

JOSÉ ADALID MEDRANO

- Abogado especialista en derecho informático
- Conferencista internacional, consultor y capacitador sobre ciberdelincuencia y protección de datos personales.
- Coordinador de la Comisión de Innovación regulatoria.
- Miembro fundador de la Comisión de Derecho Informático del Colegio de Abogados y Abogadas.
- Miembro de la comisión de asuntos jurídicos de la ONG internacional sobre ciberseguridad, Fundación Capa Ocho, con sede en Argentina.
- adalid@ciberjuristas.com



José Adalid Medrano

Abogado especialista en derecho informático
Conferencista internacional, consultor y capacitador sobre ciberdelincuencia
y protección de datos personales.
Coordinador de la Comisión de Innovación regulatoria.
Miembro fundador de la Comisión de Derecho Informático del Colegio de
Abogados y Abogadas.
Miembro de la comisión de asuntos jurídicos de la ONG internacional sobre
ciberseguridad, Fundación Capa Ocho, con sede en Argentina.
Correo: adalid@ciberjuristas.com

El delito de violación de datos personales.

RESUMEN:

La violación de datos personales es un tipo penal que tutela el derecho de autodeterminación informativa tanto de personas físicas como de las jurídicas y representa una serie de conductas que realizan los grupos cibercriminales para la comisión de distintos delitos tradicionales e informáticos.

La ciberdelincuencia se dirige a una modalidad de operación que afectará cada vez más bienes jurídicos de una manera acelerada y con gran impacto.

En la presente investigación se ha encontrado que España, Ecuador, Colombia y Costa Rica tutelan de forma expresa el derecho de autodeterminación informativa en sus códigos penales.

Palabras clave: delitos informáticos, ciberdelitos, datos personales, violación de datos personales, autodeterminación informativa, protección de datos personales, ciberdelincuencia, cibercrimen.

ABSTRACT:

The violation of personal data is a type of crime that protects the right to informational self-determination of natural and legal persons and represents a series of conducts carried out by cybercriminal groups for the commission of different traditional and computer crimes.

Cybercrime is aimed at a way of operation that will increasingly affect almost every legal assets in an accelerated manner and with great impact.

This research has found that Spain, Ecuador, Colombia and Costa Rica expressly protect the right to informational self-determination in their criminal codes.

Keywords: computer crime, cybercrime, personal data, personal data breach, informational self-determination, personal data protection, cybercrime.

I. Introducción.

La sociedad costarricense del siglo XXI se encuentra en una transición entre el uso intensivo de la tecnología propiciado por la constante reducción de la brecha digital -acelerada por la pandemia Covid-19- y la cada vez más cercana ubicuidad tecnológica a la que nos dirige la cuarta revolución industrial, en donde el concepto de privacidad, construido con base a paradigmas de siglos pasados, está siendo desafiado por la constante recopilación de datos personales.

Con el uso intensivo de medios sociales y el aumento de sensores y cámaras de vigilancia -inclusive con reconocimiento facial- que rastrean el paso por las vías físicas y electrónicas de los usuarios, muchas personas se cuestionan si ya hemos renunciado a la privacidad, en favor del crecimiento económico y tecnológico, o si todavía hay tiempo de cambiar el camino.

La duda es importante porque las empresas tecnológicas e inclusive los gobiernos dependen, cada vez más, de la recopilación y análisis de los datos de los ciudadanos para un mejor ejercicio de sus actividades. El problema deriva en que con este tipo de vigilancia se generan cantidades ingentes de

información, que sin una regulación y controles adecuados puede debilitar los cimientos de cualquier democracia.



Figura 1. La violación de datos personales favorece la comisión de distintos tipos de delitos. [Elaboración propia]

Casos recientes, a nivel nacional e internacional, como UPAD y Cambridge Analytica, generan interesantes debates regulatorios sobre cuál es la mejor manera de combatir la violación de la privacidad y en dónde debemos establecer los límites de protección, tomando en cuenta que estas acciones contra los datos personales potencia la comisión de otros delitos.

En Costa Rica, desde el año 2012¹ sancionamos penalmente la violación de los datos personales, mientras en Estados Unidos -que es el país donde residen la mayoría de empresas tecnológicas cuyos servicios usamos- el comercio de los

¹ Delito de violación de datos personales, incluido en el Código Penal costarricense a través de la Ley No 9048.

datos personales de los consumidores, inclusive sin su consentimiento², es una práctica permitida. A pesar de lo anterior, estamos lejos de ser una autoridad en esta materia, ya que a pesar de la estricta regulación, es claro el comercio ilegal de datos personales en nuestro país se hace a vista y paciencia de todos, lo que alimenta el cibercrimen organizado local de estafas informáticas y tradicionales.

Como parte del análisis que debe realizarse de manera frecuente sobre normativa que involucre las TIC en la presente investigación analizaremos el tipo penal costarricense, así como su regulación en el derecho comparado, con el fin de analizar si requiere reformas y propuestas de *lege ferenda*.

II. La ciberdelincuencia costarricense.

La ciberdelincuencia es la actividad delictiva que tiene como eje central la utilización de medios electrónicos con el objetivo de vulnerar bienes jurídicos tutelados penalmente. En la lucha contra la ciberdelincuencia se debe tener presente que nos encontramos ante un fenómeno transfronterizo de elevada complejidad, donde los grupos criminales no son homogéneos y se dedican a diferentes acciones delictivas que impactan a la sociedad de distintas maneras, por lo que es imperativo crear una estrategia nacional que permita establecer un norte a las autoridades.

Lo anterior es necesario, ya que el nivel de impunidad con el que operan las bandas locales de estafadores cibernéticos es tan grande que requiere que en

2 En los Estados Unidos el comercio de datos personales por parte de “data brokers” es parte de la dinámica del desarrollo comercial de las empresas tecnológicas quienes utilizan esta información como objeto de comercio el cual tiene un valor. A los usuarios se les permite “optar por que sus datos no se vendan a terceros, pero no les permite elegir el que sus datos se recopilen y usen en primer lugar” (Dean, 2020)

la sociedad costarricense cada parte asuma su responsabilidad y colabore para detener este flagelo que erosiona la confianza en el sistema financiero nacional, al mismo tiempo que genera un gran daño en la ciudadanía. Lo más grave de la situación es que mientras estamos siendo derrotados por los cibercriminales locales, la ciberdelincuencia internacional no solo atenta contra empresas, organizaciones o individuos, sino que también dirige sus ojos hacia los gobiernos. Los ataques contra distintas naciones son parte de una estrategia delictiva de muchos gobiernos atacantes, quienes utilizan el ciberespacio para espiar a sus rivales y/o desestabilizarles, por lo que la capacidad de daño que tienen las acciones delictivas informáticas son ilimitadas.

Sin importar el área de acción de las bandas criminales o su ubicación geográfica, todas se alimentan de la información de carácter personal, ya sea para crear perfiles de sus víctimas para ataques posteriores o para utilizarla de forma directa en contra de estas, por lo que toda política criminal que busque mitigar el impacto de la ciberdelincuencia debe sancionar penalmente diferentes acciones informáticas que buscan violar la privacidad ciudadana.

Los datos personales de los costarricenses no solo son violentados por grupos organizados, o ciberdelincuentes especializados, sino que también por personas con pocos conocimientos en informática, pero que se encuentran en sus grupos sociales más cercanos, por lo que es habitual que en esos espacios - como el hogar, trabajo o inclusive en un comercio de confianza - se comentan delitos informáticos, sin que la víctima tenga la menor sospecha.

Con el fin de combatir la ciberdelincuencia nuestro país ha promulgado distintas leyes con el fin de sancionar penalmente los delitos informáticos, las cuales han venido a robustecer el derecho penal sustantivo, al contener tipos penales novedosos que sancionan las acciones digitales ilícitas más utilizadas por los

ciberdelincuentes modernos. Lo anterior, aunque le permite a las autoridades judiciales saltar el obstáculo de la atipicidad -motor de la impunidad- no les resulta suficiente ya que no se les ha dotado de normas procesales y herramientas aptas para los retos que conllevan los entornos digitales y de una capacitación robusta que les permita enfrentar este flagelo de la mejor manera.

a. Delitos informáticos.

La informática ha generado una transformación sin precedentes en la humanidad, marcada por una ‘Ley de Moore’³ que funge como un derrotero de crecimiento exponencial que se ha venido cumpliendo en las últimas décadas, llevando a la sociedad a experimentar cambios de forma continua, sin descanso y sin un espacio para un profundo debate regulatorio sobre cómo debería el derecho intervenir.

En ese sentido, al estudiar la ciberdelincuencia, es importante tomar en cuenta que el medio electrónico es un agente óptimo, potente y pluriofensivo de bienes jurídicos, con resultados que son difíciles de prever a nivel legislativo, por lo que históricamente muchas de las conductas cometidas por medios informáticos han resultado atípicas, lo que ha generado una necesidad urgente de sancionar penalmente conductas novedosas que tutelan bienes jurídicos vinculados con la informática, en un proceso circular que va de la mano con el desarrollo tecnológico.

