UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

UNIDAD DE ESTUDIOS DE POS GRADOS

MAESTRÍA EN DERECHO PENAL ECONÓMICO

TEMA

“Estudio del delito de hurto de identidad digital y su instrumentalización para el manejo ilícito de datos de los usuarios de las nuevas tecnologías de la información y comunicación desde la perspectiva del derecho penal económico en El Salvador**.”**

TESIS PARA OBTENER EL GRADO DE

MASTRA EN DERECHO PENAL ECONÓMICO

PRESENTANDO POR

LICDA. DAMARIS SARAI MARTÍNEZ ALBERTO

DOCENTE ASESOR

DR. ARMANDO ANTONIO SERRANO

CIUDAD UNIVERSITARIA, SAN SALVADOR, NOVIEMBRE 2022

UNIVERSIDAD DE EL SALVADOR

Msc. Roger Armando Arias

RECTOR

Dr. Raúl Ernesto Azcunaga López

VICE RECTOR ACADÉMICO

Ing. Juan Rosa Quintanilla Quintanilla

VICE RECTOR ADMINISTRATIVO

Msc. Francisco Antonio Alarcón Sandoval

SECRETARIO GENERAL

Lic. Rafael Humberto Peña Marín

FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dra. Evelyn Beatriz Farfán Mata

DECANA

Dr. Edgardo Herrera Medrano

VICE DECANO

Msc. Digna Reina Contreras de Cornejo

SECRETARIO

Msj. Hugo Dagoberto Pineda Argueta

DIRECTOR DE LA ESCUELA DE CIENCIAS JURÍDICAS

Dr. José Miguel Vásquez LÓPEZ

JEFE DE LA UNIDAD DE POST GRADOS

TRIBUNAL CALIFICADOR

PRESIDENTE

DR. GILBERTO RAMIREZ MELARA

SECRETARIO

MSC. LUCIO ALBINO ARIAS

VOCAL

Dr. ARMANDO ANTONIO SERRANO

AGRADECIMIENTOS

Agradezco a Dios mi creador, quien me ha guiado desde mi nacimiento, soberano de mi vida.

A mi madre, Concepción Alberto, quien me ha impartido las lecciones más importantes de mi vida: amor a Dios, enfrentar con valentía cada situación de la vida, cumplir mis metas y superarme a mí misma. Por su apoyo, sin el cual habría sido imposible invertir el tiempo necesario para realizar este trabajo.

Dedico este esfuerzo a mi hija, Iliana Saraí a quien espero inspirar para que viva plena, fuerte, determinada y feliz.

A mi asesor de tesis, Dr. Armando Serrano, por su paciencia, guía, disposición e incluso brindarme aliento y motivación para concretar este esfuerzo. Ha sido una experiencia honrosa poder trabajar bajo su dirección; por su trayectoria y aporte al estudio del Derecho Penal en el país.

ÍNDICE DE CONTENIDOS

SUMARIO

Actualmente, la sociedad de la información se encuentra en apogeo debido al uso masivo de las tecnologías de la información y comunicación para resolver asuntos propios de la vida cotidiana, por un gran porcentaje de la población. Incluso sin tener plena conciencia de ello, todos los usuarios de las TIC´S somos titulares de una identidad digital para interactuar en el ciber espacio. En algunas ocasiones dichas interacciones trascienden y sirven para el establecimiento de relaciones contractuales a través del *comercio electrónico*, siendo esta una de las formas más elaboradas de relacionarse a través de las TIC´S.

Se presenta un estudio del concepto de identidad digital, así como el derecho a la protección y autonomía de este, como un supuesto *sine que non,* para interactuar en el ciber espacio, siendo un punto de partida para la existencia de una realidad virtual que posteriormente se perciben efectos también a través de los sentidos en la realidad objetiva, trascendiendo al ciber espacio. Sin menospreciar los innumerables beneficios de brinda el uso de las TIC´S, se expone la instrumentalización de la identidad digital, para cometer hechos delictivos, especialmente en el delito de hurto de identidad, sobre el cual se presenta un análisis a la luz de la teoría general del delito, subrayando su trascendencia desde la perspectiva del derecho penal económico.

ABREVIATURAS UTILIZADAS

Art. .....Artículo

Cn. .....Constitución de la Republica

C.P. ..... Código Penal

C.P.P. .....Código Procesal Penal

C.S.J. .....Corte Suprema de Justicia de El Salvador

D.L. .....Decreto Legislativo

D.O. .....Diario Oficial

FGR .....Fiscalía General de la Republica

IP .....Protocolo de Internet

LECDIC.....Ley Especial Contra los Delitos Informáticos y Conexos

PNC .....Policía Nacional Civil

RAE .....Real Academia de la Lengua Española

TIC´S ..... Tecnologías de la Información y la Comunicación

LeCrim……...Ley de Enjuiciamiento Criminal

INTRODUCCIÓN

Los seres humanos, a lo largo de nuestra vida hemos establecidos una serie de relaciones de diversa naturaleza: relaciones sociales, de amistad, de trabajo, familiares, afectivas, de consumo, de comercio, jurídicas, etc. En cada uno de estos ámbitos, todos ejercemos la titularidad de una identidad personal, la cual debe entenderse como aquella información personal propia, que nos hace diferentes a cualquier otro individuo. El uso de nuestra propia identidad se realiza con tal naturalidad que poco se ha razonado sobre su carácter esencial al momento de relacionarnos y comunicarnos con otros.

Lo anterior ocurre, ya que al relacionarnos de manera directa con otros los códigos de lenguaje funcionan de manera inmediata y nos auxiliamos de nuestros sentidos los cuales facilitan el ejercicio comunicativo. Sin embargo, cuando no nos relacionamos de manera directa con otros, sino a través de las tecnologías de la información y comunicación (TIC´S), es importante identificarnos con el resto de usuarios de las TIC´S, y establecer relaciones de comunicación confiables y seguras. A través de esta nueva forma de relacionarnos con otros, nacen relaciones de consumo, de oferta y demanda, de *comercio electrónico,* por lo que es importante que nuestra *identidad digital* sea protegida y su uso se encuentre garantizado a través de los mecanismos legales aun mínimamente.

La protección formal de la identidad digital es importante y contribuye al fortalecimiento del crecimiento económico, puesto que brinda nuevas modalidades para llegar a toda clase de acuerdos a través de los cuales es posible perfeccionar relaciones de consumo, o relaciones de carácter legal, tal es así, que es esencial que se asegure su uso para los fines que su titular los introdujo al ciber espacio y desvirtuar la creencia que en el ciber espacio se encuentra la tierra de nadie.

De manera muy sintetizada, se puede anunciar la importancia y contenido de la investigación que a continuación se presenta en la forma de cuatro capítulos:

En el primer capítulo encontraremos aspectos generales relacionados con el derecho a la identidad digital, el surgimiento de este como parte del desarrollo tecnológico. En este capítulo se hace referencia al reconocimiento en la Unión Europea del derecho a la identidad digital como tal, de manera referencial. Siguiendo ese orden de ideas, se plantea su autonomía respecto de otros derechos previamente consagrados tales como el derecho a la intimidad y el derecho a la protección de datos, sin obviar la vinculación con los mismos.

En el segundo capítulo, se hace un repaso en relación a las disposiciones legales vigentes en El Salvador que protegen la identidad digital, entre los cuales se analizan los artículos 1, 2 y 101 de la Constitución de la República de El Salvador, siendo estos la base del planteamiento en cuanto a la trascendencia de los derechos individuales, que posteriormente pueden convertirse en derechos colectivos, brindando un punto de vista desde la perspectiva del derecho penal económico. Enseguida se hace referencia a la Ley Especial Contra Delitos Informáticos y Conexos, prestando atención a su estructura, bien jurídico protegido, así como algunos comentarios a la agrupación de los tipos delictivos a través de cinco capítulos, mediante el establecimiento de notas características o comunes entre estos. Así como su título lo anuncia, también se hace referencia a las disposiciones de carácter internacional protectoras de la identidad digital, señalando entre las más destacables el Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, el cual ha sido retomado por El Salvador, para regular el tema de la ciberdelincuencia a través de la ley especial mencionada, y finalmente se relacionan las disposiciones relacionadas con la protección de la identidad digital en países de la región, como Costa Rica, Guatemala y Honduras.

En el tercer capítulo, denominado *análisis crítico sobre los ataques a la identidad digital en El Salvador, desde la perspectiva del Derecho Penal Económico,* se presenta un diagnostico sobre la situación actual en El Salvador en cuanto a la utilización de la identidad digital para el cometimiento de hechos delictivos, presentando datos concretos en cuanto a las denuncias presentadas por el delito de hurto de identidad de acuerdo al art.22 de la Ley Especial Contra Delitos Informáticos y Conexos, así como la situación

actual en cuanto a la resolución de esta clase de casos. Se logra identificar, además, los principales obstáculos de las investigaciones por el delito mencionado: limitantes en cuanto al recurso humano para la investigación de hechos delictivos contenidos en la LECDIC y el carácter transnacional de las investigaciones; todo ello siempre desde la perspectiva del derecho penal económico, siendo este el objeto de la investigación.

En el cuarto capítulo, se realiza y ofrece un análisis del tipo de hurto de identidad, a la luz de la teoría general del delito, descomponiendo cada uno de los elementos que integran el tipo, en cuanto a su significado y sus alcances; tomando en consideración la especialidad de este, en cuanto una forma sofisticada de criminalidad, por cómo se requiere la ejecución o consumación del tipo, sin omitir hacer referencia a las consideraciones doctrinarias relacionadas con los elementos objetivos y subjetivos del tipo. Finalmente se adopta una postura determinada en cuanto a aspectos puntuales propios en cuanto al sujeto activo y sus atributos especiales; como el tratamiento de los errores de tipo y de prohibición para el delito de hurto de identidad.

Finalmente se encuentran las conclusiones y recomendaciones, las cuales son producto del estudio del problema planteado a través de la investigación, con las cuales se cierra el contenido de este documento, imprimiendo la finalidad del mismo que es contribuir al estudio de temas de actualidad a la luz de la perspectiva del derecho penal económico, a través del estudio de la ciberdelincuencia o realizar al menos una aproximación al estudio de este fenómeno.

CAPITULO I: GENERALIDADES DEL DERECHO A LA IDENTIDAD DIGITAL.

SUMARIO: 1.1. Surgimiento del concepto y derecho de Identidad Digital, características propias en el contexto de las TIC´S.1.2. La Identidad Digital y su vinculación con el Derecho a la Protección de Datos.1.3. El Derecho a la Intimidad y el Derecho a la Privacidad Virtual. 1.4. La Identidad Digital como instrumento para la comisión de hechos delictivos a través de las TIC´S. 1.5. El derecho a la Identidad Digital, un Derecho Humano de Cuarta Generación.

RESUMEN:

Tal como el nombre de este capítulo lo anuncia, se presentan generalidades relacionadas al concepto de identidad digital, así como un acercamiento a la acepción de este como un derecho o facultad reservada para todas aquellas personas naturales o jurídicas usuarias de las TIC´S. De manera muy concreta se hace referencia a la historia del surgimiento del internet como el factor *sine qua non* se habría generado la problemática identificada a través de la presente obra. Sucesivamente, se realiza un análisis sobre el derecho a la identidad digital y otros derechos o facultades (derecho a la protección de datos, a la intimidad), los cuales se han desarrollado con anterioridad a la misma, esto se realiza por dos motivos: primero por su íntima vinculación y segundo, porque es necesario subrayar que el derecho a identidad digital se encuentra dotado de autonomía. Sobre este último aspecto se hace referencia a la experiencia española mayoritariamente, por ser pioneros en el tema a nivel doctrinario y de legislación vigente. Se presenta luego una reseña sobre la experiencia salvadoreña en cuanto a la utilización de la *identidad digital* como instrumento para la comisión de hechos delictivos a través de las TIC´S, trayéndose a cuenta casos de especial interés por su impacto al orden

socioeconómico. Finalmente podremos encontrar el estatus del derecho a la identidad digital: un Derecho Humano de Cuarta Generación.

1.1. Surgimiento del concepto y derecho de Identidad Digital. Características propias en el contexto de las TIC´S.

El surgimiento del derecho a la Identidad digital, indudablemente merece un repaso por lo menos breve de sus antecedentes históricos, que en este caso pueden atribuirse al surgimiento del internet, que tiene sus raíces en Estados Unidos de Norte América. Estos antecedentes, han sido retomados ya por muchos autores estudiosos de la problemática vinculada con el cibercrimen o ciberdelincuencia, por lo que en este capítulo se hará referencia concretamente a aspectos esenciales.

En torno al surgimiento y evolución de internet, y en consecuencia de los delitos vinculados con las Nuevas Tecnologías de la Información y Comunicación, Josefina Quevedo González distingue cuatro etapas:

a) La denominada etapa militar, comprendida en la década de los años 70 del siglo pasado.
b) La denominada etapa académica: años 80 y primeros 90 del siglo XX.
c) La denominada etapa comercial: años 90 y posteriores.
d) La denominada etapa social: siglo XXI[1].

En la primera etapa, se destaca el origen de internet vinculado con DARPA, “Defense Advanced Research Projects Agency”, (Agencia del Departamento

[1] Quevedo González, Josefina. “Investigación y prueba del ciberdelito”. Tesis doctoral, Universitat de Barcelona, 2017. Pág. 35 y siguientes.

de Defensa de Estados Unidos), donde se desarrollaron las nuevas tecnologías para uso militar, desarrollaron la manera de conectar varios ordenadores de diferentes centros de investigación en una red. El aporte relevante, según señala el Doctor Agustina Quevedo González, fue que desde esta etapa se producen la acumulación de datos, que el gobierno iba captando, correspondientes a la ciudadanía, así como la preocupación el uso de estos, surgiendo el concepto de "*privacy"* y del derecho a la misma.

En la segunda etapa, las redes similares a DARPA, ARPANET o MILNET, se desvincularon de las operaciones militares y se dio un enfoque académico, se crearon redes informáticas con propósitos científicos, como la *NSFNET (National Sciencie Foundation Network),* que absorbió a Arpanet, fue así que las redes se unieron, creando internet.

La tercera etapa, surge la Word Wide Web (www), Agustina Quevedo la llama "telaraña mundial", en este punto el acceso a la misma se hizo masivo y su crecimiento se intensificó. Asimismo, se comenzó a utilizar contenido ilícito como la pornografía infantil.

En cuanto a la cuarta etapa, el autor plantea el acceso masivo que los ciudadanos tienen a internet y a las diferentes plataformas virtuales a través de las cuales no únicamente se accede a información, sino que además puede nutrirse la *web,* es así que se sofistica los métodos o mecanismos delictivos, desarrollándose una gran cantidad de conductas delictivas por medio de las nuevas tecnologías de la información y comunicación. Otro aspecto importante que subraya Agustina Quevedo es la dependencia que en general, incluso los Estados tienen de los sistemas informáticos, que al mismo tiempo les ubican en un estado de vulnerabilidad frente a la delincuencia.

En El Salvador, estadísticamente, el uso de las Nuevas Tecnologías de la Información y comunicación ha registrado gran aumento, en el año 2000 en El Salvador había aproximadamente 40,000 usuarios de internet, para el 2012 25%de la población salvadoreña (aproximadamente 1.5 millones de personas) tienen acceso a internet. En doce años, el número de usuarios de internet en el país se ha incrementado en un 97%[2].

Este incremento en cuanto al acceso a las nuevas tecnologías de la información y comunicación en El Salvador y el mundo, al margen de los avances o desarrollo que representan, también han significado gran ventaja para la comisión de hechos delictivos. Para el caso nacional, según información analizada por la Oficina de las Naciones Unidas contra la Droga y El Delito (UNODC), informe El Salvador, documento interno; las nuevas tecnologías han propiciado el modus operandi en los delitos como difamación, amenazas, estafa, violación de derechos de autor, distribución de pornografía infantil, robo de identidad, entre otros.

La UNODC, señala que legislación penal de El Salvador vigente desde el año 1998, hacía referencia al cometimiento del delito mediante el uso de las tecnologías de la información y la comunicación, utilizando términos como “a través de medios electrónicos”, esto se ejemplifica en los artículos 172 y 346 del Código Penal, “informática” o “virtual”, como en el 173 del mismo cuerpo legal, por lo que tal regulación lo hacía de forma asistemática, siendo ello insuficiente para la investigación y enjuiciamiento de los delitos vinculados con las TIC´S. La Ley Especial Contra delitos Informáticos y Conexos, viene a suplir en gran medida dicha deficiencia, la cual en su parte filosófica menciona

[2] Oficina de las Naciones Unidas contra la Droga y el Delito. *“Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos”.* Copyright 2018. Pág. 12.

la importancia relacionada con la protección de los datos personales de los usuarios de las TIC´S.

En ese sentido, podemos ubicarnos históricamente en el contexto del surgimiento del concepto de identidad digital, que ocurre cuando surge internet, aunque inicialmente no se encontrara claramente diferenciado, pero desde la primera etapa señalada se comenzó a captar datos de la ciudadanía, los cuales eran aptos para determinar su identidad real, esta información era gestionada por personas físicas en representación del Estado, poseedor de una identidad abstracta, pero definida.

Asimismo, conviene retomar aspectos relacionados con el acceso masivo a internet por parte de usuarios alrededor del mundo en la década de los noventa, puesto que, desde ese primer momento histórico, se manifestó uno de los mayores problemas, que en la actualidad subsisten: la comisión de hechos delictivos desde las nuevas tecnologías de la información – aunque este último concepto aún no se utilizaba- que aportó desde el inicio, ese elemento problemático sobre la identidad del autor del hecho, que consecuentemente dificulta la individualización del mismo.

Lo anterior sucede, puesto que una de las principales características de la utilización de plataformas digitales asociadas al uso de internet, es que inevitablemente el usuario debe introducir sus datos de identificación, siendo lógico que la información que utilice no será la misma que corresponda con su identidad en la realidad objetiva, si lo que se propone es el cometimiento de hechos delictivos. Pero no es menos cierto, que esa información que introdujo el delincuente a internet, incluso camuflada o distorsionada, constituye su identidad digital, ya que, aunque su finalidad es permanecer en el anonimato, aún de manera involuntaria introduce información que van revelando su

identidad, que con frecuencia corresponde con la realidad objetiva, aunque esto no siempre es así.

Juan Carlos Riofrio Martínez Villalba sostiene que la identidad digital es la expresión electrónica del conjunto de rasgos con los que una persona, física o jurídica, se individualiza frente a los demás[3]. Tal como el autor sostiene, el punto de partida es la persona natural, ya que depende de ésta la construcción de la identidad digital, incluso, la existencia de la persona jurídica. Nuestra Constitución de la República reconoce al ser humano como el origen y el fin de la activid.ad del Estado, por lo que no debemos perder de vista cuestiones básicas, como la persona humana dotada de capacidad de ejercer sus facultades.

Conviene cuestionar si la información que forma parte de la identidad digital, únicamente debe entenderse como un nombre de usuario y una clave de acceso a las diversas plataformas digitales, ya que estas son alimentadas por los usuarios con diferentes insumos de carácter personal, tales como ubicaciones de lugares frecuentados, otras usuarios con quienes interactúan, gustos personales como alimentos, música, opiniones personales sobre diferentes temas de trascendencia social, política o económica, incluso sitios o cuentas afines, o a las cuales constantemente se frecuenta contenido, publicaciones a las cuales de manera manifiesta se le brinde aprobación a través de la pestaña “me gusta”, o incluso emitiendo una “reacción”, -positiva o negativa- a cualquiera que sea el contenido en la web. Sobre esta clase de información, la Sala Segunda del Tribunal Constitucional de España, en la STC 173/2011, de 7 de noviembre de 2011, menciona que *cada visita a un sitio en*

[3] Riofrio Martínez-Villalba, Juan Carlos. <<La Cuarta ola de Derechos Humanos: Los Derechos Digitales>>. Pág. 34.

internet deja una serie de "rastros electrónicos" que pueden utilizarse para establecer "un perfil de su persona y sus intereses" … Todo ello, debe ser analizado de manera conjunta para construir la identidad digital de los usuarios de las nuevas tecnologías de la información, que finalmente sería corroborable técnicamente a través de una dirección IP[4], culminando con una correspondencia entre la identidad digital con una identidad en la realidad objetiva, la cual no será nominalmente la misma, en todas las ocasiones.

1.2 La Identidad Digital y su vinculación con el Derecho a la Protección de Datos.

Cuando analizamos el concepto de identidad digital, no obstante, que la problemática se encuentra vinculada con una instrumentalización de la misma para la comisión de delitos, no debemos extraviarnos en cuanto a que este concepto es propio de los usuarios de las nuevas tecnologías de la información y que predominantemente se trata de usuarios de buena fe.

Los usuarios de buena fe son personas naturales o jurídicas que ingresan a diferentes plataformas con fines determinados, entre los cuales pueden encontrarse la prestación de servicios para solucionar aspectos propios de la vida cotidiana, y la contratación de estos servicios, por lo que ingresan información personal cierta. Es en atención a esta realidad que los estados han realizado esfuerzos para proteger los derechos de los usuarios de buena fe que representan a la mayoría, surgiendo el denominado *Derecho a la Protección de Datos.*

[4] Dirección IP: es un número identificativo y único de cada dispositivo que se conecta a internet.

De manera aclarativa, debemos dejar por establecido que *los datos de carácter personal*, comprende toda información relativa a una persona física, identificada o identificable. La información puede ser de todo tipo, es decir puede consistir en información relativa a la identidad física, fisiológica, psíquica, económica, cultural o social de la persona, y no ha de ser necesariamente privada. Puede constar en diversos formatos (alfabética, numérica, gráfica, sonora), sin ser necesario que identifique al individuo por su nombre, sino que basta con que permita identificar a la persona concernida, singularizarla o individualizarla[5]. Todo ello, representa información suficiente para analizar conjuntamente y crear el perfil de una persona determinada, tal como se mencionó en el apartado anterior.

Es en Europa donde mayoritariamente se registra un avance significativo, para garantizar el derecho a la protección de datos, por lo que se aprobó el Convenio 108 del Consejo de Europa, de 28 de enero de 1981[6], para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. Desde entonces, se hicieron aportes que actualmente tienen vigencia, aun cuando la utilización de internet no se encontraba desarrollada como lo está actualmente. El Objeto y fin de dicho convenio es justamente, garantizar que en el territorio de cada parte cualquier persona física fuera respetada, a si como su vida privada, con respecto al tratamiento automatizado de sus datos de carácter personal; y, expresamente introduce el concepto de, protección de datos. Incluso brinda una definición legal sobre

[5] Rivacoba, Ramón Durán, Castilla Barea, Margarita. et. al. Protección de Datos Personales. Tirant lo Blanch. 1 edición, 2020. Consultado en versión digital, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788490333907

[6] Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, consultado 11/06/2022 en versión PDF, en https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf

“datos de carácter personal”, estableciendo que su significado, es cualquier información relativa a una persona física identificada o identificable.

La Unión Europea asume además una labor educativa en relación a facilitar información sencilla y comprensible para todos los ciudadanos europeos a fin de que estos comprendan las facultades que les asisten en relación a la protección de datos y se sirve para tales fines de las nuevas tecnologías de la información y comunicación para su difusión. Así introduce títulos con invitaciones para los usuarios tales como “Asuma el control de su IDENTIDAD VIRTUAL” (las mayúsculas son propias), y educa sobre otros derechos conexos tales como derecho de oposición, derecho a ser informados sobre filtración de datos y el derecho al olvido[7]. El propósito de la labor educativa, es asegurar que el usuario cuente con la información necesaria, que le permita tomar el control de los datos que comparte. Esto último podría ser la clave para solucionar los problemas de inseguridad virtual que enfrentan los usuarios de las nuevas tecnologías de la información.

A partir de eventos de conocimiento público relacionados con la recolección de datos de parte de Facebook/Cambridge Analytica[8], la Unión Europea, promueve una reforma a la protección de datos a través de la aprobación del Reglamento General de Protección de Datos., la cual entró en vigencia el 25 de mayo de 2018, la cual ha sido promovida como una mejora significativa ya que establece con claridad la obligación de aquellos que recopilen, almacenen

[7] Normas de la UE para la protección de datos. Consultado el 11/06/2022 en el sitio Web oficial de la UE, en: https://ec.europa.eu/info/sites/default/files/virtual_identity_es.pdf

[8] BBC NEWS, <<5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día>>. Consultado el 25 de octubre de 2021 en https://www.bbc.com/mundo/noticias-43472797

o utilicen datos, a hacer llegar de manera sencilla y comprensible a los usuarios las condiciones de privacidad, para la protección de su información.

El Convenio suscrito por los miembros de la Unión Europea, relacionados a la protección de datos les obligó a legislar en relación al tema. A partir de esto, España hace lo propio para garantizar ese derecho, así lo regula en la misma Constitución Española, art. 18.4, y también mediante la aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y jurisprudencialmente, también existen ya varias resoluciones procedentes del Tribunal Constitucional que vienen instruyendo en relación con la ejercicio práctico de este derecho.

Evidentemente, la experiencia europea y española, en materia de garantía y promoción del derecho a la protección de datos amplia. Esto puede ser visto como algo positivo, en virtud que se han sentado los precedentes normativos a los cuales podremos abocarnos de manera referencial, en lo que fuere posible, ya que no debe olvidarse que las condiciones de criminalidad son sustancialmente diferentes.

Si realizamos un diagnóstico para el caso salvadoreño, constitucionalmente, no existen una mención expresa sobre el derecho a la protección de datos en el tráfico de las nuevas tecnologías de la comunicación e información. La Ley Especial Contra Delitos Informáticos y Conexos,[9] se aprobó y en su exposición de motivos se menciona a la persona humana como origen y fin de la actividad del Estado. Del análisis de la misma, se obtiene que no introduce

[9] Ley especial Contra Delitos Informáticos y Conexos, aprobada por medio de decreto legislativo N°260, la cual entró en vigencia en el mes de marzo del año 2016.

expresamente el concepto de “protección de datos”, aunque en el artículo 1, si menciona la importancia de *sancionar delitos en perjuicio de datos almacenados, procesados y transferidos y que estos afecten intereses asociados a la identidad, intimidad e imagen de las personas*, que materialmente resultaría ser lo mismo, aunque con una redacción un poco menos explícita que la española.

En el artículo 3 de la misma ley, se definen los datos personales, *como la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar*. En los tipos penales regulados se advierte en su redacción que constantemente se relaciona la obtención de datos, incluso se utilizan expresiones como “datos en general”, aunque puede entenderse que el sujeto pasivo debe ser una persona humana a los cuales los datos se encuentren vinculados. Para referirse al sujeto activo, en su articulado, va indicando que será el que utilice las nuevas tecnologías de la comunicación e información.

En cuanto a la protección de datos, contiene un capítulo que se titula *delitos informáticos relacionados con el contenido de los datos,* que contiene doce tipos penales destinados directamente a la protección de datos. Regula en el art. 24 el delito de Utilización de datos personales y en el art. 26, el delito de Revelación Indebida de Datos o Información de carácter personal. En el artículo 22, se regula el delito de hurto de identidad, el cual es mencionado únicamente como identidad de un apersona, natural o jurídica, por medio de las nuevas tecnologías de la información. Lo anterior indica, que trata sobre la identidad digital, tal como se ha venido analizando, ya que una vez que se involucran las nuevas tecnologías de la comunicación e información, se ha

abierto la puerta a la realidad virtual, que puede generar efectos en la realidad objetiva.

Por otro lado, tampoco es cierto que no se haya realizado ningún esfuerzo por establecer mecanismos directos para la protección de datos. El 24 de junio de 2019, el grupo parlamentario Alianza Republicana Nacionalista (ARENA), presentó ante la Asamblea Legislativa un proyecto de la Ley de Protección de Datos Personales y Habeas Data. Su objeto era evidentemente proteger integralmente los datos personales de personas naturales, la cuales podrían encontrarse en posesión de particulares o persona jurídicas, entidades públicas o privadas, o cualquier tipo de entidad sin personalidad jurídica, para regular el tratamiento legítimo e informado de datos. Introdujo conceptos como la garantía de la privacidad y la autodeterminación informativa de las personas naturales[10].

Por su parte el grupo parlamentario del FMLN, también presentó el proyecto de Ley General de Protección de Datos Personales. A propósito de ello, la Fundación Salvadoreña para el Desarrollo Económico y Social, a través de su departamento de estudios legales, publicó en octubre de 2019[11], algunas observaciones a los proyectos de Ley de Protección de Datos Personales. En este documento, se analizó el contenido de ambos proyectos, destacando los aspectos positivos de cada uno de estos. Finalmente, se recomendó fusionar

---

[10] Iniciativa de Ley de Protección de Datos Personales y Habeas Data, versión PDF, consultado el 11/06/2022, en https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/2A326CE8-F13A-4828-8640-648235C228BF.pdf

[11] Análisis legal e institucional. Observaciones a los Proyectos de Ley de Protección de Datos Personales, versión digital, consultada 11/06/2022, en http://fusades.org/publicaciones/AL_200_Oct2019_II%20parte_Observaciones%20a%20los%20proyectos%20de%20Ley%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

los mismos para retomar lo mejor de cada uno. En este documento, FUSADES, introdujo conceptos divulgados por la agencia de la Unión Europea por los Derechos Fundamentales del Consejo de Europa, como el derecho al olvido, así como contenido explicativo de las creaciones de perfiles para divulgar datos de usuarios, tratando de integrar las construcciones internacionales vinculadas con el tema, sin embargo, estas observaciones no fueron retomadas por la asamblea legislativa.

El 13 de abril de 2021, la Comisión de Economía de la Asamblea Legislativa emitió el dictamen favorable no 46, para la aprobación de la Ley de Protección de Datos Personales. El articulado publicado, dejó de lado algunas disposiciones contenidas en los proyectos presentados por los grupos parlamentarios. Específicamente el proyecto presentado por ARENA, contenía en el art. 66, que establecía que sería la defensoría del consumidor la que difundiría el conocimiento del derecho a la protección de datos personales, así como promover su ejercicio y ejercer facultades enfocadas a la vigilancia, supervisión, investigación, inspección de las obligaciones previstas por la ley para los sujetos obligados.[12] Este significaba un primer paso, en materia de protección de datos, sin embargo fue suprimido por la comisión de economía tal y como se verifica del contenido del dictamen relacionado.

Entre las observaciones realizadas por FUSADES, mencionaron que en materia de ente garante, la tendencia internacional era la creación de autoridades especializadas para vigilar el cumplimiento del derecho a la

[12] Dictamen No 46 Favorable, de fecha 13 de abril de 2021, suscrito por la Comisión de Economía de la Asamblea Legislativa de la República de El Salvador, versión PDF, consultado el 11/06/2022, en https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/498798FA-A563-4830-A0C8-306AFBC71497.pdf

protección de datos, pero como en el caso de El Salvador, se menciona la falta de recursos para crear dichas entidades garantes, entonces lo recomendable sería otorgarle provisionalmente dicha potestad de proteger los datos personales en registros públicos y privados al Instituto de Acceso a la Información Pública. Posteriormente, el dictamen favorable para la aprobación de la ley, regulaba en el art.58 la creación de la Autoridad Nacional de Protección de los Datos Personales, estableciendo sus atribuciones y composición. La Ley de Protección de Datos personales fue aprobada mediante decreto legislativo 875 de fecha 22 de abril de 2021.

El 11 de mayo de 2021, el presidente de la República Nayib Armando Bukele Ortez devolvió la Ley de Protección de Datos Personales a la Asamblea Legislativa, ejerciendo su facultad de VETO por inconveniente[13]. Entre los argumentos presidenciales se mencionó que el articulado era precario pues no consideraba las condiciones propias de la República de El Salvador, en cuanto existían disposiciones relacionadas, a las cuales no se hizo referencia, que además la composición de la Autoridad Nacional de Protección de Datos Personales era inconveniente y finalmente alegó los obstáculos presupuestarios, y así finalizó el único esfuerzo en materia de protección de datos en El Salvador.

1.3 El Derecho a la Intimidad y el Derecho a la Privacidad Virtual.

El derecho a la protección de datos y a la identidad digital o virtual, se les puede dotar de autonomía propia, ya que son resultado del inevitable

[13] Veto Presidencial sobre el decreto No 875 por inconveniente, de fecha 07 de mayo de 2021, versión PDF, consultado el 11/06/2022 en https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/EFBA7BEE-871B-40BE-BD0A-5BD80237CA90.pdf

desarrollo tecnológico, que ha generado riesgos que nunca antes existieron, tal como ya se ha reiterado en varias oportunidades. Estos mismos derechos, tienen relación con la intimidad, pues antes de configurarse cada uno de ellos, fue necesario que primero se construyera teóricamente el derecho a la intimidad.

La intimidad como tal tiene diversas acepciones, y al tratar de abordar el concepto puede resultar un tanto complejo, porque podrían mencionarse diferentes discusiones doctrinarias y hasta filosóficas sobre su significado y distinción con otros conceptos jurídicos con los que tiende a confundirse, sin embargo, el enfoque sobre el mismo es claro: su vinculación con el manejo de la información relacionada con la identidad digital de las personas naturales y jurídicas en las nuevas tecnologías de la información.

Manuel Iglesias Cubría, menciona que íntimo es lo reservado de cada persona, que no es lícito a los demás invadir, ni siquiera con una toma de conocimiento[14]. Así el autor menciona, que existen aspectos personales que no pueden mantenerse reservados, como puede ser el aspecto físico, característica del rostro y hay otros aspectos que permanecerán ocultos, siempre que el individuo así lo procure.

En sentencia definitiva emitida por la Sala de lo Constitucional de la República de El Salvador, ha sostenido que existe una manifestación del derecho a la intimidad, que es precisamente el derecho a la protección de los datos y consiste en que el individuo pueda controlar el uso o tratamiento de los

[14] Cubría, Manuel Iglesias. “El derecho a la Intimidad”, editada por la Universidad de Oviedo en el año 1970, consultada en versión PDF.

mismos, a fin de impedir una lesión a su esfera jurídica[15]. Ciertamente, aunque se encuentran vinculados estrechamente, es posible diferenciar entre el derecho a la intimidad y el derecho a la protección de datos, ya que el segundo, exige concretamente una tutela por parte del Estado para establecer las condiciones idóneas para que esa condición de íntimo, de secreto, se mantenga, según sea el deseo del usuario de las TIC´S.

Asimismo, convine revisar el derecho a la intimidad como un derecho fundamental, ya que este tema ha sido abordado de manera suficiente por la Sala de lo Constitucional de la Corte Suprema de Justicia, a propósito del artículo 2 inciso dos de la Constitución de la República y menciona que *el derecho a la intimidad personal hace referencia al ámbito que se encuentra reservado ad intra de cada persona y cuyo conocimiento importa únicamente a éste y en su caso, a un círculo concreto de personas seleccionadas por el mismo; por tanto, en dicho ámbito opera la voluntad del individuo para disponer de todos aquellos aspectos que puedan trascender al conocimiento de los demás*.[16]

Mencionado lo anterior, resulta bastante evidente que el derecho a la intimidad, a la identidad digital, a la protección de datos y a la privacidad virtual, son derechos interrelacionados e individuales propios de la persona humana. Sin embargo, aunque estos derechos individuales naturalmente protegen bienes jurídicos individuales, al introducir otro variable: que es el uso de las TIC´S.

---

[15] STC Definitiva en proceso de amparo, Sala de lo Constitucional, Corte Suprema de Justicia de El Salvador, de fecha 02 de marzo de 2004, marcada con referencia 118-2002, consultada el 11/06/2022, en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php

[16] STC Definitiva en proceso de Hábeas Corpus, Sala de lo Constitucional de la Corte Suprema de Justicia, de fecha 16 de mayo de 2008, marcada con referencia 135-2005 AC, consultada el 11/06/2022, en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php

En El Salvador, se registran miles de usuarios de las TIC´S, que en determinado momento han resultado afectados por el manejo abusivo e ilícito de datos, afectando su bien jurídico protegido desde con contenido personalista o "microsocial" luego, al revisar el fenómeno desde una óptica panorámica pueden apreciarse que se lesionan bienes jurídicos de una gran cantidad de individuos, que tienen elementos comunes entre sí, como usuarios o consumidores de un servicio determinado, convirtiéndose entonces en un bien jurídico macrosocial (los derechos de los consumidores). Así lo plantea Raúl Cervini:

"*De acuerdo con estos principios constitucionales, el llamado orden socioeconómico es del interés y está al servicio de todos los ciudadanos; en esto radica su contenido personalista microsocial. Así, por ejemplo, la difusión de una noticia falsa con la intención de alterar los precios de un producto debe entenderse e interpretarse como una intervención intolerable desde una posición de poder en el funcionamiento del mercado, lo que, en último término, perjudica a los consumidores. Ese obstáculo que impide la realización de la libre competencia y la formación del justo precio viene, en último término, a afectar también al patrimonio del consumidor. La protección de la libre competencia como factor específico del orden socioeconómico implica, en última instancia, la protección de un bien jurídico macrosocial. La lesión de este bien jurídico macrosocial, en este caso la libre competencia, produce distorsiones en el funcionamiento del sistema, ya que obstaculiza la libre circulación de las mercancías. Pero esta lesión del bien jurídico macrosocial, en la medida en que está referida al funcionamiento del sistema, también*

perjudicará el patrimonio de uno de los sujetos de la relación económica de mercado. [17]

En cuanto al Derecho a la Privacidad Virtual, Juan Carlos Riofrio sostiene, que el concepto de privacidad es mucho más amplio que el de "intimidad", ya que, solo las personas naturales son capaces de ejercer el derecho fundamental a la intimidad, sin embargo, el derecho a la privacidad puede ser ejercido también por personas jurídicas[18]. Por otro lado, se plantea que, en internet, lo que verdaderamente prevalece es la exposición, por lo que los usuarios de las diferentes TIC´S, deberían de dar por hecho que tal privacidad es imposible.

Como todo punto de vista, esto resulta debatible, ya que hay algo cierto, en el sentido de que todo usuario de las TIC´S, voluntariamente se expone desde que hace uso de las diferentes plataformas virtuales, pero no es menos cierto, que la gran mayoría de personas tiene un nivel de confianza en que sus datos personales serán utilizados para los fines que han sido proporcionados. Así, aquellos que proporcionan información relacionada con cuentas bancarias personales, las proporcionan para fines específicos y limitados, sin plantearse al momento de proporcionarlo que estos fuesen utilizados en perjuicio propio, pues si así fuese esta información no habría sido proporcionada nunca, a la vez, el desarrollo económico también se ha apoyado en el uso de las TIC´S, por lo que es necesario que dichas relaciones en el espacio virtual se encuentren reguladas por tema de seguridad jurídica.

---

[17] Cervini, Raúl. Derecho Penal económico. Perspectiva integrada. Revista de Derecho, Universidad Católica del Uruguay, página consultada en versión pdf.

[18] Riofrío Martínez Villalba, Juan Carlos, para la Revista Latinoamericana de Derechos Humanos, volumen 25 (1), I semestre 2014 (ISSN:1659-4304).

Ahora, retomamos el derecho a la privacidad virtual, ha de mencionarse que fue en Estados Unidos, durante la década de los sesenta y setenta, que se desarrollaron contribuciones teóricas relacionadas con el derecho a la privacidad virtual. Fried, entendía el derecho a la privacidad con el poder de control sobre la información personal, no solo cuantitativa, si no cualitativa, es decir, no solamente cantidad de información sino, el tipo de información de que se disponga. Así, en ese mismo sentido Westin, definió la privacidad como el derecho de decidir cuándo, cómo y en qué medida la información personal es comunicada a los otros, y a esto lo denomina autodeterminación informativa[19].

El elemento que se introduce con el análisis del derecho a la privacidad virtual, es el depositar en el usuario de las TIC´S la facultad - responsabilidad de, primero, clasificar la información que exhibirá a través de las TIC´S y que tenga completa conciencia de que aquello que hubiere expuesto, probablemente permanezca en ese estado de exposición de manera permanente. En ese orden de ideas, el usuario debe estar suficientemente informado sobre los alcances de su exposición y sobre las acciones concretas que debe poner en marcha para prevenir la utilización abusiva de sus datos en internet.

Claramente, otros países se encuentran realizando esfuerzos plausibles en cuando a la educación de los usuarios o consumidores de las TIC´S, y también los criterios judiciales vienen registrando avances en cuanto a la aplicación de estos derechos.

---

[19] Galán Muñoz, Alfonso; Arribas León, Mónica, Caruso Fontán, María Viviana, et al., La Protección Jurídica de la Intimidad y de los Datos de carácter Personal frente a las Nuevas Tecnologías de la Información y Comunicación, editado en España, por la editorial Tirant Lo Blanch, en el año 2014, consulta en edición digital en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788490537657

Cuando pensamos en la experiencia salvadoreña, la situación actual es la siguiente: los usuarios de las TIC´S son abundantes, miles de miles de persona que se exponen voluntariamente, por diferentes motivos, entre los cuales puede mencionarse la contratación de servicios de todo tipo legalmente imaginable, y la gran mayoría también para fines propiamente recreativos o de ocio. Al escudriñar sobre la educación de los usuarios, desde instituciones del Estado, tampoco se ha registrado algún antecedente reciente.

