.

Antijuricidad

La antijuridicidad tiene dos sentidos uno formal y material, en su sentido formal, es el juicio de valor negativo sobre una conducta (acción u omisión) que infringe la normatividad penal. No toda conducta es contraria a la normatividad penal, por lo que, en sentido material, la antijuricidad tiene su fundamento en la lesión o puesta efectivamente en peligro de uno o más bienes jurídicamente tutelados por la ley penal, sin justa causa, es decir para que exista antijuricidad material el hecho no debe enmarcarse en alguna de las causales de ausencia de responsabilidad del artículo 32 código penal Salgado (2020).

Formal

En el tipo de violación de datos personales para que exista antijuricidad formal el sujeto activo debió realizar con su conducta lo descrito en el artículo 269F del código penal, infringiendo con su conducta la normatividad penal vigente, en consecuencia, existe antijuricidad formal.

Material

Una vez constatada la antijuricidad formal del delito de violación de datos personales, es necesario verificar si el hecho lesiono o puso efectivamente en peligro el bien o interés jurídico tutelado de la protección de la información y de los datos y otros, sin justa causa; para ello debemos remitirnos al artículo 32 - Ley 599 de 2000 (2000,24 julio) Congreso de la República. Diario Oficial No. 44.097, 2000:

ARTÍCULO 32. AUSENCIA DE RESPONSABILIDAD. No habrá lugar a responsabilidad penal cuando:

1. En los eventos de caso fortuito y fuerza mayor.

2. Se actúe con el consentimiento válidamente emitido por parte del titular del bien jurídico, en los casos en que se puede disponer del mismo.

3. Se obre en estricto cumplimiento de un deber legal.

4. Se obre en cumplimiento de orden legítima de autoridad competente emitida con las formalidades legales.

No se podrá reconocer la obediencia debida cuando se trate de delitos de genocidio, desaparición forzada y tortura.

5. Se obre en legítimo ejercicio de un derecho, de una actividad lícita o de un cargo público.

6. Se obre por la necesidad de defender un derecho propio o ajeno contra injusta agresión actual o inminente, siempre que la defensa sea proporcionada a la agresión.

Se presume la legítima defensa en quien rechaza al extraño que, indebidamente, intente penetrar o haya penetrado a su habitación o dependencias inmediatas.

7. Se obre por la necesidad de proteger un derecho propio o ajeno de un peligro actual o inminente, inevitable de otra manera, que el agente no haya causado intencionalmente o por imprudencia y que no tenga el deber jurídico de afrontar.

> El que exceda los límites propios de las causales consagradas en los numerales 3, 4, 5, 6 y 7 precedentes, incurrirá en una pena no menor de la sexta parte del mínimo ni mayor de la mitad del máximo de la señalada para la respectiva conducta punible.
>
> 8. se obre bajo insuperable coacción ajena.
>
> 9. Se obre impulsado por miedo insuperable.
>
> 10. Se obre con error invencible de que no concurre en su conducta un hecho constitutivo de la descripción típica o de que concurren los presupuestos objetivos de una causal que excluya la responsabilidad. Si el error fuere vencible la conducta será punible cuando la ley la hubiere previsto como culposa.
>
> Cuando el agente obre en un error sobre los elementos que posibilitarían un tipo penal más benigno, responderá por la realización del supuesto de hecho privilegiado.
>
> 11. Se obre con error invencible de la licitud de su conducta. Si el error fuere vencible la pena se rebajará en la mitad.
>
> Para estimar cumplida la conciencia de la antijuridicidad basta que la persona haya tenido la oportunidad, en términos razonables, de actualizar el conocimiento de lo injusto de su conducta.
>
> 12. El error invencible sobre una circunstancia que diere lugar a la atenuación de la punibilidad dará lugar a la aplicación de la diminuente.