A finales del siglo pasado, era todavía común el debate sobre si era necesario incluir en el Código Penal los delitos informáticos, porque algunos autores

³ Se conoce como Ley de Moore a la predicción que hizo Gordon Moore, cofundador de Intel, en 1965 respecto del aumento de la cantidad de transistores en los procesadores. En aquel entonces dijo que el número se duplicaría cada año. Luego, en 1975, redefinió este concepto y explicó que este aumento ocurriría cada dos años. (Jaimovich, 2019)

sostenían que simplemente eran nuevas formas de lesionar bienes jurídicos tradicionales, por lo que no había necesidad de tener legislación especial. Lo anterior se afirmaba sin tomar en cuenta el principio de legalidad, la prohibición de la interpretación analógica y la regla de interpretación restrictiva que rigen en materia penal, por lo que aunque este debate se encuentra superado, lo cierto es que sigue vigente que la comunidad jurídica debe mejorar en la comprensión de las acciones delictivas informáticas, que son la base de las operaciones de la ciberdelincuencia, la cual tiene un impacto transversal en todos los sectores de la sociedad.

El aumento de la calidad del debate regulatorio vinculado con esta materia permitirá avanzar hacia la construcción de una política criminal eficiente y moderna, que en respeto del principio de mínima intervención penal, permita combatir este flagelo sin poner en riesgo las bases de un Estado democrático de derecho.

Es importante tomar en cuenta que toda nueva regulación vinculada con las TIC, principalmente la relacionada con la función punitiva estatal, puede no solo servir para la protección de derechos fundamentales, sino que también para lesionarlos. Lo anterior, ya que como músculos que permiten el ejercicio de derechos fundamentales, los medios electrónicos al regularse, pueden potenciarse o atrofiarse, por lo que hay que tener precisión quirúrgica al diseñar legislación relacionada con la informática, para no generar un impacto negativo en el desarrollo democrático y/o económico que se encuentra estrechamente vinculado con el de índole tecnológico.

b. Primeras reformas sobre delitos informáticos.

En Costa Rica, en el mes de agosto de 1999 se promulgaron dos leyes que incluían en nuestro ordenamiento jurídico a los delitos informáticos, una como reforma al Código Penal sobre la pornografía infantil⁴ y otra vinculada con la protección de los sistemas de información y bases de datos tributarias. Como dato anecdótico, de lo que son los cambios culturales entre la Costa Rica de este siglo y finales del anterior, es que solo dos años antes que se decidiera sancionar penalmente la difusión de la pornografía infantil en el país, el diario La Nación incluyó una noticia que vertía una crítica camuflada de un ciudadano estadounidense hacia la decisión de un juez de retirar de circulación, en Oklahoma, la película *El Tambor Escarlata* que contenía escenas de un menor de edad sosteniendo relaciones sexuales orales con una joven:

"Nadie discute que la pornografía infantil es condenable, pero no podemos dejar las decisiones culturales a gente que pondría una hoja de higuera en una estatua de Miguel Angel", consideró Michael Salem, abogado de la Asociación de EE.UU. para las Libertades Civiles" (La Nación, 1997).

En aquellos tiempos nos conectábamos a internet principalmente por un modem que utilizaba la línea telefónica como medio de conexión, por lo que descargar cualquier contenido se hacía eterno y caro. En aquel tiempo RACSA, aprovechando su monopolio nos cobraba "\$30 por 30 horas de uso más un dólar por cada hora adicional" (La Nación, 1999), mientras en Estados Unidos ya se cobraba tarifa plana. Por lo anterior, era claro que en aquellos tiempos la velocidad de propagación de contenidos era menor, por lo que todavía no había conciencia del daño que podría generar la compartición masiva de un contenido audiovisual, ya que su consumo se hacía principalmente en VHS -que alquilábamos en un videoclub- y no como en el presente a través de Netflix,

⁴ La ley №7899 del 3 de agosto de 1999, incluyó en nuestro Código Penal los delitos de fabricación y difusión de material pornográfico infantil, acciones que no son necesariamente deben desarrollarse por medios informáticos.

Youtube, Tik Tok o distintos medios sociales, donde en pocas horas se pueden alcanzar millones de reproducciones.

En el año 2001, a través del proyecto de ley Nº8148, se adicionaron al Código Penal 3 tipos penales informáticos:

- a) 196 bis. Violación de las comunicaciones electrónicas. Penas de seis meses a dos años.
- b) 217 bis. Fraude informático. Penas de uno a diez años.
- c) 229 Bis. Alteración de datos y sabotaje informático. Penas de uno a cuatro años.

De acuerdo con Chinchilla (2002) en su libro Delitos Informáticos, esta reforma vino motivada por un proyecto que presentó la Procuraduría General de la República, el cual fue determinante para incorporar las novedosas tres figuras penales y señala que lamentablemente quedó fuera el hurto agravado mediante la utilización de tarjetas magnéticas o perforadas. En otras palabras, esta reforma, aunque novedosa para la época, quedó debiendo.

c. Definición de delito informático.

Debido al avance que han tenido en la última década los delitos informáticos, su naturaleza pluriofensiva de bienes jurídicos y la diversidad de los sujetos involucrados, la labor de definirle es altamente compleja. En esta tarea, no se puede caer en el error de usar definiciones tan restringidas que limiten el objeto de estudio, ni tan amplias que pierdan todo sentido práctico.

1. Delitos informáticos en *stricto sensu*

En sentido restringido, nos permitimos definirlo como toda aquella acción delictiva informática dirigida a vulnerar la confidencialidad, integridad, disponibilidad y/o normal funcionamiento de los sistemas informáticos, así como toda aquella dirigida contra la autodeterminación informativa y la identidad en medios electrónicos.

Esta es una definición de índole purista, al incluir únicamente los tipos penales informáticos que cuentan con verbos rectores de naturaleza informática, y que nacieron con el fin de tutelar bienes jurídicos relacionados con la tecnología.

Se es consciente que este concepto deja por fuera a todas aquellas acciones donde el medio informático es solo la herramienta a través de la cual se realiza un delito tradicional, sin embargo, su utilidad conceptual reside en la necesidad de un análisis jurídico de la ola de nuevos tipos de delincuencia que aparecieron con la creciente adopción de la informática por parte de la población.

2. Delitos informáticos en *lato sensu*

Parece claro que el enfoque restrictivo permite el estudio del núcleo de las acciones que suelen desplegarse por parte de los grupos delictivos, con el fin de conseguir sus diversos objetivos criminales, pero la naturaleza híbrida y pluriofensiva de la ciberdelincuencia organizada moderna, cuyo marco de acción es tan amplio que genera un impacto en los principales intereses de la sociedad del Siglo XXI, lo que hace imperativo adoptar una definición que no restrinja el estudio de este fenómeno cambiante y resiliente.

Por ende, en sentido amplio nos permitimos definir al delito informático como toda aquella acción delictiva que se desarrolla especialmente por medios informáticos. Este concepto, nos permite incorporar el estudio de ciertas

modalidades de delitos tradicionales, en las cuales el elemento informático es protagonista y que son parte de la ciberdelincuencia moderna.

Una modalidad delictiva que nos permite ilustrar lo anterior, es la ‘sextorsión’, en la cual los ciberdelincuentes por medio de la seducción, usualmente a través de la utilización de identidades falsas⁵, establecen comunicaciones de contenido sexual o erótico con sus víctimas, para obtener fotografías o videos íntimos, con el fin último de amenazarles con la difusión del material íntimo sino le pagan un monto económico. En este caso nos encontramos ante una modalidad de extorsión simple que:

- a) Se despliega principalmente en el ciberespacio.
- b) Involucra el tratamiento ilegal de datos personales.
- c) Amenaza de/y/o difusión de documentos electrónicos de índole privada.
- d) Es una figura explotada por el cibercrimen organizado⁶.

Por otro lado, el *ransomware*⁷ es una modalidad de extorsión calificada, la cual es potenciada por la tecnología y que está siendo utilizada de forma

⁵ Una identidad falsa es toda aquella utilizada con fines fraudulentos o de engaño, al no corresponder con la identidad real del individuo.

⁶ “Cientos de miles de hombres de todo el mundo caen víctimas cada año de un crimen en internet llamado “sextorsión”. Primero los hombres son atraídos y tentados a participar en chats sexualmente explícitos con cámara web, y después son chantajeados: o pagan o hacen públicos los videos. Los extorsionistas son grupos organizados que operan desde diferentes países, como Filipinas. (BBC Mundo, 2014)

⁷ Definición del programa informático malicioso tipo ‘ransomware’: El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos (Instituto Nacional de Ciberseguridad, 2017, p. 31)

agresiva⁸ por grupos cibercriminales, la cual consiste en la utilización de un programa informático malicioso con el fin de ‘secuestrar’⁹ la información contenida en un ordenador, como medio de presión para obtener un lucro a cambio de devolverle el acceso a la víctima de su información. Adicionalmente, algunos grupos recurren a la modalidad de doble extorsión, que consiste en extraer bases de datos personales de clientes y/o información confidencial de sus víctimas, antes de cifrarla¹⁰, incrementando así la presión extorsiva, ya que si el cliente no cumple las demandas de los extorsionistas¹¹ -que suele pedirse a través de criptomoneda¹²- los delincuentes no solo no brindarán las claves, para descifrar la información, sino también publicarán las bases de datos con información sensible, generando un daño grave tanto a la reputación de la empresa, como a la privacidad de ciudadanos.