1.4 La Identidad Digital como instrumento para la comisión de hechos delictivos a través de las TIC´S.

Pablo García Mexía, citaba en su obra *"Historias de Internet",* información proporcionada por *World Information Society Report 2006,* que acuño la frase: *la cibercriminalidad es la variedad delictiva de más rápido crecimiento en el mundo actual*. Además, otras fuentes afirmaban que Internet soporta hoy en día una economía criminal madura.[20]

Como ya se ha dicho en este capítulo, la identidad digital juega un papel esencial, pues para la comisión de cualquier hecho delictivo en el contexto de la ciberdelincuencia, en cualquiera de sus modalidades las cuales resultan complejas. En el territorio salvadoreño, además, puede aportarse que esa complejidad aumenta por el desconocimiento sobre las técnicas empleadas para la sustracción de información, que, si bien es cierto, un usuario no está obligado a conocerlas en un lenguaje elaborado, pero si debe ser apto para

[20] García Mexía, Pablo. Historias de Internet, ISBN: 9788415442615. Editorial: Tirant Lo Blanch. Fecha de publicación del libro: 2012-05-01. México, consultada en versión digital el 12/06/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788415442615?showPage=0

detectar los riesgos que corre al hacer uso de las TIC´S. Se sostiene que el punto de partida común es el acceso a la información que constituye la identidad digital o virtual de los usuarios de las TIC´S. Esta es la llave para ingresar al territorio de la delincuencia impune (hasta el momento) o ciberdelincuencia si se le quiere dar un nombre.

Cuando se habla de ciberdelito se hace referencia a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta, fundadamente internet. Así, Josefina Quevedo González, en su tesis doctoral realiza reflexiones en cuanto a la delimitación del ciberdelito, pues para considerar una conducta como tal, debe de darse la utilización de sistemas y datos informáticos en tres perspectivas: a. como objeto mismo sobre el que se produce el delito, b. como instrumento para la comisión delictiva y c. como simple soporte de información[21].

Se retoma una de esas perspectivas: como instrumento para la comisión delictiva y añadimos otro elemento, el apoderamiento de información personal (identidad digital), que es parte de ese instrumento delictivo. Ya que una vez se materializa el apoderamiento de determinada información propia de la identidad digital de los usuarios, se procede a perjudicar a su titular mediante el cometimiento de otra conducta delictiva.

Sin embargo, esto no es tan sencillo como se plantea, puesto que ese apoderamiento se da en la realidad virtual a través técnicas tales como, *programas espía (spyware), virus, spam, programa o software malicioso (malware), redes zombies o bonets (red de robots), triangulo vicioso.* [22] Esta

[21] Josefina Quevedo González. “Investigación y prueba del ciberdelito”. Ob. Cit. Pág. 58.
[22] Pablo García Mexía, Historias de Internet. Ob. Cit. Pág. 90.

variedad de técnicas implica la invasión de ordenadores o cuentas, ya se para apoderarse de información o el control de equipos propiamente, en el caso de *las redes zombies*, se pueden recopilar contraseñas, números de tarjetas de crédito u otros datos personales. Luego del uso de estas técnicas, cuando la identidad digital o virtual de los usuarios de las TIC´S ha sido vulnerada, se comenten una gran variedad de conductas *ciberdelictivas.*

En cuanto a las diferentes conductas delictivas, teóricamente se nombran de acuerdo vocablos en inglés. Al revisar los vocablos y su significado, vemos que la Ley Especial Contra Delitos Informáticos y Conexos vigente en El Salvador, los retoma y nos encontramos con sus equivalentes, tales como:

- *Spoofing*[23] (hurto de identidad, art. 22 LECDI), consiste en una persona o programa logra con éxito hacerse pasar por otros, mediante obtención de datos. Al examinar el art. 22, vemos que invoca como verbos rectores *suplantar o apoderarse de la identidad…*
- *Phishing* (estafa informática, art.10 LECDI), que consiste en engañar a otra persona, a efectos que revele datos sensibles, como bancarios que suponen una afectación patrimonial posterior. El art. 10 de la LECDI, cita como verbos rectores la manipular o influir en el ingreso de datos a las TIC´S, valiéndose de artificio y generando perjuicio patrimonial para otro.
- *Pharming* (fraude informático art. 21 de la LECDI), se entiende como el desvío de tráfico desde un sitio web hacia otro de similar apariencia, para el engaño de usuarios. El art. 21 de la LECDI, establece que la conducta típica consiste en interceptar por medio tecnológico una transmisión hacía, desde o dentro de un sistema

[23] Pablo García Mexía, Historias de Internet. Ob. Cit. Pág. 91.

informático…ubicándose también esta figura delictiva en nuestra ley especial.

- la denegación de servicio (Técnicas de denegación de servicio, art. 14 de la LECDI) se trata de un ataque lanzado contra un ordenador o una red a través de ordenadores “zombies”, para impedir el acceso al dueño legítimo. El artículo 14 de la LECDI, tiene una redacción referencial ya que castiga utilización de la técnica de denegación de servicio, pero no contiene una definición legal sobre esta.
- *Backdoor o* puerta trasera (Obtención y divulgación no autorizada, art. 23 LECDI) Se trata de un *software* que permite el acceso al sistema operativo del ordenador saltándose todos los métodos usuales de autenticación, para realizar actividades no autorizadas. El artículo 23 castiga la obtención no autorizada mediante las TIC´S, códigos, contraseñas, para acceder a programas o datos, siempre haciendo énfasis en la finalidad de lucro.

Lo anterior, por mencionar algunos ejemplos que doctrinariamente se retoman. Asimismo, hacer énfasis que estos tipos penales se encuentran previstos en el Capítulo III de la Ley Especial Contra Delitos Informáticos y Conexos, que se titula “Delitos Informáticos relacionados con el contenido de los Datos”. Ciertamente, se persigue garantizar el derecho a la protección de datos, pero no puede obviarse, que cada modalidad delictiva claramente procura obtener datos, información, pero con otro fin aún más claro que es obtener un provecho patrimonial para el delincuente. Por ello, se va en busca de la información sensible vinculada con cuentas bancarias, o contraseñas respectivas, no se trata de una diversidad de conductas al azar sin propósito. Por ello, es que se advierte que la identidad digital o el hurto de la misma es instrumental para una modalidad sofisticada de delincuencia.

Recientemente la experiencia salvadoreña ha sido abundante en cuanto a las modalidades de ciberdelincuencia, que involucra el uso indebido de la identidad digital. Los hechos de trascendencia en materia penal que involucran una sustracción de información de usuarios de las TIC´S, entre los cuales pueden mencionarse las estafas informáticas realizadas a clientes del Banco Agrícola [24], las cuales se realizaron a través de diferentes modalidades, pero con un denominador común: la utilización de información proporcionada por los usuarios de las TIC´S. Aun, cuando las entidades bancarias puedan desvincularse de responsabilidad, no se ha discutido si los usuarios habían sido suficientemente instruidos en el manejo de sus cuentas.

También, en octubre del año 2021 a través de la cuenta oficial de la Policía Nacional Civil, en la red social de Facebook se hacían advertencias sobre una modalidad novedosa a través de la cual desconocidos establecían comunicación a través de WhatsApp[25], eligiendo víctimas al azar para que les brindasen ayudan para retirar equipajes en el aeropuerto, solicitando depósitos de cantidades de dinero. Tal aviso fue necesario, ya que muchas personas se abocaron a las diferentes delegaciones policiales para presentar denuncias, identificándose esa modalidad de delincuencia a través de una aplicación, que dicho sea de paso es de las más complejas para rastrear información de creación de cuentas, debido a las políticas de privacidad de la misma, ya que las solicitudes de información a las mismas requieren de trámites largos, en cuanto se trate de circunstancias que no comprometan la vida de las personas.

---

24 "Banco agrícola simplifica proceso de denuncia por estafas", consultado el 25 de octubre de 2021 en https://www.elsalvador.com/noticias/negocios/estafas-bitcoin-bancos/871906/2021/

[25] Cuenta Oficial de Facebook Policía Nacional Civil, Consultado 11/06/2022 en https://www.facebook.com/PoliciaNacionalCivil/photos/a.10150539998650950/10158814835640950/?type=3 publicación de fecha 22/01/2021.

El día 07 de julio de 2021, a través de la cuenta oficial del Ministerio de Hacienda en la red social se difundió un aviso, en el cual se alertaba a la ciudadanía en relación a personas inescrupulosas que solicitaban datos o información personal, haciendo el llamado a utilizar los canales oficiales de los requisitos o pasos para realizar trámites, proporcionando la el sitio oficial, lo que supone el empleo de técnicas delictivas complejas a través de inducir a los usuarios a creer que realizaban gestiones en páginas oficiales, tratándose de sitios fraudulentos[26].

La Policía Nacional Civil, también sufrió una vulneración en la seguridad informática de sus plataformas, ya que en redes sociales se difundieron los datos personales de casi 30,000 policías[27], generando un estado de alarma entre los agentes policiales, no solamente por la vulneración a su derecho a la intimidad, sino por probables afectaciones a su seguridad personal. Entre otros casos destables, lo que es claro, es la existencia del problema al cual nos enfrentamos, así como lo necesario de realizar esfuerzos mas enérgicos para solucionar el mismo.

1.5 El derecho a la Identidad Digital, un Derecho Humano de Cuarta Generación.

[26] Cuenta Oficial de Twitter, Ministerio de Hacienda, consultado 11/06/2022, en https://twitter.com/haciendasv/status/1412768606480482308?lang=es, publicación de fecha 07/07/2022.

[27] **<<** hackeo de web de la PNC pone en peligro datos de policías>>. consultado el 25 de octubre de 2021 en https://www.laprensagrafica.com/elsalvador/hackeo-de-web-de-la-pnc-pone-en-peligro-datos-de-policias-20210909-0059.html

Los derechos humanos son atribuciones inherentes a toda persona por su sola condición de serlo, sin distinción de edad, raza, sexo, nacionalidad o clase social;[28] La Declaración Universal de los Derechos Humanos fue adoptada por la Asamblea General de la ONU, el 10 de diciembre de 1948.

En el estudio de los Derechos Humanos, Ana Lilia Ulloa Cuéllar y Érika Verónica Maldonado Méndez, establecen una clasificación generacional de los derechos humanos:

Primera generación: Se refieren a los derechos civiles y políticos, conocidos también como "libertades clásicas". Los cuales registran su surgimiento en la Carta Magna de Inglaterra (1215), su posterior reconocimiento en la Declaración de los Derechos Humanos del Ciudadano (Francia 1789). Entre estos derechos se pueden mencionar, el derecho a la vida, la libertad, seguridad jurídica, entre otros.

Segunda Generación: Se refieren a los derechos económicos, sociales y culturales. En relación a estos derechos, el Estado tiene la obligación de actuar y se dice que estos derechos son progresivos. Surgieron con la aparición de los movimientos obreros del siglo XX. Entre estos pueden mencionarse el derecho al trabajo, derecho a seguridad social, derecho a la salud, la educación, entre otros.

[28] Ulloa Cuéllar, Ana Lilia; Maldonado Méndez, Érika Verónica, et al. Nociones de Derechos Humanos. Editorial Tirant lo blanch, 2019, 1° Edición, consultada en versión digital el 12/06/2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788491909842

Tercera Generación: Se pueden mencionar el derecho de los puebles a su libre determinación, derecho a un medio ambiente saludable, derecho a la paz, entre otros.[29]

Como puede observarse, dicha clasificación atiende a un criterio cronológico, según su aparición que se encuentra ligada también a acontecimientos históricos y sociales, que han provocado el reconocimiento de los Estados de nuevos derechos o facultades reservadas para el ser humano.

Robert B. Gelman, en 1997 fue el primero en difundir una propuesta de "Declaración de los Derechos Humanos en el Ciberespacio", y posteriormente se van registrando más documentos que subrayan la importancia del acceso a internet como camino a la mejora de la condición humana. Así lo menciona Juan Carlos Riofrio Martínez Villalba, quien dedica un artículo al análisis sobre el surgimiento de una cuarta ola de derechos humanos.[30]

Riofrio, sostiene que el surgimiento de una nueva generación de derechos humanos, depende de lo novedoso de los nuevos derechos que se proponen y reconocen. Además, menciona que el derecho a la identidad digital, podría en alguna medida equipararse al derecho de la persona natural a tener su propia identidad, situación que podría dar pie a cuestionarnos sobre su carácter de novedoso. Pero finalmente, entre sus reflexiones, concluye en que todas las generaciones de derechos humanos que surgen, se encuentran de alguna manera vinculada a la anterior y ello no les resta necesariamente ese carácter de novedoso.

---

[29] Ana Lilia Ulloa Cuéllar, Érika Verónica Maldonado Méndez, et al. Nociones de Derechos Humanos. Ob. Cit. Página. 20.
[30] Juan Carlos Riofrio Martínez-Villalba. <<La Cuarta ola de Derechos Humanos: Los Derechos Digitales>>. Pág. 19.

El Dr. Javier Bustamante Donas, se una en la reflexión sobre la necesidad o el reconocimiento de una Cuarta Generación de Derechos Humanos y reconoce el protagonismo que ha cobrado la utilización del internet y la universalización del acceso a la tecnología. Plantea aspectos muy importantes en relación a la aparición de nuevos valores y paradigmas éticos, ya que el mundo ha cambiado de forma sustancial a partir del desarrollo tecnológico, o como el lo conceptualiza, el desarrollo de la "tecnociencia".[31]

Ana Lilia Ulloa Cuéllar y Érika Verónica Maldonado Méndez, por su parte los clasifican como derechos humanos de quinta generación, y de manera ejemplificativa relaciona el derecho de acceso informática, a la seguridad digital, a acceder al espacio de la nueva sociedad de la información, a formarse en las nuevas tecnologías y el uso del espectro radioeléctrico y de la infraestructura para los servicios en línea[32].

Lo cierto es, que este nuevo universo de posibilidades de conductas que se manifiestan en las plataformas virtuales, no puede dejarse desprovistas de regulación y reconocimiento formal de los Estados. Esto, porque su impacto en la vida cotidiana de los usuarios de las TIC´S, es perceptible a nuestros sentidos de manera concreta y desde esa perspectiva, no resultan insuficientes los motivos para consolidación como derechos humanos de cuarta generación, entre los cuales se encuentra el derecho a la identidad digital. Probablemente, nos cuestionemos si es realmente inherente al ser

---

[31] Bustamante Donas, Javier. Hacia la Cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica. Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, no. 1. Versión digital, consultado 12/06/2022 en https://www.corteidh.or.cr/tablas/r22470.pdf

[32] Ana Lilia Ulloa Cuéllar, Érika Verónica Maldonado Méndez, et al. Nociones de Derechos Humanos. Ob. Cit. Página. 22.

humano el uso de las TIC´S, el acceso a internet, el ser titular de una identidad digital, ya que subsisten muchas personas alrededor del mundo que no hacen uso de las mismas.

Sobre ello, debe considerarse, que el acceso a las TIC´S forma parte del desarrollo y avance del ser humano. Tanto así, que cuando se utilizan adecuadamente puede percibirse una mejora en la calidad de vida de las personas, ya que se superan barreras impuestas por la distancia, ayuda a potenciar el tiempo, permite acceder a información noticiosa en tiempo real y ha logrado descentralizar el manejo de los medios para comunicarnos, ya que es posible difundir contenido y lograr que el mismo alcance a grandes cantidades de personas sin necesidad de depender de los medios masivos de información tradicionales. Este abanico de nuevas posibilidades de mejora, debería de ser accesible para todas las personas, de una forma segura y con suficientes.

CAPITULO II: REGULACIÓN NACIONAL E INTERNACIONAL QUE ESTABLECEN MECANISMOS DE PROTECCIÓN DEL DERECHO A LA IDENTIDAD DIGITAL.

SUMARIO: 2.1. Regulación Nacional relativa a la Protección de la Identidad Digital. Alcances.2.2 Regulación Internacional Aplicable al caso de El Salvador relativa a la Protección de la Identidad Digital. 2.3. Estudio de las disposiciones de derechos comparado relacionadas con la protección de la Identidad Digital y Protección de Datos.

RESUMEN:

A continuación, se ofrece un breve análisis en cuanto a las disposiciones legales aplicables en relación a la protección del derecho a la identidad digital, en el Caso de El Salvador. Como es necesario se citan primero, las disposiciones constitucionales entre las cuales se invocan los artículos 1, 2 y 101 de la Constitución; las cuales fundamentan la aptitud del derecho a la identidad digital para proteger un bien jurídico individual; así como también bienes jurídicos colectivos. Seguidamente, se alude a las disposiciones de la Ley Especial Contra Delitos Informáticos y Conexos, desde su promulgación y vigencia, descomponiendo su contenido y aportando un análisis sobre la clasificación de los tipos delictivos empleada por el legislador, con la finalidad de establecer la técnica legislativa y criterios empleados para su sistematización. Uno de los aspectos de especial atención es el bien jurídico legalmente establecido en la LECDIC: la información. En relación a la información como bien jurídico protegido se expone un primer acercamiento a la definición del concepto, aunque bastante breve, sin embargo, sobre este aspecto se presenta a través del capítulo cuatro otras consideraciones más amplias. En cuanto a las disposiciones de carácter internacional aplicables a

El Salvador, relativas a la protección de la identidad digital es necesario mencionar el Convenio de Budapest, como el principal aporte ofrecido por la Unión Europea, al cual muchos otros se adhirieron, y en el caso de El Salvador, aunque no se ha finalizado su proceso de adhesión, más si se ha retomado su contenido a través del texto de la LECDIC. En el último apartado, se presentan las disposiciones vigentes en la región, en países como Honduras, Guatemala y Costa Rica. En el caso de Costa Rica, es el país mejor evaluado de la región en tema de ciberseguridad, sin embargo, dicho lugar ha sido conquistado en base a la labor preventiva y de educación de los usuarios de las TIC´S.

2.1 Regulación Nacional relativa a la Protección de la Identidad Digital.

La protección del derecho a la identidad digital como tal, se vincula con la regulación de las relaciones de los individuos por medio de las nuevas tecnologías de la información y comunicación. Como ya anteriormente se ha mencionado, su estudio no puede desvincularse de conceptos como la protección de datos y ciberdelincuencia.

No debe omitirse que, en El Salvador, el concepto “Identidad Digital”, tampoco ha sido desarrollado como tal, ni en textos académicos, ni jurisprudencialmente. Incluso la Ley especial contra delitos informáticos hace referencia al concepto de *“identidad”,* en su sentido ya ordinariamente desarrollado, más no como la identidad digital propiamente, sin embargo, no significa que no exista una regulación del derecho a la identidad digital en el país, por lo que a continuación se señalara mediante un esfuerzo de interpretación extensiva, si así podemos llamarlo.

En algunos países, como España, de manera expresa se establece en su Constitución, artículo 18.4 una limitación del uso de la informática para garantizar el derecho a la intimidad de las personas.[33] En lo sucesivo a través del desarrollo de criterios jurisprudenciales se da una aplicación de esta disposición a fenómenos procedentes de situaciones concretas, sin perjuicio de la abundancia de instrumentos jurídicos en materia de protección de datos aplicables, emanados de la Unión Europea.

2.1.1 Constitución de la República de El Salvador.

En El Salvador, se encuentra vigente la Constitución de la República que data del año 1983, por tanto, es razonable que ésta no contemple expresamente el derecho a la protección de datos, identidad digital o que no se empleen conceptos relativamente novedosos como la "informática", ciberdelincuencia o nuevas tecnologías de la información y comunicación.

No obstante, lo anterior, en el caso de El Salvador, la protección del derecho a la identidad digital, deviene de la existencia de la persona humana como tal, por lo que, puede citarse el artículo 1, inciso 1 de la Constitución como su fundamento constitucional: "*El Salvador reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizada para la consecución de la justicia, de la seguridad jurídica y del bien común*[34]*."*

---

[33] Constitución Española, aprobada por las Cortes en sesiones plenarias del Congreso de los Diputados del Senado Celebradas el 31 de octubre de 1978, ratificada por el pueblo español en referéndum de 6 de diciembre de 1978 y sancionada por S.M. el Rey ante Las Cortes el 27 de diciembre de 1978. Consultada en edición digital PDF el 09 de julio de 2022 en https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

[34] Constitución de la República de El Salvador, aprobada por medio Asamblea Constituyente y decreto No 38, publicada en Diario Oficial No 234, Tomo No 281 de fecha 16 de diciembre de 1983, consultada en edición PDF el día 09 de julio de 2022 en https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf

Evidentemente, se trata de una interpretación bastante extensiva, aunque, también debe ser complementada por el artículo 2, inciso 2, de la misma Constitución de la República que establece que "*se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*.

Es innegable la relación entre el derecho a la intimidad personal y el derecho a la identidad digital, el cual, no podría concebirse si quiera, si no existiese primero la persona humana, como titular de derechos, entre los cuales, pueden encontrarse el derecho a la vida, el honor, la propia imagen, la intimidad, entre otros derechos individuales de novedoso surgimiento como la identidad digital.

Lo más importante es tener claridad sobre la finalidad de todo el esfuerzo de las creaciones jurídicas, las cuales se manifiestan en el establecimiento de derechos, sean estos individuales o colectivos: garantizar un beneficio para la persona humana; así como tan poéticamente lo señala el artículo 1 de la Constitución. En este mismo sentido el Tribunal de Sentencia de Usulután, en sentencia definitiva citó que "*Nunca se puede invertir el orden y concebir a la persona como un medio para que otra persona, agrupación y por excelencia el Estado cumpla sus fines; este último tiene tan solo el carácter de medio para el desarrollo de la personalidad humana, porque no es sino una creación humana, por y para la persona humana"*[35]*.*

El derecho a la identidad digital, que como ya hemos venido desarrollando, se trata de esa expresión por medios electrónicos de rasgos o información personal a través de medios digitales, que sirven para identificar a las

[35] Sentencia definitiva emitida por el Tribunal de Sentencia de Usulután, de fecha 04 de marzo de 2004, en proceso marcado con referencia judicial P0501-06-2004, consultada el día 10/07/2022 en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php

personas. Esta información personal que constituye la identidad digital, debe ser protegida, dando paso al surgimiento de otro derecho, como el de la protección de datos.

El carácter de fundamental del derecho a la intimidad personal, se transmite también al derecho a la identidad digital, puesto que, ambos son importantes para el desarrollo, bienestar y beneficio de la persona humana, que como ya se ha dicho, es el fin del Estado mismo.

Cada persona humana y también jurídica que tiene existencia en el mundo digital, se convierte en un usuario de las tecnologías de la comunicación e información, capaz de ejercer derechos y contraer obligaciones en esa realidad virtual, porque su accionar trasciende a la realidad objetiva, perceptible a los sentidos. Es este último aspecto, el que le da vida al estudio del derecho a la identidad digital, así como su instrumentalización en el cometimiento de hechos delictivos.

Este accionar delictivo, o como algunos autores lo denomina “cibercrimen”, se hace más visible en la medida que afecta a mayor cantidad de usuarios de las nuevas tecnologías de la comunicación e información. Es decir, individuos que han integrado las TICS en su cotidianeidad, como un medio para mejorar su calidad de vida y desarrollo como ser humano, facilitando toda clase de actividades a través del uso de las mismas. Este grupo de personas, no está integrado únicamente por personas naturales, sino que también, personas jurídicas confían, los fines de su existencia a las TICS, convirtiéndoles en usuarios de las mismas. Como todo usuario, se sirven de sus ventajas, pero también se exponen a los riesgos. Los usuarios de las TICS, entonces constituyen una colectividad de sujetos con derechos comunes entre sí.

En relación a lo anterior, la jurisprudencia constitucional nacional indica: *cuando se trate de intereses colectivos el sujeto al que aparecen atribuidos los bienes a los que el interés se refiere es individualizado o individualizable, ya que está relacionado con colectividades de carácter permanente y con la consecución de los fines que las caracterizan; es decir, los intereses colectivos se identifican con aquellos de un grupo determinado, por lo que atañen al individuo en tanto parte de un grupo*[36]*.*

Los usuarios de las TICS, tienen fines claramente identificables, como ya se ha venido sosteniendo. Estos fines, independientemente se trate de una persona natural o jurídica, siempre resultarán ser un mayor aprovechamiento de los recursos, tiempo y mejor calidad de vida para sus usuarios. Ello, les hace parte de esa colectividad bien determinada, identificable y merecedora de una tutela de sus derechos por parte del Estado.

Sobre lo anterior, la doctrina indica que *el que un derecho o un interés pertenezca a muchos no quiere decir que no pertenezca a ninguno, sino que todos los potenciales titulares han resultado igualmente afectados. El problema no consistirá ya en determinar si ese concreto interés existe o no a un determinado sujeto, sino en ver quién es el portador legítimo en un juicio de un interés o de un derecho que pertenece a muchos, sean considerados o no globalmente por el ordenamiento jurídico*[37]*.* Esta colectividad de personas

---

[36] Resolución que admite, demanda de amparo, de fecha 09 de octubre de 2020, emitida por la Sala de lo Constitucional de la Corte Suprema de Justicia, en proceso marcado con referencia 430-2020, consultada en versión digital, en fecha 17 de julio de 2022, en https://www.jurisprudencia.gob.sv/busqueda/showExtractos.php?bd=1&nota=922929&doc=921522&&singlePage=false .

[37] Bonachera Villegas, Raquel. Tutela Procesal de los Derechos e Intereses de Los Consumidores. Pág. 24. Nota al pie. Editorial Tirant lo blanch, Valencia, 2018. Consultada en versión digital en fecha 17 de julio de 2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491699149

titulares de un derecho, que además pueden denominarse usuarios, bien puede denominarse también consumidores, aunque como veremos la protección de estos significa la creación de instituciones cuya finalidad sea de contraloría en cuanto al manejo de datos de los usuarios, los cuales componen su identidad digital.

Así puede mencionarse que, los intereses colectivos, *tratan sobre intereses de personas que son individualizables, pero que sumadas conforman una colectividad; lo mismo ocurre también, cuando una asociación de consumidores y usuarios, o una asociación de ecologista defiende los intereses colectivos de sus miembros*[38].

En este orden de ideas, es posible identificar otra disposición de rango constitucional que sirve como fundamento en cuanto a la protección del derecho a la identidad digital, entendida esta como, un derecho de los usuarios o consumidores de las TICS, así el artículo 101 de la Constitución establece:

El orden económico debe responder esencialmente a principios de justicia social, que tiendan a asegurar a todos los habitantes del país una existencia digna del ser humano.

El Estado promoverá el desarrollo económico y social mediante el incremento de la producción, la productividad y la racional utilización de los recursos. Con igual finalidad, fomentará los diversos sectores de la producción ***y defenderá el interés de los consumidores.***

[38] Blanquer Criado, David. Esquemas de Derecho Administrativa. TOMO XLIII, Editorial Tirant lo Blanch, Valencia, 2016. Consultada en versión digital, en fecha 17 de julio de 2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491192572

De esta forma, puede sostenerse el argumento en cuanto a que el Estado si tiene el deber de crear mecanismos para proteger a los usuarios de las TICS, como parte de un sector incipiente de consumidores, esto sucede, porque el manejo de información sí puede generar consecuencias perceptibles en la realidad objetiva que influyen en el bienestar de la persona humana y el desarrollo económico mismo.

2.1.2 Ley Especial Contra Delitos Informáticos.

La ley especial contra delitos informáticos fue aprobada por medio de decreto número 260, publicado en el Diario Oficial No 40, Tomo 410. Estableció cuatro considerandos, entre los cuales citó el artículo 1 de la Constitución de la República de El Salvador, así como los nuevos desafíos del desarrollo tecnológico y la necesidad regular nuevas formas de cometimiento de hechos delictivos a fin de evitar la impunidad de los mismos.

La ley especial contra delitos informáticos está dividida en tres títulos, y cada título está dividido en capítulos. Los tipos delictivos relacionados con el manejo, hurto, interceptación y protección de datos son abundantes, los cuales componen en su mayoría el contenido de la ley.

El título uno, contiene disposiciones generales, las cuales se encuentran detalladas en tres artículos. Se establece que el objeto de la ley es proteger los bienes jurídicos de las conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación y también establece expresamente la sanción de delitos en perjuicio de datos. En lo sucesivo, por disposición legal se establece el bien jurídico protegido, en el artículo 3, letra

b) de la Ley Especial Contra Delitos Informáticos, el cual se entiende de manera genérica "*es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros."* En ese sentido, la determinación del bien jurídico protegido devendrá el análisis del tipo de que se trate, sin embargo, el punto de partida es la información.

2.1.2.1 La información como bien jurídico protegido.

Primero debemos acercarnos a una definición aproximada del concepto "información" el cual se conforma de dos partes: "in" – "formatio". En latín "formatio" se refiere a la acción de formar o de dar forma, de generar algo. Por su parte el prefijo "in" indica dirección hacia dentro. Generar algo hacia adentro, algo que proviene desde afuera".[39] Otra aproximación al concepto "Información, es un conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y reestructurarlos de una manera determinada, de modo que le sirvan como guía de su acción.[40]

Al buscar una definición concreta de la palabra *"información",* es evidente que no se trata de una tarea fácil, puesto que generalmente se hace alusión al concepto como a determinado conocimiento sobre una cosa, acontecimiento o persona, y el significado del concepto, parece estar claro, ya que no se hacen esfuerzos por definirlo, sino que se hace referencia al mismo, como algo ya conocido. Más, para aplicarlo a la investigación es necesario navegar en el contexto de la realidad virtual. Así, José Fabián Roa Buendía, sostiene que,

---

[39] Consultado en sitio *Definiciona. Definición y etimología, el día 16 de septiembre de 2022 en* https://definiciona.com/informacion/

[40] "El diseño de Información", consultado en versión digital el 16 de septiembre de 2022 en: http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/capitulo1.pdf

en *el fondo, todo es información, sean los escasos 140 caracteres de un tweet, sean ficheros de varios megabytes, están en nuestro equipo y alguien puede intentar obtenerlos. La clave es la motivación: quien está interesado en nuestra información*[41].

Al retomar la definición legal que nos brinda la ley especial contra delitos informáticos, debemos establecer que dependerá de la casuística, si esa información relacionada garantiza el ejercicio de los derechos fundamentales de las personas naturales y jurídicas. Con todo ello, resulta necesario analizar, lo conveniente de establecer elementos diferenciadores entre la información en sentido general y la información de relevancia penal.

Por lo anteriormente planteado, conviene mencionar el Informe en el Nonagésimo Primero Período Ordinario de Sesiones del Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA) a celebrarse en Río de Janeiro, Brasil del 7 al 16 de agosto de 2017. En dicho contexto, se sostuvieron reuniones de la Red Iberoamericana de Protección de Datos (RIPD), cuya finalidad fue el estudio del tema de la protección de Datos Personales y como producto de ello se crearon estándares de protección de datos personales para la región.

---

[41] Roa Buendía, José Fabián Roa Buendía. "Seguridad Informática." Edición digital, ISBN, año 2013. Pág. 9, Consultado el 16 de Septiembre de 2022 en, : https://d1wqtxts1xzle7.cloudfront.net/34758985/Seguridad_Informatica_McGraw-Hill_2013__www.FreeLibros.me_-_copia-with-cover-page-v2.pdf?Expires=1663343456&Signature=Jyb~~9KD~1eZWk6en7RKdtFFjkGBoAWhT1~Vj5x5xdRJaaUcQuQMODTYqFCJxDi2RMMn0EPr9STWJQfkES6~IMcf1e2G9eNB8VPdXmcrZGBboK-1a~FqEmxttn6jeoQ-PHIOSeM6qCh~SHqjRwgL3yoOKFeEucgMaK4LF3-Z2LDYMxvWE0dYaAdmssy464ZHtM9Rf7s3VOLXH~iX8WDxgyO0mLhhsh8IC27qwTsaS7xxHJ8WR6b3nhhqHLPABo3bF~9NJmjPSnD-9VwdIwBns5y5z3QNzhzcikm3NZnqMV1Sb4MCILSht5E3gkY0MOlfIl8tq-rI5cvVUCTNs1iw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

En dicho informe la doctora Ana Elizabeth Villalta Vizcarra, concluye que *"Los "Datos Personales" implican toda aquella* ***información*** *inherente a una persona, que permiten identificarla, abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta, es decir,* ***la información*** *de una persona física identificada o identificable, como por ejemplo: nombre, apellidos, correo electrónico, estado civil, profesión, número de documento de identidad, entre otros."* Aunque, la información también puede ser relativa a las personas jurídicas, según lo indica el mismo texto de la ley especial de delitos informáticos. Incluso se establece un tipo en perjuicio del orden socioeconómico en el artículo 34, que se denomina Suplantación de Actos de Comercialización. La conducta penalmente relevante consiste, precisamente en vender o comercializar bienes o servicios, suplantando la identidad del productor, proveedor o distribuidor autorizado, quien evidentemente puede ser una persona jurídica.

Ya en este punto, podemos referenciar en cuanto a la identidad digital, según lo analizado en el capítulo I de esta obra. Y ya mencionamos que, según Juan Carlos Riofrio Martínez Villalba, la identidad digital es la expresión electrónica del conjunto de rasgos con los que una persona, física o jurídica, se individualiza frente a los demás.

Es decir que todo los que circula en el ciber espacio es información, parte de esa información pueden clasificarse como datos personales, y la expresión electrónica de estos componen la identidad digital. Es posible vincular desde los elementos generales a los más particulares los conceptos de Información-datos e identidad digital. Este último concepto, que, aunque no es abordado expresamente en la ley, se encuentra presente en la misma de manera imbíbita en la mayoría de conductas castigadas por la ley especial.

Claramente, el concepto de datos es importante para determinar qué información resulta relevante para que los usuarios ejerzan sus derechos fundamentales según lo establece la ley especial contra delitos informáticos.

2.1.2.2. Breve análisis sobre los tipos penales comprendidos en la Ley especial Contra Delitos Informáticos.

El capítulo I, del titulo II, se denomina *"De los Delitos contra los sistemas tecnológicos de información".* En lo sucesivo, se encuentran seis tipos delictivos relacionados. Sin embargo, esta primera clasificación de tipos penales no responde a un orden que considere el bien jurídico protegido, como sucede mayoritariamente en el Código Penal. Por otro lado, al anunciar que los tipos penales atentan contra los sistemas tecnológicos de la información, podría considerarse que dicha clasificación toma como parámetro uno de los elementos descriptivos de los tipos penales: **los sistemas tecnológicos de información.**

Aun, a pesar de esta denominación, es claro que lo que se protege en términos generales es la información, los datos personales, datos personales sensibles, datos informáticos. Todos estos, necesariamente pertenecen a un titular determinado, quien exige la protección de los mismos. Pero que conllevan necesariamente alguna especie de vulneración de sistemas tecnológicos, siendo este el elemento común, el cual elige el legislador para agruparlos.

En el capítulo II, se denomina **"De los Delitos Informáticos"**. Contempla seis tipos penales, entre los que se encuentra la estafa informática, el fraude informático, falsedad de documentos u firmas, espionaje informático, hurto por medios informáticos y técnicas de denegación de servicio.

Cabe preguntarse por qué motivo este reducido grupo de delitos se consideran expresamente como delitos informáticos. La respuesta resulta de considerar varios factores comunes entre las conductas mencionadas: se trata de tipos cuyo resultado significa alguna clase de afectación patrimonial para la víctima. Además, la víctima puede ser una persona jurídica en cada uno de los casos. Ahora, el empleo de las tecnologías de la información es un elemento *sine qua non* de todas las conductas que contiene la ley especial en comento.

En este sentido Leyre Hernández Díaz, se dedica a realizar un esfuerzo por determinar qué debemos entender por *delito informático.* Hace mención sobre la evolución que ha sufrido la definición de tal concepto. Así las primeras definiciones de lo que debía entender por delito informático se limitaban al ámbito patrimonial[42]. En este sentido podría comprenderse, que ha sido éste el criterio utilizado para agrupar los tipos delictivos mencionados en el capítulo II de la ley especial contra delitos informáticos.

La misma autora Hernández Díaz, enuncia una variedad de definiciones sobre el concepto de *delito informático.* Entre estas, la definición proporcionada por González Rus, contiene componentes que brindan más elementos interesantes y pertinentes para nuestro estudio. Este menciona que los *ilícitos informáticos son* un conjunto de delitos de carácter heterogéneo que puede dividirse en dos grandes grupos: por un lado, el de las amenazas para la intimidad personal y la esfera privada derivadas de la ingente acumulación de

[42] Hernández Díaz, Leyre. El Delito Informático. EGUZKILORE, número 23, San Sebastián, diciembre 2009. Pág.230. Consultado en versión digital el día 16 de septiembre de 2022 en: https://addi.ehu.es/bitstream/handle/10810/24953/18-Hernandez.indd.pdf?sequence=1

datos; y, por otro, el de los delitos patrimoniales, favorecidos en su comisión por las posibilidades que ofrecen las nuevas tecnologías[43].

Aun, considerando los elementos de la definición citada, si analizamos las conductas típicas establecidas en la ley especial contra delitos informáticos, resulta que para la comisión de los mismos se requiere una obtención, interceptación, adquisición, difusión, apoderamiento, o cualquier otra acción debe recaer en determinando momento en datos y necesariamente en información valiosa para su titular.

El capítulo III, del título dos se denomina ***Delitos Informáticos Relacionados Con El Contenido De Los Datos***. El capítulo III, contiene catorce tipos delictivos vinculados con la protección de datos, aunque, al darle lectura a la ley, toda se encuentra íntimamente relacionada con la protección de datos de las personas o usuarios en el ciberespacio, aunque no contempla expresamente el concepto de *"identidad digital",* pero si al concepto ordinario de identidad de la persona humana como tal.

Al revisar los tipos penales a los cuales se hace alusión, puede mencionarse la manipulación de registros, manipulación fraudulenta de tarjetas inteligentes o instrumentos similares, obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares, provisión indebida de bienes o servicios, entre muchos otros. Sobre este tercer grupo de delitos se puede hacer una observación bastante evidente y es que se trata de tipos penales de resultado, puesto que cada conducta descrita requiere una acción consistente en un acceso, una utilización, alteración, copia, inutilización, daño, obstrucción o un apoderamiento, el cual debe recaer sobre datos. Estos datos también son

[43] Leyre Hernández Díaz. Ob. Cit. Pág. 232.

mencionados indistintamente como la identidad de una persona, contraseñas, datos informáticos o en ocasiones como información confidencial. Todo lo mencionado puede ser clasificado como datos e información.

El capítulo IV se denomina **Delitos Informáticos contra Niñas, Niños y Adolescentes o Personas con Discapacidad.** Este capítulo contiene nueve tipos penales, cuyo contenido se encuentra vinculado con el uso de las nuevas tecnologías de la información y el tráfico de información de contenido sexual o erótico con niños, adolescentes o personas con discapacidad. En esta clase de delitos, el autor del hecho generalmente utiliza como medio para establecer comunicación con la víctima la creación de cuentas con datos o información falsa, generando una identidad digital ficticia, que le permite permanecer en el anonimato e impunidad. Sin embargo, este tema, encierra otro universo de estudio, el cual no pertinente para el presente documento.

El capítulo V, **Delito contra el Orden Económico.** Dicho capitulo lo compone el artículo 34: Suplantación en Actos de Comercialización, el cual tipifica la venta a nombre de un tercero y suplantando su identidad, mediante el uso de las TICS, dicha venta debe recaer sobre bienes o servicios, de los cuales la víctima ostente calidad de productor, proveedor o distribuidor autorizado. Al estudiar el tipo, es posible advertir que se castiga justamente, esa intromisión en el comportamiento del mercado, mediante un apoderamiento de la identidad digital de la víctima, que en este caso sería una persona jurídica.

En cuanto al orden económico como bien jurídico protegido, Muñoz Conde, destaca que este se vincula exclusivamente a la actividad del Estado como director e interventor de la economía. Se refiere entonces a la regulación jurídica del intervencionismo estatal de la economía y a la tutela de los intereses patrimoniales individuales. En cuanto al orden socioeconómico

indica que trasciende su esfera de protección fundamentalmente a los intereses colectivos supraindividuales[44]. En ese punto, se considera que es erróneo establecer como bien jurídico el orden económico y no el orden socioeconómico, ya que se ha comprobado ampliamente con acontecimientos recientes que los hechos delictivos cometidos por medio de las TICS, pueden alcanzar a grandes sectores de la población al mismo tiempo, afectar la reputación comercial de las empresas en redes sociales, generando un impacto en las ventas de bienes o prestación de servicios, trascendiendo de un plano individual al supraindividual, ya que logra poner en peligro el orden económico. Hay varios factores que coadyuvan a ello, entre los que se encuentran la influencia en el papel de las TICS como nuevo medio de difusión de información noticiosa, que alcanza a un porcentaje considerable de la población.

Así tenemos, que en la actualidad empresas u organizaciones han elaborado manuales de estilo o manuales de identidad corporativa en los que se especifican aspectos tanto de contenido como formales: fuentes, colores, distribución de la información, etc. En el siglo XXI, estos manuales tienen también en cuenta la presencia de la organización en Internet y todos los productos asociados como dominios, redes sociales o correos electrónicos[45].

Finalmente, la ley especial contra los delitos informáticos y conexos indica la necesidad de la especialización en la investigación de los delitos informáticos, refiriéndose a la Policía Nacional Civil, la Fiscalía General de la República y la

---

[44] MUÑOZ CONDE, Francisco: "Delincuencia económica. Estado de la cuestión y propuestas de reforma", en *Hacia un derecho penal económico europeo, Jornadas en honor al profesor Klauss TIEDEMANN,* Boletín Oficial del Estado, Madrid, 1995, p. 267. Versión digital.