Las causales de justificación son acontecimientos en la que la realización de un tipo penal como el del del artículo 269F C.P se encuentra permitido, debido a que se encuentra justificado por el legislador por entrar en conflicto con otros intereses, que pueden ser

preferentes en circunstancias especiales. Un ejemplo puede ser el fiscal que investiga un tipo penal y para esto debe realizar actos de indagación e investigación, previo o posterior control del juez de garantías contra un sujeto, esto implica realizar actos tendientes a obtener códigos y/o datos personales, el actuar del fiscal y demás colaboradores está justificado por causales como la 3, 4 y 5 dependiendo el caso concreto, como consecuencia no habría antijuricidad material.

Culpabilidad

La culpabilidad según la (Corte Constitucional, sentenciaC-181, 2016, p.24) de la MG.Gloria Stella Ortiz Delgado, define lo siguiente:

> La culpabilidad es aquel juicio de reproche sobre la conducta del actor que permite imponer una sanción penal a su acción típica y antijurídica. Tiene como fundamento constitucional la consagración del principio de presunción de inocencia y el avance hacia un derecho penal del acto, conforme al artículo 29 Superior. En ese sentido, el desvalor se realiza sobre la conducta del actor en relación con el resultado reprochable, más no sobre aspectos internos como su personalidad, pensamiento, sentimientos, temperamento entre otros. Conforme a lo anterior, está proscrita cualquier forma de responsabilidad objetiva, pues la base de la imputación es el juicio de reproche de la conducta del sujeto activo al momento de cometer el acto. Por último, la culpabilidad permite graduar la imposición de la pena de manera proporcional, puesto que el análisis no se agota en la verificación del dolo, la culpa o la preterintencion, sino que además, debe tenerse en cuenta el sentido específico que a la acción u omisión le imprime el fin perseguido por el sujeto.

Para que una conducta se culpable se requiere que el sujeto activo sea imputable, tenga conciencia de la antijuricidad y la exigencia de un comportamiento diferente. En el

presente delito se presenta cuando se realiza un juicio de reproche o valoración sobre el comportamiento del sujeto que tiene la capacidad de comprender y querer el injusto de su actuar, es decir que el sujeto conoce y es consciente que con su conducta o actos incurre en el delito de violación de datos personales artículo 269F del código penal y aun así quiere realizar la conducta, pudiendo actuar de una manera diferente, en consecuencia si un comportamiento es antijurídico, típico y culpable es una conducta punible merecedora de una pena.

Sin embargo, existen condiciones de imputabilidad disminuía o inimputabilidad, la primera se presenta cuando el sujeto sufre de un trastorno que no le impide comprender la ley penal ni lo hace indeterminable frente a esta, pero sí disminuye su capacidad de autodeterminación o de comprensión de la ley penal, cuando ocurre esto debería considerarse como un atenuante de la pena, un ejemplo es la pobreza extrema, la ira e intenso dolor, ignorancia, marginalidad o, artículo 56 y 57 del código penal. Ospina (2018).

La segunda es la imputabilidad, cuando el sujeto padece o sufre condiciones como el trastorno mental, inmadurez psicológica y la diversidad sociocultural o estados similares, es decir el sujeto no comprende la capacidad de su ilicitud y no tiene la capacidad de determinarse. En consecuencia, una conducta inimputable es punible cuando sea antijurídico, típico y se compruebe la carencia de causales de ausencia de responsabilidad como el error de tipo y de prohibición, debido a esto se le impone a el sujeto una medida de seguridad del artículo 69 del código penal, esto con el fin de salvaguardar y rehabilitar al sujeto.

Técnicas que se utilizan para indagar e investigar delito de violación de datos personales y sus dificultades.

El último capítulo tiene como objetivo identificar que técnicas se utilizan para indagar e investigar el delito de violación de datos personales y que dificultades existen para el fiscal, policía judicial y auxiliares para obtener evidencia física y/o digital, elementos materiales probatorios o información legalmente obtenida y conservar la cadena de custodia.

Según la Fiscalia General de la Nacion (2009) las etapas de indagación e investigación son dos fases en el que el Fiscal, por medio de la policía judicial, en la indagación examina los hechos que tiene características de delito y llegan a su conocimiento por medio noticia criminal, esta etapa va hasta la formulación de imputación. posteriormente se entra en etapa de investigación, esta busca robustecer la evidencia física y elementos materiales probatorios o información legalmente obtenida, para poder acusar a los presuntos autores o partícipes de la conducta investigada, en el presente caso articulo 279 F C.P esta etapa culmina con la presentación del escrito de acusación, aunque el artículo 344 CPP permite excepcionalmente descubrir en juicio EF y EMP muy significativos.