⁸ Si se compara con los datos de 2019, los ataques de ransomware a nivel global crecieron un 485% en 2020, según el análisis que ha hecho Bitdefender de la evolución de las ciberamenazas más importantes. (IT Digital Security, 2021)

⁹ Los delincuentes lo que realizan es un cifrado de la información, para que no esté disponible para el titular, salvo que pague el rescate. Podríamos decir que la información se encuentra “secuestrada” en el propio equipo de la víctima.

¹⁰ Los delincuentes cifran la información con fines delictivos, sin embargo, es una operación que puede realizarse con fines de proteger la privacidad de la información. El concepto de cifrado o algoritmos de cifrado es el siguiente:

Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado atendiendo a las características de las claves de cifrado, estos son el cifrado simétrico y cifrado asimétrico. (Instituto Nacional de Ciberseguridad, 2017, p. 31)

¹¹ En nuestro país, el caso más emblemático que se ha dado de ransomware es el caso del Banco de Costa Rica, en donde el grupo cibercriminal Maze amenazó con publicar la base de datos con información de los clientes del banco sino se realizaba el pago que ellos pedían. Los delincuentes cumplieron parcialmente su amenaza y publicaron alguna de la información prometida, lo que deja dudas sobre si, en primer lugar, la tenían completa.

¹² La criptomoneda o criptodivisa es un tipo de moneda digital que utiliza la criptografía para proporcionar un sistema de pagos seguro. Estas técnicas de cifrado sirven para regular la generación de unidades monetarias y verificar la transferencia de fondos. No necesitan de un banco central u otra institución que las controle. Las criptomonedas son un tipo de moneda digital, que son aquellas que no existen de forma física, pero que sirven como moneda de intercambio, permitiendo transacciones instantáneas a través de Internet y sin importar las fronteras. (Criptomoneda - qué es, definición y concepto , 2017)

Por lo anterior, no podríamos imaginarnos estudiar los delitos informáticos sin incluir estas nuevas modalidades delictivas. Como puede verse, nos dirigimos a un momento donde un gran porcentaje de delitos que se encuentra en el Código Penal podrían tener una modalidad informática, que sin duda podría estudiarse dentro de lo que conocemos como delincuencia informática.

El lector podría sorprenderse con que, en las próximas décadas, lo que los ciberdelincuentes ataquen, ya no solo sean los sistemas informáticos como los conocemos ahora, sino que también a los seres humanos cuyo sistema incorpore elementos informáticos, como algún chip¹³ que potencie su rendimiento. Un ataque informático de esta índole podría atacar de forma directa contra la vida¹⁴, los sentidos y/o alguna función biológica del ser humano (e inclusive de animales), de forma permanente o temporal, lo que cambiará la percepción que tendrá la sociedad sobre la ciberdelincuencia¹⁵.

Por lo anterior, con el avance hacia el transhumanismo¹⁶ de darse un debate regulatorio sano sobre la tutela penal especial en esta materia, la cual podría inclusive resultar extensiva a animales, que con ayuda de la tecnología puedan

¹³ La definición de chip es "Pequeña pieza de material semiconductor que contiene múltiples circuitos integrados con los que se realizan numerosas funciones en computadoras y dispositivos electrónicos. (RAE, 2021)

¹⁴ Aunque se pueda ver como un análisis de ciencia ficción lo cierto es que dispositivos médicos como los marcapasos están siendo ya objetivo por parte de los ciberdelincuentes. En este sentido un reportaje de la ABC nos alerta:

"Para los pacientes con desfibriladores implantables, es posible que los hackers interrumpen las comunicaciones inalámbricas, lo que inhibe el valor de la telemonitorización y permite que el sistema no detecte ningún evento clínicamente relevante. La sobredetección puede inhibir la estimulación o dar lugar a descargas inapropiadas o potencialmente mortales." (ABC, 2018)

¹⁵ En este sentido, en nuestro Código Penal, en el artículo 232 que sanciona la instalación y propagación de programas informáticos maliciosos, contiene un agravante en el caso que se ataque un sistema informático de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

¹⁶ "El transhumano es el ser humano mejorado física, cognitiva, moral o emocionalmente por medio de la tecnología" (Ethic, 2017).

comunicarse de forma fluida con nosotros. El anterior, sin lugar a dudas, es un tema controversial que nos saca de la zona de confort y cuyo análisis requiere de profesionales en derecho que comprendan el entorno tecnológico y el científico.

d. Características de los delitos informáticos.

Para Chinchilla (2002), estos delitos poseen peculiaridades que les hacen de alguna manera *sui generis*, por una parte, en cuanto a su forma de comisión y, por otra, respecto a su detección. El autor cita 3 siguientes características de los delitos informáticos, que consideramos vigentes hasta la actualidad:

a) Rapidez (en tiempo) y acercamiento (en espacio): las acciones delictivas a través de medios informáticos permiten una rapidez sin precedentes y pueden inclusive realizarse desde lugares a miles de kilómetros de distancia del lugar donde se producen los efectos. Lo que es particularmente peligroso, en la actualidad, cuando se atacan infraestructuras críticas de las naciones y cuyo riesgo aumentará con la implementación de las redes 5G.

b) Facilidad para encubrir el hecho: Los delincuentes pueden hacer parecer que su procedencia es de un lugar distinto al real o pueden programar rutinas que dificulten la detección de sus acciones. Adicionalmente, podríamos agregar que actualmente el anonimato forma parte de las ventajas con las que cuenta el ciberdelincuente, por lo que resulta difícil vincular sus acciones con su identidad real.

c) Facilidad de borrar las pruebas: aunque similar a la anterior, en casos donde la actividad delictiva ha cesado, la facilidad con la que se pueden borrar

las pruebas representa un reto enorme para las fuerzas del orden.

e. El Sujeto activo

Con la reducción de la brecha digital y el amplio catálogo de acciones delictivas que se encuentran en nuestro Código Penal nos permite concluir que cualquiera puede ser un ciberdelincuente y víctima de un delito informático.

A pesar de la afirmación anterior, para fines de comprensión, sin pretender abarcar todos los tipos de actores que hay, se puede limitar a los sujetos activos en dos categorías no excluyentes:

- a) **Caza-vulnerabilidades:** este tipo agente se encuentra en constante búsqueda de errores en los sistemas informáticos que puedan facilitarle la comisión de actos delictivos. Al encontrar vulnerabilidades, puede venderlas y/o crear herramientas que automaticen su explotación, con las cuales pueden lucrar o ponerlas a disposición del público de forma gratuita¹⁷.

Este tipo de delincuente es especializado, puede trabajar de forma individual, para un Estado atacante o cualquier otro tipo de organización criminal.

- b) **Usuarios de herramientas:** ya sean herramientas tecnológicas dirigidas especialmente para la comisión de actividades delictivas o que son abusadas para distintos fines. En esta clase de categoría encontramos a todo usuario que, aunque no contara con conocimientos especializados

¹⁷ Importante destacar que hay *hackers* éticos que también se dedican a detectar vulnerabilidades y las reportan de forma responsable a los desarrolladores.

sobre informática, puede utilizar estas herramientas que automatizan la comisión de los abusos informáticos.

f. Delitos informáticos contra la privacidad.

Como hemos comentado, este tipo de delitos tienen una naturaleza pluriofensiva de bienes jurídicos y es difícil imaginar acciones desplegadas por la ciberdelincuencia, en la actualidad, que no lesionen de forma directa o indirecta la privacidad de sus víctimas, como lo es el caso de la compra y venta de bases de datos personales.

A manera de ejemplo, en las estafas informáticas que se dan de forma tan frecuente en Costa Rica, como *conditio sine qua non* para iniciar con el 'vishing'¹⁸ el estafador debe haber obtenido, de cualquier vía, alguna base de datos con información de sus víctimas. De la misma manera, cuando obtiene las credenciales necesarias para ingresar en la cuenta de la víctima para realizar las transacciones ilegales, el actor logra acceder información sensible de su víctima porque en la banca electrónica se encuentran todos los datos de hábitos de consumo del cliente del sistema financiero¹⁹.

IV. El delito de violación de datos personales. (Artículo 196 bis)

¹⁸ Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. (INCIBE, 2017). Cuando la misma se realiza a través de la utilización de llamadas utilizando la voz, se denomina '**vishing**'.

¹⁹ Estos datos se reconocen como sensibles en nuestra legislación de protección de datos personales, al ser de carácter socioeconómico.