[45] Muñoz Feliu, Miguel C. Reputación Online y huella digital. Departamento de Comunicación Audiovisual, Documentación e Historia del Arte. Universidad Politécnica de Valencia. Tirant lo blanch.

Procuraduría General de la República. Las limitantes son las mismas: los recursos.

La Ley Especial Contra Delitos Informáticos está compuesta por treinta y seis artículos. Algunos de ellos fueron reformados recientemente por medio del decreto legislativo No 236, de fecha 07 de diciembre de 2021, publicado en el Diario Oficial No 8, Tomo 434 de fecha 12 de enero de 2022. Las reformas se realizan en atención a la implementación del Bitcoin como moneda de curso legal en la República de El Salvador. Así, se ha establecido en algunos casos, que cuando la conducta castigada recaiga sobre transacciones en Bitcoin u otras criptomonedas, será considerado como circunstancia agravante del tipo, así sucede con el delito de Interferencia del Sistema informático (art.6), Daños a Sistemas Informáticos(art.7), Fraude Informático (Art. 11), Secuestro de Sistemas, Programas o Datos Informáticos, previsto en el art. 26-A, todos los artículos de la Ley especial Contra delitos Informáticos.

Así también se crearon tipos penales, para castigar conductas las cuales no habían sido consideradas con anterioridad, como en el caso del artículo 11-A Falsedad de Documentos y Firmas. En otros casos se añadió texto a delitos existentes, siempre para sancionar conductas delictivas novedosas, como la descrita en el art. 23 incisos 1 y 2, de la misma ley especial.

El Código Procesal Penal, también fue reformado recientemente, por lo que se adicionaron algunos artículos como 259-A, 259-B, 259-C, 259-D, 259-E, el cual regula la evidencia digital, cadena de custodia, incorporación de la misma al proceso y valida la utilización del agente encubierto digital. Esta reforma complementa la LECDIC, puesto que señala que se utilizará para los delitos contenidos en esta.

2.2. Regulación Internacional Aplicable al caso de El Salvador relativa a la Protección de la Identidad Digital.

En el presente apartado, se realizará un repaso sobre la regulación internacional aplicable al caso de El Salvador, en cuanto a la protección de la identidad digital. Sin embargo, también resulta productivo hacer una referencia breve sobre la situación actual en otras regiones del mundo que reportan mayores avances en relación con el tema.

El mejor ejemplo es la unión europea es pionera en cuanto a la promulgación de cuerpos normativos relacionados con la protección de datos y la identidad digital. Este último concepto, es de gran importancia ya que la UE, ha desarrollado una actividad educadora e informadora de sus ciudadanos a través de medios digitales, a la cual denominó “Identidad Digital para todos los europeos”. En dicha campaña se hace énfasis de las ventajas de contar con una identidad digital reconocida en cualquier lugar de la UE. Esta consistiría según mencionó Ursula Von der Leyen, presidenta de la Comisión Europea en su discurso sobre el estado de la unión, el 16 de septiembre de 2020: *Cada vez que una aplicación o un sitio web nos pide que creemos una nueva identidad digital o que nos conectemos fácilmente a través de una gran plataforma, en realidad no tenemos ni idea de lo que sucede con nuestros datos. Por este motivo, la Comisión propondrá una identidad electrónica europea segura. Una identidad en la que confiemos y que todo ciudadano pueda utilizar en cualquier lugar de Europa para cualquier tipo de operación, desde el pago de sus impuestos hasta el alquiler de una bicicleta. Una*

tecnología que nos permita controlar qué datos se utilizan y cómo.[46] *El propósito de la UE resulta ambicioso y utópico, pero se comparte la visión de generar el uso de las plataformas digitales de manera segura y reducir el riesgo al cual los usuarios de las TICS se exponen diariamente.*

Entre los documentos aprobados por la UE se encuentra la Carta de los Derechos Fundamentales de la Unión Europea, la cual expresamente dispone el derecho a la protección de datos y su tratamiento para fines concretos. También, se encuentra vigente el reglamento general de protección de datos, asimismo se creó el Comité Europeo de Protección de Datos, entre otros cargos creados para garantizar el respeto y tratamiento de la información de los usuarios de las TICS[47].

2.2.1 Declaración de la Naciones Unidas sobre la Utilización del progreso Científico y Tecnológico en Interés de la Paz y en Beneficio de la Humanidad.

En nuestra región, la preocupación derivada de los riesgos que implica el uso de las tecnologías de la información y comunicación en la actividad económica y social en todos los países y particularmente en El Salvador, ha merecido la consideración expresa de la comunidad internacional que al mismo tiempo de reconocer sus virtudes y potencialidades, advierte sus riesgos, así lo señala la ***"Declaración de las Naciones Unidas sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la***

[46] Consultado en Web oficial de la UE, el 17/09/2022 en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es#documents

[47] Consultado en Web oficial de la UE, el 16/09/2022 en https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es#legislacin

humanidad" (Proclamada por la Asamblea General de la Organización de las Nacionales Unidas a través de la Resolución 3384 del 10 de noviembre de 1975)[48].

En los considerandos de la declaración destaca el progreso científico tecnológico como uno de los factores más importantes del desarrollo de la sociedad humana y también lo enfatiza como una oportunidad de mejorar las condiciones de vida de los pueblos. Uno de los puntos importantes es que en dicha declaración se expone que la ciencia y la tecnología como uno de los medios para acelerar el desarrollo económico de los países en desarrollo.

Es comprensible que los conceptos vertidos en la *Declaración de las Naciones Unidas sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad,* no sean más precisos o vinculados con las TICS, puesto que fue promulgada en el año 1975, por lo que aún no se registraban los avances tecnológicos de la actualidad y tampoco los problemas aparejados con esta, vinculadas con la criminalidad o cibercrimen. No obstante, ello, los nueve puntos que componen la declaración continúan teniendo vigencia en la actualidad, precisamente por esa naturaleza general del discurso que contiene el documento.

En resumidas cuentas, el espíritu de la declaración, es que los Estados miembros velen porque el desarrollo de la ciencia y la tecnología sirvan de instrumento para asegurar al ser humano el goce de sus derechos y garantías, de carácter social y económico, no a la inversa. Aún cuando no se menciona expresamente la protección de datos, ni el derecho a una identidad digital, se debe comprender que el manejo de las nuevas tecnologías de la información

[48] Consultado en Naciones Unidas, Derechos Humanos, oficina del Alto Comisionado, el día 17/09/2022 en: https://www.ohchr.org/es/instruments-mechanisms/instruments/declaration-use-scientific-and-technological-progress-interests

debe ejercerse con completo respeto de los derechos humanos y libertades fundamentales de los pueblos.

2.2.2. Convenio Sobre la Ciberdelincuencia. Convenio de Budapest.

El Convenio de Budapest es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos, cuyo objetivo es establecer una legislación penal y procedimientos comunes entre sus Estados Partes.

Está considerado como un referente obligado en los esfuerzos de la Comunidad Internacional para fortalecer el Estado de Derecho en el ciberespacio.

El Convenio sobre Ciberdelincuencia es un acuerdo internacional destinado a combatir los ciberdelitos, o los delitos cometidos por medio de Internet. Busca establecer una legislación penal y procedimiento que fue aprobado durante la Sesión N°109 del Comité de Ministros del Consejo de Europa, celebrada el 8 de noviembre de 2001, se adoptó el Convenio sobre Ciberdelincuencia, el que fue presentado para su firma en la ciudad de Budapest, con fecha 23 de noviembre de 2001, entrando en vigencia el 1 de julio de 2004.

Actualmente, el Convenio de Budapest tiene 63 países firmantes de los cuales República Dominicana, Panamá y Costa Rica son los únicos de la región centroamericana en ratificar el mismo. Guatemala, El Salvador y Honduras se encuentran en proceso de firma y adecuación de sus legislaciones. El poco o muy poco compromiso de los centroamericanos quedó demostrado en el Informe Global de Ciberseguridad, en el cual solamente Panamá fue calificado como un país con un compromiso mediano, mientras que los demás fueron categorizados como países poco comprometidos.

En el contexto de ese proceso de adhesión que no ha concluido aún, El Salvador puso en vigencia muchos de los postulados en el Convenio de Budapest en la promulgación Ley Especial Contra Delitos Informáticos y Conexos aprobada el 26 de febrero de 2016 mediante el Decreto Legislativo No. 260, publicado en el Diario Oficial No. 40 Tomo No. 410, de la misma fecha; la cual sistematiza los tipos penales relacionados con la ciberdelincuencia, generando en los operadores de justicia nuevos desafíos para su aplicación y sanción penal, por cuanto la referida normativa se encuentra relacionada con la utilización de tecnologías de la información y comunicación; de tal manera que la investigación, procesamiento y juzgamiento, están condicionadas a la aplicación de actividades técnicas y periciales de carácter informáticos en respuesta al hecho de que en la actualidad, los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país; por lo que se vuelve la intervención del Estado.

Entre los considerandos del convenio se subraya el carácter prioritario para crear una política penal que proteja a la sociedad de la ciberdelincuencia, así como la adopción de legislación adecuada y mejora de la cooperación internacional[49]. Dichos aspectos resultan claves al momento de combatir la ciberdelincuencia o la delincuencia vinculada con la TICS, puesto que no basta únicamente con contar con las disposiciones legales idóneas, si no, con procedimientos de cooperación mas efectivos y expeditos, ya que en la mayoría de casos la ciberdelincuencia o cibercrimen es criminalidad transnacional.

[49] Convenio sobre la Ciberdelincuencia, consultado en versión digital el 17 de septiembre de 2022 en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

A pesar de ello, El Salvador no retomó ninguna de las disposiciones encaminadas a fortalecer la cooperación internacional a través de la Ley Especial Contra Delitos Informáticos. Ello resulta desafortunado, porque en la mayoría de los casos (podría asegurarse incluso que en todos los casos), el cibercrimen tiene como característica su naturaleza transnacional, ya que al instrumentalizar las plataformas digitales, redes sociales, correos electrónicos, etc.; obligatoriamente, al momento de investigar un hecho delictivo, la Policía Nacional Civil o la misma Fiscalía General de República, deberá realizar peticiones a entidades extranjeras, quienes resguarden servidores en donde yace la información requerida para individualizar a los autores de los hechos que se investiguen. Claro es, que aún sin haberse retomado dichas disposiciones las peticiones en el marco de investigaciones policiales se realizan, pero, queda sometido tal acto investigativo a un procedimiento que puede tardar varios meses y en la mayoría la información llega tarde, haciendo el cibercrimen más atractivo para el delincuente dotado de competencias técnicas.

Asimismo, El Salvador obvió una gran cantidad de disposiciones relacionadas con infracciones de la propiedad intelectual y de los derechos afines, así como, muchas otras disposiciones contenidas en la Convención. Así observamos que El Salvador, escogió solamente algunas disposiciones y aun creó otras conductas típicas a través de la última reforma de la ley. Esto anterior, se puede interpretar, por un lado, como tomar aquellas conductas sobre las cuales también el país ya percibía la necesidad de una regulación, en virtud que se suscitaban hechos delictivos bajo las modalidades o formas delictivas descritas en la ley. Aún la reforma más reciente de la ley especial contra delitos informáticos del año 2021, incluyó elementos especiales propios de la realidad

nacional, como la implementación del Bitcoin como moneda de curso legal, así como el acceso indebido o vulneración de sistemas informáticos del Estado.

Eduardo Ferreyra, analista de políticas públicas del Área Digital de la Asociación por los Derechos Civiles (ADC), expone algunas críticas a la convención de Cibercrimen. Principalmente, señalando que algunos países latinoamericanos decidieron no adherirse al Convenio, bajo el argumento de que no habían participado en la discusión y redacción del mismo. Uno de los países en sostener dicho argumento fue Brasil. Asimismo, hace una breve reflexión sobre la redacción de las conductas propuestas a través del convenio, las cuales califica como ambiguas y que, por tal motivo, dejaría un margen extremadamente amplio para la vulneración de derechos fundamentales de la población, ya que subraya la tradición de irrespeto por los derechos y garantías de las personas en América Latina[50].

Ciertamente la crítica realizada al convenio es válida, sin embargo, no debe omitirse que el Convenio de Budapest, debería de retomarse como una especie de guía al momento de redactar leyes que sanciones el cibercrimen o ciberdelincuencia, por lo que su utilidad debe encaminarse a la adecuación de la norma con la realidad de cada país. Que en el caso de El Salvador debe agotarse el proceso de formación de la ley que engloba etapas diseñadas para que el contenido de las mismas pueda discutirse, observarse, volver a redactar si esto fuese necesario, para establecer normativa idónea para el país y su realidad criminal.

[50] Ferreyra, Eduardo. La Convención de Cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas. Consultada en versión digital, el 18/09/2022, en https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf

2.3. Disposiciones de derechos comparado relacionadas con la protección de la Identidad Digital y Protección de Datos.

Actualmente, nuestra región se encuentra realizando esfuerzos en relación a la adopción de normativa relacionada con la ciberdelincuencia. Se hará una breve referencia a los casos más cercanos:

Guatemala:

Guatemala no cuenta con una ley especial de ciberdelincuencia, protección de datos o de reconocimiento legal del derecho a la identidad digital como tal. Sin embargo, el Código Penal Guatemalteco, en el capítulo VII, *DE LOS DELITOS CONTRA EL DERECHO DE AUTOR, PROPIEDAD INDUSTRIAL Y DELITOS INFORMÁTICOS.* Contiene algunos tipos penales relacionados, entre los cuales se encuentran, en el art. 274-A Destrucción de Registros informáticos, 274-B Alteración de Programas, 274-C Reproducción de instrucciones o programas de computación, 274-D Registros Prohibidos, 274-E Manipulación de Información, 274-F Uso de Información, 274-G Programas destructivos[51]. Las penas oscilan entre los seis meses a cinco años de prisión y multas. Se maneja también el concepto de datos y mayoritariamente hace alusión a "registros informáticos". También la redacción de dichos artículos es limitada a hacer referencia expresa a computadoras o programas de computación, lo cual establece una limitante frente al uso de otros dispositivos que actualmente son utilizados por gran parte de la población.

[51] Decreto Número 17-73. Código Penal de la República de Guatemala, consultado en versión digital el día 18 de sep. de 22 en : https://tse.org.gt/images/UECFFPP/leyes/Codigo_Penal.pdf

Cabe relacionar que el congreso guatemalteco, el 04 de agosto de 2022 emitió el decreto 39-2022, que contenía la Ley de Prevención y Protección conta la Ciberdelincuencia. Recientemente se informó que dicho decreto sería archivado atendiendo algunas críticas de expertos que consideraron que la ley vulneraba la libertad de expresión y podría callar críticas contra funcionarios políticos[52].

Honduras:

En cuanto a la experiencia hondureña, cuentan con la Ley de Estrategia de Ciberseguridad nacional de Prevención de Campaña de Odio u Discriminación en Redes Sociales. Sin embargo, su aplicación se limita según su nombre lo anuncia al uso de las redes sociales. Actualmente no cuenta con una ley de protección de datos personales. En el año 2015, se dio una iniciativa de ley para la protección de datos personales y fue presentada al Congreso. Se buscaba crear protecciones en sintonía con la cooperación de la Agencia Española de Cooperación Internacional para el Desarrollo, sin embargo, esta no dio frutos.[53]

Por medio del decreto 130-2017, se emite el Código Penal de Honduras. En el *"título XXII, Seguridad de las Redes y de los Sistemas informáticos"*, dicho título contiene los artículos 398 Acceso no Autorizado a Sistemas Informáticos, 399 Daños a Datos y Sistemas Informáticos, 400 Abuso de dispositivos, 401 Suplantación de Identidad, 402 Circunstancias Agravantes y 403

[52] Román, Julio. Congreso oficializa que se archiva el decreto 39-2022 que contenía la Ley contra la ciberdelincuencia. Prensa Libre, consultada en versión digital el día 18 de sep. de 22, en https://www.prensalibre.com/guatemala/politica/congreso-oficializa-que-se-archiva-el-decreto-39-2022-que-contenia-la-ley-contra-la-ciberdelincuencia-breaking/

[53] IPANDETEC. Paso a paso para una política de Ciberseguridad Integral HONDURAS. Consultada en versión digital el día 18 de sep. de 22 en: https://www.ipandetec.org/wp-content/uploads/2021/06/HONDURAS.pdf

Responsabilidad de las Personas Jurídicas[54]. Las disposiciones vinculadas con el cibercrimen son limitadas y puede advertirse que las penas a imponer son bajas. También, algunos tipos penales como las amenazas, contempla una agravante cuando el delito se cometa utilizando medios informáticos. Por lo anterior, la necesidad de adecuar la normativa a la realidad del accionar delincuencial a través de las TIC´S, es latente.

Costa Rica:

Recientemente el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones **(Micitt) de Costa Rica anunció la creación de una Estrategia Nacional de Ciberseguridad** (ENC). Ello en respuesta a algunos acontecimientos vinculados con hackeos realizados a sistemas informáticos propios del Estado.

De acuerdo al Índice Global de Ciberseguridad 2020 de la Unión Internacional de Telecomunicaciones (ITU), el cual ubica a Costa Rica como sexto en América Latina y el setenta y seis a escala global, es decir, que escaló 39 puestos. El índice mide el nivel de compromiso de cada país con la Agenda de Ciberseguridad Global de la ITU, y evalúa los pilares: medidas legales, medidas técnicas, medidas organizativas, desarrollo de capacidades y cooperación.[55]

---

[54] Código Penal de Honduras, emitido mediante decreto N° 130-2017, consultado en versión digital el 18 de sep. de 22, en https://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/CodigoPenalNo.130-2017(actualizadojulio2020).pdf

[55] Garza, Jeffry. Costa Rica escaló 39 puestos en Índice Global de Ciberseguridad. DPL News. Consultado en versión digital el 18 de sep. de 22 , en: https://dplnews.com/costa-rica-escalo-39-puestos-en-indice-global-de-ciberseguridad/

Mejores países en ciberseguridad (Puntuación)

- 1. Estados Unidos (100)
- 2. Reino Unido y Arabia Saudita (99,5)
- 3. Estonia (99,4)
- 4. Corea del Sur, Singapur y España (98,5)
- 5. Rusia (98,0)
- **76. Costa Rica (67,4)**

Mejores países latinos en ciberseguridad (Puntuación)

- 1. Brasil (96,6)
- 2. México (81,6)
- 3. Uruguay (75,1)
- 4. República Dominicana (75,0)
- 5. Chile (68,8)
- **6. Costa Rica (67,4)**[56]

El presidente de la República de Costa Rica, la ministra de la Presidencia y la Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones, el día 21 de abril de 2022 emitieron la directriz N° 133-MP-MICITT, la cual está dirigida a la administración pública central y descentralizada sobre las mejoras en materia de ciberseguridad para el sector público del Estado. Dicha directriz busca realizar una laborar preventiva frente a las amenazas que representa el uso de las TICS, las cuales podrían trascender en materia penal.[57] Asimismo, se crea el protocolo Ciberseguridad MICITT-ICE-CNE, como Decreto Nº 37052-MICITC, asimismo se habilitó un Centro de Respuesta de incidentes de

[56] Jeffry Garza, Ob. Cit.
[57] DIRECTRIZ N° 133-MP-MICIT, consultada en versión digital el 18 de septiembre de 2022 https://www.micitt.go.cr/wp-content/uploads/2022/05/DIRECTRIZ-N%C2%B0-133-marca-de-hora.pdf

Seguridad Informática CSIRT-CR y confeccionó la Estrategia Nacional de Ciberseguridad (2017-2021)[58]

Evidentemente la labor de combate al cibercrimen que desarrollan las autoridades costarricenses consiste en tomar medidas concretas para generar un control en el uso y manejo de la tecnología. Se advierte una labor preventiva y educativa, aunque, también han sufrido grandes ataques a la seguridad en cuanto al manejo de datos.

En cuanto a disposiciones penales, el Código Penal de Costa Rica, establece en el artículo 196 bis Violación de datos personales, 217 bis Estafa Informática, 229 bis Daño informático, 229 Ter. Sabotaje Informático, 230 Suplantación de identidad, 231 Espionaje Informático, 233 Suplantación de página electrónicas, 234 Facilitación del delito Informático, 236 Difusión de Información Falsa.[59]

[58] Sitio Web oficial Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones consultado el día 18 de sep. de 22, en https://www.micitt.go.cr/ciberseguridad/
[59] Código Penal de Costa Rica. Ley 4.573, actualizado al 30 de junio del año 2019, consultada en versión digital el día 18 de sep. de 22 en https://defensapublica.poder-judicial.go.cr/media/attachments/2020/11/23/codigopenal2019.pdf

CAPITULO III: ANÁLISIS CRÍTICO SOBRE LOS ATAQUES A LA IDENTIDAD DIGITAL EN EL SALVADOR DESDE LA PERSPECTIVA DEL DERECHO PENAL ECONÓMICO.

SUMARIO: 3.1. El problema sobre la sustracción de datos y utilización de identidad digital para la comisión de hechos delictivos en El Salvador.3.2. Análisis sobre el estado actual de la seguridad Informática en El Salvador y su impacto en el orden socioeconómico. (Factores de Riesgo). 3.3. Identificación de los obstáculos en la investigación de delitos vinculados con la identidad digital cometidos por medio de las TIC´S, en El Salvador. 3.4. Análisis de la delincuencia informática que se comete a través del internet desde la perspectiva del Derecho Penal Económico.

RESUMEN:

El contenido que se presenta a través del siguiente capítulo, bien puede ser sinónimo de un diagnóstico sobre la situación de actual de la problemática que envuelve la sustracción de datos, entre los cuales se encuentran aquellos que componen la identidad digital. Se van matizando casos concretos sobre ataques a la ciberseguridad de relevancia social, por la inclusión de instituciones estatales, las cuales captan información, datos e identidades digitales, y aunque se trata de un apoderamiento de un elemento inmaterial e intangible, tiene la aptitud para generar graves consecuencias nocivas a sectores de la población concretos, tales como usuarios de las TIC´S y consumidores de bienes y servicios; el denominador común identificado es ese estado de impunidad. Asimismo, para referirse al estado actual de la seguridad informática en El Salvador, se presenta información concreta en relación con los casos denunciados y casos resueltos por el delito de hurto de identidad, lo que expone una evidente situación de ineficacia en la resolución de casos, incluso en un plano jurisdiccional por la falta de criterios dogmáticos

relacionados con el tipo delictivo. Ese estado de ineficacia deviene de complejidad que se presenta en las investigaciones relacionadas con el cibercrimen, debido al eterno problema de la insuficiencia del recurso humano y el problema del carácter transnacional de la cibercriminalidad, por lo que se describen dichos obstáculos. Se cierra con algunas consideraciones esenciales a través de las cuales se fundamenta la naturaleza de la situación problemática identificada como parte de los fenómenos que incluye envuelve el derecho penal económico, así como el fundamento constitucional a través del estudio del surgimiento del concepto de Constitución Económica, según construcciones jurisprudenciales citadas.

3.1 El problema sobre la sustracción de datos y utilización de identidad digital para la comisión de hechos delictivos en El Salvador.

En El Salvador la situación de criminalidad ha sido el mayor problema a combatir durante las últimas tres décadas, pues se encuentra relacionada mayoritariamente con delitos violentos. Así, se ha vuelto frecuente encontrar en medios de comunicación información noticiosa relacionada con homicidios, robos, extorsiones, privaciones de libertad, desapariciones de personas, entre otros tipos delictivos que atentan directamente contra derechos individuales de la población y que acaparan la atención no solamente de los medios de comunicación, sino del gobierno y las entidades encargadas de combatir el fenómeno.

Es razonable que la comisión de hechos delictivos violetos genere un impacto y reacción en diversos ámbitos: social, político, en el desarrollo económico y legislativo. Asimismo, los hechos delictivos violentos pueden influir en la

percepción que se tiene de hechos delictivos de diferente naturaleza, tales como los delitos relacionados con las TIC´S, puesto que aun cuando se trata de delitos totalmente distintos, sin lugar a comparación, en muchas ocasiones la opinión pública percibe que los delitos informáticos no son tan graves como un homicidio, una extorsión, etc., y que los usuarios de las TIC´S, se han ubicado voluntariamente en un posición de vulnerabilidad al utilizar dichos medios. Sin embargo, la experiencia ha comprobado que no es necesario ser un usuario directo de las TIC´S, para resultar afectado por un hecho que involucre la sustracción de datos personales, ya que, tanto las instituciones financieras, empresas que prestan servicios, así como las entidades estatales, captan recursos y datos, por lo que es importante prestar atención al tratamiento y protección de los mismos.

Recientemente, en El Salvador, se suscitaron acontecimientos notorios relacionados con la sustracción de datos en una proporción masiva, que generaron impacto en diferentes instituciones del Estado, que sufrieron vulneraciones de sistemas informáticos. Así la Policía Nacional Civil, sufrió un hackeo, producto del cual los datos de casi treinta mil policías fueron divulgados a través de redes sociales. Entre los datos divulgados se encuentran los nombres, números de identificación, lugar donde se encontraban destacados y números telefónicos[60]. Ante semejante exposición, la respuesta de muchos elementos policiales fue presentar la denuncia ante las autoridades correspondiente, sin embargo, no se ha conocido sobre los resultados de las investigaciones iniciadas ya hace un año aproximadamente. Por tanto, el hecho actualmente continúa en la impunidad.

---

[60] Bernal, David. Hackeo de web de la PNC pone en peligro datos de policías. Artículo publicado el 09 de septiembre de 2021, consultado el 08/10/2022 en: https://www.laprensagrafica.com/elsalvador/Hackeo-de-web-de-la-PNC-pone-en-peligro-datos-de-policias-20210909-0059.html

En el mes de agosto de 2021, el Ministerio de Hacienda a través de su cuenta oficial de Twitter, difundió un comunicado a través del cual alertan sobre estafas realizadas por personas que se identificaban como empleados del ministerio de hacienda, quienes solicitaban formalizar trámites realizados a través de la web por los usuarios o contribuyentes. Así, realizaron aclaraciones sobre las cuentas oficiales de la institución[61]. Para la consumación de estos hechos delictivos, los delincuentes accedieron a datos relacionados con las víctimas con perfiles idóneos para consumar los hechos, tampoco existe claridad ni pronunciamiento formal de las autoridades en cuanto a las investigaciones.

En el mes de septiembre de 2021, el Banco Agrícola reportó incremento de denuncias por casos de fraude, por lo cual habrían reforzado las medidas de seguridad. Informaron que el equipo de ciberseguridad había desmontado alrededor de mil trecientos sitios web que se dedicaban a diversas modalidades de estafa.[62] Sobre estos hechos debe precisarse que, para consumar el delito de estafa informática o Hurto por Medios Informáticos, fue necesario acceder a base de datos para alcanzar a los usuarios de la entidad bancaria que además hicieran uso de las plataformas virtual para el manejo de cuentas de débito y crédito. Esto puede afirmarse, ya que algunos de los usuarios fueron víctimas de delitos como hurto por medios informáticos, aún cuando no proporcionaron información relacionada con usuarios y

---

[61] Consultado el 08/10/2022 en: https://twitter.com/HaciendaSV/status/1431632671981981700?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1431632671981981700%7Ctwgr%5Ec993c282f3a104e714ce94c242826d0b8e8c2f64%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fquepasasv.com%2Fministerio-de-hacienda-alerta-a-los-salvadorenos-ante-estafas%2F

[62] Pastrán, Rosa María. Banco Agrícola alerta a clientes ante alza de denuncias por fraude. Artículo publicado el 07 de septiembre de 2021. Consultado el 08/10/2021 en https://www.eleconomista.net/economia/Banco-Agricola-alerta-a-clientes-ante-alza-de-denuncias-por-fraude-20210907-0005.html

contraseñas por ningún medio electrónico diferente a las plataformas formalmente habilitadas[63]. La modalidad utilizada sería el acceso a los datos, previo envío de un correo electrónico a las cuentas de los usuarios, aun cuando estos no proporcionaran otra información o datos sensibles. Posterior a los eventos mencionados la institución financiera desplegó esfuerzos para educar a los usuarios sobre no proporcionar información como contraseñas y usuarios de sus respectivas cuentas (aunque esta no fue la única modalidad utilizada para la consumación de los delitos), e hicieron hincapié en que los sistemas de la entidad financiera no fueron vulnerados[64]. Sin embargo, tales campañas no respondieron interrogantes sobre cómo los delincuentes informáticos accedieron a las cuentas de correos electrónicos utilizadas por los titulares de las cuentas bancarias. La mayoría de estos hechos delictivos continúan en la impunidad.

No obstante, lo anterior, la Fiscalía General de la República, durante el año 2022, a través de su sitio oficial difundió la emisión de ordenes administrativas de capturas por los delitos de estafas informáticas y hurto por medio informáticos.[65]

En los primeros días del mes de octubre de 2022, medios nacionales e internacionales, reportaron las denuncias masivas relacionadas con hurto de identidad para la activación y acceso a cuentas de la aplicación "*Chivo Wallet",* puesto que para activar una cuenta es preciso ingresar datos personales, tales como nombre, número de teléfono, número de documento único de identidad

---

[63] Denuncia presentada en Fiscalía General de la República de referencia 02564-UDPP-2021-SS, delito de Hurto por medios Informáticos, denunciante Damaris Saraí Martínez Alberto.
[64] Sitio oficial Bancoagrícola, consultado el 08/10/2022 en: https://www.bancoagricola.com/financiera-mente
[65] Sitio web Fiscalía General de la República. Estafadores Informáticos son capturados por orden de la Fiscalía. Noticia publicada 25 de marzo de 2022. Consultado el 08/10/2022 en: https://www.fiscalia.gob.sv/estafadores-informaticos-son-capturados-por-orden-de-la-fiscalia/

y fecha de nacimiento. Los denunciantes manifestaban que sus datos habían sido utilizados aun cuando no habían descargado la aplicación[66]. No ha existido un pronunciamiento formal de parte de las autoridades en cuanto a cómo se obtuvieron los datos personales de las víctimas.

En el mes de octubre de 2021, a través de medios masivos de comunicación, el Instituto Salvadoreño del Seguro Social, mediante un comunicado realizado a través de redes sociales informó sobre dificultades técnicas en sus servidores y sistemas informáticos, haciendo ver que el equipo técnico de dicha entidad identificó indicios de que la institución fue blanco de un ataque informático, por lo que se habían realizado coordinaciones para que las autoridades correspondientes investigaran el hecho. Los inconvenientes experimentados fueron en relación con verificaciones de citas de usuarios, obtención de incapacidades y gestiones de medicamentos. Sobre este caso, tampoco se obtuvo información sobre los resultados de las investigaciones realizadas por la Policía Nacional Civil y la Fiscalía General de la República, por tanto, se trata de otro hecho en estado de impunidad.[67]

A raíz de estos acontecimientos, se reformó la Ley Especial contra Delitos Informáticos, en el mes de diciembre de 2021, en cuanto al delito de daños a sistemas informáticos (art.7 L.E.C.D.I), Posesión y uso de equipos o prestación de servicios para la vulneración de la seguridad (art.8 L.E.C.D.I), Estafa informática (art.10 L.E.C.D.I), Obtención y divulgación No autorizada (art.23 L.E.C.D.I), Fraude Informático (art.11 L.E.C.D.I). Se tipifica el delito de

---

[66] Del Cid, Merlín. Policía Salvadoreña investiga suplantación de identidades para robar bono de US$30 en bitcoin. Artículo publicado el 07 de octubre de 2021, consultado en CNN Latinoamérica el 08/10/2022: https://cnnespanol.cnn.com/2021/10/07/policia-salvadorena-investiga-suplantacion-de-identidades-para-robar-bono-de-us-30-en-bitcoin-orix/

[67] López Vides, Carlos. ISSS informa suspensión temporal de trámites por supuesto ataque informático. Artículo publicado el 19 de octubre de 2021, consultado el 08/10/2022 en: https://www.elsalvador.com/noticias/nacional/isss-ataques-ciberneticos/891436/2021/

Falsedad de Documentos y Firmas (ar. 11-A L.E.C.D.I), entre otros tipos. Entre las reformas, se incluyeron las transacciones en Bitcoin u otras criptomonedas. También se adicionó el capítulo III, “Delitos Informáticos Relacionados con el contenido de los Datos”[68].

Por medio del Decreto Legislativo N° 280, de fecha 01 de febrero de 2022, el cual fue publicado en el Diario Oficial N° 45, Tomo 434, en fecha 04 de marzo de 2022, la asamblea legislativa aprobó reformas al Código Procesal Penal, las cuales calificó como indispensables para actualizar el marco normativo que regula la incorporación de evidencia digital. Así, a través de los considerandos se anuncian modificaciones necesarias para adecuar la norma a los estándares internacionales para facilitar la detección, investigación y sanción de delitos informáticos[69] .

Las disposiciones adicionadas a través del Decreto Legislativo N°280, fueron los artículos 259-A de la evidencia digital, art. 259-B Registro de cadena de custodia, 259-C Incorporación y producción de la Evidencia digital en el proceso penal, 259-D Agente Encubierto Digital y otras técnicas de investigación informática y 259-E Medidas Cautelares.

Las reformas establecidas para el artículo 259 del Código Procesal Penal generaron opiniones diversas en El Salvador, al momento de su aprobación, principalmente porque se criticó la legalización del espionaje a través de la figura del agente encubierto. Sin embargo, no es menos cierto que dicha figura novedosa había sido adoptada por España, desde el año 2015. Su

---

[68] Consultado el 08/10/2022, en: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/D1F13E1E-9860-428F-8703-2B61D5DF1D47.pdf

[69] Consultado el 09/10/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/R/2/2000-2009/2009/01/EE38E.HTML?embedded=true

antecedente en dicho país data desde el 13 de enero de 1999, en *el art. 282 bis en la modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves.*[70] Inicialmente, se estableció el supuesto de su utilización en relación con la criminalidad organizada, así, la figura de agente encubierto autoriza a la autoridad policial para actuar bajo identidad supuesta. Posteriormente, ante el auge de la criminalidad relacionada con las tecnologías de la información y comunicación, se llevó a cabo la reforma procesal por Ley Orgánica 13/2015, de fecha 05 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. De manera esencial, se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, previa autorización judicial. También se regula la figura de agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación y que se permita intercambiar archivos con contenido ilícito.

En cuanto a la experiencia salvadoreña, la figura del agente encubierto se clasifica dentro de los métodos especiales de investigación, comprendido en el art. 5 y 6 de la Ley Contra El Crimen Organizado, denominada como operaciones encubiertas. Esta disposición en conjunto con los Arts. **175** Inc. 4° y **282 letra d**) del Código Procesal Penal, en relación con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la cual identifica estos procedimientos como **Técnicas Especiales de Investigación** en el numeral 1º del Artículo 20º, han servido de fundamento legal para la autorización de agentes encubiertos en las investigaciones de delitos de

[70] Quevedo González, Josefina. “Investigación y prueba del ciberdelito”. Tesis doctoral, Universitat de Barcelona, 2017. Versión PDF, Pág. 272 y siguientes.

narcotráfico, agrupaciones ilícitas, contrabando de mercaderías, tráfico ilegal de personas, secuestros, etcétera.

En ese orden de ideas, y tal como lo regula el art. 259-D del Código Procesal Penal, se requiere una autorización por escrito, emanada por la Fiscalía General de la República, para el empleo de la técnica especializada de agente encubierto digital y otras técnicas de investigación informática. Sin duda, será necesario que el ministerio publico exponga a través de esa autorización escrita, argumentos sobre la necesidad e idoneidad de la aplicación de dicha técnica especializada de investigación, así como las diligencias iniciales de investigación realizadas, fundamentando cómo estas son insuficientes para cumplir con el propósito de la resolución de casos a través de la individualización de los autores de hechos delictivos, siendo necesario aplicar técnicas especializadas como la del agente encubierto digital.

El problema sobre la sustracción de datos en El salvador es de reciente y suma actualidad, el cual ha generado reacciones tales, como reformas recientes al Código Procesal Penal y la Ley Especial Contra delitos Informáticos. Sin embargo, las investigaciones vinculadas con el ciber crimen y la sustracción, vulneración, divulgación de datos, comienzan a incrementarse y a fundamentar ordenes de detenciones administrativas.

3.2 Análisis sobre el estado actual de la seguridad Informática en El Salvador y su impacto en el orden socioeconómico.

La española doctora Patricia Faraldo Cabana, menciona que se reconoce con carácter general que el *Derecho Penal Informático,* es una de las facetas más características del Derecho Penal de la sociedad del riesgo. Así menciona la

naturaleza transnacional de la delincuencia a través de las tecnologías de la información, como uno de los factores que abonan a los riesgos a los cuales se exponen todos los usuarios de las TICS. Otros autores, consideran incluso que todas las relaciones sean comerciales o no, pero sostenidas a través de la web, suceden en la tierra de nadie, aludiendo precisamente a la complejidad de ejercer control y garantizar la seguridad en las relaciones a través de las TIC´S. Aunque sobre ello, ya se han hecho algunas consideraciones previas en este documento.

Debe acotarse, que la comisión de hechos delictivos que significan una sustracción o vulneración de datos, los cuales forman la identidad digital de las personas, se han percibido en El Salvador ya hace algunos años, pero estos no habían sido suficientes para generar un estado de preocupación o alarma, como los eventos en los cuales se vieron envueltas diversas entidades estatales y también privadas en los últimos meses del año 2021.

Al realizar un repaso sobre los ataques percibidos a la seguridad informática en El Salvador durante el año 2021, puede subrayarse que la trascendencia de dichos eventos radica, fundamentalmente en la puesta peligro de intereses colectivos supraindividuales y no únicamente intereses patrimoniales individuales.

En ese aspecto, Muñoz Conde señala que *el orden económico en sentido estricto y orden público económico se debe distinguir claramente del orden socioeconómico.* Así destaca, que el primero se vincula exclusivamente a la actividad del Estado como director e interventor de la economía. Se refiere a la regulación jurídica del intervencionismo estatal de la economía y a la tutela de los intereses patrimoniales individuales; en el segundo (orden

socioeconómico) trasciende su esfera de protección fundamentalmente a los intereses colectivos supraindividuales[71].

De esta manera, cuando el usuario de las TICS y también consumidor de bienes y servicios percibe que no existe seguridad en las transacciones de adquisición y pago de estos, realizadas a través de las tecnologías de la información y comunicación, se deteriora el sector del comercio electrónico y el crecimiento de la economía.

Por comercio electrónico entendemos la celebración de contratos, las negociaciones que los preceden y las actividades complementarias posteriores necesarias para su ejecución, como los pagos electrónicos, que se realizan a través de Internet[72].

La autora española Patricia Faraldo Cabana, menciona diferentes clases de transacciones comerciales que pueden suscitarse por medio de las TICS, en atención a sus intervinientes, así indica que e*n el concepto de comercio electrónico se incluyen cinco tipos distintos de comercio que tiene lugar en el ciberespacio: el comercio B2C ("business-to-consumer"), esto es, entre empresarios y consumidores finales; el comercio B2B ("business-to-business"), entre empresarios; el comercio C2C ("consumer-to-consumer"), entre consumidores a través de una plataforma online; el comercio P2P ("peer-to-peer"), que supone compartir archivos y recursos informáticos a través de*

---

[71] Cervini, Raúl. Derecho penal económico. Perspectiva integrada. Revista de Derecho, Universidad Católica del Uruguay. Versión PDF, Pág. 25, consultada el 09/10/2022, en https://revistas.ucu.edu.uy/index.php/revistadederecho/article/view/838/841

[72] Faraldo Cabana, Patricia. Las Nuevas Tecnologías en los Delitos Contra el Patrimonio y el Orden Socioeconómico. Editorial Tirant Lo Blanch, libro publicado 01/06/2009. Consultado en versión digital el 09/10/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788499855943?showPage=37

la tecnología ad-hoc; y el comercio móvil ("m-commerce"), basado en el uso de tecnología "wireless" para facilitar las transacciones en el ciberespacio. La autora menciona que los tipos más interesantes son el comercio B2C y el comercio C2C, ya que son las formas más vulnerables al fraude o al cibercrimen[73]. En El Salvador, es fácilmente identificables esta clase de comercio a través de la web.

En este orden de ideas, cuando los usuarios de las TICS, quienes también forman parte del comercio electrónico, perciben inseguridad en sus transacciones, así como desconfianza en cuanto a los mecanismos de protección del manejo de sus datos, puede ocasionar una desaceleración en el crecimiento de la economía y el dinamismo de ésta. En este punto se advierte el impacto que se puede generar ya en las relaciones de comercio y no únicamente una vulneración de derechos patrimoniales individuales.

Para efectos de referirnos al estado actual de la seguridad informática en El Salvador, debemos señalar algunos datos estadísticos concretos:

La Fiscalía General de la República, por medio de la resolución de las doce horas con treinta minutos del día dos de marzo de dos mil veinte, en atención a la solicitud de información No 103-UAIP-FGR-2020, de acuerdo a la Ley de Acceso a la Información Pública[74], hizo saber estadísticas en relación a los delitos de estafa informática y el delito de hurto de identidad, desde el año 2016 de la entrada en vigencia de la Ley especial contra delitos informáticos, al año 2019. En este período de tiempo la incidencia de denuncias era

---

[73] Faraldo Cabana, Patricia. Ob. Cit.