La recolección de evidencia fisica, elementos materiales probatorios y información legalmente obtenida tendiente a esclarecer la comisión del tipo penal de violación de datos personales y el presunto responsable, es realizada por medio de la participacion del fiscal y la policia judicial a través de actuaciones y según su naturaleza requieren control posterior o previo del fiscal o del juez de garantias. En este caso se analiza en específico sobre la actuación de recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes.

La recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes está fundamentada normativamente en los artículos 14, 236 y 237 del CPP, establece lo siguiente: Toda persona tiene derecho al respeto de su intimidad. No podrán ser molestados los ciudadanos en su vida privada, sin embargo, el fiscal, con base en los informes de policía judicial, siempre que haya fundamentos fundados, dispondrá la aprehensión, retención o recuperación de información de la computadora, servidores, dispositivos o semejantes, para que peritos en informática forense, analicen recuperen y custodien la información de acuerdo a los requerimientos sobre cadena de custodia. (Fiscalia General de la Nación, 2009)

Según el FBI “la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional” (FBI, 2000 citado en López, Amaya, & León, 2001). La Informática forense posibilita solventar problemas de seguridad informática y la protección de datos, por medio de métodos que aseguran, identifican, analizan, extraen y presentan pruebas generadas y guardadas electrónicamente en medios de depósito de información (Canedo Estrada, 2010).

Afirma el Ministerio de Tecnologías de la Información y las Comunicaciones (2016) que la informática forense es la “aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información” (p.10).

Según el manual de (Fiscalía General de la Nación, 2004) los estudios y análisis que realiza los informáticos forenses son los siguientes, los primeros son los que pueden ser requeridos dentro del acto urgente como son: Extracción de información a equipos terminales móviles, servidores, la Identificación y recolección de evidencia digital Logs y Recolección de datos volátiles, sistemas de información, bases de datos, máquinas virtuales y datos volátiles.

Posteriormente dentro de las treinta y seis (36) horas siguientes la policía judicial debe presentar informe ejecutivo al fiscal.

Por orden previa del fiscal y después control posterior del juez de garantías, los informáticos forenses realizaran los siguientes análisis y estudios: elaborar imágenes forenses, tratamiento y análisis de la evidencia digital, adquisición de imagen forense de medios de almacenamiento digital, examen en laboratorio de dispositivos de almacenamiento digital y dispositivos móviles, recuperación de información eliminada u oculta búsqueda de información específica, identificación de software empleado incurrir en hechos delictivos, desciframiento de archivos, extracción de información, obtención de información dejada al navegar, verificación de software en casos de usurpación de código fuente, duplicado de medios de almacenamiento digital con fines de traslado de evidencia a otros procesos judiciales, análisis de malware.

La cadena de custodia que debe realizar la policía judicial es la siguiente, el servidor de policía judicial, al iniciar la recolección de los EF Y EMP, debe despojarse de cualquier elemento metálico o magnético, este puede requerir diestros en informática forense que documentaran la escena del crimen, indagando sobre información relacionada con claves de acceso a equipos, archivos y aplicativos, se respeta el derecho a la no auto incriminación, se debe dejar consignado en el acta. también se debe documentar topográficamente y fotográfica la escena del hecho, fijando la ubicación, el estado en el que se observan las conexiones y elementos. Además, en el formato de nombre acta de inspección a lugares se mencionará narrativamente todos los hallazgos. (Fiscalía General de la Nación, 2004)