VIOLACIÓN DE DATOS PERSONALES

(ARTÍCULO 196 BIS DEL CÓDIGO PENAL)

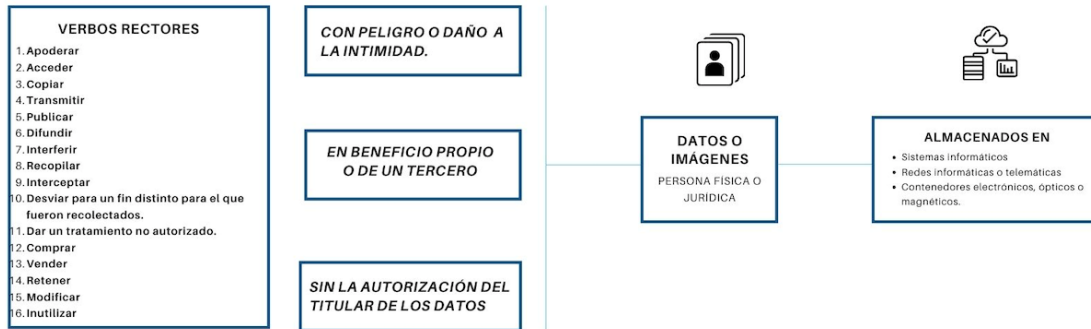


Figura 2. Elaboración propia

En la reforma al Código Penal de la sección VIII, denominada *Delitos Informáticos y Conexos*, del título VII, a través de la ley № 9048, se incorporó la violación de datos personales, cuyo fin es proteger a los datos personales de su tráfico ilegal.

Este comercio ilegal de datos es piedra angular de distintas acciones delictivas del cibercrimen, por lo que los ataques informáticos más frecuentes, a nivel mundial, están vinculados de forma directa o indirecta con el abuso de los datos personales, ya sean estos perpetrados por organizaciones criminales, individuos o Estados atacantes²⁰. Debido a esto, el legislador costarricense, de manera acertada, incorpora este tipo penal inspirado en el Código Penal colombiano, que el año 2009, en su artículo 269F incluyó el delito de violación de datos personales con elementos bastante similares al nuestro, lo que para ambas naciones es un paso importante hacia el fortalecimiento de la protección de los

²⁰ El Estado atacante es toda aquella nación que forma parte de la llamada 'ciberguerra', realizando ataques a otras naciones con fines políticos o de información.

datos de los habitantes:

El artículo 196 bis del Código Penal costarricense en su primer párrafo reza:

“Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores, electrónicos, ópticos o magnéticos.”

El tipo penal puede sanciona cualquier tratamiento no autorizado por el titular que cumpla con los siguientes elementos:

1. En beneficio propio o de un tercero.
2. Con peligro o daño a la intimidad.
3. Datos, de persona física o jurídica, almacenados en sistemas informáticos.
4. Sin autorización del titular de los datos.

Bien jurídico tutelado.

La autodeterminación informativa sobre los datos electrónicos.

De acuerdo a la ley № 8968 y a diversas resoluciones de la Sala Constitucional, la autodeterminación informativa es un derecho fundamental derivado del derecho a la privacidad, que tiene toda persona sobre el flujo de informaciones

que conciernen a su persona, de acuerdo a las garantías y excepciones que contiene el ordenamiento jurídico, con el fin de evitar que se propicien acciones discriminatorias.

Es importante destacar que este tipo penal protege únicamente al dato personal que se encuentra alojado en soportes electrónicos, por lo que toda conducta ilegal realizada sobre datos en soportes físicos no es sancionable penalmente a través de este tipo penal. Aunque es discutible el porqué no se extendió la tutela penal a todos los datos, sin hacer distinción en cuanto al soporte en el que se encuentra almacenado, lo cierto es que la informática aumenta el riesgo y la potencia con la que se puede lesionar un bien jurídico, por lo que no puede negarse que la decisión o preocupación del legislador se encuentra fundamentada.

Por lo anterior, no resulta sorprendente, que el desarrollo de la informática generó en el continente europeo una serie de reformas vinculadas con este derecho que han influido de forma importante en nuestro país.

La primera ola de reformas legales surgió en el campo de la protección a la intimidad en los años setenta del siglo XX. Las nuevas tecnologías brindaban la posibilidad de formas de procesamiento, almacenamiento y transmisión de datos inexistentes hasta aquel momento. Datos relativos a las personas aparentemente insignificantes, sin comportar un riesgo a la intimidad personal en caso de encontrarse en manos de otros distintos a su titular, se convertían en una información valiosísima después de ser agrupados, tratados en forma conjunta, interrelacionados y analizados mediante los modernos medios tecnológicos. (Davara, 2017, p.47)

En ese sentido, la Constitución Española de 1978 reconoce el riesgo de la informática sobre la intimidad personal y otros derechos, por lo que ordena que mediante la ley esta debe limitarse, a través de su artículo 18.4 que reza de la siguiente manera:

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. (Constitución de España, 1978)

En línea similar, veinte años después y de manera visionaria, la Sala Constitucional costarricense decide reconocer lo que llama el nuevo derecho de la intimidad en la sociedad informatizada.

Lo que hoy conocemos como “sociedad informatizada” plantea nuevos retos al concepto clásico del derecho a la intimidad. En la década de los ochenta y noventa, en nuestro país, la libertad individual, la personal y la colectiva, estaban relativamente lejos de la influencia de la tecnología. Así por ejemplo, el ciudadano no se cuestionaba con qué fin le eran solicitados sus datos personales, quienes tienen acceso a ellos con cual objeto. Consecuentemente, el derecho a la protección de la persona frente al procesamiento de sus datos personales es una cuestión que se deja sólo a la academia. Es pronto también para cuestionarse si la manipulación de los datos personales puede vaciar el contenido esencial de algunos de los derechos fundamentales. Menos aún se concibe que el desarrollo informativo pueda implicar alguna forma de violencia. En la actualidad, la doctrina nacional y extranjera, admite que la manipulación de la información posibilita el control sobre el ciudadano como una alternativa real y efectiva. De tal manera que los derechos individuales de los ciudadanos puedan quedar prácticamente sin contenido efectivo. Así ocurre, cuando se

desarrollan perfiles de las personas utilizando información aislada y aparentemente inofensiva.

La informática, no sólo representa uno de los más grandes avances del presente siglo, sino que pone en evidencia las posibilidades de inspección de la vida interior de las personas, desde este punto de vista, la personalidad de los ciudadanos y su fuero interno cada vez se hacen más transparentes. Esta situación hace necesario que los derechos fundamentales amplíen también su esfera de protección. La esfera privada ya no se reduce al domicilio o a las comunicaciones, sino que es factible preguntarse si es comprensible incluir “la protección de la información” para **reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar. Lo expuesto, significa que el tratamiento electrónico de datos, como un presupuesto del desarrollo de nuestra actual sociedad democrática debe llevarse a cabo afianzando los derechos y garantías democráticas del ciudadano** (arts. 24, 22, 123, 2824, 3025, 3326 y 4127 de la Constitución). Es obvio, que el acceso a la información es un poderoso instrumento de progreso individual, y para el ejercicio de los derechos políticos y sociales. Pero también debe reconocerse que el progreso no significa que los ciudadanos deban quedar en situación de desventaja frente al Estado o a los particulares. El nuevo derecho a la intimidad, debe ponderar los intereses en conflicto, entre el legítimo interés de la sociedad a desarrollarse utilizando la información, como la también necesidad de tutelar a la persona frente al uso arbitrario de sus datos personales. **La tutela a la intimidad implica, la posibilidad real y efectiva para el ciudadano de saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias, para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta** (arts. 24 de la

Constitución y 13 inciso 1, de la Convención Americana de Derechos Humanos).”²¹ (Sala Constitucional, Resolución N° 01345 - 1998).

Los datos personales en entornos informáticos.

La Sala Constitucional en su jurisprudencia ha manifestado que “la garantía del derecho fundamental no depende de la titularidad del medio sino que es independiente de la titularidad del soporte” (Sala Constitucional, N° 2005-15063), principio que es de alto interés en materia de derechos digitales, como el caso del derecho de protección de datos personales objeto de la presente investigación, donde el titular tiene el derecho de control sobre sus datos, sin importar cuál es el soporte en el que se encuentren alojados. En esa línea, desde que nacemos la ley y nuestros representantes legales dan licencia a terceros para el tratamiento de nuestros datos personales, labor la cual pueden realizar en entornos digitales ajenos a nuestro control, en apego a los fines para los que fueron recopilados y para los tratamientos que se encuentren debidamente autorizados.

Este tratamiento en entornos que no son de nuestra propiedad aumentan los riesgos de lesionar la privacidad y generar acciones discriminatorias, las cuales en casos de bases de datos públicas pueden darse de manera masiva²².

La violación de datos personales (artículo 196 bis, CP) tutela los datos que se encuentren en:

²¹ Las negritas contenidas en esta resolución no corresponden a su original.