[74] Consultado el 09/10/2022 en: https://portaldetransparencia.fgr.gob.sv/documentos/RESOLUCION%20103-UAIP-FGR-2020.docx.

notablemente baja; aun así, predominaron las denuncias por el delito de hurto de identidad sobre las denuncias por el delito de estafa informática y sus modalidades. Lamentablemente, en el periodo de tiempo mencionado, solo se judicializaron dos casos por el delito de hurto de identidad a nivel nacional.

1- **Cantidad de casos ingresados por los delitos de Estafa Informática, art. 10 de la Ley Especial Contra Delitos Informáticos y Conexos, y por el delito de Hurto de Identidad art. 22 de la misma ley, a nivel nacional durante el período de marzo de 2016 a enero de 2019. Detallado por delito**

R//

CANTIDAD DE CASOS INICIADOS POR LOS DELITOS DE ESTAFA INFORMÁTICA (10 L.D. INFORMÁTICOS) Y HURTO DE IDENTIDAD (22 L.D. INFORMÁTICOS), A NIVEL NACIONAL, DEL AÑO 2016 AL 2019; DETALLADO POR AÑO Y DELITO.				
DELITOS	**Año 2016**	**Año 2017**	**Año 2018**	**Año 2019**
Estafa informática (10 L.D. Informáticos)	0	6	7	2
Estafa informática (10 Lit. a. L.D. Informáticos)	1	1	0	0
Estafa informática (10 Lit. c. L.D. Informáticos)	1	0	0	0
Hurto de identidad (22 L.D. Informáticos)	19	45	82	10
Total	**21**	**52**	**89**	**12**

Fuente: Departamento de Estadística, según Base de Datos SIGAP FGR al 25022020

2- **De la cantidad de casos resultantes en el numeral anterior proporcionar la cantidad de casos judicializados por los delitos antes referidos a nivel nacional durante el período de marzo de 2016 y enero 2019 detallado por delito.**

R//

CANTIDAD DE CASOS JUDICIALIZADOS, POR LOS DELITOS DE ESTAFA INFORMÁTICA (10 L.D. INFORMÁTICOS) Y HURTO DE IDENTIDAD (22 L.D. INFORMÁTICOS), A NIVEL NACIONAL, DEL AÑO 2016 AL 2019; DETALLADO POR AÑO Y DELITO.				
DELITOS	**Año 2016**	**Año 2017**	**Año 2018**	**Año 2019**
Estafa informática (10 L.D. Informáticos)	0	0	1	1
Estafa informática (10 Lit. a. L.D. Informáticos)	1	0	0	0
Estafa informática (10 Lit. c. L.D. Informáticos)	0	1	0	0
Hurto de identidad (22 L.D. Informáticos)	0	0	2	0
Total	**1**	**1**	**3**	**1**

Fuente: Departamento de Estadística, según Base de Datos SIGAP FGR al 25022020

La información extraída nos proporciona elementos objetivos para inferir que en aquellos años la incidencia del delito de hurto de identidad era baja, así como su solución a través de procesos penales. Aún y con esto, fue el delito mayormente denunciado, no obstante, lo novedoso de la ley. Sin embargo, las estadísticas en cuanto a las denuncias por delitos informáticos varían en un período reciente. Lo anterior puede deberse a diversos factores: uno puede ser el aumento de hechos delictivos consumados a través de las TICS; y otro

podría ser mayor difusión de información o conocimiento de los usuarios de las TICS, sobre los hechos delictivos establecidos en la Ley Especial Contra Delitos Informáticos, y por consiguiente mayor iniciativa para la presentación de denuncias.

En esa línea de ideas, es relevante mencionar que el día seis de septiembre de dos mil diecinueve, el Tribunal Segundo de Sentencia de San Salvador, en la causa con referencia judicial 160-2019, emitió sentencia condenatoria por el delito de Hurto de Identidad de conformidad al art. 22 de la Ley Especial Contra Delitos Informáticos y Conexos[75]. Del contenido de dicha sentencia se pueden extraer elementos puntuales relacionados con la investigación de delitos informáticos:

- Que la condena se emitió en aplicación del procedimiento abreviado, por lo fue el imputado quien reveló que utilizó un *Software* llamado *ranswer*, para hackear cuentas de Facebook e Instagram, circunstancias que no constaban en la relación circunstanciada de los hechos.
- La individualización del imputado se dio de forma circunstancial, por lo que no se emplearon técnicas especiales, relacionadas con la investigación de delitos informáticos.
- La captura del imputado se dio durante el término de la flagrancia.
- La incautación de hardware relacionado con el hecho delictivo se realiza posteriormente a la etapa de diligencias iniciales de investigación, sin embargo, no se realizaron experticias en la computadora portátil que el

[75] Sentencia Definitiva, en Procedimiento Abreviado, emitida por el Tribunal Segundo de Sentencia de San Salvador, de fecha 06 de septiembre de 2019, consultada el 15/10/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2019/09/DCEA0.PDF

imputado utilizó para cometer el hecho delictivo, por lo que no se extrajo la prueba pericial idónea.

- En la fundamentación del Tribunal de Sentencia, se ubican consideraciones relacionadas con las circunstancias de hecho, más no hay actividad de fundamentación en cuanto a los elementos del tipo de hurto de identidad.

En seguida, se verifica otra información relacionada con el desenvolvimiento del fenómeno de los delitos informáticos, especialmente con el delito de hurto de identidad, siguiendo la línea cronológica. Así, en respuesta a otras peticiones de información, la Fiscalía General de la República, por medio de la resolución de las diez horas del día seis de enero de dos mil veintidós, emitió resolución de entrega de información No 630-UAIP-FGR-2021, de acuerdo a la Ley de Acceso a la Información Pública, en relación a la cantidad de casos ingresados por los delitos regulados en la Ley Especial Contra Delitos Informáticos y Conexos en los meses de octubre, noviembre y diciembre del año 2021[76].

En relación al período de tiempo de la información solicitada, este se redujo considerablemente, solo a tres meses, sin embargo se incluyeron dieciocho tipos delictivos establecidos en la Ley Especial Contra Delitos Informáticos y Conexos. Notablemente, la presentación de denuncias fue más variada, predominando cuatro tipos delictivos con mayores denuncias presentadas. El único delito que superó en casos ingresados al delito de hurto de identidad fue el delito de Hurto por Medios Informáticos (art.13 LDI), con un total de 445 denuncias de octubre a diciembre de 2021. Posteriormente, se sitúa el delito

[76] Consultado en versión PDF el 09/10/2022 en: https://portaldetransparencia.fgr.gob.sv/documentos/Resoluci%C3%B3n%20630-UAIP-FGR-2021.pdf.

de Hurto de Identidad (art.22 LDI), con un total de 288 denuncias en el mismo período de tiempo y como tercer peldaño se ubicó el delito de Estafa Informática art.10 LDI. Esto sin precisar, aquellos casos en los cuales se instrumentaliza el delito de hurto de identidad para la consumación de otros hechos delictivos. De manera más detallada, se expuso la siguiente información:

CANTIDAD DE CASOS INGRESADOS POR LOS DELITOS REGULADOS EN LA LEY ESPECIAL CONTRA DELITOS INFORMATICOS Y CONEXOS.

Cantidad total de casos ingresados, por todos los delitos regulados en la Ley Especial Contra Delitos Informáticos y Conexos , regulados en los artículos desde el 4 hasta el 32 de la LECDIC y art. 34 de la LECDIC, a nivel nacional del período comprendido desde el 22 de octubre al 08 de diciembre del 2021; desagregado por: Delito y mes del hecho

Delitos	Año 2021			
	Octubre	Noviembre	Diciembre	Total
Acceso Indebido a Sistemas Informáticos (Art. 4 L.D. Informáticos)	0	0	1	1
Acceso Indebido a los Programas o Datos Informáticos (Art. 5 L.D. Informáticos)	1	1	1	3
Estafa Informática (Art. 10 L.D. Informáticos)	17	33	9	59
Estafa Informática (Art. 10 Lit. A. L.D. Informáticos)	3	0	1	4
Fraude Informático (Art. 11 L.D. Informáticos)	6	10	4	20
Hurto por Medios Informáticos (Art. 13 L.D. Informáticos)	128	276	41	445
Obtención Indebida de Bienes o Servicios por Medio de Tarjetas Inteligentes o Medios Similares (Art. 17 L.D. Informáti	0	1	1	2
Alteración, Daño a la Integridad o Disponibilidad de los Datos (Art. 19 L.D. Informáticos)	0	1	1	2
Interferencia de Datos (Art. 20 L.D. Informáticos)	0	1	0	1
Hurto de Identidad (Art. 22 L.D. Informáticos)	100	172	16	288
Divulgación no Autorizada (Art. 23 L.D. Informáticos)	4	10	1	15
Utilización de datos Personales (Art. 24 L.D. Informáticos)	11	33	4	48
Obtención y Transferencia de Información de Carácter Confidencial (Art. 25 L.D. Informáticos)	2	9	1	12
Revelación Indebida de Datos o Información de Carácter Personal (Art. 26 L.D. Informáticos)	4	25	7	36
Acoso a través de TIC (Art. 27 L.D. Informáticos)	0	5	2	7
Pornografía a través de TIC (Art. 28 L.D. Informáticos)	0	1	0	1
Corrupción de NNA o Personas con Discapacidad a través del uso de las TIC (Art. 31 L.D. Informáticos)	0	2	0	2
Acoso a NNA o Personas con Discapacidad a través del uso de las TIC (Art. 32 L.D. Informáticos)	0	1	1	2
Total	**276**	**581**	**91**	**948**

Fuente: Departamento de Estadística-DATI, según registros de la Base de Datos de SIGAP a la fecha 04/01/2022.

Sobre la información proporcionada, se hizo la consulta en cuanto a los casos puestos en conocimiento de la autoridad judicial competente. Ante ello, razonablemente, se incluyó una aclaración en la resolución citada, en el sentido que, debido al poco tiempo transcurrido entre la presentación de las

denuncias y la fecha en la cual se rinde el informe, probablemente dichos números no se encuentren apegados a la realidad, ya que los casos resueltos podrían aumentar, debido a que las diligencias iniciales de investigación eran de reciente apertura. Por lo que en ese punto se hizo saber:

RESPECTO DE LOS DATOS DEL PUNTO ANTERIOR (LOS AVISOS Y DENUNCIAS RECIBIDAS), LOS DATOS ESTADÍSTICOS DE LOS CASOS QUE FUERON JUDICIALIZADOS POR LA FISCALÍA GENERAL DE LA REPÚBLICA POR LA COMISIÓN DE LOS DELITOS CONTEMPLADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS.

Cantidad de casos judicializados, por todos los delitos regulados en la Ley Especial Contra Delitos Informáticos y Conexos, regulados en los artículos desde el 4 hasta el 32 de la LECDIC y art. 34 de la LECDIC, a nivel nacional del período comprendido desde desde 22 de octubre al 08 de diciembre del 2021; desagregado por: Delito y mes de la judicialización			
Delito	Año 2021		
	Noviembre	Diciembre	Total
Hurto por Medios Informáticos (Art. 13 L.D. Informáticos)	0	1	1
Pornografía a través de TIC (Art. 28 L.D. Informáticos)	1	0	1
Corrupción de NNA o Personas con Discapacidad a través del uso de las TIC (Art. 31 L.D. Informáticos)	1	0	1
Total	**2**	**1**	**3**

Fuente: Departamento de Estadística-DATI, según registros de la Base de Datos de SIGAP a la fecha 04/01/2022.
La información es producto de la cantidad de casos ingresados en el periodo solicitado.
Nota: En virtud de los plazos del proceso penal, es muy prematuro registrar a la fecha casos judicializados como lo solicita.

Los datos estadísticos proporcionados en relación al procesamiento judicial de hechos delictivos comprendido en la Ley Especial Contra Delitos Informáticos y Conexos, especialmente en relación al delito de hurto de identidad, brindan elementos importantes para inferir que la situación actual de la seguridad informática en El Salvador se encuentra en una etapa de desarrollo y definitivamente dirigida hacia su fortalecimiento. Las instituciones involucradas en garantizarla también se enfrentan con un desafío importante en cuanto al despliegue de la actividad investigativa. Aun así, su impacto en el orden socioeconómico, también ha sido reciente, pero ha sido esto último que ha dado paso a la actualización de la norma en El Salvador. Lo anterior, encuentra sentido ya que al entender al orden socioeconómico como un bien jurídico

supraindividual, el cual debe ser tutelado en un estadio de peligro, ya sea peligro abstracto o concreto[77] en virtud de su trascendencia para el equilibrio de las relaciones en el mercado.

Los bienes jurídicos supraindividuales, también son denominados doctrinariamente como *bienes colectivos, comunitarios, generales, universales, sociales, intereses difusos o intereses generales*[78], siendo el orden socioeconómico parte de estos. Según diferentes autores, esta clase de bienes jurídicos pertenecen al Estado, otros entes públicos, a la comunidad o también a los miembros de un grupo o sector en tanto tal. Entre esos grupos o sectores que en la etapa moderna se vienen configurando, podemos ubicar a los usuarios de la tecnología de la información y comunicación que ingresan al terreno del comercio electrónico, puesto que se encuentran en ese estado de peligro con la mera utilización de la web en el marco de esas relaciones de mercado, bien pueden ser estos usuarios, en toda clase de relaciones que le representen la satisfacción de necesidades, e incluso por el hecho de facilitar la captación de información y datos a las entidades estatales y privadas .

3.3 Identificación de los obstáculos en la investigación de delitos vinculados con la identidad digital cometidos por medio de las TIC´S, en El Salvador.

Toda investigación de hechos delictivos conlleva la aplicación de una técnica policial que es dada por las circunstancias de los hechos objeto de la

---

[77] Gaddi, Daniela, Beaucells, Joan, García Arán, Mercedes. Justicia Restaurativa y Delincuencia Socioeconómica. 1 edición, Tirant Lo Blanch, 2021. Consultado en versión digital el 11/10/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413786322

[78] Sauquillo Muñoz, Carmen Pérez. Legitimidad y Técnicas de Protección Penal de Bienes Jurídicos Supraindividuales. Editorial Tirant Lo Blanch, Valencia 2019. Consultado en versión digital el 12/10/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413131245

investigación. En cuanto a la investigación del delito el Código Procesal Penal ha dispuesto las reglas para su práctica, estableciendo sabiamente el principio de libertad probatoria.

Para efectos de establecer protocolos en cuanto a la investigación de delitos, la U.S. Agency for International Development (USAID), financió el esfuerzo que se materializaría en la edición de un *Manual Único de Investigación Interinstitucional, en el cual participaron la Fiscalía General de la República, la Policía Nacional Civil y el Instituto de Medicina Legal "Dr. Roberto Masferrer", de la Corte Suprema de Justicia,* siendo estas las instituciones encargadas de la investigación por ministerio de ley. Así se desarrollan las técnicas de investigación del delito, establecidas en el Código Procesal Penal.

En el manual citado se establece un procedimiento bastante simplificado respecto del resguardo de la información electrónica, denominado el procedimiento como *"obtención y resguardo de información electrónica",* asimismo se establecen seis pasos a seguir para realizar dicha diligencia de investigación, sin embargo, se trata de una incautación de quipo tecnológico o hardware y posterior peritaje de extracción y análisis de información, invocando el art. 201 del Código Procesal Penal[79]. No obstante, dichos pasos a seguir resultarían infructuosos para desplegar una investigación relacionada con los delitos establecidos en la Ley Especial Contra Delitos Informáticos y Conexos, puesto que la obtención de hardware relacionado con el hecho

[79] Manual Único de Investigación Interinstitucional. Fiscalía General de la República, Policía Nacional Civil e Instituto de Medicina Legal "Dr. Roberto Masferrer", Corte Suprema de Justicia, con financiamiento de USAID. Imprenta y OFFSET Ricaldone, febrero 2012, consultado el 12/10/2022 en versión digital: https://escuela.fgr.gob.sv/wp-content/uploads/leyes/leyes-2/mui-final.pdf

delictivo, probablemente pueda incautarse en una etapa de resolución de caso mediante la emisión de órdenes de capturas administrativas.

Así verificamos, que, en materia de investigaciones de delitos informáticos, el Código Procesal Penal no ha establecido diligencias puntuales para su desarrollo. Aún al examinar las reformas realizadas al art. 259 del Código Procesal Penal, no establece procedimientos o técnicas puntuales sobre la obtención de la "evidencia digital", siendo este concepto introducido a través de la reforma. Más ciertamente, la Policía Nacional Civil de la Republica de El Salvador Cuenta con la Unidad de Investigaciones de Delitos Informáticos, cuya competencia puntual es la investigación de los delitos establecidos en la Ley Especial Contra Delitos Informáticos y Conexos vigente.

La Unidad de Investigaciones de Delitos Informáticos, cuenta con formación técnica financiada por diversas organizaciones, entre las cuales puede mencionarse a la Oficina de la Naciones Unidas contra La Droga y el Delito (UNODC). En el año 2016, la UNODC impartió el "Curso Práctico para la investigación de casos de cibercrimen y análisis forense digital", desarrollados por expertos en investigación de cibercrimen y análisis forense digital, así como otros talleres y cursos cuya finalidad es dotar de capacidades técnicas a los elementos policiales encargados de realizar la investigación de esta clase de delitos[80].

En este orden, puede identificarse un primer obstáculo:

[80] Consultado en sitio oficial de la Oficina de las Naciones Unidas Contra la Droga y el Delito, el 12/10/2022, en: https://www.unodc.org/ropan/es/unodc-apoya-a-la-policia-nacional-civil-de-el-salvador-en-el-abordaje-de-los-desafios-de-la-lucha-contra-el-cibercrimen.html

3.3.1 La Unidad de Investigaciones de Delitos Informáticos de la Policía Nacional Civil de la República como única dependencia técnicamente capacitada para la investigación de hechos delictivos establecidos en la Ley Especial Contra Delitos Informáticos y Conexos (LECDI), a nivel nacional.

De más esta mencionar, que el recurso humano es insuficiente para dar respuesta a las exigencias emanadas por la incidencia de hechos criminales, por lo que, en cuanto a ese punto, dicho obstáculo se lee y explica de manera evidente.

Acá conviene reflexionar sobre otros aspectos importantes generado por esta situación, y es que como ampliamente se ha mencionado en este documento, la sustracción de datos, o el hurto de identidad puede instrumentalizarse para cometer otros hechos delictivos. Así sucede de manera muy frecuente, por ejemplo, con delitos como la extorsión. Sin embargo, este delito no se encuentra comprendido expresamente en la LECDI, por lo que no se dispondría de un equipo policial capacitado técnicamente para el desarrollo de la investigación, puesto que sale del ámbito de competencia señalado para dicha división[81].

Sobre lo anterior, también es importante establecer, que los delitos informáticos, tal como sucede con el hurto de identidad, pueden cometerse bajo modalidades sofisticadas o complejas de realización, cuya investigación no puede practicarse a través de pasos inamovibles. Por tanto, la formación técnica de los intervinientes en las investigaciones debe ser continua a fin de mantener un estado de actualización en cuanto al conocimiento de las nuevas modalidades que se detecten.

---

[81] Vásquez Laínez, Juan David, Licenciado en Ciencias de la Computación, Especialista en Cibercrimen, JEFE UNIDAD DE INVESTIGACIONES DE DELITOS INFORMATICOS, PNC El Salvador, comunicación personal, en septiembre 2021.

3.3.2 Carácter Transnacional de la Investigaciones relacionadas con delitos Informáticos.

A través de su tesis doctoral, Josefina Quevedo Gonzalez, menciona la experiencia de España, en cuanto a la regulación adoptada que regula expresamente técnicas de investigación tecnológica, a través de una reforma a la Ley de Enjuiciamiento Criminal (LECrim).

Enumera las técnicas de investigación tecnológica que no precisan autorización judicial y las enumera: Obtención de una IP, identificación de IMEI IMSI y MAC, obtención de datos desvinculados de los procesos de comunicación, la orden de conservación de datos, captación de conversaciones públicas y actuación en casos de urgencia.[82]

> La dirección IP es una etiqueta numérica que identifica una interfaz (elemento de comunicación/conexión) de un dispositivo (ordenador, móvil, pda, ipad, televión, ebook, consola de videojuegos) dentro de una red que utiliza el protocolo IP (Internet Protocol). Las direcciones IP son asignadas por los ISP (Internet service provide) Los rastreos policiales para localizar IP ´pueden realizarse sin necesidad de autorización judicial ya que no se trata de datos confidenciales preservados del conocimiento público.
> El término IMSI se hace referencia a un código de identificación único para cada línea de telefonía integrada en la tarjeta SIM (Subscriber Identy Module) que le permite la identificación del abonado a través de las redes GSM y UMTS. El término IMEI es un código pregrabado en los teléfonos móviles que identifica al aparato unívocamente a nivel mundial y se trasmite por el móvil a la red de telefonía al conectarse a ésta. Es el equivalente al número MAC, cuando nos referimos a móviles, pue identifica ese número de serie al equipo. El término MAC es un identificador de 48 bits que corresponde de forma única para cada dispositivo. Las direcciones MAC son únicas a nivel mundial y constituyen una huella digital que permite determinar desde qué dispositivo de red se ha emitido un determinado paquete de datos.

[82] Quevedo González, Josefina. Ob. Cit. 173 y ss.

> Obtención de datos desvinculados de los procesos de comunicación, permite a la policía, en caso de urgencia, acceder al contenido de los dispositivos sea cual sea el mismo, sin especificar si se accede a datos vinculados o no a procesos de comunicación y siempre que se informe al juez competente dentro del plazo máximo de veinticuatro horas. La Orden de conservación de datos, pueden ser de contenido o de tráfico. Los de tráfico incluyen IP, los relativos a los sistemas o equipos de tránsito, servidores de la red o proveedores de acceso o de servicios y los referidos a equipo o sistema destinatario final. La captación de conversaciones pública, tiene lugar cuando las comunicaciones son accesibles para cualquier usuario de internet, no pueden tener la consideración de conversaciones privadas pues es el propio usuario de la red quien se introduce en la misma y asume que muchos de los datos se convierten en públicos para todos los usuarios. Actuación en casos de urgencia, estas operan por razones fundadas de urgencia y deben convalidarse mediante autorización judicial ex post, tales como la interceptación de las comunicaciones telefónicas y telemáticas, registro de dispositivos de almacenamiento masivo de la información.[83]

Naturalmente, que esta clase de técnicas, comprende las prácticas relacionadas con la obtención de información que es pública esencialmente (así el autor cita constantemente la máxima *"no se precisa autorización judicial para conseguir lo que es público*). El Ministerio Público a través de la Policía puede solicitar, bajo los medios y plataformas legalmente establecidas, pero siguiendo procedimientos específicos diseñados para tales efectos.

En El Salvador no se encuentran expresamente señaladas las técnicas especificas a aplicar, sin embargo, bajo el principio de libertad probatoria, el empleo de estas es ampliamente válido y legal. Aun sin constar expresamente en la ley, varias de estas técnicas enumeradas por la LECrim, ya han sido ejecutadas en investigaciones en El Salvador, desde hace ya varios años.

[83] Quevedo González, Josefina. Ob. Cit. 173 y ss

El obstáculo que se presentaría es, que, al realizar una diligencia consistente en conservación de datos, tal petición, al momento de formalizarse se debe plantear ante servidores de plataformas en el exterior, en la mayoría de los casos en Estados Unidos. Dichos servidores, se rigen al momento de proporcionar una información por las leyes vigentes en el país en donde se encuentra establecido el servidor, por lo que en ocasiones las respuestas a peticiones de información podrían denegarse o retardarse por criterios de gravedad de los hechos delictivos investigados. En ese sentido, las investigaciones de esta naturaleza podrían prolongarse durante largos periodos de tiempo y encima, denegar la información requerida. *Los servidores o Hosts (ordenador principal) son los sistemas informáticos que forman los nodos de internet. Estos hosts pueden ser equipos informáticos de usuarios individuales o pueden ser también servidores conectados a la internet de empresas.*[84]

A la vez, el carácter transnacional de los delitos informáticos incluye barreras básicas como el idioma que varía de país en país, por lo que algunos servidores imponen un idioma diferente al del país que origina la solicitud de información, lo que generaría diligencias adicionales tales como traducciones de parte de las entidades respectivas, con la finalidad de obtener y darle curso al trámite a las investigaciones.

A pesar de dichos impases, no puede omitirse, que los procedimientos para hacer solicitudes de información varían, según la empresa y aplicación, así como la plataforma habilitada para darle trámite a las mismas. Por tanto, existen formas más simplificadas de obtener información decisiva para la investigación de hechos delictivos, en los cuales se hayan involucrado las

[84] Quevedo González, Josefina. Ob. Cit., pág. 45

TICS. A manera ejemplificativa: la aplicación UBER, ha habilitado un portal con la finalidad de recibir peticiones de información relacionadas con los servicios de transporte prestados a través de la aplicación, que actualmente es de uso común en muchos lugares del mundo. En el portal *"Public Safety Response Portal",* se encuentran espacios de consulta para *Autoridades de Ley,* las cuales pueden estar integradas por miembros de la Policía Nacional Civil o por miembros de la Fiscalía General de la República, de cualquier país en donde la aplicación se esté utilizando. A través de dicho portal pueden crearse cuentas de agentes investigadores o agentes auxiliares del Fiscal General de la República (en el caso salvadoreño), quienes constantemente pueden realizar peticiones de información, acreditando su calidad y la existencia de una investigación en curso. La información que puede extraerse puede ser, nombre de usuarios de la aplicación de UBER, así como la información de choferes, información registrada al momento de crear una cuenta de usuario, correos electrónicos vinculados, características de vehículos reportados, incluso escaneos de documentación presentada por las personas que se acreditan como conductores de la aplicación, puede obtenerse información a cerca de todos los recorridos realizados por un chofer determinado, incluso mediante un detalle de coordenadas geográficas: latitud y longitud, las cuales fácilmente puede permitir la ubicación exacta de determinado vehículo que haga uso de la aplicación, a través del Sistema de Posicionamiento global (GPS)[85].

Esta clase de peticiones, son resueltas entre dos a cuatro semanas. Sin embargo, cuando se trata de hechos delictivos que ponen en riesgo la vida de las personas, las peticiones de información son atendidas en cuestión de

[85] Consultado el 15/10/2022 en: Uber Law Enforcement and Public Health Portal https://lert.uber.com/s/login/?language=en_US

horas. El portal incluso, cuenta con campañas para hacer del conocimiento de las autoridades la forma de obtener información relacionada con la aplicación.

Sin embargo, no todas las empresas o aplicaciones cuentan con las mismas políticas de privacidad, hay unas más rigurosas que otras y de ello dependerán los procedimientos, requisitos y tiempo de resolución de peticiones.

3.4 Análisis de la delincuencia informática que se comete a través del internet desde la perspectiva del Derecho Penal Económico.

En el transcurso de esta investigación se ha expuesto cómo la delincuencia informática puede observarse bajo la lupa del derecho penal económico. Por qué puede considerarse que esta novedosa modalidad criminal genera un impacto trascendental para un grupo o comunidad de personas y que además la delincuencia informática es apta para atentar contra bienes jurídicos supraindividuales o colectivos.

Al observar el fenómeno de la delincuencia informática desde una perspectiva del derecho penal económico, se hace en honor a sus alcances y su potencial, no solamente para ubicar en un estado de peligro a los bienes jurídicos protegidos, sino que esta modalidad delictiva también puede producir lesiones de estos en proporciones masivas.

El desarrollo tecnológico se ha infiltrado en todas las áreas de la vida del ser humano: para mejorar su calidad de vida y también incluye un potencial destructivo al cual la criminalidad ha sacado el mayor provecho. El ámbito de los negocios no se encuentra excluido de los riesgos que el uso de las TICS incluye, aún, representa quizá el área más atractiva para el delincuente

informático, que busca el mayor aprovechamiento de su actividad criminal con la certeza de que no será sorprendido mientras desarrolla su conducta delictiva.

En cuanto al Derecho Penal Económico, resulta teóricamente complejo definirlo, más se dice que el Derecho Penal *Económico se refiere al conjunto de normas jurídico penales que protegen el orden socioeconómico*. Así, se dice concretamente que *el orden socioeconómico como objeto de protección, se puede entender en sentido estricto, como la participación estatal en la economía, o en sentido amplio, como el conjunto de normas de protectoras de la producción, distribución y consumo de bienes y servicios*. De manera concluyente, se dice que el derecho penal económico, *no sería otra cosa que la intervención directa del Estado en la relación económica, imponiendo coactivamente una serie de normas y planificando el comportamiento de los distintos sujetos económicos*.[86]

De lo anterior, es posible ir integrando cómo la delincuencia informática puede lesionar el orden socioeconómico, ya que puede afectar las relaciones comerciales que incluyen el consumo de bienes y la prestación de servicios, a través del comercio informático, cuyo desarrollo ya es amplio. Tal es el caso que en El Salvador en Estado ha comenzado a reglar las relaciones comerciales informáticas y en ese sentido se encuentra vigente la Ley de Firma Electrónica, desde el año de 2016. Entre los considerandos de dicha ley, se menciona que el desarrollo de las tecnologías de información y comunicación se ha convertido un factor estratégico que mejora la eficiencia de la educación, fomenta la competitividad y el crecimiento económico de los pueblos. Así, el

[86] Moreno Castillo, María Asunción; Aráuz Ulloa, Ismael Manuel. Delincuencia Económica, Revista de Derecho (2003), consultado en versión digital el 15/10/2022, en http://repositorio.uca.edu.ni/964/1/215-230.pdf

legislador continúa enumerando los beneficios que aportan el uso de las TICS y se promueve su utilización para lograr el dinamismo y desarrollo económico.[87]

En el mes de julio del año 2021, la Asamblea Legislativa reformó cuarenta y seis artículos, de un total de sesenta y un artículos que contiene la Ley de Firma Electrónica, bajo el argumento de actualizarla para que respondiera a las necesidades actuales.[88] Dicha ley incluso contiene una definición del concepto *datos personales* y establece reglas para el tratamiento de estos.
En ese aspecto, se logra visualizar un elemento esencial del derecho penal económico en la delincuencia realizada a través de medios informáticos, puesto que el Estado ha comenzado a reglar cómo debería de ser la conducta de los usuarios de las TICS en el comercio informático.

Alrededor de este tema, también existen amplias discusiones relacionadas con la diferencia un delito contra el patrimonio y contra el orden socioeconómico, puesto que es importante saber establecer las diferencias entre estos. María Asunción Moreno Castillo, señala que el orden económico es un concepto superior al orden patrimonial clásico. El aspecto esencial a considerar, es que en los delitos de carácter socioeconómico se hace referencia a aquellos que suponen la lesión de bienes jurídicos supraindividuales o colectivos, relacionados con la producción, distribución y consumo de bienes y servicios[89].
Esto último se viene mencionando de manera reiterada y es que, en cuanto a la delincuencia informática, incluso en la ley especial (LECDI), se tutela la

---

[87] Ley de Firma Electrónica, emitido mediante decreto legislativo N°133 de fecha uno de octubre de 2015, consultada en versión PDF, el 15/10/2022.
[88] Sitio Oficial de la Asamblea Legislativa, *Pleno legislativo aprueba reformas a la Ley de Firma Electrónica para facilitar y simplificar su uso*, consultada el 15/10/2022 en: https://www.asamblea.gob.sv/node/11395
[89] María Asunción Moreno Castillo e Ismael Manuel Aráuz Ulloa. Ob. Cit., pág.224 y ss.

captación, uso y manejo de datos, lo que puede afectar a personas individuales y derechos patrimoniales individuales, tal como puede ocurrir con el delito de estafa informática. Sin embargo, esto no excluye que otros delitos previstos en esa ley especial posibiliten y den pie a la lesión de bienes jurídicos colectivos, tales como el orden socioeconómico (mediante el uso de las TICS en las relaciones de comercio), así como en los derechos de ese grupo de personas o comunidad de usuarios de las TICS o consumidores de las mismas.

3.4.1. El orden económico, los elementos que lo integran y su vinculación con el derecho penal económico.

3.4.1.1. Definición de orden económico.

El Orden Económico puede definirse como aquel conjunto de principios y normas constitucionales que organizan la actividad económica de un país y facultan al Estado para regularla e intervenir para corregir las distorsiones o aspectos que afecten su normal funcionamiento en armonía con los principios sobre la materia regulados en la Constitución de la República de El Salvador.

Es así como en El Salvador surge el denominado, para unos, “Derecho Constitucional Económico” y, para otros, la “Constitución Económica”, que puede definirse corno el conjunto de preceptos de rango constitucional sobre la ordenación de la vida económica *(Cfr.* con Sentencia de 26-VIII1999, Inc. 2-92).

Esta parte del Derecho Constitucional Salvadoreño de lo da en llamarse “La constitución Económica de El Salvador” encuentra su principal fundamento en el Título V de la Constitución, el cual contiene las normas destinadas a

proporcionar el marco jurídico fundamental para la estructura y funcionamiento de la actividad económica *(Cfr.* con Sentencias de 10-IV-2013, Inc. 9-2010).

En esta línea de pensamiento, el orden económico y el ejercicio del poder penal del Estado en el ámbito de la actividad económica son dos nociones vinculadas la una a la otra. Por un lado, el orden económico incorpora una serie de principios a los cuales debe sujetarse el Estado cuando ejerce su función ordenadora en la actividad económica mediante el ejercicio de su poder sancionador y por la otra la determinación de que en aquellos casos en que el Estado interviene en la actividad económica previniendo y reprimiendo aquellas conductas delictivas que afecten su normal funcionamiento, dicha intervención solo estará justificada si dicha intervención tiene por finalidad garantizar o preservar el interés social a que hace referencia el Artículo 102 inciso 2° de la Constitución de la República.

3.4.1.2. Elementos que integran el orden económico.

Dentro del Orden Económico están integrados como elementos orientadores de la intervención del Estado en la actividad económica, los siguientes principios:

A) LIBERTAD ECONOMICA.

En cuanto a la libertad económica, se debe afirmar que es una manifestación más del derecho general de libertad, entendido como la posibilidad de obrar o de no obrar, sin ser obligado a ello o sin que se lo impidan otros sujetos (libertad negativa) así como la real posibilidad de las personas de orientar su voluntad hacia un objetivo, es decir, la facultad de tomar decisiones sin verse determinado por la voluntad de otros, incluido el Estado, lo cual constituye una

Libertad positiva para el ejercicio de la actividad económica (Sentencia del 14-XII-95, Inc. 17-95).

A partir de lo anterior, si bien el Estado debe garantizar el pleno y efectivo ejercicio de la libertad económica, esto no implica que la misma pueda ser absoluta e ilimitada, dado que el Estado pueda intervenir en el mercado, por medio de la amplia gama de alternativas normativas (límites, regulaciones, ejercicio de facultad sancionadora, etc.) que la Constitución y el orden jurídico permitan, a fin de asegurar su ejercicio armónico y congruente con la libertad de los demás y con el interés y el bienestar de la comunidad.

Sobre esta base se bebe afirmar, que si bien es cierto, toda persona tiene derecho a crear una actividad económica lícita que le proporcione un flujo de efectivo con el cual financiar sus necesidades comerciales y personales, la actividad económica que desarrollan las personas para crear u organizar flujos de efectivo, utilizando herramientas informáticas y tecnologías de la información para dañar bases de datos, software, equipos informáticos y otros ***es ilícita*** porque el dinero que se obtenga de dichas actividades procede de la comisión de delitos tales como Hurto de Identidad digital, conducta delictiva que afecta el interés de los consumidores de las tecnologías de la Información, la seguridad informática y la confianza en el comercio electrónico de bienes y servicios razón por la cual el Estado debe corregir para corregir esa circunstancia que afecta el normal funcionamiento de la actividad económica.

B) LIBERTAD DE EMPRESA.

La *libertad de empresa* (art. 102 Cn.) tiene como finalidad la protección de la empresa, es decir, la forma de organización productiva que propicia las condiciones para el intercambio o circulación de bienes o servicios en el

mercado, cuyo límite radica en el interés social. Entonces, la libertad de empresa es una manifestación de la libertad económica e implica, la libertad de los ciudadanos de afectar o destinar bienes a la realización de actividades económicas, con el objeto de producir e intercambiar bienes y servicios, conforme a las pautas y modelos de organización típicos del mundo económico contemporáneo, y de obtener un beneficio o ganancia. (Cfr. Sentencia del 3-V-2011, Amp. 206-2008)

Desde esa perspectiva, la libertad de empresa se manifiesta en: *(i)* la libertad de los particulares de crear empresas, es decir, de elegir y emprender las actividades económicas *lícitas* que deseen y de adquirir, utilizar, destinar o afectar los bienes y servicios necesarios para el real y efectivo ejercicio de esa actividad; *(ii)* la libertad de realizar la gestión de la empresa*, por ejemplo* el establecimiento de los objetivos propios de la empresa, su planificación, dirección, organización y administración–; y *(iii)* la libertad de cesar el ejercicio de dicha actividad.

El Estado tiene obligación de "(…) garantizar la Libertad empresarial" (art. 110 inc. 2° Cn). y sobre esta base toda persona tiene derecho de emprender cualquier actividad económica lícita y el Estado tiene obligación de proteger al ciudadano emprendedor.

La práctica delictiva de utilizar la informática y las tecnologías de la información y comunicación para cometer delitos, tales como el de Daños Informáticos en el ámbito de la actividad económica es una actividad que es ***ilícita,*** razón por la cual no goza de la protección del Estado y por tal razón debe prevenirla y reprimirla mediante el ejercicio de u poder punitivo.

C) PROTECCIÓN DEL CONSUMIDOR.

La Constitución de la república ha regulado dentro de su texto una multiplicidad de áreas que conciernen al desarrollo de la persona humana, entre ellas, la económica; y es que, de acuerdo con el art. 1 inc. 3°, en relación con los arts. 101 inc. 2° y 102 Cn. se ha determinado que uno de los fines del Estado es alcanzar el “bienestar económico” de los habitantes de la República, lo que ineludiblemente obliga a asegurar --entre otros aspectos- la "libertad económica" y la defensa de los intereses de los consumidores *(Cfr.* con Sentencia de 19-VII1996, Inc. 1-92).

Sobre de lo dicho en el párrafo anterior, es necesario hacer notar que uno de los pilares del Orden Económico en El Salvador es el derecho de los consumidores, lo cual es congruente con el sentido actual de la economía global, dentro de la cual la protección de los derechos del destinatario final del mercado no puede considerarse como una política aislada del Estado, más bien se encuentra relacionada directamente con la idea de dignificar a la persona consumidora de bienes y servicios como el acceso y uso de las tecnologías de información y comunicación, todo ello con la finalidad de lograr el crecimiento económico y, principalmente, el bienestar de la población.

En El Salvador el conjunto de normas que integran el denominado derecho del consumidor está contenido en la Ley de Protección al Consumidor dentro de la cual para efectos de esta investigación destaca lo regulado en el Artículo 13- C de dicha Ley denominado “Protección al consumidor en el ámbito del Comercio electrónico” lo cual obedece a la necesidad de resguardar o tutelar los niveles básicos de satisfacción de las necesidades de los individuos para lograr un nivel de protección coherente con los valores garantizados en la Constitución cuando interviene en la actividad económica como usuario o consumidor de la tecnologías de la información y comunicación que propicie el fortalecimiento de su confianza.

Desde esta perspectiva, el derecho de los consumidores se relaciona íntimamente con el mercado y sus vicisitudes, por ello la normativa que los tutele debe estar orientada a corregir las eventuales fallas de la dinámica comercial, sin dejar de lado que las relaciones económicas del mercado involucran fenómenos contrarios al espíritu de la Constitución Económica, dentro de las cuales destaca la regulación del Delito de Hurto de Identidad Digital como conducta delictiva cuya naturaleza jurídica está vinculada con los postulados y contenidos del Derecho Penal Económico.

D) **SUBSIDIARIDAD DE LA INTERVENCIÓN DEL ESTADO EN LA ACTIVIDAD ECONOMICA**.

La realidad social de carácter local derivada de la realidad global, pone de manifiesto que el catálogo delincuencial de los ilícitos penales vinculados a la informática y el uso de tecnologías de la información y comunicación lejos de disminuir o desaparecer tienden a crecer porque los recursos de la tecnología tienden a generalizarse en su uso cada día más, de forma tal que su manipulación dolosa se ha extendido a otras esferas de la población diferentes de las expresadas, en consideración a que buena parte de las actividades de la vida moderna tienden a verificarse a través de medios informáticos.

Los sistemas de pagos, la transferencia de recursos monetarios, el acceso al domicilio o al lugar de trabajo, la correspondencia particular, las matrículas escolares, el control del consumo de servicios públicos, en fin, cualquier actividad de la vida cotidiana puede programarse y aun desarrollarse a través del Computadoras Personales, Tablets y teléfonos o de cualquier otro tipo de terminales a estas grandes bases de datos.

De esta forma, las oportunidades y los medios para delinquir se han multiplicado sustancialmente, sin que pueda reducirse la criminalidad informática a un sector específico de la población, ni limitar el perfil de este tipo de delincuencia a las características que se han venido señalando.