El embalaje de medios de almacenamiento electrónico se debe etiquetar o identificar en bolsa antiestática, caja de cartón, plástica o papel, los adhesivos o rótulos no se pueden colocar directamente sobre su superficie. Los celulares una vez aprehendidos debe ponerse en modo avión, el embalaje de un computador de escritorio o portátil, se conduce a fijar por medio de fotografía la información que se encuentra expuesta en la pantalla si esta encendido, en los

computadores portátiles que se encuentren encendidos se deben desenchufar del cargador y retirar la batería para apagarlo, posteriormente se sella o cubre las tapas, y las ranuras de inserción de discos, puertos delanteros y traseros conexiones, conexiones de energía eléctrica, se debe identificar y rotular, registrando el modelo, la marca y el número serial, Si el computador esta encendido, además la evidencia de tipo digital no puede ser expuesta a cargas de tipo magnético. (Fiscalía General de la Nación, 2004)

Los diestros en informática forense serán quienes recuperen, descubran, recojan, custodien y analicen la evidencia de tipo digital obtenida, En tiempo no superior a doce (12) horas, una vez terminada las actuaciones el fiscal recibirá informe de la policía judicial, Posteriormente el experto presentara informe de investigador de laboratorio con los resultados del análisis. El tiempo que dura la captura de la información y de datos será lo que dure la incautación, por último, previa consulta con el fiscal devolverá lo incautado por parte de la policía judicial al propietario o tenedor legítimo, de ser procedente su devolución (Fiscalía General de la Nación, 2004).

Posteriormente a la incautación y procedimiento de cadena de custodia en el lugar de los hechos, para hacer informe de investigador de laboratorio, según Ministerio de Tecnologías de la Información y las Comunicaciones (2016) se realizara los siguientes procedimientos: Se debe identificar la fuente de información como computadoras, servidores, dispositivos, entre otros, en seguida se procede a la adquisición de los datos, primero se planifica a que dispositivos se les sustraerá la información y la secuencia en el que se debe hacer, teniendo en presente la dificultad para obtener los datos y la volatilidad de la información, Segundo, el proceso general de acopio usualmente requiere del uso de instrumentos forenses para copiar los datos volátiles y poderlos almacenar, también para conseguir la información de fuentes no volátiles. Por último, se debe garantizar que la información es integra y no fue modificada, para

esto se empleara la herramienta hash. Esto se utiliza para certificar su autenticidad e integridad de la prueba recolectada.

El segundo procedimiento, se debe realizar el acopio y examinación de los datos disponibles, primero se debe crear y asegurar un documento, electrónico o físico, que permita llevar un historial de las actividades que se llevan a cabo durante el proceso y de los hallazgos, esto para cadena de custodia, después el perito creara las imágenes de datos que correspondiente al caso que se investiga. Se aconseja usar instrumentos de extracción de imágenes como Linux dd o Encase Forensic Software. En seguida se debe verificar la integralidad de la imagen, después es necesario que se haga una copia maestra y con esto se reproducen las imágenes necesarias, se debe asegurar que las imágenes adjuntas no se dañen Cualquier virus conocido (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).

Luego comienza con la identificación de particiones, que incluye conocer su sistema de archivos, con lo cual se pueden identificar las características específicas de la organización de la información, y se puede determinar la estrategia de acopio de archivos adecuada, a continuación, se procede a un análisis para decidir si representan algún tipo de información significativo para la investigación. Enseguida se debe realizar la posible detección de existencia del hpa (host protected area) en los metadatos, estos son volátiles es decir se pierden al reiniciar, por último, se necesita reconocer el sistema de archivos, para elegir la manera de hacer las actividades posteriores del examen de datos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).

Lo siguiente en el procedimiento según Ministerio de Tecnologías de la Información y las Comunicaciones (2016) es la restauración de información escondida, restauración de los archivos borrados, reconocimiento de archivos existentes y reconocimiento de archivos protegidos con el fin de descifrarlos o romper tal seguridad en estos archivos, lo anterior se

hace para unirlos al grupo de archivos potencialmente analizables, después se debe diagnosticar las aplicaciones instaladas y el sistema operativo, también se debería hacer una comprobación diligente de la información registrada por los dispositivos de red, esto ayuda a reedificar y estudiar ataques basados en la red o investigar algún tipo de acceso o movimientos específicos.