²² En Costa Rica se ha vuelto práctica común fisgonear la vida de otros ingresando al Registro Civil para conocer sobre las relaciones familiares que el Tribunal Supremo de Elecciones ha decidido que son de acceso irrestricto.

a) Contenedores electrónicos, ópticos o magnéticos: el legislador cuando realizó la reforma al Código Penal contenida en la ley Nº 9048 sobre delitos informáticos, decidió adoptar el concepto de contenedor como sinónimo de soporte²³ para este y otros tipos penales informáticos. No estamos de acuerdo con esta imprecisión, ya que a los materiales que contienen información no se les conoce a nivel técnico como contenedores y esto podría generar que conductas donde los datos violados se encuentren en dispositivos aislados de almacenamiento no puedan ser sancionadas penalmente por atípicas.

El concepto técnico y más preciso para referirse a los materiales que permiten el almacenamiento de información es el de soporte²⁴, los cuales pueden contar con capacidad de almacenamiento en formato electrónico²⁵. Los soportes de información pueden ser magnéticos, ópticos, magneto-óptico, telemáticos, de estado sólido, biológicos²⁶, entre otros.

Sistema informático: “todo dispositivo²⁷ aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan en ejecución de un programa” (Convenio sobre la Ciberdelincuencia, artículo 1 inciso a)). Importante destacar, que todo sistema informático requiere de un soporte de almacenamiento para funcionar, ya que esto es parte de sus funciones.

²³ Este concepto fue el utilizado en el artículo 196 bis del Código Penal, llamado Violación de comunicaciones electrónicas, el cual fue incluido por la ley Nº 8148 (2001) y fue reformada por la ley Nº 9048 (2012).

²⁴ **Soporte:** Material en cuya superficie se registra información, como el papel, la cinta de video o el disco compacto. (RAE, 2021)

²⁶ Para solucionar los problemas de memoria, Microsoft tiene previsto tener un sistema de almacenamiento de datos en ADN funcionando en unos pocos años. Microsoft tiene previsto tener un sistema de almacenamiento de datos en ADN funcionando en unos pocos años. Así lo han asegurado arquitectos informáticos de la compañía en MIT Technology Review, donde afirman que están desarrollando un dispositivo que reemplaza las unidades magnéticas por unidades biológicas para guardar información digital. (Arteaga, 2017)

²⁷ **Dispositivo:** Aparato, o elementos de un sistema, conectados para poder ser reconocidos por el sistema operativo cumpliendo determinadas reglas de configuración. (González, 2018, p.16).

Red informática: Conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones. (González, 2018, p.50).

Sobre datos digitalizados.

El tipo penal requiere que al momento de realizar la acción contenida en el verbo típico se aplique sobre datos que se encuentren almacenados en sistemas informáticos o contenedores informáticos, por lo que si un dato se encuentra en soporte de papel y se digitaliza, este adquiere tutela penal al almacenarse en un sistema informático, aunque la acción de digitalización la realice el delincuente. A manera de ejemplo, si una persona compra bases de datos en papel y las digitaliza para difundirlas por internet, la difusión sí podría ser sancionada penalmente, más no la digitalización, la cual es un tratamiento no autorizado, el cual podría denunciarse ante Prodhav²⁸.

El sujeto pasivo.

La ley de protección de la persona frente al tratamiento de sus datos personales, reconoce el derecho de autodeterminación informativa únicamente a personas físicas, sin embargo, la Sala Constitucional que desarrolló este derecho a finales del siglo pasado, cobijó a las personas jurídicas, de similar manera que el Código Penal en el año 2012, con la inclusión del tipo penal bajo estudio. Por lo anterior,

²⁸ Sería una falta grave, de acuerdo al artículo 3, inciso a) de la Ley № 8968.

el sujeto pasivo en esta clase de delitos puede ser tanto una persona física como una jurídica.

En ese sentido la Sala Constitucional, al definir el derecho de autodeterminación informativa, manifiesta:

En este caso, también estamos ante una lesión **al derecho a la autodeterminación informativa** de la parte tutelada, el cual fue definido por este Tribunal en su sentencia número 4847-99, como el “ **derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que esa información se destine y a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión.** Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir.”. (Sala Constitucional, Resolución N° 14676 - 2020)

Es importante subrayar que los datos de las personas jurídicas están contenidos en los repositorios que almacenan y distribuyen los ciberdelincuentes con fines delictivos, al ser información de alto valor para sus operaciones criminales, por lo que la tutela penal de los datos personales de persona jurídica es relevante y tiene sentido desde la perspectiva de la política criminal en contra de la ciberdelincuencia.

En España, de igual manera, se permite tutelar penalmente los datos reservados de carácter personal de una persona jurídica, ya que extiende la

protección del capítulo *Del descubrimiento y revelación de secretos a las personas jurídicas*:

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cedere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código. (Código Penal de España de 1995, artículo 200)

Concepto de dato personal.

La ley № 8968 define al dato personal como “cualquier dato relativo a una persona física identificada o identificable” (Ley de la protección de la persona frente al tratamiento de sus datos personales, artículo 3, inciso a.)

Por otro lado, el concepto de dato personal de persona jurídica no lo encontramos en nuestro ordenamiento jurídico, sin embargo la Sala Constitucional nos da luz sobre este concepto en su jurisprudencia, al definirle de igual manera que el de persona física:

III.- El objeto de protección del hábeas data y los principios básicos para la protección de datos. Objeto de protección del hábeas data son los “datos de carácter personal”, es decir, **cualquier información relativa a una persona física o jurídica identificada o identificable**. El grado de protección de los datos dependerá de la naturaleza de los mismos, así, debe el Estado procurar que los datos íntimos (también llamados “sensibles”) de las personas no sean siquiera accedidos sin su expreso consentimiento. (Sala Constitucional, Resolución N° 08996 – 2002)

Verbos rectores.

El tipo penal incluye los siguientes verbos rectores o acciones que se pueden ejercer sobre el dato de una persona física o jurídica, cuyas acciones deberán entenderse en un contexto informático y ejercidas sobre un dato personal:

- a) **Apoderar**: Acción a través de la cual un usuario toma posesión de la información de carácter personal de otro²⁹.
- b) **Acceder**: Acción informática a través de la cual el agente tiene acceso al dato personal³⁰. Un ejemplo de esta acción es cuando una persona ingresa a una base de datos electrónicas y ejecuta un comando para acceder al dato.
- c) **Copiar**: Acción de duplicar un dato³¹.
- d) **Transmitir**: trasladar o transferir un dato de un lugar a otro³².
- e) **Publicar**: Incorporar al acceso público un contenido en un entorno digital (RAE, 2021)
- f) **Difundir**: Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas (RAE, 2021). De acuerdo al reglamento de la ley Nº8968, se define distribución, difusión de la siguiente manera: “Cualquier forma en la que se repartan o publiquen datos personales, a un tercero” (Reglamento N° 37554-JP, 2016)

²⁹ **Apoderar**: “Hacerse dueño de algo, ocuparlo, ponerlo bajo su poder”. (RAE, 2021)

³⁰ **Acceder**: “Tener acceso a algo, especialmente a una situación, condición o grado superiores, o llegar a alcanzarlos. (RAE, 2021)

³¹ **Copiar**. La Real Academia Española no contiene una definición precisa y aplicable para el campo de la informática, por lo que ante una consulta del diccionario Merriam-Webster (2021) que contiene una definición para la informática la cual podemos traducir como “hacer una copia o duplicado de... un documento o archivo de computadora” (Merriam Webster, 2021). De acuerdo a la RAE, duplicar es: “Repetir exactamente algo, hacer una copia de ello”

³² **Transmitir**:

1. Trasladar, transferir.
2. Dicho de una emisora de radio o de televisión: Difundir noticias, programas de música, espectáculos, (RAE, 2021)

- g) por cualquier medio siempre que medie un fin de comercializar el dato o medie el lucro con la base de datos.
- h) **Interferir:**
dicho de una señal: Introducirse en la recepción de otra y perturbarla. (RAE, 2021)
- i) **Recopilar:** recoger datos personales con un fin³³.
- j) **Interceptar:** apoderarse de datos contenidos en una comunicación³⁴ antes de que lleguen a su destino final³⁵.
- k) **Desviar³⁶ para un fin distinto para el que fueron recolectados:** los datos personales deben recopilarse para fines específicos, que fueron autorizados por el titular o una ley facultativa, que no pueden ser variados por el responsable de la base de datos de manera unilateral.
- l) **Dar un tratamiento no autorizado:** cada una de las acciones que se realicen sobre un dato deben estar debidamente autorizados por el titular o por ley. De acuerdo al reglamento de la ley №8968, se define como tratamiento: “Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.” (Reglamento N° 37554-JP, 2016)
- m) **Comprar:** obtener el dato por un precio.

³³ **Recopilar:** Juntar en compendio, recoger o unir diversas cosas, especialmente escritos literarios. (RAE, 2021)

³⁴ **Comunicación:** Transmisión de señales mediante un código común al emisor y al receptor. (RAE, 2021)

³⁵ **Interceptar:** Apoderarse de algo antes de que llegue a su destino. (RAE, 2021)

³⁶ **Desviar:** Apartar o alejar a alguien o algo del camino que seguía. (RAE, 2021)

- n) **Vender:** Traspasar a alguien por el precio convenido la propiedad de lo que se posee. (RAE, 2021).
- o) **Retener:** Impedir que algo salga, se mueva, se elimine o desaparezca. (RAE, 2021).
- p) **Modificar:**
Transformar o cambiar algo mudando alguna de sus características. (RAE, 2021).
- q) **Inutilizar:** hacer inútil, vano o nulo algo. (RAE, 2021).