A partir de lo anterior, si bien el Estado debe garantizar el pleno y efectivo ejercicio de la libertad económica, esto no implica que la misma pueda ser absoluta e ilimitada, dado que el Estado pueda intervenir en el mercado, por medio de la amplia gama de alternativas normativas -límites, regulaciones, etc.- que la Constitución y el orden jurídico permitan, a fin de asegurar su ejercicio armónico y congruente con la libertad de los demás y con el interés y el bienestar de la comunidad.

Es en este contexto donde resulta aplicable el denominado Principio de Subsidiaridad de la Intervención del Estado en la Actividad Económica como un mecanismo excepcional al cual se debe recurrir para eliminar los riesgos de afectación a bienes jurídicos supraindividuales como consecuencia de la realización de prácticas delictivas como el “Hurto de Identidad Digital” que el funcionamiento del mercado por sí mismo no puede prevenir ni reprimir, razón por la cual se requiere de la intervención del Estado para realizar esa función mediante la creación de normas propias del ***Derecho Penal Económico***, como las contenidas en la Ley Especial Contra Delitos Informáticos y Conexos, teniendo siempre presente que dicha intervención solo estará justificada si dicha intervención tiene por finalidad garantizar o preservar el interés social a que hace referencia el Artículo 102 inciso 2° de la Constitución de la República.

Esta manifestación del intervencionismo del Estado en la actividad económica

guarda relación con el derecho penal económico y justificaría la inclusión de nuevas conductas delictivas en donde el legislador ha pretendido sancionar de forma directa a los responsables de las conductas cometidas a través de medios informáticos contra medios informáticos, ante la aparición de nuevos medios de cometer delitos a través de la tecnología de la información y comunicación; considerando que con la criminalización de estas se quiere proteger de conductas que atentan contra el orden económico como un bien supra individual y a los consumidores y proveedores de las herramientas tecnológicas.

CAPITULO IV: ANÁLISIS CRÍTICO DE LA REGULACIÓN DEL DELITO DE HURTO DE IDENTIDAD INFORMÁTICA EN LA LEGISLACIÓN SALVADOREÑA Y EL PROCESO DE REFORMA DE DICHA LEGISLACIÓN.

SUMARIO: 4.1TIPICIDAD. 4.1.1 TIPO OBJETIVO. Bien Jurídico Protegido. Acción. Objeto de Ataque. Medios Informáticos. Resultado. Elementos Normativos y Descriptivos del Tipo. Sujeto activo del delito. Víctima. Circunstancias de tiempo, lugar y desarrollo tecnológico. Relación de causalidad en imputación objetiva. 4.1.2. TIPO SUBJETIVO. Dolo. Error de Tipo. Autoría y Participación. Elementos Especiales de Autoría. 4.2. ANTIJURICIDAD. 4.2.1. Formal. 4.2.2. Material. 4.2.3. Causas de Justificación.4.3. CULPABILIDAD. 4.3.1 Imputabilidad/Inimputabilidad. 4.3.2 Conocimiento de la Antijuricidad. 4.3.3 Exigibilidad de otra conducta. 4.3.4 Causas de Exclusión de Culpabilidad. 4.3.4.1 Error de Prohibición.

RESUMEN:

A través del presente apartado se hace un esfuerzo teórico para guiar la presente investigación hacia un recorrido por el camino del *iter criminis.* Se parte del tipo de hurto de identidad de conformidad al art.22 de la Ley Especial Contra Delitos Informáticos y Conexos, el cual puede ser entendido como el corazón de toda la actividad investigativa que se ha realizado a través de este documento. Uno de los aspectos de mayor importancia lo constituye el bien jurídico protegido sobre el cual se hace una serie de consideraciones sobre los diferentes criterios adoptados en cuanto al mismo, ya que este puede ser muy variado. Como es necesario se descompone el tipo penal en todas sus partes, llámese tipo objetivo y tipo subjetivo. En cada uno de sus elementos se hacen ver las características propias de la cibercriminalidad, los cuales le dotan de una naturaleza jurídica diferenciada respecto de la criminalidad asociada con la violencia o delincuencia comúnmente conocida en El Salvador. Uno de estos aspectos es el perfil criminológico del delincuente

informático, su carácter, motivaciones y finalidad misma. No obstante, esos aspectos especiales, existe circunstancias mas complejas de analizar como las circunstancias de tiempo y lugar en las cuales se desarrollar el accionar criminal del delincuente informático, siendo este el tema quizá de mayor complejidad, novedoso y retador para el combate a esta clase de delincuencia sofisticada. No puede obviarse introducir la perspectiva del derecho penal económico, lo cual le brinda en definitiva la razón de ser al abordaje de este tipo delictivo.

4.1 TIPICIDAD.

Muñoz Conde, define la tipicidad como la adecuación de un hecho cometido a la descripción que de ese hecho se hace en la ley penal. Así destaca que, por imperativo del principio de legalidad, en su vertiente del *nullum crimen sine lege*, sólo los hechos tipificados en la ley penal como delitos pueden ser considerados como tales[90]. En lo sucesivo, se procederá a descomponer el tipo de hurto de identidad, establecido en el art. 22 de la Ley Especial Contra Delitos Informáticos y Conexos, a efectos de establecer su naturaleza.

4.1.1 TIPO OBJETIVO.

Al establecer los elementos del tipo de hurto de identidad, debemos mencionar al menos algunas definiciones del concepto, puesto que ello resulta útil para ir aproximándonos a la comprensión de cada elemento del tipo, objeto de análisis.

[90] Muñoz Conde, Francisco. Teoría General del Delito. 5ª Edición. Editorial Tirant lo Blanch, España, publicado el 02/09/2022., consultado en versión digital el 25/10/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411307604?showPage=41

En El Salvador, la Oficina de las Naciones Unidas Contra La Droga y el Delito (UNODC), en coordinación con la Fiscalía General de la República de El Salvador, realizaron un esfuerzo académico, materializado en la publicación del *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial Contra los Delitos Informáticos y Conexos.* En cuanto al delito de hurto de identidad contenido en el art. 22 de la LECDI, menciona que desde el punto de vista del derecho la *identidad,* hace referencia a un conjunto de características, datos o informaciones que permiten individualizar a una persona. Asimismo, se van desarrollando las diferencias entre identificar una persona o individualizarla.

Como todo concepto, la identidad puede tener diferentes acepciones. Desde el punto de vista médico legal, la identidad es el conjunto de características que nos hacen iguales a nosotros mismos y diferentes a los demás[91]. Morelba Rojas de Rojas, sostiene que la identidad es la expresión de un conjunto de rasgos particulares que diferencian a un ser de todos los demás. Así también cita, que la idea de identidad supone la idea de verdad, de autenticidad, puesto que identidad significa, sobre todo, idéntico a sí mismo[92].

Pérez Porto & Gardey, cita que *identidad* es una palabra de origen latín *(identitas) que permiten hacer referencia al conjunto de rasgos propios de un sujeto o de una comunidad. Estas características diferencian a un individuo o*

---

[91] *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial Contra los Delitos Informáticos y Conexos. Ob.Cit. pág. 74. Consultada el 27/10/2022 en versión PDF.*

[92] Rojas de Rojas, Morelba. Identidad y Cultura. Educere, Volumen 8, 2004, Universidad de los Andes Mérida, Venezuela, consultada el 27/10/2022, en versión digital en: https://www.redalyc.org/pdf/356/35602707.pdf

a un grupo de los demás. La identidad también está vinculada con la conciencia que una persona tiene sobre sí misma[93].

Entre otras definiciones, no esta de más mencionar que el diccionario de la lengua española define el concepto de identidad como un conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás[94].

En ese sentido, hay elementos comunes en las definiciones citadas, y es que la identidad, será aquella compuesta por elementos característicos propios de la persona (natural o jurídica) que le hacen diferente a cualquier otra entidad o persona. En ese sentido resulta necesaria la tutela penal de la misma, puesto que al producirse una afectación de su titularidad y suscitarse la utilización de esta por terceros criminales, las afectaciones o consecuencias son percibidas por el propio titular de dicha identidad.

Bien jurídico protegido.

El bien jurídico protegido constituye el elemento sustancial para el establecimiento de nuevos tipos penales. Existe abundancia de teoría y doctrina relacionada con su contenido y función. Para los efectos de este documento, conviene hacer un análisis del bien jurídico protegido procurando

---

[93] Hernández Vera, Daniel Antonio. La Suplantación de identidad Cibernética en el Ecuador. Maestría en Derecho Informático y de las Nuevas Tecnologías, Bogotá, D.C., Colombia, 2019, pág. 29, consultado en versión digital el 31/10/2022 en: https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f36afdf-40eb-4cba-a38f-5827107779a9/content

[94] Sitio Web: Real Academia Española, consultado el 27/10/2022 en: https://dle.rae.es/identidad

el discernimiento del mismo en el tipo del hurto de identidad, desde un enfoque pragmático.

Muñoz Conde, sostiene que bienes jurídicos son aquellos presupuestos que la persona necesita para su autorrealización y el desarrollo de su personalidad en la vida social. El autor menciona que los presupuestos materiales para conservar la vida y aliviar el sufrimiento (alimentos, vestido, vivienda, etc), estos presupuestos existenciales se les llama bienes jurídicos individuales; y aquellos que afectan mas a la sociedad como tal, al sistema social que constituye la agrupación de varias personas individuales y supone un cierto orden social y estatal, son los llamados bienes jurídicos colectivos.[95]

Los bienes jurídicos serán aquellos valores relevantes para la sociedad y ello también dependerá de la coyuntura social, económica y política imperante en cada país y región, como viene sucediendo desde el siglo pasado. Así se reconocieron diferentes derechos de primera, segunda, tercera y cuarta generación, como se ha repasado en el capítulo uno de este documento.

El desarrollo tecnológico abrió la puerta para el establecimiento de nuevos tipos delictivos que incluyen las nuevas tecnologías de la información y comunicación. Estas conductas pueden ser atentatorias contra los sistemas informáticos propiamente tales o instrumentalizar las TICS para lesionar otros bienes jurídicos.

---

[95] Muñoz Conde, Francisco, García Arán, Mercedes. Derecho Penal, Parte General, 8ª edición, revisada y puesta al día. Tiran lo Blanch, Valencia 2010. Consultada en versión digital 29/10/2022, en: https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

En cuanto al establecimiento del bien jurídico protegido por los delitos informáticos ha existido una discusión sobre la existencia de un bien jurídico autónomo y novedoso, o si, por otro lado, se trata de bienes jurídicos preexistentes, por ejemplo, el patrimonio, la intimidad, etc.

La autora chilena Laura Mayer Lux, aborda el tema sobre el bien jurídico protegido por los delitos informáticos y menciona las diferentes posturas en cuanto al mismo. En cuanto a la experiencia en chile, el bien jurídico protegido por los delitos informáticos, según señala la ley es *la calidad, pureza e idoneidad de la información contenida en un sistema informático como objeto de tutela penal*. Sobre ello, hace la crítica en cuanto a la excesiva amplitud de dichos conceptos y la falta de connotación técnica de los mismos. También hace especial referencia al concepto de *"información"* citado, puesto que, según la autora, dicho concepto es impreciso, por lo que generaría un problema al tener por establecido, como un bien jurídico la información. Esta crítica se fundamenta en que la información puede resultar ser cualquier cosa, dejando abierta la posibilidad de elevar a la categoría de bien jurídico cualquier clase de información que pueda no ser suficientemente relevante o lesiva[96].

A lo largo de su estudio, va enumerando una serie de posturas en cuanto al bien jurídico protegido por los delitos informáticos, mencionando algunos de ellos: a) el sofware como objeto de tutela penal, b) el internet como objeto de tutela penal, c) la confianza en el correcto funcionamiento del sistema informático como objeto de tutela penal, d) la confidencialidad, integridad y disponibilidad de los datos, e) sistemas informáticos como objeto de tutela

[96] Mayer Lux, Laura. El Bien Jurídico Protegido en los Delitos Informáticos. Revista Chilena de Derecho, Vol.44, No 1, Santiago abr. 2017. Consultado el 29 /10/2022 en versión digital en: https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_arttext&tlng=pt

penal y f) el correcto funcionamiento del procesamiento de datos como objeto de tutela penal. Sobre todos estos puntos de vista planteados en relación con el bien jurídico protegido, realiza argumentaciones del por qué no resulta viable tenerlos por válidos.

Esencialmente, las críticas que realiza, por ejemplo, del "*internet como objeto de tutela penal*" tienen relación con la inconveniente de utilizar algunos conceptos, puesto que no se adecúan o comprenden totalmente la naturaleza de la delincuencia informática, ya que el internet entendido como esa interconexión entre ordenadores, no abarca la cibercriminalidad en su totalidad.

En cuanto al bien jurídico protegido como *la confianza en el correcto funcionamiento del sistema informático como objeto de tutela penal,* razona que en cuanto a las relaciones de comunicación o de cualquier índole, establecidas a través de medios informáticos, están ya nacen con un componente de riesgo, por tanto, es un tanto ambicioso establecer como un bien jurídico protegido la "confianza", ya que además dicho planteamiento es en exceso impreciso, porque el concepto confianza está dotado de emotividad, lo que le hace inadecuado.

Finalmente, la autora Laura Mayer Lux, expone su punto de vista y se decanta por establecer el bien jurídico protegido en los delitos informáticos la *funcionalidad informática,* puesto que ésta la considera como un presupuesto para llevar actividades relevantes para las personas e instituciones. Se refiere entonces, a ese conjunto de condiciones que hacen posible que los sistemas informáticos realicen las operaciones de almacenamiento, tratamiento y

transferencia de datos, dentro de un marco tolerable de riesgo[97]. Un punto importante a destacar, es que entre las conclusiones citadas en este estudio es que el bien jurídico protegido de la funcionalidad informática debe entenderse como un bien jurídico instrumental de carácter colectivo.

En el caso de El Salvador, la LECDIC señala directamente el concepto de "información", como bien jurídico protegido. En el art. 3 de la ley citada, se establece, que *para los efectos de la ley se entenderá: b) Bien Jurídico Protegido: es* ***la información*** *que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros…* Evidentemente, que el legislador realiza un mínimo esfuerzo por delimitar la clase de contenido, sobre el bien jurídico protegido entendido como la "información", mencionando de forma ejemplificativa derechos que protegen bienes jurídicos de carácter individual; en la parte final empleó las palabras "entre otros…", lo que significa que podría incluirse toda clase de información vinculada con cualquier derecho o facultad de las personas, así como bienes jurídicos, sean estos individuales o colectivos.

En términos generales, desde el punto de vista de esta investigación, es posible concluir que no es descabellado tener por cierto que el bien jurídico protegido en cuanto a los delitos informáticos lo constituye la *información.* Evidentemente, no cualquier clase de información, si no aquella con relevancia suficiente para que su manejo inadecuado genere una afectación sensible para sus titulares. Con la finalidad de combatir imprecisiones en el concepto,

---

[97] Mayer Lux, Laura, Ob. Cit., Consultado el 29 /10/2022 en versión digital en: https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_arttext&tlng=pt

debemos indicar que estas afectaciones deben vincularse con derechos o facultades reconocidos por el ordenamiento jurídico.

Lo anterior resulta válido, porque al examinar cada uno de los tipos que se encuentran tipificados en la LECDIC, es posible identificar el componente de la información en cada tipo. Aún, cuando hablamos de tipos como, *acceso indebido a sistemas informáticos, acceso indebido a los programas informáticos o interferencia del sistema informático.* La existencia de dichos tipos tiene sentido, en función de la información o datos que a través de los sistemas informáticos se capta, de otra forma ¿Qué sentido tendría proteger el acceso a sistemas informáticos, por el mero hecho de evitar al ingreso de estos? Ciertamente, la finalidad que se persigue es evitar el acceso indebido a la información o datos, su divulgación ilegal o el tratamiento de datos en general, ya que ello comprendería desde su captación, utilización, divulgación, protección, etc.

En este orden de ideas, al analizar cada conducta delictiva tipificada en la LECDIC, permitirá ir estableciendo cuál es el bien jurídico protegido específico en cada caso.

El delito de hurto de identidad, se encuentra en el capítulo III de la LECDIC, que se denomina "*Delitos Informáticos relacionados con el contenido de datos", en su artículo 22.* En el tipo se establecen dos verbos rectores, y establece una sanción privativa de libertad para la mera suplantación o apoderamiento de la identidad de una persona. A continuación, establece otros supuestos. Sin embargo, para efectos de determinar cuál es el bien jurídico protegido debemos partir de la mera suplantación o apoderamiento de la identidad de las personas por medio de las TICS.

En el análisis jurídico de la ley especial contra los delitos informáticos y conexos auspiciado por la UNODC, en cuanto al bien jurídico protegido en el delito de hurto de identidad, se sostiene que el tipo penal también buscaría proteger una serie de intereses jurídicos de la persona cuya identidad se suplanta, para el caso *la privacidad o intimidad* de las personas a quienes sus datos personales les han sido sustraídos o apropiados. Asimismo, establecen el criterio de que podría extenderse su tutela al ámbito de intereses colectivos para garantizar *la veracidad* en las relaciones sociales a partir de internet, en particular de las que se emprenden a través de las redes sociales.
Es muy interesante la postura expuesta ya que se afirma que el tipo penal puede ser entendido como pluriofensivo, pues tutela principalmente la intimidad o privacidad y de forma derivada el patrimonio[98].

El punto de vista anteriormente citado es importante, puesto que señala bienes jurídicos individuales, los cuales resultan evidentes; pero también es posible visualizar desde un enfoque panorámico la existencia de un bien jurídico protegido autónomo propio del surgimiento de los avances tecnológicos. Con este incluso se puede confirmar el carácter pluriofensivo advertido, del bien jurídico protegido en el delito de hurto de identidad.

En ese sentido, puede identificarse como bien jurídico protegido la ***Seguridad en el tratamiento de la información personal que comprende la identidad de las personas naturales o jurídicas, por medio de las tecnologías de la información y comunicación.*** Sobre esta aseveración, hay varios aspectos relevantes a considerar:

---

[98] Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial Contra los Delitos Informáticos y Conexos. Ob.Cit. pág. 77. Consultada el 30/10/2022 en versión PDF.

Al hablar del concepto *seguridad, desde un enfoque genérico,* se hace referencia a la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable, la seguridad puede considerarse como una certeza[99]. Cierto es, que parece sumamente utópico esperar que exista certeza en cuanto al tratamiento de la información o a la custodia de la misma en las tecnologías de la información y comunicación, que tal finalidad de seguridad es inalcanzable y este aspecto específico, para algunos puntos de vista, haría no viable que se establezca como bien jurídico protegido a la *seguridad en el tratamiento de la información personal que comprende la identidad de las personas naturales o jurídicas, por medio de las tecnologías de la información y comunicación.*

Este último razonamiento no resulta válido, pues sería como considerar, que sería ambicioso o extremo entender que cómo no es posible evitar los robos, hurto, homicidios y extorsiones; no se tenga que proteger el bien jurídico de la vida, la propiedad, etc. Es comprensible que el riesgo de su vulneración siempre será una probabilidad para cualquier bien jurídico, no únicamente los protegidos por tipos relacionados con la criminalidad a través de las tecnologías de la información y comunicación.

Incluso, conviene mencionar que en España, se encuentran reconocidos una gran cantidad de derechos digitales, entre lo cuales se encuentra el *Derecho a la Ciberseguridad,* entendido como el que tiene toda persona a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad,

[99] Sitio Web Definición. De, consultado el 30/10/2022 en: https://definicion.de/seguridad/

confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados[100].

En conclusión, al establecer el tipo de hurto de identidad, se busca proteger la seguridad en el tratamiento de información personal, específicamente aquella que compone la identidad de las personas naturales o jurídica, a fin de disminuir los riesgos de su indebida divulgación o utilización, que generarían afectaciones concretas a los derechos de las personas titulares de dicha identidad. Al encontrarse comprendidas en este supuesto las personas naturales en grupos o colectivos, así como afectaciones que pudieran surgir para personas jurídicas, podría elevarse a la categoría de bien jurídico colectivo. Esto sí, y solo si, para el caso concreto se logra establecer un caso de esa trascendencia, como es ampliamente imaginable a partir de los sucesos de hecho considerados en este documento.

Acción.

Muñoz Conde define la acción, *como todo comportamiento dependiente de la voluntad humana* y hace ver que *sólo el acto voluntario puede ser penalmente relevante y la voluntad implica siempre una finalidad. No se concibe un acto de la voluntad que no vaya dirigido a un fin u objetivo determinado. El contenido de la voluntad es siempre algo que se quiere alcanzar, es decir, un fin. De ahí que la acción humana regida por la voluntad sea siempre una acción final, una acción dirigida a la consecución de un fin*[101].

---

[100] Cotino Hueso, Lorenzo. La Carta de Derechos Digitales. Editorial Tirant Lo Blanch 2022. Consultado en versión digital, pág. 401, el 02/11/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411472050

[101] Francisco Muñoz Conde. Ob. Cit., consultado en versión digital el 25/10/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411307604?showPage=41

Otros autores señalan a la acción, como una de las formas de la conducta humana penalmente relevante, constituyendo por tanto una de las especies del género de esta. Asimismo, trae a cuenta la existencia de diversas teorías sobre la acción acotando los puntos comunes que la definen: "*aquel comportamiento humano que requiere de un hacer del sujeto que trascienda a la esfera criminal al haber causado un daño o haber puesto en peligro un bien protegido".*[102]

Para Jiménez de Asúa, como para otros muchos autores, la acción propiamente dicha no deja de ser más que un actuar o acción "strictu sensu" voluntario que produce en el mundo exterior un resultado concreto o específico; o bien, pone en evidente peligro un bien penalmente protegido[103].

En el inciso 1 del artículo 22 de la LECDIC, establece los verbos rectores del tipo, los cuales representan las acciones delictivas: *El que* ***suplantare o se apoderare*** *de la identidad de una persona natural o jurídica por medio de las tecnologías de la información y la comunicación, será sancionado con prisión de tres a cinco años…* en los incisos 2 y 3 establece algunas circunstancias agravantes del tipo.

---

[102] Martínez Garza, Julio César. El Delito. Monografías. Editorial Tirant lo blanch, ciudad de México, 2021, consultado en medio digital, pág. 201, el 02/11/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413783611

[103] Martínez Garza, Julio César. Ob. Cit. Pág. 201. https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413783611

Suplantación.

Cuando se hace referencia a suplantar, el concepto es definido de manera genérica como *ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba*[104].

Daniel Antonio Hernández Vera, define la suplantación como el hecho que realiza una persona para tomar la representación de otro ser, sea este en la vida cotidiana, en el ámbito civil, comercial o penal, esta acción la realiza de mala fe y con dolo, buscando el tan solo hecho de tener un beneficio particular causando daño al titular de esa información ya sea a su imagen, su integridad y en algunos casos hasta de forma económica[105]. El autor continúa desarrollando los medios por los cuales se puede proceder a tal acto de suplantación, así sostiene que se puede suplantar una persona de forma física, por medios informáticos y por telecomunicaciones.

En el art. 22 de la LECDIC, se hace referencia a la acción de tomar el lugar de otro y establece que debe realizarse a través de las tecnologías de la información y comunicación. Este elemento agrega al tipo cuál es el medio empleado para que se configure la acción típica. En un primer momento, la mera suplantación de la identidad de una persona, natural o jurídica, se tendrá por consumada la conducta penalmente relevante, lo que indicaría la lesión del derecho a la intimidad de las personas, en un primer supuesto.

La descripción que realiza el tipo en el primer inciso, podría encuadrarse en una gran cantidad de casos, las cuales se han vuelto comunes en el uso de

---

[104] Sitio Web Real Academia Española, consultado el 30/10/2022 en: https://dle.rae.es/suplantar

[105] Hernández Vera, Daniel Antonio. Ob. Cit., pág. 31, consultado en versión digital el 31/10/2022 en: https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f36afdf-40eb-4cba-a38f-5827107779a9/content

las diferentes redes sociales. Al ingresar a las redes sociales, tales como Facebook, en al menos una ocasión nos encontramos con publicaciones de personas que solicitan colaboración para denunciar determinadas cuentas, porque utilizan datos incluso imágenes a través de la creación de perfiles, suplantando la identidad de una persona determinada. En este supuesto, generalmente se busca afectar la imagen del titular de la identidad, se distribuye información por lo general injuriosa que atenta contra la imagen, la dignidad o decoro de determinada persona. Actualmente, las plataformas de las redes sociales, establecen mecanismos de control para evitar tales situaciones y al registrarse la denuncia a través de la misma red social es posible inhabilitar dicha cuenta. Por esta razón, ese primer supuesto deja de trascender penalmente, ya que existen mecanismos efectivos para su control, sin perjuicio de las denuncias existentes relacionadas con esta modalidad.

Al tomar ese lugar de otro por medio de las TICS, se encuentra imbíbito el empleo de sofisticados mecanismos para consumar la acción, puesto que los datos que componen la identidad digital de determinada persona, deben ser adquiridos previamente. Algunos datos personales que conforman la identidad digital los introducen los usuarios de las TICS, los cuales son de acceso público y hay otros datos a los cuales el acceso no es inmediato. En este segundo supuesto, podrían emplearse técnicas, como la utilización de software destinado para tales fines, conocidos como *malware, que es un término general que se le da a todo aquel software que tiene como propósito infiltrarse o dañar la computadora.*

Sólo al hablar de malware, pueden mencionarse numerosos tipos de estos: *como virus, gusanos, troyano, adware, spyware, sniffers, bombas lógicas,*

botnets, exploit, droppers, rootkit, ddos, el spam[106]. Todos estos tipos de Malware son utilizados para cometer una gran cantidad de delitos informáticos, se caracterizan por acceden a los sistemas informáticos de manera maliciosa, generando datos en los equipos. Este acceso les permite además acceder a los datos de los usuarios. Una nota característica que hace el autor Josefina Quevedo González, es que se trata de técnicas de ingeniería social que permiten suplantar identidades. Constituyen parte del medio por el cual se ejecuta la acción típica de suplantar la identidad de otro.

Para consumar la acción de suplantar la identidad, también puede preceder el *Phising, el cual consisten en un engaño para obtener información confidencial, como números de tarjetas de crédito, claves de acceso, etc.,*[107] la cual posteriormente es utilizada para suplantar la identidad de los usuarios de la TICS. También es posible identificar diferentes modalidades para tomar el lugar de otros a través de la TICS.

Eleno Quiñónez Acevedo, expone un punto de vista mas restringido sobre el tema y estudia la suplantación de identidad en las redes sociales. Sobre ello menciona las modalidades de suplantar la identidad en redes sociales: 1- Registrar un perfil falso, incluyendo en este sentido el uso de imágenes, fotografía y el nombre, sin hacer referencia necesariamente a otra información. 2- Crear un perfil falso utilizando los datos personales de la víctima (identidad digital). 3- Acceder de forma no autorizada al perfil de la víctima en un servicio de internet para hacerse pasar por él[108]. En este punto, debe comentarse la

---

[106] Quevedo González, Josefina. Ob. Cit. Pág. 77 y ss.
[107] Quevedo González, Josefina. Ob. Cit. Pág. 27 y ss.
[108] Quiñónez Acevedo, Eleno. La suplantación de identidad en las redes sociales. Artículo de actualidad. Ministerio público. Asunción, Paraguay, publicado en fecha 08/12/2016, Consultado en versión digital, pág. 8, el día 02/11/2022 en: https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/7/6

tercera modalidad, no correspondería de acuerdo al tipo de hurto de identidad vigente en nuestro país a la acción de suplantar, sino a la acción de apoderamiento.

Apoderarse.

La Real Academia Española define el concepto como, hacerse dueño de algo, ocuparlo, ponerlo bajo su poder[109].

Una perspectiva útil a considerar, es el tipo base existente, el delito de hurto tipificado en el art. 207 del Código Penal salvadoreño, en el cual se emplea el verbo rector *Apoderarse.* Esta acción, incluye algunas notas características de acuerdo a la Sala de lo Penal de la Corte suprema de Justicia, que en el análisis del tipo de hurto, establece que *"el centro de la acción es el "apoderamiento" del bien, lo que trae consigo necesariamente que el propietario se vea "desapoderado" del bien mueble, pues sólo así se lesiona el bien jurídico tutelado; produciéndose esto último, cuando la conducta del sujeto activo impide que la víctima ejerza sobre el objeto sus poderes de disposición o hacer efectivas sus facultades, porque ahora es el autor del ilícito quien puede someter el objeto al propio poder de disposición". (Ver Ref. 285-CAS-2010, del diez de Julio del año dos mil trece)[110].*

Eva María Souto García, hace referencia al concepto: *"en el apoderamiento se inscribe la total secuencia del delito: desapoderamiento como alejamiento del poder fáctico sobre la cosa del titular legítimo de la custodia y apropiación, en*

[109] Sitio de la RAE, consultado el 02/11/2022 en: https://dle.rae.es/apoderar
[110] Sentencia definitiva, emitida en recurso de Casación por la Sala de lo Penal de la Corte Suprema de Justicia. Referencia 17-CAS-2013, de fecha 03 de marzo de 2015, consultada en versión digital el 03/11/2022 en https://www.jurisprudencia.gob.sv/busqueda/tesauro.php#

el sentido de configuración por el autor de un poder autónomo sobre la misma cosa"[111].

La misma autora Souto García, hace referencia a la postura del Tribunal Supremo Español y cita la sentencia de 8 de septiembre de 2003 (Tol 312037) a través de la cual precisó sobre "el verbo "apoderar", como *requisito formal y núcleo o esencia de la definición ofrecida por el art. 237, implica la apropiación de la cosa ajena, que pasa a estar fuera de la esfera del control y disposición de su legítimo titular, para entrar en otra en la que impera la iniciativa y autonomía decisoria del aprehensor, a expensas de la voluntad del agente*"[112].

Sobre el mismo asunto, otros autores como BRANDARIZ GARCÍA, exponen que *"la acción típica supone la aprehensión y el desplazamiento físico de la cosa desde el ámbito patrimonial del sujeto pasivo al del sujeto activo. La acción de apoderamiento irá seguida del resultado de desposesión del sujeto pasivo y la correlativa incorporación de la cosa al ámbito de disposición del sujeto activo*"[113].

Con las aportaciones de las definiciones citadas, podemos ir concluyendo que la acción de apoderamiento ha recaído tradicionalmente sobre bienes muebles. En este sentido, es propio comentar que el art.22 de la LECDIC, hace referencia a un desapoderamiento, desposesión o apropiación de un elemento

---

[111] Souto García, Eva María. Los Delitos de Hurto y Robo: Análisis de su regulación tras la Reforma operada por la LO 1/2015, 30 de marzo. Editorial Tirant Lo Blanch, Valencia 2017, pág. 54 y ss. Consultado en versión digital el 03/11/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491436867

[112] Souto García, Eva María. Ob. Cit. Pág.55. https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491436867

[113] Souto García, Eva María. Ob. Cit. Pág.55. https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491436867

intangible que se encuentra constituido por los datos que componen la identidad de la víctima, una persona natural o jurídica en la realidad virtual, pero que es capaz de producir un resultado sensible en la realidad objetiva.

En el análisis jurídico de la ley especial contra los delitos informáticos y conexos de la UNODC, se señala que la diferencia del verbo rector de apoderamiento con el verbo suplantar, consiste en que con el apoderamiento el sujeto activo se hace dueño de la identidad real o verdadera de una persona natural o jurídica en el mundo virtual – y no hace una emulación de ella, lo que ocurre al suplantar-[114]

Al igual que el verbo rector de suplantar, el apoderamiento requiere el conocimiento o captación de datos de la víctima, los cuales puede obtener forma maliciosa a través de técnicas de la *ingeniería social,* como, por ejemplo, la variedad de Malware, a los que brevemente se ha hecho referencia.

Otros conceptos utilizados: sustracción de identidad.

El delito de hurto de identidad, puede ser conceptualizado de forma variada. En la región latinoamericana y en España se utilizan conceptos para hacer referencia al uso o instrumentalización de la identidad de las personas con fines criminales. Al hacer un repaso, pueden variar en cuanto al uso, conceptos como suplantación, robo o sustracción de identidad, entre otros.

[114] Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial Contra los Delitos Informáticos y Conexos. Ob.Cit. pág. 80. Consultada el 03/11/2022 en versión PDF

Concepto de sustracción

Sustracción designa el acto de sustraer y su efecto. Se usa para hacer referencia a lo que se resta o quita. Es una palabra compuesta por los siguientes términos de origen latino: “sub” que alude a algo que está por debajo; “trahere” en el sentido de “arrastrar hacia uno” o “traer”; a lo que se agrega el sufijo de acción y efecto, “cion”[115]. Este concepto según sus efectos, puede ser comprendido en términos similares al apoderamiento, utilizado por la LECDIC.

Tiene aplicación en los siguientes ámbitos:

En **Matemática** es una operación llamada también resta, que consiste en encontrar la diferencia existente entre dos cantidades. El signo representativo es (-) que se lee “menos”. Es la antítesis de la suma, o sea la operación inversa, que consiste en determinar en cuántas unidades es mayor un número (el minuendo) con respecto a otro (el sustraendo). El resultado recibe el nombre de diferencia. A su vez, el minuendo es igual a la diferencia más el sustraendo. Entre las propiedades de sustracción podemos mencionar, que es anticonmutativa, ya que alterar el orden de los números (minuendo y sustraendo) altera el resultado. La sustracción de 5-3 es igual a 2, pero la sustracción de 3-5 es igual a -2. Tampoco es asociativa, ya que por ejemplo el resultado será distinto en los casos siguientes: (5-3) -1 = 1 y 5- (3-1) =3. Para verificar que la sustracción ha sido hecha de modo correcto, podemos sumar el sustraendo y el resultado, y deberemos obtener el minuendo.

---

[115] Fingermann, H. (13 de abril de 2017). *Concepto de sustracción*. Deconceptos.com. https://deconceptos.com/ciencias-juridicas/sustraccion

La sustracción también se aplica a cualquier acción y efecto que implique quitar algo, material o inmaterial, por ejemplo: “Me sustraje de la realidad y me evadí en mis pensamientos”, “Mis hijos sustrajeron las golosinas que guardaba en la alacena”, “Juan me sustrajo la idea de instalar un negocio de ropa”.

En Derecho Penal, la sustracción, da origen a varias figuras delictivas punibles, y puede ser de sujetos, de ideas, de objetos o datos personales. En el primer caso podemos mencionar el delito de sustracción de menores, en el segundo, la de derechos de autor, y en el tercero se configura un hurto (si es sin violencia) o un robo (si medió violencia). Ejemplos: “La sustracción de menores es un delito internacional”, “Le sustrajo el arma al policía y desapareció sin ser aprehendido”, la sustracción de datos personales alojados en plataformas informáticas, para configurar el delito de Hurto de identidad[116].

Objeto de Ataque. Medios Informáticos.

Tal como se ha venido desarrollando, la nota esencial del tipo de hurto de identidad, al igual que los demás tipos desarrollados en la LECDIC, es que estos ocurren la realidad virtual, con una característica importante: su intangibilidad. No obstante, ello, es posible identificar los medios tangibles utilizados para la comisión de los delitos en esa realidad virtual, que, además, por principios lógicos se convierten en el objeto de ataque.

La criminalidad informática se desarrolla a través de los medios informáticos. Por lo que primero, partiremos de la definición de la informática: *la cual incluye*

[116] Fingermann, Ob. Cit.

la teoría, diseño, fabricación y uso de ordenadores, es la ciencia del tratamiento automático (por realizarse mediante máquinas-hoy en día electrónica-) y racional (esta controlado mediante ordenes que siguen el razonamiento humano) de la información. El término informática apareció en Francia en 1962 uniendo las palabras "information" y "automatique". La informática se ocupa del desarrollo de nuevas máquinas (computadoras y periféricos), desarrollo de nuevos métodos de trabajo (sistemas operativos) y el desarrollo de nuevas aplicaciones informáticas (software o programas). En ese sentido, se puede establecer que la informática es el cuerpo de conocimiento que trata el análisis, diseño, implementación, eficiencia y aplicación de procesos que transforman la información[117].

Aunque mas adelante se tratará de manera mas amplia, el ataque a los medios informáticos, indudablemente debe ser orquestado por el delincuente que cumpla con el perfil idóneo para perpetrar el ataque y obtener el resultado perseguido. Lo anterior, porque no todas las personas tienen el conocimiento o formación necesaria para atacar efectivamente un medio informático (sistemas operativos, software, hardware) y vulnerar el mismo.

A los medios informáticos deben agregarse otros ingredientes como el internet, entendida como esa interconexión entre dispositivos, y el ingrediente de las

---

[117] Garrido López, Carlos Alberto y Kuro Tenshi, Ángel Eduardo. Introducción a la informática. Artículo Accelerating the world´s research. Consultado en versión digital el 03/11/2022 en https://d1wqtxts1xzle7.cloudfront.net/53790500/Informatica-with-cover-page-v2.pdf?Expires=1667475592&Signature=fp9MFri2WKk8sGH0~ETaSPC-cTE8dBkjpKmw3C3IMqSuw~aYuxCHBw-DH8g438VwAgu-KQgQhJkW8iGGPwhR4KJURgEfhhLbv8~-NSur8tGflAEjesS2iXf0Q56wduCTkrF3ydLj1EA3z7gqqbusgcVYNc4KmmLqnEDYtt5RHJtGf64gxm9JlHqazh6U2rpbensQtjkoR5LedJMzoQoRJOo~qi0mMdHaeOiwSOJsMZGQJcxSps7dRIZmGLjYZ-YkHu9oLFVlc0nRFQpenU0dXt5Zbet~QkFPzi87-r0WrMoK65GBPZKcKxZz7Gjr8lE2JA1FtpM5pEe5Jtwbs90NzQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

nuevas tecnologías de la información y comunicación: tal como lo cita la LECDIC en el artículo 3 letra l), las cuales engloban la comunicación, registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética.

Para llevar a cabo el hecho delictivo, en el delito de hurto de identidad bastará con tener acceso un dispositivo, el cual a raíz del desarrollo tecnológico puede ser variado. En la actualidad se encuentran al alcance de casi cualquier persona, puesto que existen formas de adquisición también diversas por lo que no es esencial tener poder adquisitivo muy elevado, lo que convierte a la mayoría de personas en potenciales delincuentes informáticos por cumplir con el primer supuesto que es el acceso al instrumento para llevar a cabo el ataque.

Los dispositivos con la capacidad de realizar los procesos de transformación de la información son el vehículo que traslada al sujeto activo hasta la realidad virtual, donde necesita estar para atacar a la víctima, quien sufre el ataque a bordo también de un dispositivo que la situó en el mismo lugar (realidad virtual) idóneo para sufrir la agresión.

Al hablar de un ataque hacemos referencia a las acciones necesarias para ejecutar los verbos de suplantar y apoderarse de la identidad de la víctima. Se puede considerar que *un ataque informático* consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en

la seguridad del sistema, que luego repercute directamente en los activos de la organización[118].

Resultado.

El tipo de hurto de identidad es un delito de resultado, puesto que el legislador ha establecido de una serie de consecuencias las cuales nacen de consumar las acciones señaladas como prohibidas (suplantar o apropiarse).

Muñoz Conde indica, que al realizarse en el exterior la acción siempre modifica algo, produciendo un resultado, pero este resultado ya no es parte integrante de la acción[119]. Para el autor, es importante hacer una diferencia entre la acción y el resultado, ya que esta última debe entender según razona como la *consecuencia externa derivada de la manifestación de voluntad,* la cual tiene gran importancia para el Derecho penal, según se viene estudiando. Cuando se castiga el resultado producido, se exige una relación de causalidad entre la acción y el resultado.

Al analizar el tipo de hurto de identidad digital, en el inciso 1, se observa que la acción consistente en suplantar o apoderarse de la identidad de una persona a través de las tecnologías de la información y comunicación. En este punto, podemos hacer un ejercicio intelectivo como sucede en el delito de hurto, el

---

[118] Mieres, Jorge. Ataques informáticos, artículo Debilidades de seguridad comúnmente explotadas. Publicado en 2009. Consulta en medios digitales el 05/11/2022 en: https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

[119] Muñoz Conde, Francisco, García Arán, Mercedes. Ob. Cit. Pág. 225. Consultada en versión digital 05/11/2022, en: https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

cual se considera un delito de resultado, pues el sujeto activo obtiene un bien mueble ajeno, produciéndose un desplazamiento material de la cosa hurtada. Por otro lado, autores como Alejandra Olave Albertini[120], sostiene que el delito base de hurto, es un delito de actividad, porque no puede establecerse esa separación de tiempo y espacio entre la acción de apoderamiento de la cosa mueble y la consecuencia. Sin embargo, no puede ignorarse que en el delito de hurto de identidad se desarrolla en la realidad virtual, recae sobre datos intangibles, y puede entenderse que también se produce un desplazamiento de la información, por lo que debe ser comprendido como un delito de resultado. El tipo de hurto de identidad tiene establecida una sanción privativa de libertad, de tres a cinco años de prisión, posicionándole entre los delitos graves. El art. 22 de la LECDIC establece:

El que suplantare o se apoderare de la identidad de una persona natural o jurídica por medio de las tecnologías de la información y la comunicación, será sancionado con prisión de tres a cinco años.

Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros y el apoderamiento recae sobre datos personales, datos sensibles, o datos confidenciales, definidos así por disposición legal o reglamentaria, o por acuerdo de voluntades entre personas naturales o jurídicas, será sancionado con prisión de cinco a ocho años.