Lo siguiente en el procedimiento según el Ministerio de Tecnologías de la Información y las Comunicaciones (2016) se debe realizar una purificación de archivos buenos conocidos para desechar información que no será destacada para analizar, Para obtener un grupo de archivos potencialmente estudiados, este grupo se llamará archivos sospechosos, posteriormente se hace una segunda encasillado de archivos, que consiste en tomar archivos que no se consideran prioritarios, estudiarlos y evaluarlos con dos criterios: Relación de los archivos con los usuarios participantes en la investigación y contenido sobresaliente para el caso.

En el último procedimiento, se hace un análisis de la información prioritaria, poco prioritaria y catalogará los archivos o ficheros comprometidos, después el investigador generará una lista de archivos comprometidos con el incidente, los cuales serán exhibidos como evidencia en el informe final o En el procedimiento judicial y realizara una línea de tiempo de la evidencia, es decir la reedificación de los hechos a partir de los atributos de tiempo de los archivos y por último y se hará el informe final del caso que contenga una descripción detallada de los hallazgos relevantes y el método de descubrimiento con el fin de que sea conocimiento de fiscal competente que lleve la indagación o investigación del tipo penal de violación de datos personales (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).

Adicionalmente a lo anterior se presentan dificultades para el investigador forense, según López, Amaya, & León (2002) son las siguientes:

1. Carencia de software especializado para buscar la información en varios computadores.

2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.

3. Será difícil encontrar toda la información valiosa.

4. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.

5. Los errores cometidos pueden costar caro para la persona o la organización que representa.

6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.

7. Falta de experiencia para mostrar, reportar y documentar un incidente computacional.

8. Dificultad para conducir la investigación de manera objetiva.

9. Dificultad para hacer correctamente una entrevista con las personas involucradas.

10.Reglamentación que puede causar problemas legales a la persona. (p.16).

Como se demostró anteriormente, la cadena de custodia es un método riguroso que plantea dificultades a la policía judicial, fiscales competentes y auxiliares para asegurar que los métodos utilizados para obtener pruebas informáticas sean los adecuados para lograr este objetivo, se debe velar por la integridad y esterilidad, con esto se evita la modificación, sustitución, contaminación o destrucción. Esto es para sustentar efectivamente la prueba digital ante el juez. En el llamado debido proceso, el juez necesita confiar en los elementos digitales

por considerarlos confiables. por lo que puede evaluarse bajo la sana crítica, la cadena de custodia informática forense se emplea para evidencia material o virtual relacionada con hechos delictivos, desde el lugar del suceso hasta que el encargado de administrar justicia pueda apreciarla (Arellano & Castañeda, 2012).

Conclusiones

En una era donde el mundo se ha globalizado, debido a la conectividad que nos ofrece internet por medio de dispositivos electrónicos a la cual podemos acceder a mucha información y compartirla por medio de plataformas o páginas web, se presenta una problemática la cual es la ciber delincuencia, en la cual sujetos con conocimientos informáticos y a través de un espacio digital o redes informáticas cometen conductas ilícitas por medio de programas llamados malwares o software malicioso con el objetivo de acceder sin consentimiento del propietario a datos personales ubicados ficheros, en archivos, base de datos y otros, con la finalidad de obtener provecho propio o de un tercero, dicha conducta ilícita vulnera derechos fundamentales como el habeas data, la intimidad personal, buen nombre y privacidad y dependiendo de lo que el sujeto activo o tercero realice con los datos personales del sujeto pasivo puede tener consecuencias familiares, personales, sociales y laborales.

Como primera conclusión se entiende por delitos informáticos, como aquéllas conductas punibles realizadas por omisión u acción, antijurídico, típico y culpable, que ejecuta un sujeto activo con conocimientos técnicos y científicos en informática y telemática u otros, por medio del uso indebido de cualquier medio informático dirigido a modificar, socavar, destruir, o manipular, obtener, divulgar, sustraer, interceptar entre otros verbos, algún sistema informático o algún componentes e información, para obtener un provecho propio o de un tercero, el cual lesiona o pone en peligro uno o más bienes jurídicos y/o material protegidos del sujeto pasivo.