El beneficio propio o de un tercero.

El elemento del beneficio es *conditio sine qua non* en este delito y precisamente es uno de los elementos que lo diferencian de la violación de datos personales administrativa, que la persona puede denunciar ante la Prodhav. De acuerdo a la Real Academia Española (2020), podemos definir al beneficio de la siguiente manera:

1. Bien que se hace o se recibe.
2. Utilidad (provecho): a su vez la utilidad la define como “Provecho, conveniencia, interés o fruto que se saca de algo” .

Como puede extraerse de la definición, la violación de datos personales debe generarle beneficio, provecho³⁷ o utilidad al agente, o a un tercero. Sin pretender presentar una lista taxativa, los beneficios, no excluyentes entre sí, que pueden presentarse son los siguientes:

³⁷ Como puede verse más adelante el legislador colombiano adoptó el término provecho en el tipo penal de violación de datos personales.

- a) **Comerciales:** para fines de mercadeo o conexos.
- b) **Electorales:** los datos pueden ser utilizados de forma interna para generar análisis y tomar decisiones de carácter político, pero también podrían usarse para enviar comunicaciones masivas no solicitadas.
- c) **Delictivos:** la información de carácter personal suele ser utilizada para crear perfiles de personas con la cual pueden realizar distintas actividades de carácter delictivo, como por ejemplo, para iniciar ataques de ingeniería social para realizar estafas informáticas.
- d) **Económicos:** en este caso el beneficio es directo y de contenido económico.
- e) **Laboral:** aunque de naturaleza similar a la anterior, en estos casos la persona podría obtener alguna ventaja para obtener o permanecer en un puesto debido a la acción sobre el dato.

Como puede verse, no necesariamente el beneficio debe ser de índole patrimonial, pero sí debe ser tangible y/o susceptible de ser acreditado en una investigación penal, ya que cuando el operador jurídico realice el juicio de tipicidad debe cerciorarse de que la conducta sujeta a su análisis se realice en beneficio propio o de un tercero, así como los otros elementos contenidos en la descripción típica.

El tráfico de datos personales es una conducta donde el dato es objeto comercial, el cual se transfiere a cambio de una contraprestación, la cual no necesariamente tiene contenido patrimonial. Debido a lo anterior, se puede concluir que cuando se trafican datos personales existe una persona que obtiene

un beneficio con esta acción y que esta dinámica genera un mercado ilegal de información personal y lesiona de forma sistemática la privacidad de los ciudadanos; lo que justifica la decisión del legislador de sancionarlo penalmente, al incorporar el delito de violación de datos personales en el artículo 196 bis del Código Penal. Lo anterior, en armonía con la ley de protección de la persona frente al tratamiento de sus datos personales, por lo que cuando en distintas acciones ilegales que lesionan el derecho de autodeterminación informativa, no está presente el beneficio, el ciudadano pueda siempre acudir a otras vías de resolución de este conflicto social, como lo puede ser la vía administrativa o la constitucional.

A pesar de que los tipos de beneficio que permite el tipo penal son *numerus apertus*, es importante ser claro que, de ninguna manera, el beneficio puede extenderse inclusive al sentimiento de satisfacción que puede sentir una persona al publicar de forma vengativa un dato personal de índole sexual o erótico, como en los casos de “porno-venganza”³⁸. Si una autoridad judicial hiciera uso de este criterio, no solo generaría una profunda inseguridad jurídica, sino que la misma resultaría violatoria de la regla de interpretación restrictiva, la prohibición de la interpretación analógica y del principio de legalidad, que rigen en materia penal y procesal penal³⁹.

Desafortunadamente, la formula del beneficio puede resultar insuficiente para combatir la publicación masiva de bases de datos personales por parte de la

³⁸ Esta conducta, cuando se trata de documentos privados encuadra en el artículo 196 del Código Penal en su párrafo segundo

³⁹ Inclusive si el lector quisiera hacer un ejercicio futurista, se adelantara cien años, y se imaginara que un fiscal solicite el acceso a los recuerdos del imputado contenidos en soportes biológicos, la solicitud no sería de recibo porque de acuerdo al artículo 36 de la Constitución Política nadie está obligado a declarar contra sí mismo, por lo que la extracción, no consentida, de un recuerdo sería a todas luces una declaración obligada y por ende inconstitucional.

ciberdelincuencia donde no se busca un beneficio, sino simplemente realizar un daño a la privacidad colectiva, lo que es una modalidad de lo que se conoce como “doxing”⁴⁰ y que cuando se dirige a individuos de forma individual suele realizarse como parte de un acoso cibernético⁴¹.

Agravantes.

En el delito de violación de datos personales, las penas serán de dos a cuatro años de prisión cuando las conductas descritas:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos: en este caso no solo se sanciona de manera más grave a las personas que con mayores conocimientos de informática y/o por la confianza inherente a su cargo realizan la conducta delictiva, sino que también a toda persona que debido al acceso que ha tenido al sistema debido a sus funciones decide violar los datos del titular.

b) La información vulnerada corresponda a un menor de edad o incapaz: El legislador decidió proteger los datos de los menores, sin que implique

⁴⁰ El “doxing” anglicismo que abrevia el concepto de exponer documentos: Consiste en revelar información identificadora de una persona en línea, como su nombre real, dirección particular, lugar de trabajo, teléfono, datos financieros y otra información personal. Luego, esta información se divulga al público sin el permiso de la víctima.

Si bien la práctica de revelar información personal sin el consentimiento del sujeto en cuestión existe desde antes del nacimiento del Internet, el término doxing surgió primero en el mundo de los hackers en la década de 1990, en el que el anonimato se consideraba sagrado. Las disputas entre los hackers rivales a veces provocaban que alguien decidiera “exponer docs” sobre otra persona, quien hasta ese momento solo era conocida por su nombre de usuario o alias. “Docs” se convirtió en “dox” y, finalmente, en su propio verbo (es decir, sin el prefijo “exponer”) (Kaspersky, 2021)

⁴¹ Como se analizará más adelante el Código Penal de 1995 de España sanciona las acciones que se realizan en perjuicio del titular, a diferencia del costarricense que requiere un beneficio.

necesariamente un mayor daño o que afecten una categoría de datos personales.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias la salud, el origen racial, la preferencia o la vida sexual de una persona: en este caso nos encontramos ante los datos que en nuestro ordenamiento jurídico se conocen como datos sensibles pero presentados en una lista taxativa que da mayor seguridad jurídica en su aplicación.

Aclaraciones sobre la aplicación del tipo penal.

La reforma № 9135 que vino a reformar el Código Penal, tan solo un año después de la reforma № 9048, se realizó en un contexto de señalamientos de “Ley mordaza”, los cuales nos parecen fueron infundados, pero es cierto que permitieron corregir algunos de los errores graves que contenía la reforma, más por razones de índole político, no todos pudieron corregirse.

Debido a esto, con enorme influencia de medios de comunicación, en lo que podría considerarse una mala técnica legislativa se incorporaron, a nuestro criterio de manera innecesaria, “aclaraciones” sobre qué no configura este delito⁴² en los siguientes casos:

1. No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley: en estos casos nos encontramos ante situaciones donde

⁴² Aun en los casos donde la conducta que el legislador aclara que no es delito, de acuerdo con la descripción típica del tipo no sería delito.

no existiría violación de la privacidad y se contaría con facultad legal para realizar la publicación. Lo que es cierto es que este tipo de aclaraciones trajeron tranquilidad a la prensa nacional y eso es de gran valor en una democracia.

2. Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley: nuevamente, si un tratamiento se hace conforme a la ley no contendría todos los elementos para que sea considerado delito, al no ser típico, antijurídico ni culpable.

Caso nacional

Acceso ilegal a datos de Keylor Navas.

En el Poder Judicial se presentó un caso de un acceso ilegal de datos personales confidenciales, los cuales estaban almacenados en su sistema interno para investigaciones judiciales. Este acceso fue realizado por parte de funcionarios, en donde aparentemente el fin que tenían, era el de satisfacer su curiosidad sobre la vida personal del deportista que jugaba en el Real Madrid, aprovechando el acceso con el que contaban en la Plataforma de Información Policial (PIP).

Por los motivos legales expuestos anteriormente, no podríamos concluir que la satisfacción de su deseo de fisgonear, pueda interpretarse como una utilidad que obtuvieron de su acción ilegal, ya que esa sería una interpretación extensiva y analógica⁴³.

En esa misma línea, la causa fue desestimada, como lo reportó el diario electrónico de La Nación:

El Juzgado Penal del Segundo Circuito Judicial de San José desestimó la causa penal abierta contra 25 funcionarios judiciales que, en el 2014, accedieron a información privada del portero costarricense Keylor Navas en una base de datos policial, la cual es de acceso restringido.