[120] Olave Albertini, Alejandra. Artículo: El delito de hurto como tipo de delito de resultado. Política criminal, Vol. 13, n°25, Santiago, julio 2018. Consultado el 05/11/2022, consultado en https://www.scielo.cl/scielo.php?pid=S0718-33992018000100175&script=sci_arttext

Si con el comportamiento del inciso anterior los datos obtenidos, lo fueron, con ánimo de lucro para sí o para un tercero, la pena de prisión será de seis a diez años.

En el inciso 2 del artículo, establece cinco posibles resultados (dañar, extorsionar, defraudar, injuriar o amenazar); que además deben cumplir con ciertas condiciones especiales, que se encuentran relacionadas con dos aspectos: el primero **sobre la finalidad** (la cual estaría constituida por ocasionar el perjuicio o la obtención de beneficios para el autor de la acción o un tercero). El segundo sobre **la instrumentalización de la identidad personal** (porque el tipo el apoderamiento debe recaer sobre datos personales, sensibles, confidenciales, definidos por ley, reglamento o acuerdo de voluntades). Al suscitarse alguna de estas conductas -ya que no es obligatorio que se configuren todas- incrementa la sanción, tal como se lee.

Los supuestos de hecho capaces de generar alguno de los resultados señalados por el tipo son múltiples, pues estos se encuentran constituidos por tipos penales concretos (elementos normativos del tipo que serán analizados en el apartado inmediato siguiente), cuya consumación será evidentemente posterior a la acción de suplantar o apoderarse de la identidad de la víctima, pero en la mayoría de los casos, la víctima o usuarios de las TICS tienen conocimiento del hurto de su identidad cuando percibe uno de estos resultados y no antes, aunque tal posibilidad no puede desecharse.

El autor Gilberto Martiñón Cano, sostiene que un delito es de resultado cuando la afectación del bien jurídico es separable espacio-temporalmente de la

acción[121], en este caso las acciones de suplantación y apoderamiento se realizan a través de una serie de esfuerzos sofisticados o técnicos para, para posteriormente instrumentalizarla y perjudicarle u obtener el beneficio señalado por la prohibición legal, por lo que es posible visualizar la separación a la cual se refiere el autor.

De manera concluyente, puede establecerse que el resultado que se castiga por el tipo de hurto de identidad se encuentra relacionado con la lesión de otros bienes jurídicos como la intimidad, el patrimonio, la autonomía de la voluntad, la integridad física, libertad sexual, honor, e incluso los derechos de los usuarios de las TICS, este último se encuentra imbíbito en el tipo. Si esto es cierto, también puede concluirse que se castiga la instrumentalización de la identidad digital de las personas para cometer otros hechos delictivos, puesto que sin esta instrumentalización no podría haberse obtenido el resultado prohibido.

Elementos Normativos y Descriptivos del Tipo.

Doctrinariamente, se establece la manera adecuada de configurar y redactar los tipos penales, de manera que estos sean comprensibles para la población a la cual éstos van dirigidos. Muñoz Conde, señala que su redacción debe hacerse de tal forma que su texto permita deducir claramente la conducta prohibida. Debe emplearse un lenguaje claro y preciso asequible al nivel cultural medio.

[121] Martiñón Cano, Gilberto. El delito de Secuestro. Editorial Tirant lo Blanch, Valencia 2010. Pág.99. Consultada en versión digital el 05/11/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788499858135

Se habla de los elementos normativos y descriptivos del tipo: *los elementos descriptivos son aquéllos que se refieren a términos que cualquiera puede apreciar o conocer en su significado sin mayor esfuerzo (como «matar», «aire», «lesiones», «cazar», «cosa», etc.).*
Elementos normativos son, por el contrario, aquéllos que requieren, para su comprensión, el conocimiento de alguna norma a la que el tipo se está remitiendo[122]*.*

El delito de hurto de identidad esta plagado de elementos normativos (*dañar, injuria, amenaza, extorsión, datos personales, datos sensibles, acuerdo de voluntades, tecnologías de la información y la comunicación)*. El delito de daño se encuentra regulado en el artículo 221 del Código Penal de El Salvador.

"El que con el propósito de ocasionar perjuicio destruyere, inutilizare, hiciere desaparecer o deteriorare una cosa total o parcialmente ajena, siempre que el daño excediere de doscientos colones, será sancionado con prisión de seis meses a dos años.
En igual sanción incurrirán los individuos que dañaren bienes muebles o inmuebles, públicos o privados, mediante cualquier inscripción de palabras, figuras, símbolos o marcas fueren estos grabados o pintados."

El delito de injuria, se encuentra tipificado en el artículo 179 del Código Penal:

"El que ofendiese de palabra o mediante acción la dignidad o el decoro de una persona presente, será sancionado con multa de cincuenta a cien días multa.
La injuria realizada con publicidad o cuando fuere reiterada contra una misma

[122] Muñoz Conde, Francisco. Ob. Cit, pág. 62, consultado en versión digital el 05/11/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411307604?showPage=41

persona, será sancionada con multa de cien a ciento ochenta días multa. Si la injuria reiterada se realizare con publicidad, la sanción será de ciento ochenta a doscientos cuarenta días multa."

El delito de extorsión se encuentra tipificado en el art.2 la Ley Especial Contra el Delito de Extorsión:

"El que realizare acciones tendientes a obligar o inducir a otro, aun de forma implícita, a hacer, tolerar u omitir un acto o negocio de carácter patrimonial, profesional o económico, independientemente del monto, con el propósito de obtener provecho, utilidad, beneficio o ventaja para sí o para un tercero, será sancionado con prisión de diez a quince años.

La extorsión se considerará consumada con independencia de si el acto o negocio a que se refiere el inciso precedente se llevó a cabo y responderán como coautores, tanto el que realice la amenaza o exigencia, como aquellos que participen en la recolección de dinero personalmente, a través de sus cuentas o transferencias financieras o reciban bienes producto del delito".

El delito de amenazas se encuentra tipificado en el art.154 del Código Penal:

"El que amenazare a otro con producirle a él o a su familia, un daño que constituyere delito, en sus personas, libertad, libertad sexual, honor o en su patrimonio, será sancionado con prisión de uno a tres años".

.

Los elementos normativos: datos personales, datos sensibles y tecnologías de información y la comunicación se encuentran definidos en el art. 3 de la Ley Especial Contra Delitos Informáticos y Conexos, letras l) m) y n):

“l) Tecnologías de la Información y la Comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros;

m) Datos Personales: es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar;

n) Datos Personales Sensibles: son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar;”

Cada uno de los tipos señalados por tutelan bien jurídicos concretos e individuales. En el delito de hurto de identidad, se requiere en un primer momento que este sea ejecutado en el ciberespacio, pero posteriormente los resultados castigados, se deben comprender que deben ocurrir en tiempo y espacio concreto, ya que todos estos tipos (daños, extorsión, injuria, amenazas) deben consumarse de la forma, -si podemos mencionarlo así- ordinaria dispuesta para tales tipos. Sobre cada tipo, existe suficiente material de estudio al cual recurrir en caso de identificar una de las formas descritas por el legislador.

En cuanto a los elementos normativos del tipo, la dogmática establece que se van a caracterizar con precisiones ontológicas, epistemológicas y sistemáticas que se corresponden con las siguientes notas:

a) No son perceptibles sensorialmente,
b) Están referidos a procesos de valoración o de comprensión intelectual no descriptivos, y
c) Son elementos de la antijuricidad.

Así se van haciendo interesantes acotaciones: primero que sobre la tercera nota no hay unanimidad de opiniones, y segundo en cuanto a que están relacionados con el elemento intelectivo del dolo y con el error. Entre otras precisiones dogmáticas destacables, se encuentra lo sostenido por Welzel, quien dice que los elementos normativos se diferencian de los descriptivos, en que su contenido de significación solo puede ser comprendido intelectualmente[123]. Los elementos normativos del tipo, son importantes porque vienen restringiendo y eliminando los supuestos culposos, en cuanto a la consumación del delito de hurto de identidad, como mas adelante se estudiará.

En cuanto a los elementos descriptivos del tipo, se encuentran la *"identidad, la obtención de beneficios, ocasionar perjuicio, incluso el ánimo de lucro",* los cuales son conceptos sobre los que la persona común puede comprender su alcance y sentido, o tener una noción acertada sobre su significado. Los elementos descriptivos del tipo identificados en el delito de hurto de identidad sirven para establecer ciertas circunstancias especiales que deben suscitarse en la consumación del resultado, como la obtención de beneficios, los cuales

[123] Suay Hernández, Celia, profesora titular de Derecho Penal, Universidad Autónoma de Barcelona. Los Elementos Normativos y el Error. Consultado en versión digital el 05/11/2022, en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-1991-10009700142

pueden ser diversos, un beneficio puede ser económico o de otra índole, ya que el texto legal no precisó sobre este. El perjuicio también puede ser claramente identificable si este se relaciona con alguno de los elementos normativos detallados, podemos inferir qué clase de perjuicios pueden generarse, puede tratarse de un perjuicio económico, perjuicio en su imagen, perjuicio en su libertad de decisión, etc. Será la casuística la que ira dictando la forma de analizar e identificar los mismos.

Sobre los elementos descriptivos señalados y examinados que han sido en cuanto a su significado, tienen las características establecidas por la autora Maria Magdalena Ossandón Widow, quien a través de sus estudios expone la idea de que los elementos normativos no requieren de un especial proceso intelectivo y valorativo para su comprensión. Así también sostiene que es posible reconocer todavía otro intento de definición, que en este caso opera por exclusión: los términos descriptivos son *aquellos comprensibles sin necesidad de remitirse a algún -cualquier- género de normas.* Ello puede ocurrir porque a través de él se enuncia directamente una realidad sensorial, o porque las palabras por las que se expresa pertenecen al lenguaje normal y no pretenden ofrecer una significación diferente de aquella que se deduzca de su lectura[124].

Sujeto activo del delito.

[124] Ossandón Widow, Maria Magdalena. Los Elementos Descriptivos como técnica legislativa. Consideraciones críticas en relación con los delitos de hurto y robo con fuerza. Revista de Derecho, Vol. XXII- N°1, Julio 2009, consultada en versión digital el 05 /11/2022 en: https://www.scielo.cl/scielo.php?pid=S0718-09502009000100008&script=sci_arttext&tlng=pt

Al hablar de sujeto activo, también se hace referencia al autor directo, quien es el que realiza personalmente el delito, es decir, el que de un modo directo y personal realiza el hecho típico[125].

De la redacción del tipo de hurto de identidad, y de acuerdo a la interpretación literal del texto, puede desprenderse que en apariencia la acción típica puede ser cometida por cualquier persona.

Sin embargo, esto no es del todo cierto, puesto que, aunque el tipo no lo anuncie de manera expresa, sí se requieren ciertas cualidades especiales en el sujeto activo, las cuales se pueden advertir, analizadas que han sido las acciones del tipo. Estas cualidades necesarias, se deben considerar comunes para el delincuente informático en general y no solamente al sujeto activo del tipo de hurto de identidad. Se requiere evidentemente, que este cuente con conocimiento técnico adquirido formal o empíricamente, sobre informática, ingeniería social y sus derivados.

Sobre este punto de vista el Dr. Santiago Acurio del Pino, profesor de Derecho Informático de la Pontificia Universidad Católica del Ecuador, señala que las personas que cometen delitos informáticos, poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no

[125] Muñoz Conde, Francisco. Ob. Cit, pág. 219, consultado en versión digital el 05/11/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411307604?showPage=41

desarrollen actividades laborales que faciliten la comisión de este tipo de delitos[126].

El mismo autor Acurio del Pino sostiene un argumento bastante interesante, y cita que los estudiosos de la materia han catalogado a quienes cometen delitos informáticos, como parte de “los delitos de cuello blanco”. Esta aseveración se fundamenta en la existencia de características comunes: que el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Decididamente, el sujeto activo debe contar con habilidades, interés y capacidad de aprendizaje, puesto que el desarrollo tecnológico se encuentra en constante evolución. Asimismo, debe tener una mínima capacidad adquisitiva para acceder al hardware, software y red de internet para orquestar un ataque apto para conseguir su finalidad criminal.

Tiedemann, frente a esta definición nos dice “De manera creciente, en la nueva literatura angloamericana sobre estos temas se emplea el término “hecho penal profesional” (Occupational Crime). Con esta referencia al papel profesional y a la actividad económica, la caracterización del delito económico se fundamenta ahora menos en la respetabilidad del autor y su pertenencia a

[126] Acurio del Pino, Santiago. Delitos Informáticos: Generalidades. Consultado en versión digital, pág. 15 y ss., el día 05/11/2022 en: http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf

la capa social alta y más en la peculiaridad del acto (modus operandi) y en el objetivo del comportamiento[127].

Al considerar, las técnicas utilizadas por el sujeto activo para consumar la acción de suplantación y apoderamiento de la identidad de la víctima, evidentemente que debe existir un proceso de formación o instrucción, ya sea de manera formal o empírica, la cual le permite delinquir en la web. Esto significa, que el delincuente informático no tiene límites de fronteras, el aprovechamiento económico que en la mayoría de ocasiones se persigue, puede lograrlo incluso desde otro país o continente, deberá orquestar el ataque profesionalmente, de ahí que se comparten las posturas de los autores mencionados.

Entendiendo entonces que el sujeto activo en el delito de hurto de identidad, debe reunir habilidades y aptitudes técnicas, también es cierto, que un sujeto, aun cuando no tuviere una instrucción formal sobre informática, puede adquirir el conocimiento, desarrollar habilidades y volverse apto, para cometer delitos informáticos, ya que en la web existe un universo de información al alcance una búsqueda, la cual puede instruir a cualquiera que tenga interés de aprendizaje para echar a andar las diferentes técnicas de la *ingeniería social* idóneas para cometer delitos informáticos.

Por ello, ha sido acertada la redacción del tipo al dejar abierta la posibilidad para que el sujeto activo en el delito de hurto de identidad, pueda ser cualquier persona.

---

[127] Acurio del Pino, Santiago. Ob. Cit.,consutlado: http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf

Víctima (Sujeto pasivo).

El titular del bien jurídico es el *sujeto pasivo.* En este sentido, existen ya diversos puntos de vista en cuanto a los sujetos pasivos, y se ha concluido que las personas jurídicas pueden ser sujeto pasivo, respecto de algunos bienes jurídicos. El Estado mismo también puede ser sujeto pasivo *genérico presente en todo delito*[128]*.*

El sujeto pasivo del tipo en el delito de hurto de identidad, puede estar representado por una persona natural o jurídica (incluyendo el Estado), naturalmente capaz de ejercer sus derechos y contraer obligaciones. El sujeto pasivo además debe ser usuario de las TICS, titular de una identidad definida y confrontable con la realidad objetiva, que se corresponda con la identidad digital.

Cuando se trata de víctimas son personas naturales, pueden verse afectados bienes jurídicos individuales, como ya se ha venido mencionando. No debe perderse de vista, que las personas naturales pueden utilizar las TICS, para fines diversos. En la actualidad la mayoría de personas naturales utiliza las TICS para actividades ociosas, para informarse, para comunicarse, para conocer otras personas, para adquirir bienes, para contratar servicios, para el pago de servicios y la lista puede ampliarse de manera extensa.

Todos estos posibles escenarios van ubicando a la víctima en una posición de riesgo. En algunas ocasiones de manera voluntaria y bajo engaño

---

[128] Muñoz Conde, Francisco. Ob. Cit. Pág. 68, consultado en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411307604?showPage=41

proporcionan datos que forman parte de su identidad digital. Como sujetos pasivos y también como parte importante del *comercio electrónico,* se viene advirtiendo su trascendencia para el orden socioeconómico. Generalmente, las personas naturales titulares de bienes jurídicos, son las mismas sobre las que recae la acción delictiva, aunque también pueden existir supuestos de hecho en las cuales la acción delictiva recaiga en un tercero y el titular del bien jurídico sea quien experimente el resultado.

En el caso de las personas jurídicas, las cuales pueden ser instituciones que forman parte del sistema financiero, prestadoras de servicios, con giros diversos; estas además utilizan las nuevas tecnologías para la prestación de sus servicios o el ofrecimiento de sus productos en el mercado. Son claves para dinamizar el crecimiento económico, las que le han dado vida al *comercio electrónico*, como se ha señalado en el capítulo anterior. En el caso de las personas jurídicas, la acción recaerá sobre un individuo determinado, generalmente un dependiente y el resultado será percibido por la persona jurídica. Esto, es parte de la ficción jurídica que representa la existencia de la misma.

Cristian Borghello, sostiene que se pueden categorizar a cuatro tipos de víctimas:1. Los gobiernos. 2. Empresas privadas que manipulan gran cantidad de datos personales. 3. Los servicios financieros y principalmente 4. Los clientes y usuarios[129].

[129] Borghello, Cristian, Temperini, Marcelo G.I.. Suplantación de Identidad Digital como Delito Informático en Argentina. Simposio Argentino de Informática y Derecho. Consulado el 06/11/2022 en http://sedici.unlp.edu.ar/bitstream/handle/10915/124395/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Con la reciente pandemia por COVID 19, la mayoría de personas, naturales o jurídicas, empleamos los medios informáticos para la satisfacción de necesidad básicas. Las personas jurídicas potencializaron el uso de aplicaciones para el ofrecimiento de bienes o prestar servicios. Tomó protagonismo el servicio de entregas o *"delivery",* los cuales no se limitan a entregas de alimentos, si no a toda clase de gestiones que el contratante del servicio asigne. El factor común es el uso de las TICS, para que el desarrollo del comercio electrónico se dé efectivamente.

Circunstancias de tiempo, lugar y desarrollo tecnológico.

Ampliamente se ha analizado los beneficios, aportes y riesgos del desarrollo tecnológico. Esto último es el origen de la necesidad de tipificar nuevas conductas delictivas, entre estas el hurto de identidad.

Como parte del estudio del delito de hurto de identidad, es necesario tocar puntos esenciales para la consumación del delito, como ocurre en toda conducta punible, como circunstancias de tiempo y lugar. Normalmente el tiempo y lugar de la comisión del tipo no representa mayor complejidad, pues según las normas penales vigentes, será aplicable el principio de territorialidad, según el art. 8 del Código Penal vigente, que establece que la ley penal salvadoreña se aplicará a los hechos punibles cometidos total o parcialmente en el territorio de la República, o en los lugares sometidos a su jurisdicción[130].

[130] Código Penal de la República de El Salvador, aprobado mediante decreto legislativo N°1030, publicado en el Diario Oficial N° 105, Tomo N°335, en fecha 10 de junio de 1997.Consultado el 06/11/2022 en versión PDF.

Los tipos penales establecidos en el Código Penal, se entienden cometidos dentro del territorio de la República de El Salvador. Para imputar una acción típica a determinado sujeto, generalmente también hay precisión para relatar cuando ocurrieron los hechos de relevancia penal, así se anuncia concretamente el día, mes, año e incluso es posible manejar horas o momentos aproximados, que permiten ubicar al sujeto activo en un lugar determinado a una hora determinado. Tanto es así, que, si se logra acreditar a través de los medios probatorios idóneos y útiles, que el sujeto no se encontraba en el día, la hora en el lugar del hecho; es decir que si se logra sacar de la escena del delito al sujeto activo la tesis del ministerio público se desvanece.

Esto no es tan evidente en los delitos informáticos, que incluye al delito de hurto de identidad. En cuanto a la circunstancia de tiempo, es sumamente complejo establecer con precisión cuál fue el momento exacto de su cometimiento, tan solo debe mencionarse lo complejo que es incluso la investigación e individualización del sujeto activo en estos casos. Ciertamente, puede hacerse referencias a registros de actividades u operaciones detectadas a través de los mismos medios informáticos, las cuales pueden proporcionar un punto de partida. O como suele ocurrir en la mayoría de los casos, es que el parámetro de tiempo que se puede retomar es desde que la víctima percibe el resultado de la acción, la cual no puede ser precisa pues encierra una separación espacio-temporal del resultado. Esto último reafirma la dificultad de establecer esa circunstancia de tiempo en relación al cometimiento del injusto.

Por lo anterior puede indicarse que la identificación de la circunstancia de tiempo es compleja de establecer, pero pueden tomarse parámetros de tiempo según se perciba el resultado de la acción típica, que, aunque no será preciso,

pero brindará un punto de partida, sin perjuicio, que, así como el desarrollo tecnológico evoluciona, pueda existir una técnica de la informática que permita precisar sobre este aspecto.

En cuanto a la circunstancia del lugar o el escenario en donde se desarrolla la acción, debe señalarse el ***ciberespacio,*** el cual ha sido catalogado por algunos autores como *el espacio público más amplio que jamás haya conocido la humanidad*. Esta es una forma gráfica de anunciar la complejidad que representa para la investigación del delito como tal.

El ciberespacio se ha definido de la siguiente forma: *«el espacio global en el entorno de la Sociedad de la Información que consiste en el conjunto interdependiente de infraestructuras de TIC, y que incluye a Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados propios del Internet de las Cosas*[131]*.*

Otros autores, como Jonathan López Torres, define el ciberespacio el ciberespacio como *un entorno artificial de interacción económica, social y tecnológica que permite el libre desarrollo de individuos y naciones —sujetos de derechos y obligaciones— dentro y fuera de él, a partir del desarrollo tecnológico y del libre flujo de información*[132].

El ciberespacio no distingue fronteras entre países, de ahí que tiene sentido su definición como algo global. Todos los usuarios de las TICS, podemos tener

---

[131] Barrio Andrés, Moisés. Manual de Derecho Digital. 2ª Edición, Tirant lo Blanch, Valencia 2022,consultado en versión digital el día 06/11/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411470551

[132] López Torres, Jonathan. Ciberespacio & Ciberseguridad. Elementos Esenciales. Tirant Lo Blanch, Ciudad de México, 2020, pág.30, consultado el 06/11/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413550695

acceso al ciberespacio, la diferencia la hará la educación que se tenga sobre la conducta en este espacio.

Es necesario que el delito de hurto de identidad se ejecute en este espacio global y posteriormente su resultado sea sensible por la víctima en la realidad objetiva, pero siempre deberá incluir esa fase en la comisión del tipo en el ciberespacio. Incluso este punto, ha sido analizado como uno de los obstáculos en la investigación de delitos vinculados con la identidad digital cometidos por medio de las TIC´S, en El Salvador; ya que se reconoce esa característica de transnacional al mismo, que permite en cierta medida la impunidad en la mayoría de los casos.

La indeterminación del ámbito geográfico. Lugar y tiempo de comisión.

La red informática se caracteriza por prestar un servicio de comunicación que no reconoce fronteras es decir que al ser cometidos a través del "ciberespacio" las fronteras tradicionales entre los distintos Estados pierden eficacia o desaparecen, de ahí que un rasgo que sobresale de la delincuencia informática o del llamado delito informático es su extraterritorialidad y su intemporalidad.

En línea con lo expuesto, la inexistencia de fronteras reales es una característica intrínseca del internet o de la red informática, característica que ofrece un sin número de ventajas para las sociedades modernas; sin embargo, también ofrece inconvenientes para la persecución de actividades delictivas realizadas por medios informáticos. Esto plantea en primer lugar, la obligación para iniciar cualquier política criminal de conocer cuál es o puede ser el terreno de actuación a donde se ubica *"el internet"*, este es uno de los grandes problemas, por cuanto que no se trata del hecho que internet no esté en ningún

sitio o que este en todos, pues aun cuando no está en presencia física si sabemos que está en algún lugar. En realidad, los servidores en que se encuentra la información -de internet- no son más que discos duros y otras herramientas conectadas entre sí y con la Red, situados en edificios -también llamados centros de datos-, cuyo valor económico es incalculable, pues contienen desde nuestros datos bancarios hasta saberes multidisciplinarios que ya no se encuentran en los libros.

Sumando a lo anterior, dado que a la Red informática se puede acceder desde cualquier parte del mundo prácticamente al instante, el siguiente problema relacionado con la independencia geográfica de Internet lo encontramos en la dificultad de perseguir un ilícito de estas características. Un sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientas que la información está en otro lugar diferente de éstos. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados, ya que el sujeto activo no necesita moverse del lugar en el que se encuentra para realizar la conducta delictiva, como se expuso en el apartado relativo al perfil del delincuente informático.

El “derribo de las fronteras” derivado de las características de la delincuencia moderna transnacional y el fenómeno de “globalización” surgido del uso de internet por un operador situado en cualquier lugar del mundo, valiéndose de una computadora, un teléfono, un módem y un proveedor del servicio, hacen risibles los ejemplos tradicionales de “casos difíciles”, sobre la determinación de la ley aplicable en el espacio.

Sobre este tema, Cárdenas, se refiere específicamente a los delitos cometidos a través de Internet, y asevera que: *lo corriente será que se trate de* ***“delitos a distancia”*** *en los que la conducta no se inicia o no tiene lugar en el mismo Estado que la consumación, o de “delitos de tránsito”, donde tanto la conducta*

como la consumación tienen lugar en país extranjero, sirviendo el Estado de que se trate solamente de lugar de tránsito (por ejemplo, porque la información pasa por un servidor ubicado allí). En estas clases de delito (agrega la autora) *resulta necesaria una elaboración teórica para determinar cuál o cuáles son los Estados facultados para ejercer su jurisdicción y aplicar su derecho penal sobre el caso.*[133]

Por lo demás, el problema del lugar de comisión de esta clase de infracciones no parece que pueda ser resuelto por medio del reconocimiento de que tal lugar no es otro que el "ciberespacio"; es que, si así se admitiera, el fenómeno cultural del delito informático quedaría, por virtud de la vigencia general del criterio territorial en materia de validez espacial de la ley penal, fuera de la jurisdicción de cualquier Estado, lo que no parece una alternativa plausible.

Pero la disociación entre acción y resultado típico de los delitos informáticos no se verifica sólo espacial, sino también temporalmente por existir en las computadoras un reloj interno cuya temporalidad puede ser manipulada por el sujeto activo del delito.

Esta especial mención tiene justificación. Estos rasgos demuestran que la ilicitud informática en donde al igual que otras formas de delincuencia de las sociedades postindustriales, como el terrorismo, el narcotráfico, el tráfico de armas, etcétera, imponen repensar no sólo las categorías de la parte especial del derecho penal, sino también los estratos analíticos propios de su parte general. En cuanto a esto, cabe enfatizar que el derecho penal de la globalización es, desde algún punto de vista, eminentemente práctico, pues

---

[133] Cárdenas Claudia, El lugar de comisión de los denominados ciberdelitos, Política Criminal, n°6 (Chile 2008) 4, consultado en: http://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf?sequence=1&isAllowed=)

trata de proporcionar una respuesta uniforme o, al menos, armónica a la delincuencia transnacional, que evite la conformación de “paraísos jurídico-penales o paraísos informáticos”.

La existencia de estos “paraísos” resulta especialmente disfuncional cuando se trata de combatir una modalidad de delincuencia como la delincuencia cometida por medios informáticos, en la que el lugar y el momento de la intervención de los responsables pueden resultar perfectamente disponibles, razón por la cual los Estados deben legislar sobre estos temas para cerrar espacio al accionar delictivo de la delincuencia informática.

Relación de causalidad en imputación objetiva.

La teoría de la imputación objetiva elaborada por el alemán Claus Roxin, ha ganado muchos adeptos. Esta teoría plantea un análisis más rigoroso de la tipicidad, puesto que establece criterios para determinar si la acción delictiva logra establecer ese nexo causal con el resultado y si este puede atribuirse al autor, sin considerar como decisivo la finalidad que tenía el sujeto al momento de cometer el ilícito.

Bernardo Feijoo Sánchez, señala que la teoría de la imputación objetiva, como teoría del injusto específicamente penal, permite reducir la intervención de la pena en aquéllos supuestos en los que, utilizando una terminología tradicional, realmente resulta merecida y necesaria, excluyendo así una responsabilidad penal excesivamente formal. El mismo autor, desarrolla una serie de ideas las cuales nos permiten comprender que lo decisivo no es la voluntad del sujeto, sino la incompatibilidad de la conducta realizada con lo prescrito por la norma desde una perspectiva intersubjetiva. Así, Feijoo entiende la imputación

objetiva como una teoría global sobre la imputación de injustos penales a personas[134].

La teoría de la imputación objetiva plantea criterios a examinar:

- La creación de un riesgo no permitido. (falta de diligencia)
- La realización de ese peligro o riesgo en un resultado.
- La producción del resultado dentro del fin o ámbito de protección de la norma infringida[135].

A propósito del primer criterio se puede comentar que, tal como se ha venido exponiendo la utilización de TICS, y toda clase de medios informáticos, representan ya la existencia de ciertos riesgos. Pero sus usuarios, al ingresar los datos que conforman su identidad digital, lo hacen para fines específicos, en plataformas que se consideran confiables, sin embargo, el riesgo se encuentra implícito y así lo entiende también el legislador. Cuando el Sujeto activo con su accionar supera los niveles de riesgo permitidos, pues con su accionar ha lesionado o puesto en peligro los bienes jurídicos individuales o colectivos, su conducta es ilícita.

En cuanto al segundo criterio, que es la realización de ese peligro o riesgo en un resultado: también se advierte que, en el tipo de hurto de identidad, cuando el delincuente informático, consuma el delito y obtiene el resultado exigido por

---

[134] Feijoo Sánchez, Bernardo. Imputación objetiva en el Derecho Penal Económico y empresarial. Esbozo de una teoría general de los delitos económicos. Consultado el 06/11/2022 en versión PDF.

[135] Muñoz Conde, Francisco, Mercedes García Arán. Ob. Cit. Pág. 229 y ss. Consultada en versión digital 06/11/2022, en: https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

la norma, es decir, que suplanta, se apropia, o logra dañar, extorsionar, injuriar, amenazar, a la víctima, nos encontramos en la siguiente fase del análisis.

En cuanto al tercer criterio, este requiere que la producción del resultado se dé dentro del fin o ámbito de protección de la norma infringida. Usar internet y tecnologías de la información y comunicación para sustraer información personal de la víctima para usar su identidad en perjuicio suyo o de un tercero, está dentro del ámbito de protección que el legislador le dio al regular el delito de Hurto de identidad. En este caso, resulta complejo pensar en un supuesto, que permita a una acción negligente lograr que se de el resultado, tampoco cabe hablar sobre una tentativa, ya que el resultado es esencial para que la víctima conozca sobre la existencia del delito que se ha perpetrado en su contra.

Debido a la especialidad de la redacción del tipo de hurto de identidad, sería excesivamente especial un supuesto, donde no se advirtiera el cumplimiento de los criterios establecidos por la teoría de la imputación objetiva, ya que dicho tipo requiere la concurrencia de supuestos específicos vinculados con las capacidades técnicas del sujeto activo, las cuales harán viable la obtención del resultado dispuesto en la norma, a través del ataque por medio informáticos. A menos que sucediera que la misma víctima se ubique en una posición de riesgo extremo (sin necesidad que el sujeto activo cree el riesgo no permitido) y postee o publique fotografías de una tarjeta de crédito de la cual es titular, a través de perfiles de redes sociales con acceso público de su contenido, lo que significaría que cualquier usuarios de la TICS podría acceder a su información crediticia, nombre, imagen, siendo este uno de los supuestos inusuales a los que podría referirse Claus Roxin.

4.1.2. TIPO SUBJETIVO.

El tipo subjetivo comprende el contenido de la voluntad que rige la acción.
Una vez superado el análisis de todos los elementos que componen el *tipo objetivo* es momento de realizar al análisis del tipo subjetivo. En materia probatoria, este elemento subjetivo del tipo se convierte en uno de los retos más grandes de probanza. No obstante, ello, debido a las notas características del tipo de hurto de identidad, la voluntad del sujeto activo se revela con su misma acción, por tratarse de acciones complejas y sofisticadas.

Dolo.

Al hablar de dolo, este se entiende como la conciencia y voluntad de realizar el tipo objetivo de un delito[136]. De la definición citada se desprenden sus elementos:
Elemento intelectual: se hace referencia a la capacidad de comprender del sujeto activo que su actuar es ilícita, es decir que tiene pleno conocimiento que la acción que realiza se encuentra prohibida por la norma.

Al hablar del dolo, no podemos obviar el perfil del delincuente informático, se puede entender que el sujeto conoce que acceder a la información de otros usuarios de las TICS, tomar el lugar de estos o apropiarse de cuentas, perfiles, en donde la víctima maneja su identidad digital, es un hecho delictivo, que esta prohibido. De lo contrario seria un supuesto de error de tipo.

---

[136] Muñoz Conde, Francisco, Mercedes García Arán. Ob. Cit. Pág. 267 y ss. Consultada en versión digital 06/11/2022, en: https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

El hurto de identidad es un delito eminentemente doloso. Pensar en un supuesto que permita visualizar la concurrencia de un actuar negligente resulta extremo. Esto debe ser así, puesto que hemos analizado al hurto de identidad como un delito de resultado, es decir, que el sujeto activo, quiere obtener el resultado, es precisamente la obtención del resultado lo que le motiva a actuar, por lo que no queda cabida para un dolo eventual o la negligencia, ni siquiera en el caso más sencillo. Por ejemplo: El caso donde un adolescente de dieciséis años, con habilidades básicas o avanzadas, de informática sin hacer uso de técnicas sofisticadas sustraiga o utilice la identidad digital de su padre y se apodere mediante el uso de su computadora portátil y las TICS, resultando que obtiene un beneficio para si en perjuicio de su padre. Aun en este caso, el joven, tiene conocimiento que dicha identidad no le pertenece y que dicha acción es un delito, pero, desde el inicio, proyecta que aun en caso de ser descubierto por la víctima (su padre), éste, probablemente le castigue, pero no se plantea la posibilidad de sufrir otras consecuencias.

Elemento volitivo:

Para actuar dolosamente no basta con el mero conocimiento de los elementos objetivos del tipo, es necesario, además, querer realizarlos. Este querer no se confunde con el deseo o con los móviles del sujeto. El elemento volitivo supone la voluntad incondicionada de realizar algo (típico) que el autor cree que puede realizar[137].

[137] Muñoz Conde, Francisco, Mercedes García Arán. Ob. Cit. Pág. 267 y ss. Consultada en versión digital 06/11/2022, en: https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

El sujeto activo, primero que comprende que su acción es ilícita, manifiesta su voluntad y la dirige sus acciones a través de esta. Como se ha venido sosteniendo, ese conocimiento y voluntad, debe ser obra de un sujeto activo con destrezas en el uso de las tecnologías, si es que nos ubicamos en un supuesto del tipo donde la víctima sea una persona jurídica y el ataque se dirige a la misma y no a otra persona, porque quiere perjudicar o sacar provecho de esa víctima. Hay diferentes aspectos que motivan ese ataque para esa víctima concreta, es decir, el sujeto activo conoce que de en caso de consumar la acción, indudablemente el resultado será obtener el beneficio que señala el tipo. Por el ello quiere cometer la acción.

Los textos doctrinarios sostienen que en los delitos de resultado (como se ha clasificado al hurto de identidad), consisten en la lesión de un jurídico, por tanto, el dolo debe ir también referido al resultado. Por este motivo, debería de descartarse en este caso la posibilidad de un dolo eventual para el caso de del hurto de identidad.

En El Salvador, no se cuenta con una definición legal del dolo, aunque en el art. 4 del Código Penal vigente, hace referencia al principio de responsabilidad, el cual señala que la pena o medida de seguridad no se impondrá si la acción y omisión no ha sido realizada con dolo o culpa. En lo sucesivo, el texto hace referencia reiteradamente al dolo o acciones dolosas.

Error de Tipo.

El error de tipo está relacionado con el conocimiento que el sujeto activo tiene sobre los elementos objetivos del tipo. Una distorsión en estos generaría un

error de tipo. Previo a realizar el análisis correspondiente al hurto de identidad, debemos repasar el contenido del error de tipo de manera muy concreta:

"En principio, la Teoría del Error en Derecho Penal, distingue entre error de tipo y error de prohibición. El primero, excluye el dolo si es invencible, o puede llegar a sancionarse la acción como culposo, si concurren los requisitos de éste. El ámbito que comprende está referido al desconocimiento de elementos del correspondiente tipo objetivo, es decir que puede recaer en la acción, curso causal, resultado, cualidades especiales de autor. Mientras que la segunda clase, tiene como objeto la prohibición jurídico penal, de ahí que esté comprometida la conciencia de la antijuridicidad y por esta vía la culpabilidad misma, la que será excluida cuando se trate de un error invencible, o dará lugar a una responsabilidad atenuada especialmente si es vencible. A su vez, el error de prohibición puede ser directo o indirecto, según que el sujeto actúe creyendo que su comportamiento no es delito o bien que, conociendo la prohibición penal en general, supone que en el obrar concreto, le ampara una causa de justificación. Una sub clasificación más, el error puede estar referido a la existencia de la causa de justificación (error de permisión) o respecto de los presupuestos de ésta,". (Ref. 441- CAS-2009, del 06/05/2011)[138]

Retomando el análisis sobre el tipo de hurto de identidad, partiendo de que se trata de un delito doloso, el cual exige que el sujeto activo tenga pleno conocimiento de los elementos del tipo, debemos examinar sobre la viabilidad de que pudiera surgir un supuesto de hecho en donde exista un error de tipo

[138] Sentencia definitiva emitida por la Sala de lo Penal de la Corte Suprema de Justicia, en recurso de casación, emitida en fecha 14/01/2013, consultada en versión PDF el 08/11/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2013/01/9D457.PDF

invencible, de tal manera que se pueda excluir el dolo y en consecuencia la sanción o responsabilidad penal.

Así el error de tipo podría recaer sobre la acción según se señala. Podría suceder en el caso que A quiere apropiarse de la identidad de B para extorsionar C. Para ello contrata a D, y le hace creer que su cuenta de Facebook ha sido hackeada y quiere recuperarla, haciéndole creer que la cuenta de B, es la propia. Bajo esa creencia la acción de “recuperación” de dicha cuenta mediante técnicas de la informática, D ingresa al perfil de B y lo pone a disposición de A, procediendo este último a generar el resultado. Aunque el ejemplo, ya vendría introduciendo el tema de la autoría y la participación, lo que se estudiará posteriormente.
Aunque no es sencillo, pensar en una situación de esta naturaleza, por varios motivos: lo novedoso del tipo, la complejidad de la acción, la naturaleza dolosa del tipo, etc., no pueden desecharse supuestos, y así deberá analizarse cada elemento, podrían ser elementos normativos o descriptivos del tipo.

En El Salvador, el Código Penal hace referencia al error de tipo y de prohibición con error invencible y error vencible, en el art. 28. Así menciona que si atendidas las circunstancias de hecho (elementos objetivos del tipo) y las personales del autor, la infracción será sancionada en su caso como culposa.

Autoría y Participación.

El Código Penal de El Salvador establece una definición legal sobre los autores directos o coautores, en el art.33:
"Son autores directos los que por sí o conjuntamente con otro u otros cometen el delito.”

La definición legal únicamente hace referencia a las palabras “por sí”, lo que puede entenderse que se refiere a la persona que ejecuta la acción de propia mano, y también genera la idea de que el autor actúa solo o individualmente. Esto podría adecuarse al concepto de autoría material según lo expresado por Héctor Olásolo Alonso, quien expone que: “l*a autoría material tiene lugar cuando un individuo realiza materialmente los elementos objetivos del delito con el elemento subjetivo requerido por el mismo1. El artículo 25(3) (a) ER2 se refiere a la misma mediante la expresión cometer un delito “por sí solo”.*[139]

La definición legal también contempla la figura de la coautoría, de manera que se plantea la posibilidad de que la acción pueda ser ejecutada por más de una persona, lo cual implicaría que estos tendrían un co-dominio del hecho. Lo anterior, también sería aplicable al tipo de hurto de identidad, pues no se advierte de la redacción del tipo una circunstancia que impida tal supuesto.

A propósito de este tema, el Tribunal Primero de Sentencia de Santa Tecla en Sentencia definitiva emitida en fecha 13 de diciembre de 2006, señala que *con la teoría de la autoría, se pretende determinar quién ha tenido el papel principal entre todos los partícipes, a prima facie decir quien es autor es muy sencillo si la pregunta se contesta desde el punto de vista de los tipos penales que son concebidos como si los llevara a cabo una sola persona; el problema se complica cuando varios contribuyen a la realización de los delitos y es preciso separar las diversas contribuciones para determinar cuáles de ellas determinan la autoría.*[140]

---

[139] Olásolo Alonso, Héctor. Tratado de Autoría y Participación en Derecho Penal Internacional. Tirant lo Blanch, tratados. Valencia 2013, consultado el 09/11/2022, en versión digital en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788490334287

[140] Sentencia Definitiva emitida por el Tribunal Primero de Sentencia de Santa Tecla, el día trece de diciembre de 2006, en causa judicial con referencia P0401-105-2006, consultada el día 09/11/2022 en versión digital: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php

De la redacción del tipo de hurto de identidad, se desprende que la ejecución del tipo puede desarrollarse por un individuo. El inciso 2 del tipo exige una serie de resultados, los cuales podrían ser cometidos por un sujeto diferente, dejándose abierta la posibilidad de una coautoría. También puede resultar viable para la comisión del tipo la existencia de una autoría mediata (utilizar a otro para cometer el delito), suscitándose todas las genuinas formas de autoría, tal como algunos autores les denominan.