Teniendo en cuanta lo anterior, se define y describe como violación de datos personales como: aquel comportamiento punible, que es antijurídico, típico y culpable, la cual ejecuta o realiza el sujeto activo sin consentimiento del titular, a través de cualquier medio informático, telemático o dispositivos, para ofrecer, modificar compilar, obtener, sustraer, vender, intercambiar, divulgar, emplear, interceptar, enviar y comprar archivos, ficheros, base de datos o semejantes que contienen datos personales semi privado, públicos, privados y sensibles; o códigos personales los cuales son una combinación de números, letras y símbolos que utiliza el titular para proteger y acceder a estos; el objetivo del sujeto activo es sacar provecho propio o de un tercero, además de lesionar el interés jurídico de la protección de la información y de los datos puede lesionar más bienes jurídicos y/o material protegidos del sujeto pasivo. Por esta conducta se incurre en una condena de cuarenta y ocho (48) a noventa y seis (96) meses y sanción pecuniaria de 100 a 1000 salarios mínimos legales mensuales vigentes.

Como segunda conclusión se considera que en Colombia el tipo penal de violación de datos personales es nuevo, la doctrina sobre este delito no es abundante y no estaba identificado todos los elementos de este delito. en el presente trabajo se identificó y plasmo la tipicidad subjetiva y objetiva, posteriormente la antijuricidad formal y material y por último la culpabilidad, logrando obtener la identificación completa de los elementos del delito del tipo de violación de datos personales, esto era vital para que las partes logren comprender la estructura del delito al momento de realizar la imputación y para el resto del proceso, con el fin de evitar que se afecte la teoría del caso, se presenten nulidades o errores en la defensa o acusación.

como tercera conclusión, se estableció que la técnica principal que se utiliza para indagar e investigar el delito de violación de datos personales, es la recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes. Además, la informática forense es la ciencia que permite el reconocimiento,

recolección, examen y estudio de los datos de dispositivos, computadores, medios de almacenamiento, entre otros, con la finalidad de que el informe de laboratorio rendido por experto al fiscal de conocimiento sirva como prueba en juicio al introducirlo por medio de perito informático y así el juez pueda valorarlo guiado por la sana crítica.

Sin embargo se evidencia que desde que se ha implementado este tipo penal en Colombia, el fiscal, policía judicial y auxiliares tienen dificultades para indagar e investigar porque se presentan dificultades para garantizar la cadena de custodia y otros procedimientos, porque los involucrados en ocasiones carecen de conocimientos técnicos informáticos, científicos, experticia o de los medios para obtener evidencia física o digital, material probatorio e información legalmente obtenida para demostrar la violación de datos personales.

Referencias

Guarnizo Portela, M. P. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/41392/mpguarnizop.pdf?sequence=1&isAllowed=y

Hincapié Mosquera, C., & Ferrer Urueta, T. J. (2019). *Análisis de los casos denunciados ante la fiscalía seccional Quibdó, relacionadas con la afectación a la intimidad de las personas en las redes sociales.* Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/20621/4/2019_intimidad_redes_sociales.pdf

Lazo Sanchez, J. M. (2018). *Informática Básica Concepto de Informática, Sistema Informático, el computador como herramienta fundamental de la informática. Conceptos básicos y terminología de un Computador, El Computador y la educación, la Informática y la educación.* Obtenido de https://repositorio.une.edu.pe/bitstream/handle/UNE/3473/MONOGRAF%c3%8dA%20-%20LAZO%20SANCHEZ.pdf?sequence=1&isAllowed=y

Sánchez Cano, D. F. (2016). *Análisis del delito de violación de datos personales (artículo 269f del código penal) desde una perspectiva constitucional.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/9778/S%C3%A1nchez_Cano_2016.pdf?sequence

Acurio Del Pino, S. (2016). *Delitos Informáticos: Generalidades .* Obtenido de http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf

Alvarado Carmona, M. A. (2021). Aspectos Legales al Utilizar las Principales Redes Sociales en Colombia. *Revista Logos, Ciencia & Tecnología*.

Arellano, L. E., & Castañeda, C. M. (2012). La cadena de custodia informático-forense. *ACTIVA*, 67-81.

Canedo Estrada, A. (2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano*, 81-88.