La desestimación fue solicitada por la Fiscalía Adjunta de Probidad, Transparencia y Anticorrupción, la cual argumentó que los hechos investigados “no configuraron una conducta delictiva tipificada en nuestra legislación”, lo que se conoce, técnicamente, como atipicidad (Artavia, S. 2020).

Derecho comparado.

España.

El Código Penal de España de 1995 decidió tutelar penalmente los datos reservados de carácter personal en el título X que contiene los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.

En el numeral 197.1, parte del capítulo I, correspondiente al *Descubrimiento y revelación de secretos*, sanciona penalmente la violación de correspondencia y documentos privados de manera similar al artículo 196 de nuestro Código Penal⁴⁴, con penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

⁴⁴ 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será

Apoderamiento, utilización o modificación de datos personales

ARTÍCULO 197.2 DEL CÓDIGO PENAL DE ESPAÑA

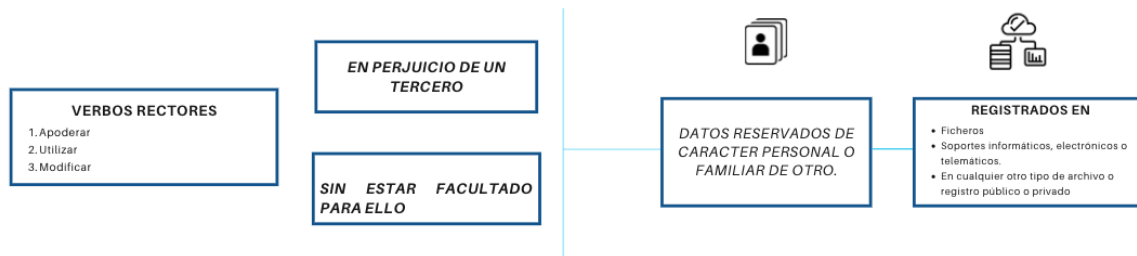


Figura 3. (ARTÍCULO 197.2 del Código Penal de España [Elaboración propia])

Por otro lado, en el numeral 197.2, sanciona el apoderamiento, utilización o modificación de datos personales, el cual cuenta con similar naturaleza al de violación de datos personales costarricense:

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Igualess penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. (Código Penal de España, artículo 197.2)

Debido al objeto de estudio de la presente investigación, procederemos a analizar los de elementos de este tipo penal:

a) Sin estar autorizado: nos parece adecuado ya que es un concepto más amplio que incluye tantos tratamientos realizados con el consentimiento

castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. (Código Penal de España, Artículo 197.1)

expreso, por autorización de carácter legal e inclusive contractual.

b) Verbos rectores: apoderamiento, utilizar y modificar: si bien es cierto la cantidad de verbos rectores es inferior en cantidad a los contenidos en la violación de datos personales costarricense, lo cierto es que el verbo “utilizar” es lo suficiente amplio como para poder extenderse a varios de los verbos que están contenidos en el nuestro.

c) En perjuicio de un tercero: Este elemento es de menor complejidad probatoria, que el contenido en nuestra legislación, ya que acreditar la lesión a la privacidad resulta más sencilla en el proceso judicial que acreditar el beneficio.

Sin embargo, con respecto al sujeto pasivo, indicar que es un “tercero”, resulta un término impreciso el cual se presta para confusión con respecto a si el daño debe ser para el titular u otro individuo, ya que el mismo tipo penal hace la diferenciación en cuanto al acceso y la alteración en perjuicio de tercero o del titular.

d) Datos reservados de carácter personal o familiar de otro: han de ser informaciones cuyo conocimiento está limitado a personas autorizadas o, lo que es lo mismo, han de ser datos no disponibles sin autorización y que incidan en la esfera personal o familiar. (Gómez, 2020, p. 341)

ACCESO, ALTERACIÓN Y UTILIZACIÓN DE DATOS PERSONALES.

ARTÍCULO 197.2 DEL CÓDIGO PENAL DE ESPAÑA



Este artículo sanciona, con las mismas penas, el acceso no autorizado a los datos reservados de carácter personal, cuando el agente realiza la acción sin contar con la autoridad para realizarlo.

De la misma manera, la alteración y utilización de los datos, en perjuicio del titular se sanciona con la misma pena, lo que a diferencia del tipo penal costarricense permite perseguir penalmente tratamientos de datos personales que, aunque se utilicen en perjuicio del titular no le genera al agente, o a un tercero, un beneficio.

Para la difusión, revelación o cesión de datos y/o secretos el Código Penal español lo regula de la siguiente manera:

Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. (Código Penal de España, Artículo 197.3)

a) Verbos rectores: difusión, revelación cesión

b) Datos o hechos descubiertos o las imágenes captadas: en los casos donde aparte de las acciones contenidas en los tipos penales anteriores el agente las difunda, revela o ceda la conducta se subsumiría en este tipo penal.

De manera acertada el legislador español decide aumentar la pena cuando la acción que realiza el agente es de difusión, ya que coincidimos con que el daño a la privacidad de la persona es mayor.

Agravantes.

El legislador español del Código Penal de 1995, aumenta las penas cuando las acciones se realizan por personal que brinda soporte al sistema informático⁴⁵, lo que en el año 2012 fue incorporado de la misma manera por el legislador costarricense.

De manera interesante, cuando los datos se difundan⁴⁶ o medie lucro, el legislador español tiene previsto que las penas aumenten, lo que sería más cercano con el delito de violación de datos personales costarricense⁴⁷.

Colombia

La República de Colombia mediante la Ley 1273 del 5 de enero del 2009, reforma su Código Penal que incluye dos nuevos bienes jurídicos al incluir el

⁴⁵ 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. (Código Penal de España, Artículo 197.4)

⁴⁶ Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. (Código Penal de España, Artículo 197.5)

⁴⁷ Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. (Código Penal de España, Artículo 197.6)

“Título VII BIS” denominado "De la Protección de la información y de los datos", con el cual incorpora la violación de datos personales, entre otros delitos informáticos:

- a) **Artículo 269A: Acceso abusivo a un sistema informático.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor

- b) **Artículo 269C: Interceptación de datos informáticos.** Pena de prisión 36 a 72 meses.
- c) **Artículo 269D: Daño Informático.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
- d) **Artículo 269E: Uso de software malicioso:** Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- e) **Artículo 269F: Violación de datos personales.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
- f) **Artículo 269G: Suplantación de sitios web para capturar datos personales.** Pena de prisión de 48 a 96 meses y en multa de 100 a 1000

salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena más grave.

g) **Artículo 269I: Hurto por medios informáticos y semejantes.** Pena de 3 a 8 años de prisión.

h) **Artículo 269J: Transferencia no consentida de activos.** Pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

VIOLACIÓN DE DATOS PERSONALES

(ARTÍCULO 269F DEL CÓDIGO PENAL DE COLOMBIA)

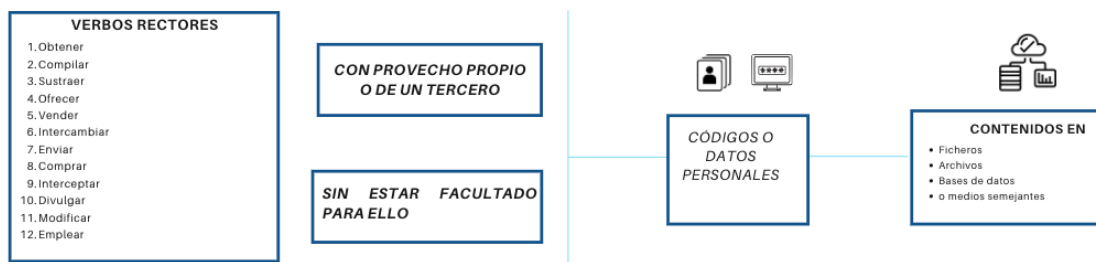


Figura 4. Artículo 269F del Código Penal de Colombia. [Elaboración propia]

La fórmula elegida por el legislador colombiano para el delito de violación de datos personales, contenida en el artículo 269F del Código Penal colombiano es la 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.

A continuación analizaremos los elementos del tipo penal:

a) Sin estar facultado para ello: este elemento pareciera mucho más amplio y acertado que el elegido por el legislador costarricense, debido a que un responsable de una base de datos podría estar facultado por una ley para realizar un tratamiento y no necesariamente contar con el consentimiento del titular, como lo establece como requisito el 196 bis de nuestro Código Penal.

b) Con provecho propio o de un tercero: el beneficio y el provecho son sinónimos por lo que este elemento no presenta mayor diferencia con respecto al tipo local.

c) Verbos rectores: obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear.

d) Códigos personales: tomando en cuenta que por información personal solo debe entenderse aquella que permite identificar o hacer identificable a un individuo, la incorporación de la protección a las contraseñas o códigos personales, aunque nos parece impreciso, favorece la lucha contra el comercio de contraseñas en los mercados negros.

e) Ficheros, bases de datos o medios semejantes: El legislador colombiano no limita la tutela del dato de acuerdo a su soporte.