Al continuar sumergiéndonos en el tema se debe hablar sobre la participación y debemos citar algunos puntos de vista en relación con la diferencia entre esta y la autoría:
Muñoz Conde, para referirse a la diferencia entre participación y autoría *sostiene que la participación es accesoria; la autoría, principal*[141]*.*

Sobre este mismo punto, existe pronunciamiento a nivel de criterio jurisdiccional puesto que en Sentencia definitiva el Tribunal Primero de Sentencia de San Salvador expone, precisamente en relación a ese carácter accesorio de la participación delincuencial: *La distinción entre autoría y participación es una distinción material, independiente de que la ley decida castigar los autores y los partícipes del mismo modo o establezca una penalidad distintas para unos y para otros, en cualquier caso subsiste que la conducta del partícipe solamente constituya la realización del delito a través*

[141] Muñoz Conde, Francisco, Mercedes García Arán. Ob. Cit. Pág. 433 y ss. Consultada en versión digital 09/11/2022, en: https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

de la conducta del autor, de suerte que el injusto del delito típico no pueda atribuirse al partícipe si no se imputa previamente al autor[142]*.*

El criterio adoptado para realizar esa distinción se encuentra dado por el criterio objetivo- material del *dominio del hecho,* lo que implica que es el autor quien tiene la potestad de definir el cometimiento del hecho delictivo y no el partícipe. Este criterio, no es el único, pero si el adoptado por los tribunales salvadoreños, mayoritariamente.

Miguel Díaz y García Conlledo, sostiene que *partícipes son los sujetos que intervienen en un delito, sin ser autores del mismo (es decir, desde la caracterización de la autoría que aquí se sostiene, sin realizar la acción típica nuclear, sin determinar objetiva y positivamente el hecho), siempre y cuando sus conductas estén recogidas en alguno de los preceptos del CP que describen formas de participación.*[143] De manera mas sencilla Muñoz Conde, hace referencia a la participación como la cooperación dolosa en un delito doloso ajeno.

Sobre el tema existe abundantes textos doctrinales, pero a fin de concretar debe decirse, que las formas de participación que sostiene la doctrina y que se corresponde con nuestro ordenamiento jurídico, se encuentra en el art. 36 del Código Penal, que relaciona la complicidad necesaria y la complicidad no necesaria. En el texto legal se confirma la teoría del dominio del hecho, así

---

[142] Sentencia definitiva dictada por el Tribunal Primero de Sentencia de San Salvador, en fecha 09 de agosto de 2002, en causa judicial marcada con referencia P0101-48-2002, consultada el 09/11/2022 en versión digital en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php#

[143] García Conlledo Miguel Díaz y. Autoría y Participación. Revista de Estudios de la Justicia, N° 10, año 2008, consultada el 09/11/2022 en versión digital en: file:///C:/Users/damaris.martinez/Downloads/laguirre,+Journal+manager,+15219-41640-1-CE.pdf

como el carácter accesorio del partícipe, que puede también configurarse en el delito de hurto de identidad. Tal es así que la pena, para autor y partícipes se señala de manera diferenciada por el legislador, determinándola de una manera atenuada para el partícipe, como resulta ya razonable.

Un supuesto podría suscitarse en los casos, en los cuales se da un hurto de identidad y la víctima además es una persona jurídica. Un cómplice podría ser un empleado de la empresa (*llamados insiders por la doctrina*) que proporcione datos que conforman la identidad de la víctima para que el autor lleve a cabo la acción de suplantar la identidad de otro. Es una cooperación necesaria y aún así el autor de la acción de suplantar tuvo el dominio de ese hecho delictivo.

A manera de conclusión, los supuestos a considerar en el tipo de hurto de identidad pueden ser tan variados, puesto que la redacción del tipo abre las posibilidades de ejecutarse de formas sencillas a lo más complejo, lo que también permite plantearnos la concurrencia de las formas de autoría y participación.

Elementos Especiales de Autoría.

Los elementos especiales de autoría que se valoran a nivel de tipo subjetivo son aquellas cualidades que tiene el sujeto[144].

[144] Serrano, Dr. Armando Antonio, Coordinador del Programa de Maestría en Derecho Penal Económico, Universidad de El Salvador, comunicación personal, el 09/11/2022.

Cuando se analizó al sujeto activo, ya se venía vislumbrando uno de los elementos especiales en el autor del tipo de hurto de identidad, puesto que necesariamente el autor debe tener un conocimiento al menos básico sobre el manejo de las tecnologías de la información y comunicación, aun sosteniendo en todo momento que el autor puede ser cualquier persona. Esta cualidad le permite al autor del tipo, obtener el resultado requerido. Puede tratarse de conocimiento, habilidades, destrezas o toda clase de características parte del autor que generan en el pensamiento de este la determinación necesaria para cometer el hecho.

Sobre este punto, ya Santiago Acurio del Pino había precisado otros elementos especiales, (aunque no los desarrolla con el concepto de elementos especiales de autoría propiamente) como algunas características propias del autor de delitos informáticos, las cuales son resultado de la formación del individuo, algunas incluso propias de la personalidad del autor del hecho, parte de su fuero interno, que le hacen determinarse para cometer el delito. Así el autor citado cita *que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos*[145].

Incluso el mismo autor Curio del Pino, menciona un dato estadístico interesante, que además confirman los elementos especiales de autoría identificados para el delito de hurto de identidad, publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Números 43 y 44), en donde se 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada

[145] Acurio del Pino, Santiago., Ob. Cit pág. 16.

(Insiders). Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (Outsiders). De más esta aclarar, que sería aplicable en los casos en donde la víctima sea una persona jurídica, mayoritariamente.

4.2 ANTIJURICIDAD.

En el desarrollo del análisis del tipo de hurto de identidad, es necesario llevar a la acción hacia otro "filtro" en el sendero de la teoría del delito que nos conduce hacia la antijuricidad. Esto es parte esencial para eliminar todo tipo de obstáculos que pudieran interponerse entre el autor de la acción y un potencial juicio de reproche.

El término antijuricidad o antijuridicidad significa contradicción con el Derecho y expresa que una acción u omisión es contraria, esto es, infringe, viola o contradice la ley.
Sin embargo, no debe identificarse la antijuricidad con la ilegalidad o tipicidad, pues esta última exige que la conducta en cuestión sea contraria al orden social (esto es, antijurídica) y que, además, comporte una infracción de lo dispuesto en una norma de Derecho.[146]

Los autores que escriben sobre el tema ponen especial atención a establecer distinciones entre el concepto de antijuricidad y otros como el injusto, ilegalidad y tipicidad, pues se considera que estos no deben emplearse de manera

[146] de Vicente Martínez, Rosario. Vademécum de Derecho Penal. 5ª edición revisada, actualizada y ampliada. Tiran lo Blanch, Valencia 2018. Consultada el 11/11/2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491901969

unívoca. Para Muñoz Conde, la antijuricidad es el predicado de la acción y explica el injusto como un sustantivo.

Fernando Molina Fernández, expone que *la antijuridicidad en un sentido restringido, se, utiliza habitualmente por quienes parten de un sistema tripartito de exposición de la teoría del delito, para referirse al segundo momento de la caracterización de la acción, posterior a la tipicidad y previo a la culpabilidad, en el que sustancialmente se examina si la acción típica es, además, contraria a derecho, para lo cual se tienen en cuenta la concurrencia de causas de justificación y, eventualmente, algún otro elemento*[147].

Conviene preguntarse si la acción cometida por el sujeto contradice la norma, y si esa contradicción conlleva además una vulneración relevante de un bien jurídico protegido por la norma, sin la concurrencia de ningún excluyente de responsabilidad, para poder continuar hacia una etapa de reproche.

4.2.1. Formal.

La definición mayormente utilizada para hacer referencia a la antijuricidad formal es *"La contradicción de un hecho con el Ordenamiento jurídico recibe el nombre de antijuricidad formal".*[148]

Se dice que es formal, porque no se hace ninguna referencia a valoraciones en cuanto a la vulneración de bienes jurídicos. Para tener mayor claridad sobre esta, Fernando Molina Fernández, en su tesis doctoral cita definiciones de autores reconocidos por sus aportes al estudio del Derecho Penal:

---

[147] Molina Fernández, Fernando. Tesis Doctoral: Antijuridicidad Penal y Sistema del Delito. Universidad Autónoma de Madrid. Consultada el 11/11/2022 en versión digital en file: https://www.editorialmetropolitana.cl/wp-content/uploads/2021/07/%C3%8Dndice-Antijuridicidad-penal-N%C2%B0-60.pdf

[148] de Vicente Martínez, Rosario, Ob. Cit. Pág. 57.

Von LISZT, Tratado, II, p. 336: «El acto es formalmente contrario al Derecho, en tanto que es transgresión de una norma establecida por el Estado, de un mandato o de una prohibición del orden jurídico»;
MEZGER, Tratado, 1, p. 279: «Actúa antijurídicamente el que contradice las normas objetivas del Derecho», p. 286-287: «sólo es correcto concebir el injusto como una lesión del orden objetivo del Derecho, como una perturbación de la manifestación de voluntad reconocida y aprobada por el Derecho mismo»;
WELZEL, AT, p- 51: «La antijuridicidad es siempre la contrariedad entre un comportamiento real y el orden jurídico»;
MAURACH / ZIPF, PG, I, § 24 nm. 20: «Una acción es formalmente antijurídica cuando se halla en oposición a un mandato normativo contenido en una norma penal»;

JESCHECK, Tratado (4a), p. 210: «Antijuridicidad significa "contradicción con el Derecho. Esta contradicción ha de entenderse del siguiente modo: el legislador establece para la protección de la convivencia del hombre en la sociedad preceptos vinculantes de comportamiento que se denomina normas jurídicas. [...] Por ello hay que ver la esencia de la antijuridicidad en un comportamiento contrario al deber de actuar o abstenerse establecido en una norma jurídica.[149]

Vemos como otros autores introducen conceptos como el Estado, y algunas precisiones en cuanto a considerar la norma como una manifestación de voluntad que se reconoce a través del derecho. En el caso de MEZGER, la explica como una lesión del orden objetivo del Derecho. Estas notas distintivas que se vienen subrayando, detallan la primera fase del análisis, pues debe

[149] Molina Fernández, Fernando. Ob. Cit.

complementarse para determinar si la acción antijuridica no solamente desde la perspectiva formal, si no *material* como a continuación se expresa.

En el delito de hurto de identidad, esta clase de análisis se hacen más sencillos para el caso de supuestos donde la víctima sea una persona natural, puesto que, en el caso de personas jurídicas, siempre trae una dosis adicional de complejidad.

Podemos plantearnos un supuesto sobre una antijuridicidad formal en la que A suplante la identidad de B, haciendo uso de las tecnologías de la información y comunicación, para difundir información relacionada con el uso de un producto, o manifestar alguna aseveración sobre una preferencia gastronómica o la recomendación de un restaurante, probablemente porque vende el producto o presta el servicio en mención. Formalmente, ejecutó la acción y se puede apreciar la contradicción con la norma tal como se ha definido anteriormente. Es por ello, que esa primera apreciación debe complementarse, para seguir en la determinación de la concurrencia de los elementos subjetivos del tipo.

4.2.2. Material.

Al hablarse de antijuricidad material, ésta se define como *la ofensa al bien jurídico que la norma protege recibe el nombre de antijuricidad material.*
La antijuricidad material se basa en su carácter de lesión o puesta en peligro de un bien jurídico (desvalor de resultado), como consecuencia de un comportamiento guiado por la voluntad de modo doloso o imprudente (desvalor de acción).[150]

[150] de Vicente Martínez, Rosario, Ob. Cit. Pág. 57.

Fernando Molina Fernández, *establece que la antijuridicidad hace referencia a la lesividad material de la acción para bienes jurídicamente protegidos (perspectiva material del injusto como lesividad para bienes jurídicos).* Habiendo sido este asunto objeto de suficiente estudio de parte de los estudiosos de la materia, conviene nuevamente citar las definiciones de estos, para indicar significado y alcance en relación a la antijuricidad material:

Von LISZT, Tratado, II, p. 262: «El delito es [...] un acto contrario al derecho; es decir, un acto que, contraviniendo, formalmente, a un mandato prohibición del orden jurídico, implica materialmente la lesión o peligro de un bien jurídico», p. 336:
«El acto es materialmente ilegal, en cuanto significa una conducta contraria a la sociedad (antisocial). El acto contrario al Derecho es un ataque a los intereses vitales de los particulares o de la colectividad, protegidos por las normas jurídicas; por consiguiente, una lesión o un riesgo de un bien jurídico»;
MEZGER, Tratado, I, p. 329: «El contenido material del injusto de la acción típica y antijurídica es la lesión o la puesta en peligro de un bien jurídico (del objeto de protección, del objeto de ataque)»;
WELZEL, AT, p. 48: «Una acción se convierte en delito cuando lesiona el orden social en una forma regulada en los tipos legales y además puede ser reprochado a la culpabilidad del autor»;
MAURACH /ZIPF, PG, I, § 24 nm. 20: «la antijuridicidad material alude al contenido del concepto de antijuridicidad y se relaciona con el bien jurídico protegido en la respectiva norma penal»;
JESCHECK, Tratado (4B), p. 210-211: «En sentido material, una acción es antijurídica en atención al menoscabo del bien jurídico protegido por la correspondiente norma»;

RODRÍGUEZ MOURULLO, PG, p. 321: «En la medida en que la acción aparece como una ofensa (lesión o puesta en peligro) de los bienes protegidos por las normas jurídicas, se habla de antijuridicidad material»;
MIR PUIG, PG, p. 111 nm. 14: «la antijuridicidad penal se entenderá aquí sólo como juicio de desvalor expresivo de la nocividad jurídico-penal de un hecho, en cuanto el mismo supone una lesión o puesta en peligro de un bien jurídico-penal no justificada por un interés jurídico superior»;
COBO DEL ROSAL / VIVES ANTÓN, PG, p. 273: «se concibe objetivamente la antijuridicidad cuando se estima antijurídica una conducta en razón de su lesividad efectiva o potencial»;
JAKOBS, AT, § 6 nm. 51: «Injusta es una acción que no es socialmente tolerable»;

OCTAVIO DE TOLEDO / HUERTA TOCILDO, PG, pp. 160-161: «la antijuridicidad penal es aquella característica imprescindible del delito conforme a la cual para poder estimar que un comportamiento es delictivo se hace menester que éste infrinja, sin causa que lo justifique, la prohibición de hacer o de omitir expresada por la norma y destruya, menoscabe o ponga en peligro -real o potencialmente- el bien jurídico que con ella se intenta amparar»;
ROXIN, AT, I, § 14 nm. 4: la acción «es materialmente antijurídica en cuanto en ella se manifiesta una lesión de bienes jurídicos socialmente dañina que no puede ser suficientemente combatida con medios extrapenales», § 7 nm. 22: «La concepción material de injusto como hecho socialmente dañoso y de la culpabilidad como reprochabilidad, que procede del sistema neoclásico y que no fue discutida por el sistema finalista, se ha mantenido en el concepto moderno de delito[151]»

[151] Molina Fernández, Fernando. Ob. Cit.

De las definiciones citadas podemos comentar sobre las notas importantes que estas nos proporcionan: la necesariedad de no solamente la lesión de un bien jurídico, si no también, la puesta en peligro de alguno de estos. Que, además, esa lesión o puesta en peligro se produzca sin la concurrencia de una causa de justificación, lo cual conduciría a establecer el juicio de reprochabilidad o por el contrario, detenernos en el camino que se ha recorrido para analizar la acción.

4.2.3 Causas de Justificación.

Al hablar de causas de justificación inmediatamente viene a nuestra mente su efecto en cuanto a excluyentes de responsabilidad penal. Las causas de justificación son supuestos en los cuales se enumeran por el legislador, aquellos casos en los que es permitido cometer la acción penalmente relevante, sin que se produzca el reproche de culpabilidad y en consecuencia se libere de responsabilidad penal al autor de la conducta.

Muñoz Conde expone con claridad, y es que en este sentido la acción es típica pero debido a la causa de justificación entonces es lícita.

El Código Penal, en su parte especial, establece en el artículo 27, seis excluyentes de responsabilidad penal, sobre los mismos se pueden hacer algunas apreciaciones.

Los excluyentes establecidos en los números 1, 2, 3, 5 y 6, constituyen causas de justificación, porque recaen sobre la acción la cual, evidentemente contiene un elemento subjetivo, (es decir el conocimiento del autor de la acción sobre

la existencia de la causa de justificación al momento que desarrolla la conducta típica) y al realizar el análisis de sus efectos se tiene por justificada o lícita la conducta típica.

En estos casos, suele ser más sencillo pensar en un supuesto en el que la acción tenga una connotación de violencia, como en delitos de lesiones o amenazas. En el caso de hurto de identidad, es complejo pensar que exista en un momento determinado algunas de estas causas de justificación, mas no imposible, porque eso lo vendrá proporcionando la casuística.

Cada una de las causas de justificación implica que el sujeto activo ejecute la acción con pleno conocimiento de su ilicitud, lesionando o poniendo en peligro el bien jurídico protegido, pero, por circunstancias que se vienen suscitando en cuanto a elementos externos, los cuales deben ser desarrollados por otras personas, con una finalidad criminal, o al menos resulta razonable plantearlo de esta manera.

En el delito de hurto de identidad, no por lo novedoso, porque ya su estudio se viene realizando desde algunos años, si no, por la poca judicialización de casos, que no ha permitido someter de manera suficiente al conocimiento jurisdiccional esta clase de tipos penales, lo que no ha permitido que la casuística introduzca estas probabilidades de supuestos y el Juzgador emita un criterio sobre ello.

Incluso, los estudios relacionados con los delitos informáticos, aún aquellos que tratan el hurto de identidad propiamente tal, tampoco se han planteado la posibilidad de que la acción sea ejecutada bajo el esquema de las causas de justificación, como la legítima defensa, estado de necesidad, la no exigibilidad

de otra conducta o la colisión de deberes. No obstante, puede hacerse un esfuerzo argumentativo a través de esta investigación:

La causa de justificación No 1:

Quien actúa u omite en cumplimiento de un deber legal o en ejercicio legítimo de un derecho o de una actividad lícita;

En el caso de la investigación de delitos informáticos, pudiera darse una causa de justificación, debido a la complejidad que representan las investigaciones de estos delitos, entre los cuales se encuentra el delito de hurto de identidad. Según lo regula la reforma del artículo 259, el cual introdujo el artículo 259-D del Código Procesal Penal, que establece al agente encubierto digital como una técnica de investigación informática. Es así como el legislador habilitó a la Fiscalía General de la República para ordenar a la Policía Nacional Civil, operaciones digitales encubiertas, en la tramitación de la investigación de los delitos que establece la Ley Especial Contra Delitos Informáticos y Conexos.
El agente policial en cumplimiento de su deber legal de investigación del delito, puede constituirse como un agente encubierto, aun suplantando o apoderándose de la identidad de la víctima o un tercero, con la finalidad de esclarecer un hecho delictivo denunciado.

Causa de justificación N°2

2) Quien actúa u omite en defensa de su persona o de sus derechos o en defensa de otra persona o de sus derechos, siempre que concurran los requisitos siguientes:

a) Agresión ilegítima;

b) Necesidad razonable de la defensa empleada para impedirla o repelerla; y,

c) No haber sido provocada la agresión, de modo suficiente, por quien ejerce la defensa.

Podríamos plantear que: A, sufre un ataque aparentemente a través de sus propias cuentas de correo electrónico, mediante una suplantación de identidad, comienza a recibir mensajes en su bandeja de entrada de carácter extorsivo para que entregue cantidades de dinero a través de transacciones de la *CHIVO WALLET,* exigiendo la cantidad de CINCO MIL DÓLARES en Bitcoin, puesto que de lo contrario comenzaran a difundir su información personal y crediticia por medio de las TICS. A no tiene dinero, pero decide deposita DIEZ DÓLARES a la cuenta de *CHIVO WALLET* con la finalidad de rastrear la cuenta, así lo hace y hackea la cuenta de Chivo wallet del extorsionista para vincularla con la identidad de su atacante, y resulta ser que la cuenta está asociada a B, que aunque no introdujo un número de dui propio, se rastrea mediante el dispositivo utilizado (aparato telefónico, computadora, etc), así actuó en legítima defensa desvirtuando o repeliendo el ataque, advirtiéndose que se suscitan las tres condiciones establecidas en la disposición legal.

Causa de justificación No 3, 5 y 6:

3) Quien actúa u omite por necesidad de salvaguardar un bien jurídico, propio o ajeno, de un peligro real, actual o inminente, no ocasionado intencionalmente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que la conducta sea proporcional al peligro y que no se tenga el deber jurídico de afrontarlo;

5) Quien actúa u omite bajo la no exigibilidad de otra conducta, es decir, en circunstancias tales que no sea racionalmente posible exigirle una conducta diversa a la que realizó; y,

6) Quien actúa u omite en colisión de deberes, es decir cuando existan para el sujeto, al mismo tiempo, dos deberes que el mismo deba realizar, teniendo solamente la posibilidad de cumplir uno de ellos.

Estas evidentemente que contienen notas distintivas entre sí, pero se procederá a plantear algunas cuestiones para valorar su posible apreciación:

Por ello, se podría plantear (sujeto a discusión), que: A es un técnico informático empleado de una persona jurídica (*insider*), con acceso a los datos que conforman la identidad de ésta víctima, y este es obligado a proporcionar esa información bajo la amenaza real y suficiente de causarle la muerte a un ser cercano (hijo, padre, madre, etc.) o su misma persona. El sujeto actúa por la necesidad de proteger su propia vida o de un pariente y proporciona todo lo necesario para que se dé el apoderamiento. Como se ha dicho, esto sería siempre discutible.

Lo anterior, porque ¿Cuál sería el sentido de que el delincuente informático utilice a otro para ejecutar el apoderamiento o suplantación de identidad cuando tiene a su disposición gran variedad de técnicas de la *ingeniería social*? Puede echar mano de malware y ejecutar la acción de *propia mano.*

También podríamos preguntarnos, ¿Constituiría en el caso la no exigibilidad de otra conducta?, podría exigirse la denuncia de las coacciones o amenazas sufridas por el informático -*insider*- y en ese orden de ideas analizar la viabilidad o no de las causas de justificación, lo que significa, no es una tarea sencilla, justificar o convertir en lícita las acciones típicas que conlleva el delito de identidad digital, tal como se ha sostenido a lo largo de todo este capítulo y ello se debe al carácter sofisticado del tipo, como también ya se dijo.

En un primer momento, podría exponerse que la existencia de esta clase de causas de justificación es compleja, más no imposible, si alguna de estas se

alegare sería aun así discutible la validez de la misma, aunque este asunto no ha sido abordado en ese nivel de profundidad.

4.3 CULPABILIDAD.

Ya se ha transitado buena parte del camino trazado por la teoría general del delito, arribando al último estadio de examen para determinar si la conducta es penalmente relevante en el delito de hurto de identidad.

Muñoz Conde, expone su desacuerdo en cuanto al abordaje tradicional de la culpabilidad como, esa exigibilidad de una conducta diferente, y lo fundamenta en que, se trata de una situación imposible de demostrar, si el sujeto que ejecutó la acción podría o no haber actuado de forma diferente.

De manera concluyente explica que *el fundamento común a estos criterios que englobamos en el concepto de culpabilidad se encuentra, por tanto, en aquellas facultades que permiten al ser humano participar con sus semejantes, en condiciones de igualdad, en una vida en común pacífica y justamente organizada. La «motivabilidad», la capacidad para reaccionar frente a las exigencias normativas es, según creo, la facultad humana fundamental que, unida a otras (inteligencia, afectividad, etc.), permite la atribución de una acción a un sujeto y, en consecuencia, la exigencia de responsabilidad por la acción por él cometida. Cualquier alteración importante de esa facultad —cualquiera que sea el origen de la misma— deberá determinar la exclusión o, si no es tan importante, la atenuación de la culpabilidad*.[152]

[152] Muñoz Conde, Francisco; García Arán, Mercedes. Ob. Cit. Pág. 355.

La culpabilidad está compuesta por algunos elementos, los cuales condicionan la aplicación de la pena que señala la norma, como en breve se señalará.

4.3.1 Imputabilidad/Inimputabilidad.

La imputabilidad o inimputabilidad es una de los elementos a examinar para determinar la culpabilidad del autor de la conducta típica y antijurídica.
La imputabilidad se refiere a la madurez psíquica y a la capacidad del sujeto para motivarse.[153]
Ello indica, que para establecer si al sujeto activo le puede ser impuesta la pena, este debe ser imputable.
Usualmente, el manejo de herramientas informáticas, se hace en mayor medida por jóvenes o adolescentes quienes se interesan por el uso de las TICS. El adolescente puede ser declarado responsable penalmente o declarada su conducta como antisocial, de acuerdo a las disposiciones de la Ley Penal Juvenil vigente. Los menores de doce años se encuentran exentos de responsabilidad, de acuerdo al artículo 2 de la Ley Penal Juvenil.

En caso de la madurez psíquica, si es que existe duda sobre la misma, esta debe ser determinada en su caso, por técnico especialista en la materia. En la experiencia salvadoreña, el ministerio público solicita, ya sea oficiosa o a petición de la defensa técnica, que se determine si un sujeto puede discernir entre la licitud o ilicitud de su actuar, o si el relato que un sujeto presenta es coherente. Entre las características que se hacen constar en dichos informes periciales, por lo general, el perito indica si el estado del sujeto es de alerta, si éste se encuentra ubicado espacio-temporalmente y en caso que existiere una clase de retardo, cuál es su desarrollo mental, haciendo distinción cronológica

[153] Muñoz Conde, Francisco; García Arán, Mercedes. Ob. Cit. Pág. 358.

y distinción de desarrollo psíquico. Solo excluyendo dichas cuestiones y establecida la imputabilidad del delincuente informático, será posible la imposición de una pena.

4.3.2 Conocimiento de la Antijuricidad.

Si el sujeto no sabe que su hacer está prohibido, no tiene ninguna razón para abstenerse de su realización; la norma no le motiva y su infracción, si bien es típica y antijurídica, no puede atribuírsele a título de culpabilidad.[154]

En El Salvador, por disposición Constitucional establecida en el artículo 8, de la misma, nadie esta obligado a hacer lo que la ley no manda ni a privarse de lo que ella no prohíbe. Asimismo, el articulo 1 del Código Penal desarrollo el principio de legalidad que también se encuentra consagrado en la Constitución, el cual establece que nadie puede ser sancionado por una acción y omisión que la ley no ha descrito de manera previa.

Asimismo, realizando una interpretación sistemática de la ley, la cual es aplicable también en materia penal, se trae a colación lo establecido por el Código Civil vigente:

"No podrá alegarse ignorancia de la ley por ninguna persona, después del plazo común o especial, sino cuando por algún accidente grave hayan estado interrumpidas durante dicho plazo las comunicaciones ordinarias entre el lugar de la residencia del Gobierno y el departamento en

[154] Muñoz Conde, Francisco; García Arán, Mercedes. Ob. Cit. Pág. 358.

que debe regir. En este caso dejará de correr el plazo por todo el tiempo que durare la incomunicación."

La posibilidad de establecer que ha existido un estado de interrupción de las comunicaciones, tal como lo establece la ley, no es un supuesto viable, tomando en consideración la realidad que se vive con el desarrollo tecnológico. Aún, son pocos los sectores de la población sin acceso a medios de comunicación de cualquier tipo.

Probar un desconocimiento sobre la prohibición de la conducta también puede traer dificultades, por lo complejo que ello resulta. No obstante, si así fuese nos encontraríamos en un supuesto de error de prohibición con en adelante se expone.

4.3.3 Exigibilidad de otra conducta.

Cuando la obediencia de la norma pone al sujeto fuera de los límites de la exigibilidad, faltará ese elemento y, con él, la culpabilidad. [155]

Aunque hablar de la exigibilidad de otra conducta, pudiera resultar impreciso debido qué parámetros se pueden establecer como los "normales" para dirigir la actuación de un sujeto. Por ello, razonable es lo expuesto por Muñoz Conde quien expresa, que el Derecho no puede exigir comportamientos heroicos; así señala que la norma jurídica tiene un ámbito de exigencia, fuera del cual no puede exigirse responsabilidad alguna[156].

[155] Muñoz Conde, Francisco; García Arán, Mercedes. Ob. Cit. Pág. 358
[156] Muñoz Conde, Francisco; García Arán, Mercedes. Ob. Cit. Pág. 358

En los delitos informáticos, y, sobre todo, en el hurto de identidad la conducta del autor del tipo es manifiestamente dolosa, por lo que al analizar si una persona tenía posibilidad de dirigir sus acciones de manera diferente, la respuesta evidente, será que sí. Incluso, la conducta típica envuelve una situación de emprendimiento de parte del sujeto activo, pues requiere que este visualice mentalmente su objetivo y a partir de ello, comience a realizar esfuerzos o acciones concretas para suplantar o apropiarse de la identidad de la víctima. Por lo que ese juicio de reprochabilidad puede ir construyéndose razonablemente para el sujeto que ha cometido el delito de hurto de identidad.

4.3.4 Causas de Exclusión de Culpabilidad o Causas de inimputabilidad.

La culpabilidad tiene entonces una vertiente negativa.
La diferencia entre las causas de exclusión de la culpabilidad y las causas de justificación, es que las causas de exclusión de culpabilidad dejan intacto el tipo de injusto, con todo lo que ello comporta en orden a la aplicación de sanciones no penales, medidas de seguridad, admisión de la legítima defensa frente al que actúa, la posibilidad de participación de terceras personas, etc[157].

El legislador salvadoreño ha planteado en la misma disposición (artículo 27 del Código Penal) de manera indistinta las causas de justificación con las causas que excluyen la culpabilidad, aunque existen diferencias entre estas, tal como se ha señalado.

Las causas de exclusión de la culpabilidad tienen relación con el fuero interno del sujeto activo, con esa capacidad de comprender la naturaleza, alcance y

[157] Muñoz Conde, Francisco; García Arán, Mercedes. Ob. Cit. Pág. 359

efectos de su conducta. Debe, además, valorarse que el sujeto activo tuvo que encontrarse en ese estado mental al momento de cometer el hecho.

4) Quien, en el momento de ejecutar el hecho, no estuviere en situación de comprender lo ilícito de su acción u omisión o de determinarse de acuerdo a esa comprensión, por cualquiera de los motivos siguientes:

a) Enajenación mental;

Jurisprudencialmente se ha hecho referencia a estados de enajenación mental producto de condiciones o enfermedades mentales, establecidas a través de diagnósticos médicos concretos. En las diferentes resoluciones que imponen una medida de seguridad se hace referencia a ese estado de enajenación mental sin definirlo, pero, puede establecerse del análisis de hechos probados, que ese estado de enajenación, debe ser permanente bajo control médico, que no le permita al sujeto comprender la ilicitud de sus acciones- El Tribunal de Sentencia de San Vicente, emitió en fecha 07 de marzo de 2001, en proceso especial de imposición de medidas de seguridad marcado con referencia judicial P1301-6-2001:

"Pruebas Realizadas: Test de Inteligencia en septiembre de 1997; la cual lo ubica en un C.I. de 87 lo cual indica una inteligencia un poco bajo de lo normal. Electroencefalograma, septiembre 1997; el cual fue normal. Diagnóstico Final es de esquizofrenia Paranoide, la cual al momento de la evaluación se encuentra en fase de síntomas negativos, es decir sin síntomas psicóticos activos, los cuales se expresan con mucha apatía, desinterés por las actividades laborales, sociales y sin un plan de futuro; jurídicamente ***este diagnóstico se categoriza como una enajenación mental****. Recomendaciones: Que se continúe con el tratamiento farmacológico ambulatorio ya que sin este se podrían presentar explosiones de violencia y síntomas psicóticos que podrían poner en peligro la integridad para contrarrestar el desinterés y la apatía. "*

No obstante, el comportamiento humano es complejo, sería remota la posibilidad de que el delincuente informático actúe bajo un estado de enajenación mental.

b) Grave perturbación de la conciencia; y,

Existen criterios jurisprudenciales que ya han realizado un esfuerzo por desarrollar la grave perturbación de la conciencia:

La Grave Perturbación de la Conciencia, puede ser relacionado con el "trastorno mental transitorio" figura que abarca alteraciones psíquicas no permanentes, estados pasionales muy intensos y reacciones vivenciales anormales, reflexionando que puede tener origen en alteraciones anímicas severas o por otra parte: "Puede tener un origen exógeno, como consecuencia de un choque psíquico producido por un agente exterior cualquiera y que se presenta bajo múltiples fenómenos perturbadores de la razón humana, exigiéndose: a) Una brusca aparición; b) Una irrupción en la mente del sujeto con pérdida de facultades intelectivas o volitivas, o ambas; c) breve duración; d) curación sin secuelas; y e) que no sea auto provocado" [Climent Duran, Carlos., Código Penal con Jurisprudencia Sistematizada, Editorial Tirant Lo Blanch, Valencia, 2011, P. 103].[158]

Sobre la base de lo anterior, llama la atención que debe suscitarse una pérdida de facultades intelectivas o volitivas, incluso ambas, por lo que podría inferirse que, si una persona atraviesa una condición de tales características, no podría finalizar una actividad compleja como hurtar la identidad de otra persona.

---

[158] Sentencia emitida en recurso de apelación, por la Cámara Primera de lo Penal de la Corte Suprema de Justicia, de fecha 23/04/2019, en proceso judicial marcado con referencia INC-APEL-68-SC-2019, consultado el 12/11/2022 en https://www.jurisprudencia.gob.sv/busqueda/tesauro.php

c) Desarrollo psíquico retardado o incompleto.

En estos casos, el juez o tribunal podrá imponer al autor alguna de las medidas de seguridad a que se refiere este Código. No obstante, la medida de internación sólo se aplicará cuando al delito corresponda pena de prisión;

Sobre el desarrollo psíquico retardado o incompleto, también nos remitimos a criterio judicial:

"En un estado de desarrollo psíquico retardado o incompleto. Obviamente todas estas situaciones que tienen que ver con la estabilidad de la psiqué humana en sus diferentes dimensiones, exige una especie de normalidad en la capacidad del raciocinio de la persona de acuerdo con su ámbito social, para que se le pueda exigir capacidad de motivación, es decir de comprensión de los mandatos de prohibición de las normas penales, en cuanto tuteladoras de los bienes jurídicos de las demás personas. Pero esta relación de capacidad psíquica no es una cuestión que pueda estimarse en grados absolutos, en el sentido de si es normal o anormal, sino que tal cuestión es gradual, y a su vez compleja por cuanto se relaciona con aspectos no únicamente somáticos sino de diversa índole social, cultural, educacional, de valores, etcétera. De ahí que, ni en el mismo plano de la cuestión psíquica se pretenda actualmente una diferenciación absoluta entre anormal y normal, pues las mismas cuestiones del psiquismo pueden presentar planos diversos que puedan fluctuar entre la capacidad síquica completa, capacidades psíquicas disminuidas, capacidades psíquicas deterioradas que generan a su vez una incapacidad de mayor alcance para comprender y dirigir las actividades de la vida en sociedad."[159]

[159] Sentencia Definitiva emitida en proceso penal por el Tribunal Tercero de Sentencia, en fecha 21/10/2003, en causa marcada con referencia 179-2003-2ª, consultada el 12/11/2022

No se visualiza, que concurran excluyentes de culpabilidad, puesto que, si fuere así, no podría siquiera haberse cometido el delito. Esto es incluso congruente con las ideas que se han planteado en relación con el sujeto activo del tipo y los elementos especiales de autoría que se han señalado en este capítulo, en relación con la aproximación a una especie de perfil que se requiere para el delincuente informático. A menos que se trate en algún momento de una condición que no inhabilite sus capacidades intelectivas, y únicamente pierda la noción sobre la licitud de su accionar, si este fuera el caso se atendería a los elementos probatorios periciales que fueren capaces de establecerlo de esa forma sin margen de duda.

4.3.4.1 Error de Prohibición.

De manera concreta a fin de establecer aspectos prácticos de esta investigación debe citarse:

El error de prohibición se produce cuando el sujeto que actúa, juzgado por error, falso conocimiento o ignorancia, que su conducta no se encuentra sujeta a una sanción penal. Esto puede ocurrir cuando, por ejemplo, el autor de una conducta antijurídica cree que se encuentra justificado para realizar un determinado hecho, sin que aquello sea cierto.

La jurisprudencia de esta Sala, es ilustrativa al respecto, habiendo indicado que: "Del contenido normativo del Art. 28 Pn. y de lo que la doctrina enseña a ese respecto, es claro que el error de prohibición es viable de suscitarse en tres supuestos concretos: a) Cuando el sujeto desconoce la existencia norma prohibitiva (error directo); b) la falsa creencia de ostentar una autorización o

---

en https://escuela.fgr.gob.sv/wp-content/uploads/Leyes/Leyes-2/tribunal-tercero-de-sentencia.pdf

permisión normativa; y, c) el sujeto obra en la creencia errónea de una causa justificación inexistente (error indirecto éstos dos últimos)".

A su vez, el error de prohibición puede ser directo o indirecto, según que el sujeto actúe creyendo que su comportamiento no es delito o bien que, conociendo la prohibición penal en general, supone que en el obrar concreto, le ampara una causa de justificación. Una sub clasificación más, el error puede estar referido a la existencia de la causa de justificación (error de permisión) o respecto de los presupuestos de ésta,". (Ref. 441- CAS-2009, del 06/05/2011).[160]

Debido al abordaje que se ha realizado sobre el tipo de hurto de identidad, en cuanto a la acción, sujeto activo, así como los elementos especiales de autoría, es difícil establecer la posibilidad de la existencia de un error de prohibición. Aun si el autor del hecho fuere un menor de edad, puesto que los jóvenes con habilidades y destrezas en el manejo de las nuevas tecnologías, tienen el atributo de ser estar dotados de capacidades intelectivas superiores. Aunque podría examinarse la casuística.

Según vemos, la Sala de lo Penal de la Corte Suprema de Justicia, cita tres supuestos en los cuales es viable establecer la existencia del error de prohibición, las cuales remotamente podrían suscitarse, no únicamente en el delito de hurto de identidad, sino en los delitos informáticos como tales. Desde la perspectiva de este estudio, no podría sostenerse la existencia de supuestos que habiliten la existencia de error de prohibición en el caso del delito de hurto de identidad. Esto, es parte del aparecimiento novedoso de esta clase de

---

[160] Sentencia definitiva emitida por la Sala de lo Penal de la Corte Suprema de Justicia, en recurso de casación, emitida en fecha 14/01/2013, consultada en versión PDF el 08/11/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2013/01/9D457.PDF

delitos. No debe perderse de vista, que el error de prohibición es parte de la dogmática penal elaborada ya hace un período de tiempo considerable, pensada en el accionar delictivo del ser humano, motivado generalmente para atacar bienes jurídicos individuales.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES.

A) El desarrollo de la informática se percibe a través de la inclusión de las TIC´S en cada aspecto de la vida de sus usuarios, quienes resuelven a través de las mismas sus necesidades, desde las más sencillas hasta el manejo de cuentas bancarias, por ejemplificarlo; ya que sirven para agilizar toda clase de gestiones, ahorrando tiempo y recursos. Lo anterior significa, que esta forma de relacionarnos ha llegado para quedarse, para evolucionar y perfeccionarse; haciéndose necesario establecer los mecanismos legales para garantizar la protección de las relaciones jurídicas sostenidas a través de la TIC´S.

B) El concepto de identidad digital, entendido como aquella información de carácter personalísima que hacen al individuo diferente de cualquier otro sujeto, a través de las TIC´S, es elemental para establecer comunicación de manera eficaz, puesto que aún y cuando dicha actividad comunicativa se establece en el ciberespacio, es suficiente para generar beneficios o afectaciones perceptible a los sentidos, en la realidad objetiva, principalmente para el titular de la identidad digital, ya que ésta puede ser instrumentalizada para cometer otros hechos delictivos, generalmente de contenido patrimonial.

C) En El Salvador, la protección al derecho a identidad digital no se encuentra establecido de manera expresa en la Constitución de la República, sin embargo, al comprenderla como elemento imprescindible para el desarrollo y bienestar de la persona humana puede establecerse como fundamento constitucional, los artículos 2 y 3 de la Carta Magna. Asimismo, como resultado de una interpretación más amplia, es posible advertir la existencia un grupo de

personas que hacen uso de las TIC´S a quienes es importante asegurarle un esquema de protección legal para reducir las situaciones de riesgos en el ciberespacio.

D) En El Salvador, se encuentra vigente desde el año 2016 la Ley Especial Contra Delitos Informáticos y Conexos, en su contenido se retoman algunas disposiciones de la Convención de Budapest o Convención sobre la Ciberdelincuencia. Dicha ley, representa un esfuerzo para la protección de los usuarios de las TIC´S, la protección de datos, así como de la identidad digital misma, aún y cuando conceptualmente no se relaciona en el texto legal. La ley especial, la cual aún puede considerarse de reciente aprobación ha sufrido reformas producto de las necesidades que la experiencia ha demandado a través de la casuística; sin embargo, no ha resultado sencillo resolver y presentar ante los Juzgados competentes casos concretos relacionados con el delito de hurto de identidad, debido a la forma sofisticada de su ejecución.