Chanjan Documet, R., Cabral Mori, E., Janampa Almora, A., & Gonzalez Cieza, M. (2020). *Manual Sobre Persecución Penal de Delitos de Corrupción y Técnicas de Investigación periodística* . Obtenido de https://enterateconlesly.com/wp-content/uploads/2020/12/Manual-Persecucion-Penal.pdf#page=13

Congreso de la República Diario Oficial No. 47.219. (31 de Diciembre de 2008). *Ley Estatutaria 1266 DE 2008*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso de la República. Diario oficial 47.223 . (05 de enero de 2009). *LEY 1273 DE 2009*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República. Diario Oficial No. 44.097. (24 de Julio de 2000). *LEY 599 DE 2000*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Corte Constitucional Republica de Colombia - MG.GLORIA STELLA ORTIZ DELGADO. (13 de Abril de 2016). *Sentencia C-181/16.* Obtenido de https://www.corteconstitucional.gov.co/relatoria/2016/C-181-16.htm

De la Vega Avendaño , L. C., & Novoa Arzuaga, K. J. (2019). La protección de datos personales en Colombia desde un análisis socio-jurídico del derecho al olvido en la era digital. *Vis Iuris.*

El Presidente de la República de Colombia Diario Oficial No. 48834. (27 de Junio de 2013). *Decreto 1377 de 2013* . Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

Escobar Roa, D. A., & Jiménez Moreno, L. D. (2018). *Eficacia de las normas penales colombiana para prevenir y sancionar los ciberdelitos.* Obtenido de https://repositorio.unibague.edu.co/jspui/bitstream/20.500.12313/1925/1/Trabajo%20de%20grado.pdf

Fiscalía General de la Nación. (2004). *Manual Único de Policia Judicial.* Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

Fiscalia General de la Nación. (25 de Septiembre de 2009). *Manual de Procedimientos de Fiscalía en el Sistema Penal Acusatorio Colombiano.* Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/03/spoa.pdf

López, Ó., Amaya, H., & León, R. (2002). Informática Forence : Generalidades, Aspectos Técnicos y Herramientas. *Universidad de los Andes*.

López, Ó., Amaya, H., & León, R. (2001). *INFORMÁTICA FORENSE : GENERALIDADES,ASPECTOS TÉCNICOS Y HERRAMIENTAS.* Obtenido de http://80.30.57.188/files/1528377126_InformaticaForense_OL_HA_RL-1-77.pdf

Mesa Elneser, A. M. (2015). La evidencia digital eximente de violación a la protección del dato personal a partir de la autorregulación. *Academia & Derecho*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Seguridad y Privacidad de la Informacion.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Ojeda Pérez , J. E., Rincón Rodríguez , F., Arias Flórez, M. E., & Daza Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Vlex*.

Ospina Corrales, S. (2018). *El Principio de Culpabilidad: Fundamento Constitucional y Alcances de la Norma Rectora del Arículo 12 del Codigo Penal.* Obtenido de https://repository.eafit.edu.co/xmlui/bitstream/handle/10784/13290/Sebastian_OspinaCorrales_2018.pdf?sequence=2

Ospina Grajales, J. J. (18 de Mayo de 2021). *Perspectiva criminológica y dogmática de los de los delitos relacionados con el bien.* Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/8920/Perspectiva%20criminol%C3%B3gica.pdf?sequence=1

Puello Rincón, C. J. (2016). *Herramientas jurídicas para la protección de los datos personales en Colombia: análisis del grado de protección jurídica del habeas data.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/9677/01%20-%20PROYECTO%20de%20grado%20final%20aprobado%2025-07-16%20-%20Recomendaciones%20Incluidas%20-%2010-08-16.pdf?sequence=1&isAllowed=y

Salgado González, Á. (2020). Tipicidad y Antijuricidad. Anotaciones Dogmaticas . *Revista Juridica* .

Silva Aguirre, D. (2020). La Imputación Objetiva del Nexo Lógico en el Tipo Penal de Violación de Datos Personales. *Revista Estrado*.

Vega Arrieta, H. (2016). El análisis gramatical del tipo penal. *Justicia*.