Ecuador

El Código Penal ecuatoriano en su número 178, denominado *Violación de intimidad*, incorporado en el año 2014, se tutelan los datos personales, así como las comunicaciones de acciones violatorias a la intimidad.

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. (UNODC, 2021)

Los elementos del tipo penal son los siguientes:

a) Sin contar con el consentimiento o la autorización legal: de igual manera que el legislador colombiano, este elemento resulta más preciso.

b) Verbos rectores: acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar: si bien es cierto vemos que muchos de los verbos son similares al tipo penal nuestro, al incorporar distintos bienes jurídicos y acciones en un mismo penal hace que su aplicación sea más amplia. En este sentido, se puede ver como conductas que se aplicarían en distintos tipos penales en nuestro Código Penal, en el caso de Ecuador encuadrarían en este tipo penal.

c) Intereses protegidos: datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio.

d) No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley: nos parece un elemento incongruente que deja en desprotección, con respecto a su privacidad, a una de las partes intervinientes en la comunicación. Por otro lado, en casos de información pública no existiría lesión del bien jurídico.

En el año 2021, en una reciente reforma que elimina el párrafo segundo del tipo penal, se ha generado una gran controversia debido a que restringe las situaciones en las que se puede realizar una grabación, lo que ha despertado malestar nacional ya que cree que la misma es para proteger políticos.

En ese sentido Mae Montaña, legisladora proponente, indica que esta norma estaba orientada a combatir y prevenir la violencia sexual digital. Sin embargo, indica que “el aprovechamiento y oportunismo politiquero” hicieron una ley para “proteger a los políticos autoritarios, abusivos y corruptos”. (González, 2021)

Es importante reiterar que toda reforma sobre las TIC requiere un importante debate regulatorio que incorpore a todas las partes interesadas para evitar este tipo de controversias que no son sanas para ninguna democracia.

Conclusiones

La aceleración en la transformación digital que se está presentando en la sociedad costarricense, potencia la recopilación de los datos personales de los habitantes, los cuales corren el riesgo de ser capturados por la ciberdelincuencia, lo que requiere que se persiga de forma más activa a los actos delictivos que atenten contra el derecho de autodeterminación informativa.

Para cumplir lo anterior es necesaria una Estrategia Nacional de Lucha Contra la Ciberdelincuencia que sirva como derrotero de las autoridades en este campo, desde contar con un programa establecido de capacitación, herramientas tecnológicas y procesales que favorezcan la investigación de delitos cometidos por medios informáticos.

El tipo penal de violación de datos personales requiere una reforma que incorpore el concepto soporte informático en vez del de contenedor el cual resulta impreciso y limita la protección de datos que se almacenen en dispositivos aislados de almacenamiento.

Como propuesta de *lege ferenda* se debe reformar el Código Penal, en tipo penal independiente al de estudio, con el fin de sancionar de manera especial la violación de bases de datos electrónicas que afecten datos de múltiples personas y/o se difundan datos personales sensibles y confidenciales, aunque en las conductas no se realicen en beneficio propio, o de un tercero, pero sí en perjuicio de los titulares, de manera similar a la elegida por el legislador Español del Código Penal de 1995.

Bibliografía

Acceder, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/acceder>

Apoderar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/apoderar>

Artavia S. (7 de Junio de 2020). Juzgado desestima causa penal sobre violación de datos de Keylor Navas. Recuperado el 27 de abril del 2021 de <https://www.nacion.com/el-pais/politica/juzgado-desestima-causa-penal-sobre-violacion-de/DCRBN6NJGVHTLHAYRZR5SUB25M/story/>

Arteaga, S. (30 de Junio de 2017). Microsoft implementará el almacenamiento de datos en ADN en 2020. Recuperado el 26 de abril del 2021 de <https://computerhoy.com/noticias/hardware/microsoft-implementara-almacenamiento-datos-adn-2020-62994>

Artículo 178 (2014) UNODC, Sherlock. Recuperado el 8 de mayo del 2021 de https://sherloc.unodc.org/cld/en/legislation/ecu/codigo_organico_penal/libro_primero/articulo_178/articulo_178.html

Beneficio, Definición. Real Academia Española. Recuperado el 27 de abril del 2021 de <https://dle.rae.es/beneficio>

Criptomoneda - Qué es, definición y concepto. (26 de setiembre de 2017). Economypedia. Recuperado 25 de abril, 2021, de <https://economipedia.com/definiciones/criptomoneda.html>

Chip, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/chip>

Chinchilla, D (21 de febrero de 2020.). Alvarado crea oficina para obtener datos confidenciales de los ticos. Recuperado el 26 de abril del 2021 de <https://computerhoy.com/noticias/hardware/microsoft-implementara-almacenamiento-datos-adn-2020-62994>

Comunicación, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/comunicaci%C3%B3n>

Contenedores y la nube: una forma más sencilla de implementar cargas de trabajo (2021). Intel. Recuperado el 26 de abril del 2021 de <https://www.intel.es/content/www/es/es/cloud-computing/containers.html>

Cuidado, los marcapasos también pueden hackearse (21 de febrero del 2018). ABC. Recuperado el 26 de abril del 2021 de https://www.abc.es/salud/tecnologia-salud/abci-cuidado-marcapasos-tambien-pueden-hackearse-201802211613_noticia.html

Dávora, E y Dávora L (2017). Delitos Informáticos. Thomson Reuters Aranzandi

Dean, S. (1 de enero de 2020), Es 2020 y usted tiene nuevos derechos de privacidad en línea. Pero es posible que deba mostrar una identificación. Recuperado el 23 de abril del 2021 de <https://www.latimes.com/espanol/california/articulo/2020-01-01/es-2020-y-usted-tiene-nuevos-derechos-de-privacidad-en-linea-pero-es-posible-que-deba-mostrar-una-identificacion>

Doxing, Definición y explicación. Recuperado el 28 de abril del 2021 de <https://latam.kaspersky.com/resource-center/definitions/what-is-doxing>

Gómez, A. (2011). Enciclopedia de la Seguridad Informática. Alfaomega, Rama.

González S (2 de enero de 2018). Glosario de terminología TIC. Abogacía Española, Consejo General.

González, M. (8 de Mayo de 2021). Protección de la intimidad o censura: polémica por reformas al COIP. Recuperado el 8 de mayo del 2021 de <https://www.primicias.ec/noticias/politica/proteccion-intimidad-censura-reformas-coip/>

Glosario de Términos de Ciberseguridad: Una Guía de Aproximación Para El Empresario. (2017). Instituto Nacional de Ciberseguridad.

Interceptar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/interceptar>

Interferir, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/interferir>

Jaimovich, D. (25 de setiembre, 2019). *Qué es la Ley de Moore y cómo marcó el ritmo de la evolución digital*. Infobae. Recuperado 25 de abril, 2021, de <https://www.infobae.com/america/tecno/2019/09/25/que-es-la-ley-de-moore-y-como-marco-el-ritmo-de-la-evolucion-digital/>

Luna, N (1 de Marzo de 2018). ¿Qué es B2B y B2C en marketing? Recuperado el 27 de abril del 2021 de <https://www.entrepreneur.com/article/308985>

Los ataques de ransomware se disparan en todo el mundo (7 de abril del 2021). IT Digital Security. Recuperado el 26 de abril del 2021 de <https://www.itdigitalsecurity.es/actualidad/2021/04/los-ataques-de-ransomware-se-disparan-en-todo-el-mundo>

Modificar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/modificar>

Monopolio en Internet. (18 de agosto de 1999).). La Nación. Recuperada el 25 de abril de 2021. <https://www.nacion.com/opinion/monopolio-en-internet/RWEXHLY3YVGYXAI5MVS7CHBJ4/story/>

Peñas, E. (13 de febrero, 2017). Ethic. Recuperado el 26 de abril del 2021 de <https://ethic.es/2017/11/transhumanismo-antonio-diequez/>

Publicar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/publicar>

Resultó ser obscena. (2 de julio de 1997). La Nación. Recuperada el 25 de abril de 2021. <https://www.nacion.com/archivo/resulto-ser-obscena/SPNHX2KPPBFUPBEWGGREF6534A/story/>

Recopilar, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/recopilar>

Retener, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/retener>

Sandí, C. C (2002). *Delitos informáticos*. Editorial Investigaciones Jurídicas S.A.

Sextorsión, el chantaje por internet que deja indefensos a cientos de miles de hombres. BBC Mundo. (22 de diciembre de 2014) Recuperado el 26 de abril del 2021 de https://www.bbc.com/mundo/noticias/2014/12/141222_tecnologia_sextorsion_chantaje_internetsexo_extorsion_ig

Soporte, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/soporte>

Transmitir, Definición. Real Academia Española. Recuperado el 26 de abril del 2021 de <https://dle.rae.es/transmitir>

TRIBUNA LIBRE

EDICIÓN
DIGITAL

Edición 8/1, Octubre 2021
Costa Rica