E) Actualmente, la situación de criminalidad relacionada con la sustracción de datos y consecuentemente la utilización de la identidad digital ajena para cometer hechos delictivos en El Salvador, permanece mayoritariamente en la impunidad debido a las formas complejas de comisión y a las limitantes técnicas, así como de recursos para hacerle frente a esta clase de delincuencia, sin perjuicio de los casos resueltos, los cuales son resultado de aspectos circunstanciales y no del manejo técnico de la investigación del delito. Por ello, es importante tomar en cuenta el estado actual del fenómeno a fin de enfrentarlo con las herramientas idóneas, sin perder de vista, que la verdadera herramienta de combate de dicho flagelo es la educación de los usuarios de las TIC´S, para que puedan dirigir su conducta en el ciberespacio

de manera que evadan las situaciones de riesgo más comunes utilizadas por los delincuentes informáticos.

F) La identificación de un punto de vista de esta clase de delincuencia (ciberdelincuencia) congruente con la perspectiva del derecho penal económico es importante para visualizar afectaciones a bienes jurídicos colectivos y no únicamente a bienes jurídicos individuales. Así como la trascendencia que este fenómeno tiene para sectores o grupos de personas, para el orden socioeconómico mismo, el mercado y para la seguridad de las transacciones que hacen posible el crecimiento económico.

G) El delito de hurto de identidad de acuerdo al artículo 22 de la LECDIC, requiere para su ejecución que el sujeto activo emprenda una conducta dinámica, ingeniosa y novedosa para lograr la suplantación o apoderamiento de la identidad de la víctima. Una vez obtenido el resultado trazado, puede obtener grandes beneficios de carácter económico, que, en la mayoría de los casos, su conducta quedará en un estado de impunidad, lo cual hace aún más atractiva esta novedosa forma de delincuencia, a la cual todos tienen acceso inmediato a través de la informática y sus avances, entre los cuales se encuentran las TIC´S.

H) No puede negarse que en nuestros días el comercio electrónico un rubro lleno de oportunidades, tanto para los consumidores como para los proveedores, dando lugar a nuevos mercados donde todo está al alcance de un *clik.* Esto precisamente en línea con el contenido del Art.102 Cn, que garantiza la libertad económica como un derecho fundamental, siempre que no se oponga el interés social, es decir que no debe privar el interés particular

sobre el general.

Esta nueva forma de hacer comercio, es precisamente la que ha originado que en El Salvador el Estado intervenga de manera activa en su regulación en el conjunto de normas que integran el denominado derecho del consumidor, contenidas en la Ley de Protección al Consumidor dentro de la cual para efectos de esta investigación destaca lo regulado en el Art. 13- C) relativo a la "Protección al consumidor en el ámbito del Comercio electrónico", lo cual obedece a la tendencia de resguardar o tutelar los niveles básicos de satisfacción de las necesidades de los individuos para lograr un nivel de protección coherente con los valores garantizados en la Constitución cuando interviene en la actividad económica como consumidos o proveedor de la tecnología de la información y comunicación. donde todo está al alcance de un *clik.* Esto precisamente en línea con el contenido del Art.102 Cn, que garantiza la libertad económica como un derecho fundamental, siempre que no se oponga el interés social, es decir que no debe privar el interés particular sobre el general.

Esta nueva forma de hacer comercio, es precisamente la que ha originado que en El Salvador el Estado intervenga de manera activa en su regulación en el conjunto de normas que integran el denominado derecho del consumidor, contenidas en la Ley de Protección al Consumidor[161] dentro de la cual para efectos de esta investigación destaca lo regulado en el Art. 13- C) relativo a la "Protección al consumidor en el ámbito del Comercio electrónico", lo cual obedece a la tendencia de resguardar o tutelar los niveles básicos de satisfacción de las necesidades de los individuos para lograr un nivel de protección coherente con los valores garantizados en la Constitución cuando

interviene en la actividad económica como consumidos o proveedor de la tecnología de la información y comunicación.

La necesidad de legislar sobre el comercio electrónico obedece precisamente al uso de las tecnologías de información y comunicación en los nuevos modelos de negocio electrónicos, y se convirtió en una necesidad colectiva por la nueva forma de realizar actos jurídicos como celebrar contratos, transacciones de bienes y servicios, entre otros; sin embargo, pese a que las herramientas tecnológicas representaban un menor costo y tiempo, no se tenía una adecuada protección para los derechos de los comerciantes y consumidores, de ahí que por Decreto Legislativo 51 del 30 de julio de 2018, se introdujo en la Ley de Protección al Consumidor, la reforma que otorga garantías a los actos de comercio que se celebren de forma electrónica, derechos que si bien ya estaban regulados la ley, en el Art. 13 – D) se establece de forma más clara dichos derechos en bienes o servicios por medio del comercio electrónico.

I) En este contexto, por Decreto Legislativo 280, aprobado el 07/02/2022 y publicado en el Diario Oficial N° 45 Tomo N° 434 de fecha 04/03/2022; introduce reformas al código procesal penal, adicionando en Capítulo X, Título V “DE LA PRUEBA”, del Libro I “DISPOSICIONES GENERALES” del Código Procesal Penal, el “Capitulo X. Evidencia digital. Reforma con la que introduce figuras como Evidencia Digital Art. 259-A.- Registro de cadena de custodia Art. 259-B.- Incorporación y producción de la evidencia digital en el proceso penal Art. 259-C.- Agente Encubierto Digital y otras técnicas de investigación informáticas Art. 259-D.- Durante la investigación de los delitos Medidas Cautelares Art. 259-E.-.

El legislador deja en evidencia que la ley especial contra delitos informáticos y conexos era una ley incompleta y que por las características de

este tipo de delincuencia era indispensable la actualización del marco normativo dotando de herramientas procesales para facilitar su empleo en la detección, investigación y sanción de delitos informáticos.

J) Es importante el reconocimiento del derecho a la identidad digital a través de la normativa vigente: Ley Especial Contra Delitos Informáticos y Conexos, estableciendo su significado y alcance; como parte del compromiso asumido por el Estado, para garantizar el pleno goce de los derechos que surgen con el desarrollo tecnológico. Asimismo, es necesario generar espacios educativos para los usuarios de las TIC´S, como una medida preventiva que genere la reducción de la criminalidad relacionada con la instrumentalización de la identidad digital de las persona naturales y jurídicas, que generan impacto en el orden socioeconómico.

K) En El Salvador, el derecho a la autodeterminación informática no ha sido desarrollado a través de disposiciones legales, sin embargo, ello no ha sido obstáculo para su reconocimiento y desarrollo a través de la autoridad jurisdiccional, la cual, ante la necesidad de un pronunciamiento para casos concretos, ha destacado la importancia de que las personas naturales y jurídicas tengan la capacidad de controlar la información que sobre ellos conste en medios informáticos. Las sentencias emitidas por la Sala de lo Constitucional de 2-III-2004 y 2-IX-2005, pronunciada en el proceso de Amp.118-2002 y en el proceso de Inc. 36-2004, respectivamente desarrollan puntualmente lo pertinente en el ámbito informático: “*tal derecho implica la protección de todo individuo frente a la posibilidad de acceso a la información personal que se contenida en bancos informatizados”.*

5.2 RECOMENDACIONES.

A) Deben implementarse como parte de las políticas de prevención de delitos informáticos a través de las instituciones competentes, campañas de difusión sobre los derechos digitales de los cuales son titulares los usuarios de las TIC´S, para educar sobre el uso de estas, con la finalidad de reducir las oportunidades de riesgo, que les hacen blancos fáciles de ataques informáticos.

B) La Asamblea Legislativa debe adicionar disposiciones a la LECDIC o al CPP a fin de incluir artículos relacionadas con las técnicas de investigación especializadas para el diligenciamiento de casos relacionados con delitos informáticos. Lo anterior, pues a pesar las adiciones realizadas al art.259 en el CPP, sobre la evidencia digital, esta trata de forma generalizada la evidencia digital sin establecer técnicas específicas para su obtención, las cuales ya tienen vigencia en otros países, como España, por lo que se trata de un esfuerzo realizable.

C) Se hace necesario que la PNC, a través de la División de Delitos Informáticos, sea provista de más recurso humano para que éstos puedan hacer frente a la demanda de casos abiertos a raíz de la denuncia ciudadana. Recurso humano con las capacidades técnicas idóneas para la investigación de la ciberdelincuencia a fin de presentar las mismas a los jueces competentes, para generar criterios jurisdiccionales en cuanto al cibercrimen.

D) Es necesario que todas las instituciones encargadas de operar el sistema jurisdiccional (Policía Nacional Civil, Fiscalía General de la República, Consejo Nacional de la Judicatura, Corte Suprema de Justicia, Procuraduría General

de la República) creen unidades o dependencias especializadas en el tratamiento de la delincuencia informática a fin de garantizar el goce de los derechos digitales, así como el respeto de los derechos y garantías de los delincuentes informáticos, por respeto al Estado democrático de derecho.

GLOSARIO

En este apartado se presentan los conceptos o abreviaturas, así como sus respectivas definiciones de los términos más importantes que tendrá el desarrollo de la tesis, tal cual se presentan a continuación:[162]

ARCHIVO: Forma de estructurar la información. También es sinónimo de fichero. Todos los archivos que son sólo de texto, son archivos binarios. Hay que distinguir entre archivo de datos y archivo ejecutable. Archivo de datos, es la fórmula simple, una especie de contenedor de información. Archivo ejecutable, sería en realidad un programa, puesto que siguiendo los parámetros que da, realiza unas acciones determinadas.

CABALLO DE TROYA o TROYANOS: Programas que se ocultan dentro de otros, para no ser descubiertos, y se instalan en el sistema de un usuario, de forma que al actuar producen un auténtico sabotaje contra el sistema informático. Los Troyanos no se replican a sí mismos lo que les diferencía de los virus puros aunque algunos si son capaces de enviarse como adjuntos.

CARPETA: Espacio que podemos crear en la computadora para almacenar datos, equivale a un directorio.

CIBERCRIMEN: Es el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o

[162] Lucio Albino Arias López. Tesis para obtener el grado de maestro en derecho penal económico. Limitaciones del Sistema Penal para investigar y probar la Comisión del Ciberdelito en El Salvador. Universidad de El Salvador, diciembre 2021.

autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual[163]

CIBERESPACIO: Concepto que procede de la literatura de ficción, concretamente utilizado por Willian Gilbson, para referirse al mundo entre los ordenadores conectados, redes de información y medios digitales

CIBERDELITO: Este concepto se utiliza para referirse a una gama de actividades ilícitas cuyo denominador común es el papel central que desempeñan las redes de información y la comunicación (TIC) en su comisión. No obstante, existen autores para los cuales este concepto es sinónimo de cibercrimen, por lo que en la investigación se utilizarán como sinónimos.

CIBERPUNK: Se ha utilizado en ocasiones para los *hackers* por lo que significa movimiento social de desconfianza o ataque a las máquinas.

CRACKER: De forma simple, pirata informático malo. Persona que accede ilegalmente a un sistema informático ajeno con fines vandálicos o dañinos, para cierta parte de la doctrina este aspecto queda igualmente incluido en el *Hacking* por lo que desde este concepto restringido su objetivo sería producir daño, frente al *hacker* que busca obtener información.

DERECHO INFORMATICO: Es el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad.

---

[163] Carlos María Romeo Casabona. *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político criminales*, en El Cibercrimen. (Granada: Comares, 2006) 1-43

DELINCUENCIA INFORMATICA o CRIMINALIDAD INFORMATICA: Son los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera y todos aquellos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva

HACKER: Pirata informático. El concepto original, *Hacking,* abarcaba cualesquiera accesos no autorizados, con o sin intención dañosa, con o sin intención de lucro. Según algunas opiniones, el concepto no incluye a quien entra en el ordenador con intención criminal o vandálica, para el cual sería apropiado el término ***"Cracker".*** Según algunas fuentes, el concepto viene de "*hack"* que era el sonido que se empleaba en las empresas de telefonía al golpear el aparato telefónico para que funcionara.

HTTP: Es la abreviatura de un hipter texto que remite a un protocolo de internet, en ingles significa *"Hyper Text Transfer Protocol"* que se usa para dirigirse a una zona de internet determinada.

IP: Es la abreviatura de las palabras *"Internet Protocol"* que es un protocolo de internet para identificar la fuente y origen de una conexión o alogamiento de cierta información, así mismo son un conjunto de normas técnicas de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional, es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

IMEI: Es la abreviatura en idioma Ingles de "International Mobile Equipment Identity", que significa identidad internacional de equipo móvil, que es un código pregrabado en los teléfonos móviles GSM. Este código identifica al

aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta.

IMSI: Es el acrónimo de “International Mobile Subscriber Identity” que se traduce en “Identidad Internacional del Abonado Móvil”. Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

INTERNET: Red de redes de ordenadores a escala mundial con un sistema de comunicación común

SERVIDOR: Ordenador que permite a un usuario autorizado utilizar recursos y servicios de un ordenador remoto. El término obedece a que ese ordenador presta servicios a las otras máquinas o clientes. Los servicios pueden ser de todo tipo, almacenar o acceder a archivos, aplicaciones, correo electrónico, etc. Se les denomina también *host* y el hecho de publicar algo en ellos se denomina *“hosting”* que se podría traducir como alojar lo escrito.

SISTEMA INFORMÁTICO: Es un conjunto de elementos que hace posible el tratamiento automático de la información. Las partes de un sistema informático son: • Componente físico: está formado por todos los aparatos electrónicos y mecánicos que realizan los cálculos y el manejo de la información. • Componente lógico: se trata de las aplicaciones y los datos con los que trabajan los componentes físicos del sistema. • Componente humano: está compuesto tanto por los usuarios que trabajan con los equipos como por aquellos que elaboran las aplicaciones.

SOFTWARE: Conjunto de programas y aplicaciones informáticas que hacen funcionar a una computadora o que se ejecutan en ella.

SPYWARE: Programa espía o aplicación maliciosa que se instala sin que el usuario lo advierta, normalmente al descargar otro programa.

TCP/IP: En este caso en concreto se fusionan dos abreviaturas que literalmente se leen: *"Transmission Control Protocol/Internet Protocol"* que significa Protocolo de Control de Transmisión al protocolo de internet que indica la forma de control de toda transmisión realizada entre distintos protocolos de internet".

WEBSITE: Sitio web. Conjunto de páginas web que comparten una misma dirección.

www: Abreviatura que hace alusión al conjunto de todas las páginas web de internet, lo que se conoce como la red mundial world wide web.

BIBLIOGRAFIA

LIBROS

- Cubría, Manuel Iglesias. “El derecho a la Intimidad”, editada por la Universidad de Oviedo en el año 1970, consultada en versión PDF.
- MUÑOZ CONDE, Francisco: “Delincuencia económica. Estado de la cuestión y propuestas de reforma”, en *Hacia un derecho penal económico europeo, Jornadas en honor al profesor Klauss TIEDEMANN,* Boletín Oficial del Estado, Madrid, 1995, p. 267. Versión digital.
- Muñoz Feliu, Miguel C. Reputación Online y huella digital. Departamento de Comunicación Audiovisual, Documentación e Historia del Arte. Universidad Politécnica de Valencia. Tirant lo blanch.
- Oficina de las Naciones Unidas contra la Droga y el Delito. *“Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos”.* Copyright 2018. Pág. 12.

LIBROS CONSULTADO EN LA WEB

- Acurio del Pino, Santiago. Delitos Informáticos: Generalidades. Consultado en versión digital, pág. 15 y ss., el día 05/11/2022 en: http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf
- Barrio Andrés, Moisés. Manual de Derecho Digital. 2ª Edición, Tirant lo Blanch, Valencia 2022,consultado en versión digital el día 06/11/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411470551

- Blanquer Criado, David. Esquemas de Derecho Administrativo. TOMO XLIII, Editorial Tirant lo Blanch, Valencia, 2016. Consultada en versión digital, en fecha 17 de julio de 2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491192572
- Bonachera Villegas, Raquel. Tutela Procesal de los Derechos e Intereses de Los Consumidores. Pág. 24. Nota al pie. Editorial Tirant lo blanch, Valencia, 2018. Consultada en versión digital en fecha 17 de julio de 2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491699149
- Borghello, Cristian, Temperini, Marcelo G.I.. Suplantación de Identidad Digital como Delito Informático en Argentina. Simposio Argentino de Informática y Derecho. Consulado el 06/11/2022 en http://sedici.unlp.edu.ar/bitstream/handle/10915/124395/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y
- Cotino Hueso, Lorenzo. La Carta de Derechos Digitales. Editorial Tirant Lo Blanch 2022. Consultado en versión digital, pág. 401, el 02/11/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411472050
- De Vicente Martínez, Rosario. Vademécum de Derecho Penal. 5ª edición revisada, actualizada y ampliada. Tiran lo Blanch, Valencia 2018. Consultada el 11/11/2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491901969
- Faraldo Cabana, Patricia. Las Nuevas Tecnologías en los Delitos Contra el Patrimonio y el Orden Socioeconómico. Editorial Tirant Lo Blanch, libro publicado 01/06/2009. Consultado en versión digital el 09/10/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788499855943?showPage=37

- Feijoo Sánchez, Bernardo. Imputación objetiva en el Derecho Penal Económico y empresarial. Esbozo de una teoría general de los delitos económicos. Consultado el 06/11/2022 en versión PDF.
- Gaddi, Daniela, Beaucells, Joan, García Arán, Mercedes. Justicia Restaurativa y Delincuencia Socioeconómica. 1 edición, Tirant Lo Blanch, 2021. Consultado en versión digital el 11/10/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413786322
- Galán Muñoz, Alfonso; Arribas León, Mónica, Caruso Fontán, María Viviana, et al., La Protección Jurídica de la Intimidad y de los Datos de carácter Personal frente a las Nuevas Tecnologías de la Información y Comunicación, editado en España, por la editorial Tirant Lo Blanch, en el año 2014, consulta en edición digital en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788490537657
- García Conlledo Miguel Díaz y. Autoría y Participación. Revista de Estudios de la Justicia, N° 10, año 2008, consultada el 09/11/2022 en versión digital en: file:///C:/Users/damaris.martinez/Downloads/laguirre,+Journal+manager,+15219-41640-1-CE.pdf
- García Mexía, Pablo. Historias de Internet, ISBN: 9788415442615. Editorial: Tirant Lo Blanch. Fecha de publicación del libro: 2012-05-01. México, consultada en versión digital el 12/06/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788415442615?showPage=0
- Hernández Díaz, Leyre. El Delito Informático. EGUZKILORE, número 23, San Sebastián, diciembre 2009. Pág.230. Consultado en versión digital el día 16 de septiembre de 2022 en: https://addi.ehu.es/bitstream/handle/10810/24953/18-Hernandez.indd.pdf?sequence=1

- López Torres, Jonathan. Ciberespacio & Ciberseguridad. Elementos Esenciales. Tirant Lo Blanch, Ciudad de México, 2020, pág.30, consultado el 06/11/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413550695
- Manual Único de Investigación Interinstitucional. Fiscalía General de la República, Policía Nacional Civil e Instituto de Medicina Legal "Dr. Roberto Masferrer", Corte Suprema de Justicia, con financiamiento de USAID. Imprenta y OFFSET Ricaldone, febrero 2012, consultado el 12/10/2022 en versión digital: https://escuela.fgr.gob.sv/wp-content/uploads/leyes/leyes-2/mui-final.pdf
- Martiñón Cano, Gilberto. El delito de Secuestro. Editorial Tirant lo Blanch, Valencia 2010. Pág.99. Consultada en versión digital el 05/11/2022 en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788499858135
- Mieres, Jorge. Ataques informáticos, artículo Debilidades de seguridad comúnmente explotadas. Publicado en 2009. Consulta en medios digitales el 05/11/2022 en: https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf
- Muñoz Conde, Francisco. Teoría General del Delito. 5ª Edición. Editorial Tirant lo Blanch, España, publicado el 02/09/2022., consultado en versión digital el 25/10/2022, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788411307604?showPage=41
- Muñoz Conde, Francisco, García Arán, Mercedes. Derecho Penal, Parte General, 8ª edición, revisada y puesta al día. Tiran lo Blanch, Valencia 2010. Consultada en versión digital 29/10/2022, en:

https://www.derechopenalenlared.com/libros/Derecho_Penal_Parte_General_Munoz_Conde_Mercedes_Aran.pdf

- Olásolo Alonso, Héctor. Tratado de Autoría y Participación en Derecho Penal Internacional. Tirant lo Blanch, tratados. Valencia 2013, consultado el 09/11/2022, en versión digital en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788490334287
- Rivacoba, Ramón Durán, Castilla Barea, Margarita. et. al. Protección de Datos Personales. Tirant lo Blanch. 1 edición, 2020. Consultado en versión digital, en: https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788490333907
- Rojas de Rojas, Morelba. Identidad y Cultura. Educere, Volumen 8, 2004, Universidad de los Andes Mérida, Venezuela, consultada el 27/10/2022, en versión digital en: https://www.redalyc.org/pdf/356/35602707.pdf
- Sauquillo Muñoz, Carmen Pérez. Legitimidad y Técnicas de Protección Penal de Bienes Jurídicos Supraindividuales. Editorial Tirant Lo Blanch, Valencia 2019. Consultado en versión digital el 12/10/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788413131245
- Souto García, Eva María. Los Delitos de Hurto y Robo: Análisis de su regulación tras la Reforma operada por la LO 1/2015, 30 de marzo. Editorial Tirant Lo Blanch, Valencia 2017, pág. 54 y ss. Consultado en versión digital el 03/11/2022 en https://biblioteca.tirant.com/cloudLibrary/ebook/show/9788491436867
- Ulloa Cuéllar, Ana Lilia; Maldonado Méndez, Érika Verónica, et al. Nociones de Derechos Humanos. Editorial Tirant lo blanch, 2019, 1° Edición, consultada en versión digital el 12/06/2022, en https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788491909842

TESIS

- Hernández Vera, Daniel Antonio. La Suplantación de identidad Cibernética en el Ecuador. Maestría en Derecho Informático y de las Nuevas Tecnologías, Bogotá, D.C., Colombia, 2019, pág. 29, consultado en versión digital el 31/10/2022 en: https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f36afdf-40eb-4cba-a38f-5827107779a9/content
- Molina Fernández, Fernando. Tesis Doctoral: Antijuridicidad Penal y Sistema del Delito. Universidad Autónoma de Madrid. Consultada el 11/11/2022 en versión digital en file: https://www.editorialmetropolitana.cl/wp-content/uploads/2021/07/%C3%8Dndice-Antijuridicidad-penal-N%C2%B0-60.pdf
- Quevedo González, Josefina. “Investigación y prueba del ciberdelito”. Tesis doctoral, Universitat de Barcelona, 2017. Consultada en versión PDF, Pág. 35 y siguientes.

SITIOS EN INTERNET

- Análisis legal e institucional. Observaciones a los Proyectos de Ley de Protección de Datos Personales, versión digital, consultada 11/06/2022, en http://fusades.org/publicaciones/AL_200_Oct2019_II%20parte_Observaciones%20a%20los%20proyectos%20de%20Ley%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf
- BANCO AGRÍCOLA SIMPLIFICA PROCESO DE DENUNCIA POR ESTAFAS”, CONSULTADO EL 25 DE OCTUBRE DE 2021 EN

https://www.elsalvador.com/noticias/negocios/estafas-bitcoin-bancos/871906/2021/

- Bernal, David. Hackeo de web de la PNC pone en peligro datos de policías. Artículo publicado el 09 de septiembre de 2021, consultado el 08/10/2022 en: https://www.laprensagrafica.com/elsalvador/Hackeo-de-web-de-la-PNC-pone-en-peligro-datos-de-policias-20210909-0059.html
- BBC NEWS, <<5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día>>. Consultado el 25 de octubre de 2021 en https://www.bbc.com/mundo/noticias-43472797
- Consultado en sitio *Definiciona. Definición y etimología, el día 16 de septiembre de 2022 en* https://definiciona.com/informacion/
- "El diseño de Información", consultado en versión digital el 16 de septiembre de 2022 en: http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/capitulo1.pdf
- Cuenta Oficial de Facebook Policía Nacional Civil, Consultado 11/06/2022 en https://www.facebook.com/PoliciaNacionalCivil/photos/a.10150539998650950/10158814835640950/?type=3 publicación de fecha 22/01/2021.
- Cuenta Oficial de Twitter, Ministerio de Hacienda, consultado 11/06/2022, en https://twitter.com/haciendasv/status/1412768606480482308?lang=es, publicación de fecha 07/07/2022.
- Consultado en Naciones Unidas, Derechos Humanos, oficina del Alto Comisionado, el día 17/09/2022 en: https://www.ohchr.org/es/instruments-mechanisms/instruments/declaration-use-scientific-and-technological-progress-interests

- Consultado en Web oficial de la UE, el 17/09/2022 en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es#documents
- Consultado en Web oficial de la UE, el 16/09/2022 en https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es#legislacin
- Consultado el 08/10/2022, en: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/D1F13E1E-9860-428F-8703-2B61D5DF1D47.pdf
- Consultado el 09/10/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/R/2/2000-2009/2009/01/EE38E.HTML?embedded=true
- Consultado el 09/10/2022 en: https://portaldetransparencia.fgr.gob.sv/documentos/RESOLUCION%20103-UAIP-FGR-2020.docx.
- Consultado en versión PDF el 09/10/2022 en: https://portaldetransparencia.fgr.gob.sv/documentos/Resoluci%C3%B3n%20630-UAIP-FGR-2021.pdf.
- Consultado en sitio oficial de la Oficina de las Naciones Unidas Contra la Droga y el Delito, el 12/10/2022, en: https://www.unodc.org/ropan/es/unodc-apoya-a-la-policia-nacional-civil-de-el-salvador-en-el-abordaje-de-los-desafios-de-la-lucha-contra-el-cibercrimen.html
- Consultado el 15/10/2022 en: Uber Law Enforcement and Public Health Portal https://lert.uber.com/s/login/?language=en_US
- Del Cid, Merlín. Policía Salvadoreña investiga suplantación de identidades para robar bono de US$30 en bitcoin. Artículo publicado el 07 de octubre de 2021, consultado en CNN Latinoamérica el 08/10/2022:

https://cnnespanol.cnn.com/2021/10/07/policia-salvadorena-investiga-suplantacion-de-identidades-para-robar-bono-de-us-30-en-bitcoin-orix/

- Dictamen No 46 Favorable, de fecha 13 de abril de 2021, suscrito por la Comisión de Economía de la Asamblea Legislativa de la República de El Salvador, versión PDF, consultado el 11/06/2022, en https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/498798FA-A563-4830-A0C8-306AFBC71497.pdf
- DIRECTRIZ N° 133-MP-MICIT, consultada en versión digital el 18 de septiembre de 2022 https://www.micitt.go.cr/wp-content/uploads/2022/05/DIRECTRIZ-N%C2%B0-133-marca-de-hora.pdf
- Garza, Jeffry. Costa Rica escaló 39 puestos en Índice Global de Ciberseguridad. DPL News. Consultado en versión digital el 18 de sep. de 22 , en: https://dplnews.com/costa-rica-escalo-39-puestos-en-indice-global-de-ciberseguridad/
- << Hackeo de web de la pnc pone en peligro datos de policías>>. consultado el 25 de octubre de 2021 en https://www.laprensagrafica.com/elsalvador/hackeo-de-web-de-la-pnc-pone-en-peligro-datos-de-policias-20210909-0059.html
- Iniciativa de Ley de Protección de Datos Personales y Habeas Data, versión PDF, consultado el 11/06/2022, en https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/2A326CE8-F13A-4828-8640-648235C228BF.pdf
- López Vides, Carlos. ISSS informa suspensión temporal de trámites por supuesto ataque informático. Artículo publicado el 19 de octubre de 2021, consultado el 08/10/2022 en: https://www.elsalvador.com/noticias/nacional/isss-ataques-ciberneticos/891436/2021/

- Normas de la UE para la protección de datos. Consultado el 11/06/2022 en el sitio Web oficial de la UE, en: https://ec.europa.eu/info/sites/default/files/virtual_identity_es.pdf
- Pastrán, Rosa María. Banco Agrícola alerta a clientes ante alza de denuncias por fraude. Artículo publicado el 07 de septiembre de 2021. Consultado el 08/10/2021 en https://www.eleconomista.net/economia/Banco-Agricola-alerta-a-clientes-ante-alza-de-denuncias-por-fraude-20210907-0005.html
- Roa Buendía, José Fabián Roa Buendía. "Seguridad Informática." Edición digital, ISBN, año 2013. Pág. 9, Consultado el 16 de Septiembre de 2022 en: https://d1wqtxts1xzle7.cloudfront.net/34758985/Seguridad_Informatica_McGraw-Hill_2013____www.FreeLibros.me_-_copia-with-cover-page-v2.pdf?Expires=1663343456&Signature=Jyb~~9KD~1eZWk6en7RKdtFFjkGBoAWhT1~Vj5x5xdRJaaUcQuQMODTYqFCJxDi2RMMn0EPr9STWJQfkES6~IMcf1e2G9eNB8VPdXmcrZGBboK-1a~FqEmxttn6jeoQ-PHIOSeM6qCh~SHqjRwgL3yoOKFeEucgMaK4LF3-Z2LDYMxvWE0dYaAdmssy464ZHtM9Rf7s3VOLXH~iX8WDxgyO0mLhhsh8IC27qwTsaS7xxHJ8WR6b3nhhqHLPABo3bF~9NJmjPSnD-9VwdIwBns5y5z3QNzhzcikm3NZnqMV1Sb4MCILSht5E3gkY0MOlfIl8tq-rI5cvVUCTNs1iw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- Román, Julio. Congreso oficializa que se archiva el decreto 39-2022 que contenía la Ley contra la ciberdelincuencia. Prensa Libre, consultada en versión digital el día 18 de sep. de 22, en https://www.prensalibre.com/guatemala/politica/congreso-oficializa-

que-se-archiva-el-decreto-39-2022-que-contenia-la-ley-contra-la-ciberdelincuencia-breaking/

- Sitio Web oficial Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones consultado el día 18 de sep. de 22, en https://www.micitt.go.cr/ciberseguridad/
- Sitio oficial Bancoagrícola, consultado el 08/10/2022 en: https://www.bancoagricola.com/financiera-mente
- Sitio web Fiscalía General de la República. Estafadores Informáticos son capturados por orden de la Fiscalía. Noticia publicada 25 de marzo de 2022. Consultado el 08/10/2022 en: https://www.fiscalia.gob.sv/estafadores-informaticos-son-capturados-por-orden-de-la-fiscalia/
- Sitio Oficial de la Asamblea Legislativa, *Pleno legislativo aprueba reformas a la Ley de Firma Electrónica para facilitar y simplificar su uso*, consultada el 15/10/2022 en: https://www.asamblea.gob.sv/node/11395
- Sitio Web: Real Academia Española, consultado el 27/10/2022 en: https://dle.rae.es/identidad
- Sitio Web Definición. De, consultado el 30/10/2022 en: https://definicion.de/seguridad/
- https://twitter.com/HaciendaSV/status/1431632671981981700?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1431632671981981700%7Ctwgr%5Ec993c282f3a104e714ce94c242826d0b8e8c2f64%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fquepasasv.com%2Fministerio-de-hacienda-alerta-a-los-salvadorenos-ante-estafas%2F
- Veto Presidencial sobre el decreto No 875 por inconveniente, de fecha 07 de mayo de 2021, versión PDF, consultado el 11/06/2022 en https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/EFBA7BEE-871B-40BE-BD0A-5BD80237CA90.pdf

LEYES

- Constitución de la República de El Salvador, aprobada por medio Asamblea Constituyente y decreto No 38, publicada en Diario Oficial No 234, Tomo No 281 de fecha 16 de diciembre de 1983, consultada en edición PDF el día 09 de julio de 2022 en https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf
- Constitución Española, aprobada por las Cortes en sesiones plenarias del Congreso de los Diputados del Senado Celebradas el 31 de octubre de 1978, ratificada por el pueblo español en referéndum de 6 de diciembre de 1978 y sancionada por S.M. el Rey ante Las Cortes el 27 de diciembre de 1978. Consultada en edición digital PDF el 09 de julio de 2022 en https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf
- Ley especial Contra Delitos Informáticos y Conexos, aprobada por medio de decreto legislativo N°260, la cual entró en vigencia en el mes de marzo del año 2016, CONSULTADO EN PDF.
- Ley de Firma Electrónica, emitido mediante decreto legislativo N°133 de fecha uno de octubre de 2015, consultada en versión PDF, el 15/10/2022.
- Código Penal de la República de El Salvador, aprobado mediante decreto legislativo N°1030, publicado en el Diario Oficial N° 105, Tomo N°335, en fecha 10 de junio de 1997.Consultado el 06/11/2022 en versión PDF.
- Decreto Número 17-73. Código Penal de la República de Guatemala, consultado en versión digital el día 18 de sep. de 22 en: https://tse.org.gt/images/UECFFPP/leyes/Codigo_Penal.pdf

- Código Penal de Honduras, emitido mediante decreto N° 130-2017, consultado en versión digital el 18 de sep. de 22, en https://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/CodigoPenalNo.130-2017(actualizadojulio2020).pdf
- Código Penal de Costa Rica. Ley 4.573, actualizado al 30 de junio del año 2019, consultada en versión digital el día 18 de sep. de 22 en https://defensapublica.poder-judicial.go.cr/media/attachments/2020/11/23/codigopenal2019.pdf
- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, consultado 11/06/2022 en versión PDF, en https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf
- Convenio sobre la Ciberdelincuencia, consultado en versión digital el 17 de septiembre de 2022 en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

ARTÍCULO DE REVISTA CONSULTADO EN LÍNEA

- Bustamante Donas, Javier. Hacia la Cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica. Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, no. 1. Versión digital, consultado 12/06/2022 en https://www.corteidh.or.cr/tablas/r22470.pdf
- Cervini, Raúl. Derecho Penal económico. Perspectiva integrada. Revista de Derecho, Universidad Católica del Uruguay, página consultada en versión pdf.
- Ferreyra, Eduardo. La Convención de Cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas. Consultada en versión digital, el 18/09/2022,

en https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf

- Garrido López, Carlos Alberto y Kuro Tenshi, Ángel Eduardo. Introducción a la informática. Artículo Accelerating the world´s research. Consultado en versión digital el 03/11/2022 en https://d1wqtxts1xzle7.cloudfront.net/53790500/Informatica-with-cover-page-v2.pdf?Expires=1667475592&Signature=fp9MFri2WKk8sGH0~ETaSPC-cTE8dBkjpKmw3C3IMqSuw~aYuxCHBw-DH8g438VwAgu-KQgQhJkW8iGGPwhR4KJURgEfhhLbv8~-NSur8tGflAEjesS2iXf0Q56wduCTkrF3ydLj1EA3z7gqqbusgcVYNc4KmmLqnEDYtt5RHJtGf64gxm9JlHqazh6U2rpbensQtjkoR5LedJMzoQoRJOo~qi0mMdHaeOiwSOJsMZGQJcxSps7dRIZmGLjYZ-YkHu9oLFVlc0nRFQpenU0dXt5Zbet~QkFPzi87-r0WrMoK65GBPZKcKxZz7Gjr8lE2JA1FtpM5pEe5Jtwbs90NzQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- Mayer Lux, Laura. El Bien Jurídico Protegido en los Delitos Informáticos. Revista Chilena de Derecho, Vol.44, No 1, Santiago abr. 2017. Consultado el 29 /10/2022 en versión digital en: https://www.scielo.cl/scielo.php?pid=S0718-34372017000100011&script=sci_arttext&tlng=pt
- Moreno Castillo, María Asunción; Aráuz Ulloa, Ismael Manuel. Delincuencia Económica, Revista de Derecho (2003), consultado en versión digital el 15/10/2022, en http://repositorio.uca.edu.ni/964/1/215-230.pdf
- Olave Albertini, Alejandra. Artículo: El delito de hurto como tipo de delito de resultado. Política criminal, Vol. 13, n°25, Santiago, julio 2018. Consultado el 05/11/2022, consultado en

https://www.scielo.cl/scielo.php?pid=S0718-33992018000100175&script=sci_arttext

- Ossandón Widow, Maria Magdalena. Los Elementos Descriptivos como técnica legislativa. Consideraciones críticas en relación con los delitos de hurto y robo con fuerza. Revista de Derecho, Vol. XXII- N°1, Julio 2009, consultada en versión digital el 05 /11/2022 en: https://www.scielo.cl/scielo.php?pid=S0718-09502009000100008&script=sci_arttext&tlng=pt
- Quiñónez Acevedo, Eleno. La suplantación de identidad en las redes sociales. Artículo de actualidad. Ministerio público. Asunción, Paraguay, publicado en fecha 08/12/2016, Consultado en versión digital, pág. 8, el día 02/11/2022 en: https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/7/6
- Riofrio Martínez-Villalba, Juan Carlos. La Cuarta ola de Derechos Humanos: Los Derechos Digitales>>. Para la Revista Latinoamericana de Derechos Humanos, Volumen 25(1) I semestre 2014 (ISSN: 1659-4304) Consultado en versión PDF.
- Suay Hernández, Celia, profesora titular de Derecho Penal, Universidad Autónoma de Barcelona. Los Elementos Normativos y el Error. Consultado en versión digital el 05/11/2022, en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-1991-10009700142

CRITERIOS JURISPRUDENCIALES

- Resolución que admite, demanda de amparo, de fecha 09 de octubre de 2020, emitida por la Sala de lo Constitucional de la Corte Suprema de Justicia, en proceso marcado con referencia 430-2020, consultada en versión digital, en fecha 17 de julio de 2022, en

https://www.jurisprudencia.gob.sv/busqueda/showExtractos.php?bd=1&nota=922929&doc=921522&&singlePage=false .

- STC Definitiva en proceso de amparo, Sala de lo Constitucional, Corte Suprema de Justicia de El Salvador, de fecha 02 de marzo de 2004, marcada con referencia 118-2002, consultada el 11/06/2022, en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php
- STC Definitiva en proceso de Hábeas Corpus, Sala de lo Constitucional de la Corte Suprema de Justicia, de fecha 16 de mayo de 2008, marcada con referencia 135-2005 AC, consultada el 11/06/2022, en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php
- Sentencia definitiva emitida por el Tribunal de Sentencia de Usulután, de fecha 04 de marzo de 2004, en proceso marcado con referencia judicial P0501-06-2004, consultada el día 10/07/2022 en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php
- Sentencia Definitiva, en Procedimiento Abreviado, emitida por el Tribunal Segundo de Sentencia de San Salvador, de fecha 06 de septiembre de 2019, consultada el 15/10/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2019/09/DCEA0.PDF
- Sentencia definitiva, emitida en recurso de Casación por la Sala de lo Penal de la Corte Suprema de Justicia. Referencia 17-CAS-2013, de fecha 03 de marzo de 2015, consultada en versión digital el 03/11/2022 en https://www.jurisprudencia.gob.sv/busqueda/tesauro.php#
- Sentencia definitiva emitida por la Sala de lo Penal de la Corte Suprema de Justicia, en recurso de casación, emitida en fecha 14/01/2013, consultada en versión PDF el 08/11/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2013/01/9D457.PDF

- Sentencia Definitiva emitida por el Tribunal Primero de Sentencia de Santa Tecla, el día trece de diciembre de 2006, en causa judicial con referencia P0401-105-2006, consultada el día 09/11/2022 en versión digital: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php
- Sentencia definitiva dictada por el Tribunal Primero de Sentencia de San Salvador, en fecha 09 de agosto de 2002, en causa judicial marcada con referencia P0101-48-2002, consultada el 09/11/2022 en versión digital en: https://www.jurisprudencia.gob.sv/busqueda/tesauro.php#
- Sentencia emitida en recurso de apelación, por la Cámara Primera de lo Penal de la Corte Suprema de Justicia, de fecha 23/04/2019, en proceso judicial marcado con referencia INC-APEL-68-SC-2019, consultado el 12/11/2022 en https://www.jurisprudencia.gob.sv/busqueda/tesauro.php
- Sentencia Definitiva emitida en proceso penal por el Tribunal Tercero de Sentencia, en fecha 21/10/2003, en causa marcada con referencia 179-2003-2ª, consultada el 12/11/2022 en https://escuela.fgr.gob.sv/wp-content/uploads/Leyes/Leyes-2/tribunal-tercero-de-sentencia.pdf
- Sentencia definitiva emitida por la Sala de lo Penal de la Corte Suprema de Justicia, en recurso de casación, emitida en fecha 14/01/2013, consultada en versión PDF el 08/11/2022 en: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2013/01/9D457.PDF

DENUNCIA

- Denuncia presentada en Fiscalía General de la República de referencia 02564-UDPP-2021-SS, delito de Hurto por medios Informáticos, denunciante Damaris Saraí Martínez Alberto.

COMUNICACIÓN PERSONAL

- Serrano, Dr. Armando Antonio, Coordinador del Programa de Maestría en Derecho Penal Económico, Universidad de El Salvador, comunicación personal, el 09/11/2022.
- Vásquez Laínez, Juan David, Licenciado en Ciencias de la Computación, Especialista en Cibercrimen, JEFE UNIDAD DE INVESTIGACIONES DE DELITOS INFORMATICOS, PNC El Salvador, comunicación personal, en septiembre 2021.